Incident Master Handbook - Malware & Monsters

The Complete Guide to Facilitating Cybersecurity Learning

The Malware & Monsters Community

Aug 27, 2025

Table of contents

1 Welcome, Incident Master **10**
- 1.1 Legacy & Contemporary Malmons . . . 10
- 1.2 Your Role as Learning Facilitator . . . 10
  - 1.2.1 What Makes a Great Incident Master . . . 10
  - 1.2.2 What You're NOT . . . 11
- 1.3 Facilitation Philosophy . . . 11
  - 1.3.1 Core Principles . . . 11
- 1.4 How to Use This Handbook . . . 11
  - 1.4.1 If You're New to Facilitating . . . 11
  - 1.4.2 If You're an Experienced Facilitator . . . 11
  - 1.4.3 If You're Looking for Quick Reference . . . 11
- 1.5 Your Learning Journey . . . 12
  - 1.5.1 Getting Started (First 3 Sessions) . . . 12
  - 1.5.2 Building Expertise (Sessions 4-20) . . . 12
  - 1.5.3 Master Level (20+ Sessions) . . . 12
- 1.6 Ready to Begin? . . . 12

2 Facilitation Philosophy **13**
- 2.1 The Art of Question-Driven Learning . . . 13
  - 2.1.1 Your Role: Guide, Not Expert . . . 13
  - 2.1.2 The Power of Strategic Questions . . . 13
  - 2.1.3 Managing the Learning Environment . . . 14
  - 2.1.4 The Minimal Preparation Approach . . . 15
  - 2.1.5 Common Facilitation Challenges . . . 16
  - 2.1.6 Advanced Facilitation Techniques . . . 17
  - 2.1.7 Building Facilitation Confidence . . . 18
  - 2.1.8 The Long-Term Vision . . . 18

3 Sly Flourish Principles for Security Training Platform Facilitation **20**
- 3.1 The Lazy IM Philosophy . . . 20
  - 3.1.1 Why Less Preparation Works Better . . . 20
- 3.2 The 5-Minute Preparation Method . . . 21

3.2.1 The Complete Workflow . . . 21
3.2.2 Emergency 2-Minute Prep . . . 21
3.3 Question-Driven Discovery . . . 21
3.3.1 The Core Principle . . . 21
3.3.2 Universal Question Patterns . . . 22
3.3.3 The Question Transformation Technique . . . 22
3.4 Storytelling as the Learning Engine . . . 22
3.4.1 Why Storytelling Matters in Cybersecurity Education . . . 22
3.4.2 The Professional Story Framework . . . 23
3.4.3 Storytelling Techniques for IMs . . . 24
3.4.4 Using Hooks to Create Immediate Investment . . . 24
3.4.5 Secrets and Clues Implementation . . . 25
3.4.6 Storytelling Recovery Techniques . . . 26
3.5 Using Player Expertise as Your Content Engine . . . 27
3.5.1 The Expertise Extraction Method . . . 27
3.5.2 When Nobody Knows . . . 27
3.6 Practical Secrets and Clues Preparation . . . 28
3.6.1 The 5-Minute Secret Development Process . . . 28
3.6.2 Secret Templates for Common M&M Scenarios . . . 28
3.6.3 Advanced Secrets and Clues Techniques . . . 29
3.6.4 Session Flow with Secrets and Clues . . . 29
3.7 The Art of Productive Improvisation . . . 30
3.7.1 "Yes, And…" for Cybersecurity . . . 30
3.7.2 When Players Take Unexpected Directions . . . 30
3.8 Minimal Notes, Maximum Impact . . . 31
3.8.1 Your Essential Session Notes . . . 31
3.8.2 What NOT to Prepare . . . 31
3.9 Advanced Lazy Techniques . . . 31
3.9.1 The Expertise Redirect . . . 31
3.9.2 The Collaborative Discovery . . . 31
3.9.3 The Learning Opportunity Reframe . . . 31
3.10 Common Lazy IM Pitfalls . . . 32
3.10.1 Over-Preparing . . . 32
3.10.2 Under-Confidence . . . 32
3.10.3 Fighting Player Direction . . . 32
3.10.4 Providing Too Much Information . . . 32
3.11 The Lazy IM Mindset . . . 32
3.11.1 Core Beliefs . . . 32
3.11.2 Session Success Metrics . . . 32
3.12 Practical Application . . . 33
3.12.1 Your First Lazy Session . . . 33
3.12.2 Building Lazy IM Skills . . . 33

4 Session Preparation: Using Scenario Cards 34
4.1 IM Preparation Quick Reference . . . 34
4.2 Transforming M&M Sessions Through Rich Narrative . . . 34

4.2.1 The Integration Philosophy . . . 34
4.2.2 Example Scenario Card . . . 35
4.3 The New IM 30-Minute Scenario Card Preparation . . . 35
4.3.1 First-Time Facilitator Complete Prep Using Scenario Cards 35
4.3.2 Scenario Card Examples by Industry . . . 36
4.4 The Experienced IM 5-Minute Scenario Card Preparation . . . 38
4.4.1 Streamlined Workflow for Regular Facilitators . . . 38
4.4.2 When to Spend More Time . . . 39
4.5 Malmon Selection Decision Trees . . . 39
4.5.1 Based on Group Composition . . . 39
4.5.2 Based on Learning Objectives . . . 40
4.6 Organization Context Templates . . . 40
4.6.1 Quick Context Generator . . . 40
4.6.2 Collaborative Context Creation . . . 41
4.7 Core Integration Points . . . 42
4.7.1 Integration with Role-Based Investigation . . . 42
4.7.2 Integration with Question-Driven Discovery . . . 42
4.8 Contingency Planning . . . 43
4.8.1 Alternative Scenarios . . . 43
4.8.2 Group Dynamic Challenges . . . 44
4.8.3 Emergency Protocols . . . 44
4.9 Pre-Session Checklist . . . 45
4.9.1 24 Hours Before . . . 45
4.9.2 1 Hour Before . . . 45
4.9.3 10 Minutes Before . . . 45
4.10 Example: Following the Method in Practice . . . 45
4.10.1 Group Context . . . 45
4.10.2 Following the Preparation Activities . . . 46
4.10.3 What This Preparation Achieves . . . 47
4.10.4 During the Session . . . 48
4.11 Post-Preparation Mindset . . . 48
4.11.1 Confidence Building . . . 48
4.11.2 Session Success Indicators . . . 48
4.12 Practical Integration Workflows . . . 48
4.12.1 Scenario Card Selection Process . . . 48
4.12.2 Troubleshooting Integration Challenges . . . 49

5 Comprehensive Scenario Types Guide 51
5.1 IM Quick Reference: All Session Types . . . 51
5.1.1 Decision Matrix: Choosing Session Type . . . 51
5.2 Session Type Categories . . . 52
5.2.1 1. Standard Contemporary Sessions . . . 52
5.2.2 2. Legacy Malmon Sessions . . . 53
5.2.3 2A. Historical Foundation Sessions . . . 53
5.2.4 2B. Contemporary Legacy Sessions . . . 54
5.2.5 3. Specialized Session Formats . . . 55

5.2.6 4. Problem-Focused Sessions 56
5.3 Scenario Card System 57
5.3.1 Understanding Scenario Cards 57
5.3.2 Choosing Scenario Cards 58
5.4 Session Planning Framework 58
5.4.1 Pre-Session Decision Process 58
5.4.2 Session Execution Guidelines 59
5.5 Advanced IM Techniques 60
5.5.1 Managing Mixed Groups 60
5.5.2 Adapting Session Complexity 60
5.5.3 Real-Time Adaptation 61
5.6 Success Metrics by Session Type 61
5.6.1 Standard Contemporary Sessions 61
5.6.2 Historical Foundation Sessions 62
5.6.3 Business Leadership Sessions 62
5.6.4 Technical Deep-Dive Sessions 62
5.7 Quick Reference Cards 63
5.7.1 Session Type Quick Selection 63
5.7.2 Preparation Time Investment 63
5.7.3 Common Session Planning Mistakes 63

6 Malmon System Mastery 65
6.1 Understanding the Complete Framework 65
6.1.1 The Type System in Practice 65
6.1.2 Evolution Mechanics for Learning 67
6.1.3 Malmon Selection for Different Learning Goals 68
6.1.4 Regional Variants and Customization 69
6.1.5 Advanced Malmon Mechanics 70
6.1.6 Building Scenario Complexity 71
6.1.7 Malmon Creation and Customization 71
6.1.8 Assessment and Continuous Improvement 72

7 Role-Based Team Facilitation for Gamified Incident Response Training 74
7.1 The Power of Role-Based Collaboration 74
7.1.1 Understanding Role Dynamics 74
7.1.2 Role Modifier System 75
7.1.3 Roll Difficulty Framework 81
7.1.4 Role-Specific Facilitation Techniques 84
7.1.5 Managing Role Interactions 88
7.1.6 Advanced Team Management Techniques 89
7.1.7 Assessment and Learning Objectives 90

8 Managing the Progression System 92
8.1 Understanding Player Development 92
8.1.1 Recognizing Skill Development 92

8.1.2 The Badge System Implementation 94
8.1.3 Elite Specialization Tracks 99
8.1.4 Supporting Individual Development Plans 100
8.1.5 Organizational Integration 102

9 Containment Mechanics **104**
9.1 Facilitating Strategic Response Decisions 104
9.1.1 Understanding Type Effectiveness in Practice 104
9.1.2 Facilitating Security Control Selection 105
9.1.3 Managing Collaborative Decision-Making 106
9.1.4 Using Dice Mechanics Meaningfully 107
9.1.5 Network Security Status Three-Track System 108
9.1.6 Advanced Containment Scenarios 110
9.1.7 Environmental Factors in Containment 111
9.1.8 Assessment and Learning Integration 112
9.1.9 Building Containment Expertise 113
9.1.10 IM Guide: Containment Success Validation 113

10 Technical Foundation for Incident Masters **117**
10.1 The Right Level of Technical Knowledge 117
10.1.1 Essential Cybersecurity Concepts 117
10.1.2 Technical Concepts You Should Understand 119
10.1.3 MITRE ATT&CK as Your Facilitation Framework 120
10.1.4 Handling Technical Knowledge Gaps 121
10.1.5 Emergency Technical Protocols 122
10.1.6 Building Your Technical Foundation 122
10.1.7 The Growth Mindset 123

11 Running Sessions: Thorough Guide **125**
11.1 Session Overview and Timing 125
11.2 The Opening: Foundation for Success 125
11.2.1 Welcome and Energy Setting 125
11.2.2 Expertise Discovery and Team Chemistry 126
11.2.3 Collaborative Role Assignment 126
11.2.4 Character Development and Context Setting 127
11.3 Round 1: Discovery Phase 128
11.3.1 Phase Setup 128
11.3.2 Individual Investigation 128
11.3.3 Knowledge Sharing 129
11.3.4 Malmon Identification 130
11.4 Round 2: Investigation Phase 131
11.4.1 Phase Transition 131
11.4.2 Impact Assessment 131
11.4.3 Attack Vector Analysis 132
11.4.4 Evolution Threat 132
11.5 Round 3: Response Phase 133

11.5.1 Phase Transition . . . 133
11.5.2 Strategy Coordination . . . 133
11.5.3 Implementation . . . 134
11.5.4 Resolution . . . 134
11.6 Session Transitions and Pacing . . . 135
11.6.1 Maintaining Energy Throughout . . . 135
11.6.2 Time Management Strategies . . . 135
11.6.3 Participant Management . . . 136
11.7 Closing Strong . . . 136
11.7.1 Session Wrap-up . . . 136
11.7.2 Success Indicators . . . 137
11.8 Common Real-Time Challenges . . . 137
11.8.1 When Nobody Knows Technical Details . . . 137
11.8.2 When Sessions Go Off-Script . . . 137
11.8.3 When Technical Accuracy is Questioned . . . 138

12 Practical Facilitation Techniques 139
12.1 The Question Arsenal . . . 139
12.1.1 Universal Discovery Questions . . . 139
12.1.2 Investigation Phase Question Bank . . . 140
12.1.3 Response Phase Question Bank . . . 141
12.2 Managing Group Dynamics . . . 141
12.2.1 Encouraging Quiet Participants . . . 141
12.2.2 Managing Dominant Participants . . . 142
12.2.3 Building Psychological Safety . . . 143
12.3 Handling Technical Knowledge Gaps . . . 143
12.3.1 When Nobody Knows the Answer . . . 143
12.3.2 When Information is Incorrect . . . 144
12.3.3 Bridging Expertise Gaps . . . 144
12.4 Reading the Room and Adapting . . . 144
12.4.1 Energy Level Assessment . . . 144
12.4.2 Adaptive Difficulty Management . . . 145
12.4.3 Cultural and Communication Adaptation . . . 146
12.5 Advanced Facilitation Techniques . . . 146
12.5.1 Building Dramatic Tension . . . 146
12.5.2 Improvisation and Adaptation . . . 146
12.5.3 Seamless Transition Management . . . 147
12.6 Emergency Facilitation Protocols . . . 147
12.6.1 When Groups Get Completely Stuck . . . 147
12.6.2 When Conflict Arises . . . 147
12.6.3 When Technology Fails . . . 148
12.7 Success Indicators and Troubleshooting . . . 148
12.7.1 Session Success Metrics . . . 148
12.7.2 Common Problems and Solutions . . . 148
12.8 Scenario Card Preparation Method . . . 149
12.8.1 The 5-Minute Scenario Card Prep . . . 149

12.8.2 Why Scenario Cards Work 150
12.8.3 Emergency Shortcuts 150

13 Session Management **152**
13.1 The Art of Orchestrating Collaborative Learning 152
13.1.1 Pre-Session Setup 152
13.1.2 Opening and Character Creation 153
13.1.3 Round Management 154
13.1.4 Time Management Strategies 156
13.1.5 Energy and Engagement Management 157
13.1.6 Managing Different Group Types 158
13.1.7 Post-Session Wrap-Up (5 minutes) 159

14 Advanced Troubleshooting and Session Recovery **161**
14.1 Complex Facilitation Challenges 161
14.1.1 The "Mixed Expertise Crisis" 161
14.1.2 The "Analysis Paralysis Spiral" 162
14.1.3 The "Personality Conflict Explosion" 162
14.1.4 The "Technical Overreach Problem" 163
14.2 Advanced Group Dynamics 163
14.2.1 Managing Dominant Personalities 163
14.2.2 Cultural and Communication Challenges 164
14.3 Technology and Equipment Failures 165
14.3.1 Digital Tool Failures 165
14.3.2 Physical Environment Challenges 166
14.4 Learning Objective Misalignment 167
14.4.1 When Sessions Go Off-Track 167
14.4.2 Assessment and Adjustment 167
14.5 Post-Session Recovery and Learning 168
14.5.1 When Sessions Don't Go Well 168
14.5.2 Building Resilience 168
14.5.3 Continuous Improvement 169

15 Advanced Scenarios **171**
15.1 Beyond Basic Incident Response 171
15.1.1 Characteristics of Advanced Scenarios 171
15.1.2 Industry-Specific Advanced Scenarios 172
15.1.3 Time-Pressure Scenarios 174
15.1.4 Competitive Advanced Scenarios 174
15.1.5 Scenario Design Principles 175
15.1.6 Facilitation Techniques for Advanced Scenarios 176
15.1.7 Assessment and Learning Objectives 177
15.1.8 Building Advanced Scenario Capabilities 178

16 Community Tournaments **179**
16.1 Organizing Competitive Learning Events 179

16.1.1 Tournament Design Philosophy . . . 179
16.1.2 Speed Response Tournaments . . . 180
16.1.3 Perfect Response Competitions . . . 181
16.1.4 Red Team vs Blue Team Battles . . . 182
16.1.5 Multi-Organization Championships . . . 183
16.1.6 Assessment and Recognition Systems . . . 184
16.1.7 Tournament Facilitation Best Practices . . . 185
16.1.8 Building Sustainable Tournament Programs . . . 186
16.1.9 Educational Impact Measurement . . . 187

17 Malmon Reference **189**
17.1 Current Malmons . . . 190
17.2 Legacy Malmons . . . 191

18 Quick Reference **192**
18.1 Emergency Protocols . . . 192

19 Emergency Facilitation Protocols **193**
19.1 When Teams Get Stuck . . . 193
19.1.1 The “Analysis Paralysis” Problem . . . 193
19.1.2 The “Knowledge Vacuum” Problem . . . 193
19.1.3 The “Dominant Player” Problem . . . 194
19.2 When Sessions Lose Energy . . . 194
19.2.1 The “Low Engagement” Crisis . . . 194
19.2.2 The “Technical Overwhelm” Problem . . . 194
19.3 When Conflicts Arise . . . 194
19.3.1 The “Approach Disagreement” Situation . . . 194
19.3.2 The “Expertise Challenge” Problem . . . 195
19.4 Technical Difficulties . . . 195
19.4.1 When Game Mechanics Break Down . . . 195
19.4.2 When Technology Fails . . . 195
19.5 Time Management Crises . . . 196
19.5.1 When Phases Run Long . . . 196
19.5.2 When Teams Move Too Fast . . . 196
19.6 Participant Management . . . 196
19.6.1 The “Expert Overwhelm” Problem . . . 196
19.6.2 The “Novice Anxiety” Problem . . . 196
19.7 Session Recovery Strategies . . . 197
19.7.1 The “Complete Restart” Protocol . . . 197
19.7.2 The “Pivot to Discussion” Protocol . . . 197
19.8 Post-Crisis Learning . . . 197
19.8.1 Immediate Recovery . . . 197
19.8.2 Session Debrief Enhancement . . . 197
19.8.3 Facilitator Self-Care . . . 198
19.9 Prevention Strategies . . . 198
19.9.1 Pre-Session Risk Assessment . . . 198

19.9.2 Early Warning Systems 198
19.9.3 Adaptive Facilitation 198
19.10Role Cards Reference 199

20 Role Cards Reference for Incident Masters 200
20.1 Complete Role Cards Overview 200
20.1.1 Detective (Cyber Sleuth) 200
20.1.2 Protector (Digital Guardian) 200
20.1.3 Tracker (Network Analyst) 200
20.1.4 Communicator (Stakeholder Liaison) 200
20.1.5 Crisis Manager (Incident Commander) 200
20.1.6 Threat Hunter (Proactive Defender) 200
20.2 IM Quick Reference: Role Strengths & Modifiers 200
20.2.1 Role Modifier Quick Reference Table 200
20.2.2 Role Strengths at a Glance 201
20.3 Facilitation Tips by Role 201
20.3.1 Encouraging Balanced Participation 201
20.3.2 Role-Specific Questions to Ask 202
20.4 Team Composition Guidelines 203
20.4.1 For 4-Player Teams 203
20.4.2 For 5-Player Teams 203
20.4.3 For 6-Player Teams 203
20.4.4 For Teams with Role Overlap 203

Chapter 1

Welcome, Incident Master

"Great facilitators don't have all the answers—they ask the right questions."

As an Incident Master, you're not just running a training session—you're orchestrating a collaborative learning experience that transforms how people think about cybersecurity. This handbook is your complete guide to facilitating *Malware & Monsters* sessions that provide professional security training platform capabilities through incident response tabletop exercise methodologies. Our approach drives security professional development and cybersecurity skills development simultaneously.

1.1 Legacy & Contemporary Malmons

Your toolkit includes both historical threats that shaped cybersecurity (Code Red, Stuxnet, Ghost RAT, Poison Ivy) and modern attacks currently impacting organizations (GaboonGrabber, WannaCry, LockBit, FakeBat). This range allows you to guide teams through cybersecurity's evolution, connecting lessons from past incidents to today's threat landscape.

1.2 Your Role as Learning Facilitator

1.2.1 What Makes a Great Incident Master

- **Question architect** - You guide discovery through strategic questioning
- **Safety creator** - You build psychological safety for experimentation and learning

- **Process guide** - You manage time, energy, and group dynamics
- **Learning catalyst** - You unlock the collective wisdom in the room

1.2.2 What You're NOT

- **The expert with all the answers** - Participants provide the cybersecurity expertise
- **A lecturer** - Learning happens through collaborative discovery
- **A judge** - Success is measured by learning, not "correct" answers

1.3 Facilitation Philosophy

At the heart of Malware & Monsters is a simple but powerful principle: **your participants already know more than they think they do**. Your job is to create the conditions where that knowledge can emerge, combine, and grow through collaboration.

1.3.1 Core Principles

1. **Trust the framework** - The structure supports learning; trust it
2. **Trust your participants** - They have valuable knowledge and insights
3. **Trust the process** - Discovery-based learning is more powerful than instruction
4. **Trust yourself** - You don't need to be perfect; you need to be curious

1.4 How to Use This Handbook

1.4.1 If You're New to Facilitating

- Start with **Facilitation Philosophy** to understand question-driven learning
- Read **Sly Flourish Principles** to grasp the "Lazy DM" approach
- Focus on **Session Preparation** for your first sessions
- Use **5-Minute Prep** templates to get started quickly

1.4.2 If You're an Experienced Facilitator

- Jump to **Malmon System Mastery** to understand the mechanics deeply
- Explore **Advanced Scenarios** for complex challenges
- Check **Community Tournaments** for competitive elements
- Use **Troubleshooting** for handling difficult situations

1.4.3 If You're Looking for Quick Reference

- **Malmon Profiles** - Complete threat scenario details for all malmons
- **Question Banks - Discovery Phase** - Ready-to-use facilitation questions
- **Question Banks - Investigation Phase** - Investigation and analysis questions

- **Question Banks - Response Phase** - Response and coordination questions
- **Session Scripts - Opening** - Session opening templates
- **Session Scripts - Closing** - Session closing templates

1.5 Your Learning Journey

1.5.1 Getting Started (First 3 Sessions)

1. **Start simple** - Use GaboonGrabber for your first few sessions
2. **Focus on questions** - Trust that good questions lead to good learning
3. **Observe and learn** - Watch how participants interact and discover
4. **Reflect and improve** - Each session teaches you something new

1.5.2 Building Expertise (Sessions 4-20)

- Experiment with different Malmon types and complexity levels
- Develop your personal facilitation style and approaches

- Build relationships within the learning community
- Begin mentoring new Incident Masters

1.5.3 Master Level (20+ Sessions)

- Design custom scenarios and adaptations
- Train other facilitators in your organization
- Contribute new Malmons and techniques to the community
- Lead community initiatives and development

1.6 Ready to Begin?

The most important thing to remember is this: **every expert was once a beginner**. You don't need years of experience to be an effective Incident Master. You need curiosity, patience, and willingness to learn alongside your participants.

Your participants don't expect perfection—they expect authenticity, engagement, and someone who cares about their learning. You already have everything you need to create transformative cybersecurity education experiences.

Remember: Great Incident Masters are made through practice, not perfection. Every session you facilitate makes cybersecurity education more collaborative, engaging, and effective.

The monsters are waiting. Your learners are ready. Let's build something amazing together.

Chapter 2

Facilitation Philosophy

2.1 The Art of Question-Driven Learning

As an Incident Master, your primary tool is not technical knowledge—it's the strategic use of questions to unlock the collective wisdom in the room. Every Malware & Monsters session succeeds when participants discover insights through collaborative problem-solving, not when you provide all the answers.

2.1.1 Your Role: Guide, Not Expert

What You Are:

- **Learning Facilitator:** Creating space for collaborative discovery
- **Question Architect:** Asking the right questions at the right time
- **Process Guide:** Managing time, energy, and group dynamics
- **Safety Creator:** Establishing psychological safety for learning and experimentation

What You Are Not:

- **Technical Expert:** Participants provide the cybersecurity expertise
- **Answer Provider:** Solutions emerge from group collaboration
- **Lecturer:** Learning happens through discovery, not presentation
- **Judge:** Success is measured by learning, not "correct" answers

2.1.2 The Power of Strategic Questions

2.1.2.1 Discovery Questions

Purpose: Help teams uncover information and build understanding

Effective Examples:

- *"What patterns do you notice in these symptoms?"*
- *"How might this behavior connect to what we know about [threat type]?"*
- *"What would concern you most about these findings?"*
- *"What questions would someone with [role] expertise ask about this?"*

Avoid These Approaches:

- *"Can anyone tell me what type of malware this is?"* (Answer-seeking)
- *"This is clearly a Trojan because…"* (Answer-providing)
- *"You should look at the registry entries."* (Solution-directing)

2.1.2.2 Collaboration Questions

Purpose: Encourage teamwork and knowledge sharing

Effective Examples:

- *"How do these different perspectives connect?"*
- *"What would happen if we combined [Name's] approach with [Other Name's] insight?"*
- *"Who else might have experience with this type of situation?"*
- *"How can the team build on what we've discovered so far?"*

2.1.2.3 Reflection Questions

Purpose: Help teams learn from their experience

Effective Examples:

- *"What surprised you about how this played out?"*
- *"Which approaches worked better than expected?"*
- *"What would you do differently in a similar situation?"*
- *"How does this connect to your real-world experience?"*

2.1.3 Managing the Learning Environment

2.1.3.1 Creating Psychological Safety

Encourage Experimentation:

- *"There's no single right answer here—what are your thoughts?"*
- *"That's an interesting approach—how might that work?"*
- *"What if we tried something completely different?"*

Normalize Uncertainty:

- *"Real cybersecurity incidents involve a lot of uncertainty too."*
- *"It's okay not to know—what would you do to find out?"*
- *"Even experts disagree about the best approach in situations like this."*

Value All Contributions:

- *"That's a perspective we hadn't considered yet."*
- *"How does that connect to what [Other Name] was thinking?"*
- *"What would make that approach even more effective?"*

2.1.3.2 Balancing Structure with Flexibility

Maintain Learning Focus:

When technical discussions get too detailed: *"This is great analysis—how does it inform our team's next steps?"*

When teams get stuck: *"Let's step back—what would common sense suggest here?"*

When energy drops: *"What's at stake if we don't solve this problem?"*

Adapt to Group Needs:

- **High Expertise Groups:** Ask deeper, more complex questions
- **Mixed Groups:** Help experts teach and newcomers contribute
- **Low Expertise Groups:** Focus on concepts and collaboration over technical details

2.1.4 The Minimal Preparation Approach

2.1.4.1 What You Need to Know

Essential Understanding:

- **Basic session structure:** 3 rounds, role-based investigation
- **Core question patterns:** Discovery, collaboration, reflection
- **Malmon characteristics:** Type effectiveness and evolution concepts
- **Emergency techniques:** What to do when sessions go off track

What You Don't Need:

- **Deep technical expertise:** Participants provide this
- **Perfect scenarios:** Adapt based on group knowledge and interests
- **All the answers:** Questions are more valuable than solutions
- **Complex preparation:** Trust the framework and your participants

2.1.4.2 5-Minute Session Prep

Choose Your Malmon:

- **New groups:** GaboonGrabber (straightforward, teaches fundamentals)
- **Experienced groups:** WannaCry (complex, multi-vector)
- **Expert groups:** Stuxnet (sophisticated, strategic implications)

Prepare 3 Key Questions:

- **Discovery:** *"What patterns connect these symptoms?"*

- **Investigation:** *"How would you determine the scope of this threat?"*
- **Response:** *"What approach gives you the best chance of success?"*

Set Your Intention:

- Focus on collaborative learning, not perfect game execution
- Trust participant expertise over your preparation
- Adapt to what emerges rather than forcing predetermined outcomes

2.1.5 Common Facilitation Challenges

2.1.5.1 The Expert Overwhelm

Problem: Participants with deep expertise dominate discussion or get frustrated with simplified scenarios

Response Strategies:

- *"Help us understand—how would you explain this to someone new to cybersecurity?"*
- *"In real situations, you'd have more complexity—for learning purposes, we're focusing on [specific concept]."*
- *"Share a real-world example of how this typically plays out."*
- *"What would you teach someone just starting in this field?"*

2.1.5.2 The Knowledge Gap

Problem: Team lacks expertise in the area being explored

Response Strategies:

- *"Let's approach this from common sense—what would seem logical?"*
- *"How is this similar to something you do understand?"*
- *"What questions would you ask if this happened at your workplace?"*
- *"If you had to guess, what might be happening here?"*

2.1.5.3 The Analysis Paralysis

Problem: Team gets stuck debating technical details without making progress

Response Strategies:

- *"That's thorough analysis—what decision does this help you make?"*
- *"We have [X] minutes left—what's your priority?"*
- *"In a real incident, you'd need to act with incomplete information—what would you do?"*
- *"How does this technical detail affect your team's response strategy?"*

2.1.5.4 The Energy Drop

Problem: Group engagement decreases, discussion becomes minimal

Response Strategies:

- *"What's the worst-case scenario if this attack succeeds?"*
- *"Who would be affected if you don't solve this?"*
- *"What would make this attack particularly dangerous?"*
- *"How would you explain the urgency to your organization's leadership?"*

2.1.6 Advanced Facilitation Techniques

2.1.6.1 The Socratic Method in Cybersecurity

Build on Responses:

- Player: *"This looks like a Trojan."*
- IM: *"What makes you think that? What would that mean for how we respond?"*

Chain Questions:

- *"If this is a Trojan, what would we expect to see next?"*
- *"How would that change our investigation priorities?"*
- *"What would worry you most about that possibility?"*

Explore Implications:

- *"What happens if you're right about this?"*
- *"What happens if you're wrong?"*
- *"How would each possibility change your approach?"*

2.1.6.2 Managing Multiple Perspectives

When Players Disagree:

- *"Both approaches have merit—what are the trade-offs?"*
- *"How might we test which approach would work better?"*
- *"What would help you decide between these options?"*
- *"In what situations would each approach be most effective?"*

When Players Build on Each Other:

- *"How do these insights connect?"*
- *"What does this combination suggest about our next steps?"*
- *"How does [Name's] point change how we think about [Other Name's] observation?"*

2.1.6.3 Encouraging Deeper Thinking

Challenge Assumptions:

- *"What if that assumption is wrong?"*
- *"What evidence supports that conclusion?"*
- *"How else might you explain these symptoms?"*

- *"What would change your mind about this approach?"*

Explore Consequences:

- *"Then what happens?"*
- *"How would that affect other parts of the organization?"*
- *"What are the second-order effects of that decision?"*
- *"Who else would need to be involved if you took that approach?"*

2.1.7 Building Facilitation Confidence

2.1.7.1 Start Simple

- **Focus on questions, not answers:** Trust that good questions lead to good learning
- **Embrace uncertainty:** Not knowing creates learning opportunities
- **Follow participant energy:** Let interest and expertise guide content
- **Celebrate discovery:** Acknowledge insights and "aha moments"

2.1.7.2 Develop Your Style

- **Personal authenticity:** Be yourself rather than trying to be "the perfect facilitator"
- **Comfortable with silence:** Give people time to think before jumping in
- **Curious mindset:** Genuinely interested in what participants will discover
- **Learning orientation:** Model continuous learning and growth

2.1.7.3 Learn from Experience

- **Reflect after sessions:** What questions worked well? What would you try differently?
- **Seek feedback:** Ask participants what helped their learning most
- **Connect with other IMs:** Share experiences and learn from colleagues
- **Document insights:** Build your personal facilitation knowledge base

2.1.8 The Long-Term Vision

2.1.8.1 Building Cybersecurity Communities

Every session you facilitate contributes to:

- **Knowledge sharing:** Participants learn from each other's expertise
- **Relationship building:** Professional networks that support career growth
- **Skill development:** Practical capabilities that improve organizational security
- **Culture change:** Collaborative approaches to cybersecurity challenges

2.1.8.2 Personal Growth as Facilitator

Through facilitating Malware & Monsters sessions, you develop:

- **Leadership skills:** Guiding groups through complex problem-solving
- **Communication abilities:** Asking questions that unlock learning
- **Cybersecurity understanding:** Learning alongside participants
- **Community impact:** Contributing to improved cybersecurity capabilities

Remember: Great facilitation comes from trust—trust in the framework, trust in your participants, and trust in the power of collaborative learning. Your role is to create the conditions where that learning can flourish.

Chapter 3

Sly Flourish Principles for Security Training Platform Facilitation

3.1 The Lazy IM Philosophy

The most effective cybersecurity facilitators are often the "laziest" - not because they don't care, but because they've learned that minimal preparation creates maximum engagement. This counterintuitive approach, adapted from Sly Flourish's lazy Dungeon Master methodology, transforms how we approach cybersecurity education.

3.1.1 Why Less Preparation Works Better

Traditional approach: Detailed scenarios, scripted responses, predetermined outcomes
Lazy IM approach: Minimal setup, player-driven content, emergent storytelling

The lazy approach works because:

- **Player expertise drives content:** Your participants know more collectively than you do individually
- **Authentic scenarios emerge:** Real experiences create better learning than fictional ones
- **Engagement increases:** People invest more in stories they help create
- **Adaptability improves:** Less rigid preparation means better response to group needs

3.2 The 5-Minute Preparation Method

3.2.1 The Complete Workflow

Minute 1: Organization Context
Choose or let group decide:

- Industry type (healthcare, finance, manufacturing, etc.)
- Organization size (startup, mid-size, enterprise)
- What they protect (customer data, intellectual property, critical infrastructure)

Minute 2: Symptom Selection
Pick 2-3 observable symptoms from the bank:

- Performance issues (slow computers, network lag)
- User reports (strange emails, unexpected pop-ups)
- System anomalies (new processes, unusual traffic)

Minutes 3-4: Malmon Choice
Select based on:

- Group expertise level
- Learning objectives
- Available time
- Your comfort level

Minute 5: Mental Preparation
Review:

- Type effectiveness for chosen Malmon
- Key question patterns
- Potential evolution triggers

3.2.2 Emergency 2-Minute Prep

When you have even less time:

1. **30 seconds:** "Mid-sized company, computers acting weird"
2. **30 seconds:** Pick familiar Malmon (GaboonGrabber for beginners)
3. **60 seconds:** Remember: ask questions, don't provide answers

3.3 Question-Driven Discovery

3.3.1 The Core Principle

Never provide information that players can discover themselves.
Instead of saying: *"Process injection is when malware hides inside legitimate processes"* Ask instead: *"Marcus, you found programs using way more memory than normal - what could that mean?"*

3.3.2 Universal Question Patterns

3.3.2.1 Discovery Phase Questions

- *"What's the first thing that would seem unusual?"*
- *"Who would typically notice this kind of problem first?"*
- *"What pattern suggests this isn't normal behavior?"*
- *"Based on your experience, what would worry you most here?"*

3.3.2.2 Investigation Phase Questions

- *"What would this threat need to accomplish its goals?"*
- *"How might this connect to what we found earlier?"*
- *"What would you investigate next in your real job?"*
- *"What tools would help here?"*

3.3.2.3 Response Phase Questions

- *"What's your biggest constraint right now?"*
- *"What could go wrong with this approach?"*
- *"Who else would need to be involved?"*
- *"How would you coordinate this in the real world?"*

3.3.3 The Question Transformation Technique

Turn any technical concept into a discovery question:

Concept: *Digital signatures*
Bad: "This file has no digital signature, which means…"
Good: "This file has no digital signature - what does that suggest?"

Concept: *Command and control servers*
Bad: "The malware is communicating with its C2 server"
Good: "Something's sending data to an external server regularly - thoughts?"

3.4 Storytelling as the Learning Engine

3.4.1 Why Storytelling Matters in Cybersecurity Education

Technical cybersecurity concepts become memorable and meaningful when embedded in human stories. The most effective incident response training doesn't just teach tools and techniques - it places learners inside compelling narratives where those skills matter.

Storytelling transforms learning because:

- **Emotional engagement:** Stories create investment in outcomes

- **Memory anchoring:** Narrative context helps retain technical details
- **Professional relevance:** Realistic scenarios connect to actual work experience
- **Collaborative discovery:** Groups naturally build on story elements together
- **Mistake tolerance:** Story context makes errors feel like plot developments rather than failures

3.4.2 The Professional Story Framework

Every effective Malware & Monsters scenario follows a three-act structure that mirrors real incident response:

3.4.2.1 Act 1: The Setup (Discovery Phase)

Hook: Why is this happening NOW? - Time pressure: "Hospital goes live Monday morning…" - Business stakes: "Customer data processing deadline Friday…" - Organizational tension: "Under audit pressure, IT approved…"

Characters: Who has skin in the game? - Primary stakeholder with clear motivations - Secondary stakeholders with competing priorities - External pressure sources (regulators, customers, executives)

3.4.2.2 Act 2: The Investigation (Crisis Escalation)

Rising tension: What gets worse if not addressed? - Technical escalation: threat spreads, damage increases - Business pressure: deadlines approach, stakes rise - Political complexity: stakeholders disagree, blame emerges

Discovery moments: What do players uncover? - Technical artifacts that tell a story - Timeline reconstruction that reveals attack progression - Connection moments where pieces fit together

3.4.2.3 Act 3: The Resolution (Response and Recovery)

Climax: Decisive action under pressure - Containment decisions with imperfect information - Resource allocation under time constraints - Coordination across competing priorities

Resolution: Aftermath and learning - Impact assessment and lessons learned - Prevention planning and organizational improvement - Professional growth and capability development

3.4.3 Storytelling Techniques for IMs

3.4.3.1 Show, Don't Tell

Instead of: *"This is a polymorphic malware"*
Try: *"Each sample looks slightly different, like it's changing itself somehow"*

Instead of: *"The attack uses privilege escalation"*
Try: *"It started with a regular user account, but now it's accessing admin areas"*

3.4.3.2 Character Motivation Drives Plot

IT Director perspective: "We can't take systems down during quarter-end processing"
CISO perspective: "If this breaches customer data, regulatory penalties could be massive"
Operations perspective: "Production lines stop if the network goes down"

3.4.3.3 Professional Authenticity

Draw scenarios from: - Real organizational pressures participants recognize - Industry-specific constraints and timelines
- Authentic stakeholder dynamics and competing priorities - Technical situations that feel familiar yet challenging

3.4.3.4 Collaborative Story Building

- **Player contributions become canon:** When players add realistic details, incorporate them
- **"Yes, and..." approach:** Build on player ideas rather than correcting them
- **Shared narrative ownership:** Let groups shape organizational context and character motivations

3.4.4 Using Hooks to Create Immediate Investment

3.4.4.1 Time Pressure Hooks

- *"The merger announcement goes public tomorrow morning…"*
- *"Patient admissions resume after the holiday weekend…"*
- *"Payroll processing for 5,000 employees starts in 6 hours…"*

3.4.4.2 Professional Stakes Hooks

- *"Your reputation with the client depends on smooth deployment…"*
- *"The audit team arrives first thing Monday…"*
- *"Executive leadership is already asking questions…"*

3.4.4.3 Human Impact Hooks

- *"Night shift nurses can't access patient records…"*
- *"Customer service is fielding angry calls about system outages…"*
- *"Remote workers can't connect for the morning standup…"*

3.4.5 Secrets and Clues Implementation

The heart of Sly Flourish methodology is **secrets and clues** - concrete information that explains what happened and drives investigation forward. Each secret answers a "why" or "how" question, and multiple clues lead to each secret.

3.4.5.1 The Three-Layer Secret Structure

Layer 1: Surface Secrets (Discovered through initial investigation) - **Secret:** "The attack succeeded because IT was under extreme pressure to approve software quickly" - **Clues leading to this secret:** - Email chains showing rushed approval processes - Staff mentioning "cutting corners" for the deadline - IT Director's defensive responses about approval procedures - System logs showing normal security checks were bypassed

Layer 2: Deeper Secrets (Revealed through persistent investigation) - **Secret:** "Management has been systematically undermining security practices for months" - **Clues leading to this secret:** - Financial records showing security training budget cuts - Staff interviews revealing previous incidents covered up - Executive communications prioritizing speed over security - Pattern of successful social engineering attempts

Layer 3: Root Cause Secrets (Uncovered through comprehensive analysis) - **Secret:** "The organization's culture creates conditions where these attacks inevitably succeed" - **Clues leading to this secret:** - Employee turnover in security roles - Lack of incident response procedures - Executive compensation tied to short-term delivery goals - Previous attacks that weren't properly addressed

3.4.5.2 Practical Secret Development for M&M Sessions

For GaboonGrabber Healthcare Scenario:

Secret 1: "The software appeared legitimate because it was distributed through a compromised healthcare vendor" **Clues:** - Vendor logo and branding match legitimate company - Download came from vendor's actual domain (after compromise) - Staff recognized vendor name from previous legitimate communications - Certificate appears valid but was issued after domain compromise

Secret 2: "IT staff bypassed normal validation because of patient safety pressure" **Clues:** - Hospital leadership emphasized "patient care depends on system go-live" - Previous delays had caused criticism from medical staff - IT Director

received explicit instruction to "make it work regardless" - Normal approval committees were skipped for "emergency deployment"

Secret 3: "The attack specifically targeted healthcare organizations during high-pressure periods" **Clues:** - Similar incidents at other hospitals during go-live periods - Malware specifically designed to evade healthcare security tools - Timing coincides with industry-wide EMR implementation deadline - Threat actor demonstrated knowledge of healthcare operational cycles

3.4.5.3 Clue Distribution Strategy

Scatter clues across investigation paths: - **Detective findings:** Digital forensics reveal technical artifacts - **Protector discoveries:** System analysis shows security control failures - **Tracker observations:** Network analysis reveals communication patterns - **Communicator interviews:** Stakeholder conversations reveal organizational pressures - **Crisis Manager research:** Business analysis reveals strategic contexts - **Threat Hunter insights:** Advanced analysis reveals attribution clues

Make clues discoverable through player expertise: - Technical staff find technical clues naturally - Business professionals notice organizational pressure clues - Mixed groups collaborate to connect different clue types - Questions help groups discover clues they're positioned to find

3.4.6 Storytelling Recovery Techniques

3.4.6.1 When Groups Get Lost in Technical Details

- **Zoom out to story:** "Let's step back - what's the impact on the organization?"
- **Character perspective:** "What would the IT Director be thinking right now?"
- **Time pressure:** "Meanwhile, the deadline is still approaching…"
- **Secrets focus:** "What does this technical finding tell us about why the attack succeeded?"

3.4.6.2 When Interest Drops

- **Escalate stakes:** "Just as you think you have it contained…"
- **Add human element:** "End users are starting to complain about…"
- **Introduce urgency:** "Executive leadership just called a meeting…"
- **Reveal deeper secrets:** "This investigation is uncovering something bigger…"

3.4.6.3 When Groups Move Too Fast

- **Slow with story:** "Before we implement that, what would Legal say?"

- **Add complexity:** "That's a good plan, but what about the compliance requirements?"
- **Character perspective:** "How would you explain this decision to the CEO?"
- **Unresolved secrets:** "What still doesn't make sense about how this attack succeeded?"

3.5 Using Player Expertise as Your Content Engine

3.5.1 The Expertise Extraction Method

3.5.1.1 Direct Consultation

"Sarah, given your SOC experience, what would you check first?"
"Alex, from a network perspective, what concerns you about this traffic?"

3.5.1.2 Experience Mining

"Has anyone dealt with something similar?"
"What does this remind you of from your work?"
"Who here has seen [relevant technology] before?"

3.5.1.3 Collaborative Building

"Let's think through this together…"
"What would the group recommend here?"
"How would you approach this as a team?"

3.5.2 When Nobody Knows

3.5.2.1 The Progressive Revelation Technique

Layer 1: Simplify the question
Original: "How would you detect fileless malware?"
Simplified: "How would you notice something running that isn't supposed to be there?"

Layer 2: Provide context clues
"Think about it - if malware is hiding in memory, what might give it away?"

Layer 3: Multiple choice framework
"Would you be more concerned about: A) New files appearing, B) Processes using unusual memory, or C) Network connections to unknown servers?"

Layer 4: Graceful teaching moment
"This is actually a great learning opportunity. In the real world, security professionals look for…"

3.6 Practical Secrets and Clues Preparation

3.6.1 The 5-Minute Secret Development Process

Step 1 (60 seconds): Define the Core Question What's the one thing that explains why this attack succeeded? - *Example:* "Why did experienced IT staff fall for obvious social engineering?"

Step 2 (90 seconds): Create the Answer (Secret)
- *Secret:* "IT was under extreme deadline pressure that made normal security validation impossible"

Step 3 (90 seconds): Scatter 4-6 Clues - Email: "Need this approved by EOD or project fails" - Interview: "We've been working 80-hour weeks"
- System: Security scan skipped in deployment logs - Business: Patient safety depends on Monday go-live - Financial: Penalty clauses for late delivery

Step 4 (60 seconds): Plan Discovery Methods - **Detective:** Finds deployment logs and email chains - **Communicator:** Interviews reveal deadline pressure - **Crisis Manager:** Discovers business pressures and penalties

Step 5 (30 seconds): Prepare Follow-up Questions - *"What pressure would make experienced IT staff cut corners?"* - *"How would deadline stress affect security decision-making?"*

3.6.2 Secret Templates for Common M&M Scenarios

3.6.2.1 Trojan/Social Engineering Scenarios

Template Secret: "The deception succeeded because [organizational pressure] made [normal security practice] impossible"

GaboonGrabber Healthcare Example: - **Secret:** "Hospital staff clicked malicious links because patient safety pressure overrode security training" - **Clues:** Emergency protocols, patient criticality, staff exhaustion, management pressure

FakeBat Financial Example: - **Secret:** "Banking staff installed fake software because regulatory deadline made normal approval process too slow" - **Clues:** Audit timeline, compliance requirements, executive pressure, process shortcuts

3.6.2.2 Worm/Propagation Scenarios

Template Secret: "The worm spread because [security control] was disabled for [business reason]"

WannaCry Manufacturing Example: - **Secret:** "Network segmentation was disabled to meet production deadlines, allowing worm propagation" - **Clues:** Production schedules, network changes, efficiency demands, cost pressures

3.6.2.3 Ransomware Scenarios

Template Secret: "The ransomware succeeded because [backup/recovery system] failed due to [organizational issue]"

LockBit Education Example: - **Secret:** "Backups were compromised because budget cuts eliminated proper backup testing and monitoring" - **Clues:** Budget documents, untested backups, staff reductions, maintenance deferrals

3.6.3 Advanced Secrets and Clues Techniques

3.6.3.1 The Interconnected Secrets Method

Create secrets that build on each other for deeper investigation:

Secret Level 1: "Attack succeeded due to software approval shortcuts" **Secret Level 2:** "Shortcuts were mandated by unrealistic management deadlines" **Secret Level 3:** "Deadlines exist because organization culture prioritizes appearance over substance"

Each level explains the previous and leads to more fundamental understanding.

3.6.3.2 The Red Herring Management

Use false leads that teach real concepts: - **False lead:** "Disgruntled employee might be insider threat" - **Real lesson:** Shows importance of thorough investigation before conclusions - **Investigation value:** Teaches proper attribution and evidence evaluation

3.6.3.3 The Collaborative Secret Discovery

Design secrets that require multiple player roles to uncover: - **Detective** finds technical artifacts - **Communicator** reveals organizational context through interviews - **Crisis Manager** connects business pressures to security decisions - **Complete secret** emerges only when roles collaborate

3.6.4 Session Flow with Secrets and Clues

3.6.4.1 Discovery Phase Secret Revelation

Opening Hook: Symptoms that hint at deeper problems **Question Pattern:** *"What could cause these specific symptoms?"* **Secret Revelation:** Players discover Surface Secret through collaborative investigation **Transition:** *"Now that we understand how this happened, what's the impact?"*

3.6.4.2 Investigation Phase Secret Deepening

Scope Questions: *"How extensive might this compromise be?"* **Attribution Questions:** *"What does this tell us about the attacker?"* **Secret Revelation:**

Players uncover Deeper Secrets through persistent investigation **Transition:** *"Understanding the scope, what's our response strategy?"*

3.6.4.3 Response Phase Secret Application

Strategy Questions: *"How do we address the root causes we've discovered?"*
Prevention Questions: *"What changes prevent this from happening again?"*
Secret Application: Response addresses both immediate threat and underlying issues **Resolution:** Players feel they've solved not just the technical problem but the organizational one

3.7 The Art of Productive Improvisation

3.7.1 "Yes, And..." for Cybersecurity

3.7.1.1 The Basic Technique

Player contribution: *"I think this might be using DLL sideloading"*
Yes, and response: *"Yes, that's exactly the kind of technique this Malmon uses, and that changes how we should approach detection. What would that mean for our investigation?"*

3.7.1.2 Building on Uncertainty

Player: *"I'm not sure, but maybe we should check the registry?"*
Yes, and: *"Yes, the registry is definitely worth checking, and since you mentioned it, what specifically would you look for there?"*

3.7.2 When Players Take Unexpected Directions

3.7.2.1 The Redirect Technique

Let players pursue their interests while maintaining learning objectives:

Player interest: Deep dive into specific exploit techniques
IM response: *"That's fascinating detail. How does understanding that technique help us with our current response strategy?"*

3.7.2.2 The Incorporation Method

Fold unexpected expertise into the scenario:

Unexpected expertise: Player knows about industrial control systems
IM incorporation: *"Actually, this organization has some industrial components. How might that change our threat assessment?"*

3.8 Minimal Notes, Maximum Impact

3.8.1 Your Essential Session Notes

3.8.1.1 The One-Page Prep Sheet

```
ORGANIZATION: [Industry/Size/Stakes]
SYMPTOMS: [2-3 observable problems]
MALMON: [Name/Type/Key abilities]
QUESTIONS: [3-5 discovery prompts]
EVOLUTION: [What happens if not contained]
```

3.8.1.2 Real-Time Note Taking

Track during session:

- Player contributions that drive story
- Emerging expertise areas
- Group energy and engagement
- Natural stopping/transition points

3.8.2 What NOT to Prepare

- **Detailed technical explanations:** Players provide these
- **Predetermined outcomes:** Emerge from group decisions
- **Complex branching scenarios:** Improvise based on player choices
- **Extensive background materials:** Create just-in-time context

3.9 Advanced Lazy Techniques

3.9.1 The Expertise Redirect

When asked technical questions beyond your knowledge:
"That's a great technical question. Who here might have experience with that?"

3.9.2 The Collaborative Discovery

When uncertain about scenario direction:
"This is interesting. How do you think this situation would typically develop?"

3.9.3 The Learning Opportunity Reframe

When making mistakes:
"Actually, let's think about this differently. What would really happen in this situation?"

3.10 Common Lazy IM Pitfalls

3.10.1 Over-Preparing

Problem: Detailed scenarios that ignore player expertise
Solution: Trust that players will create better content than you can plan

3.10.2 Under-Confidence

Problem: Feeling like you need to know everything
Solution: Remember that facilitation skills matter more than technical knowledge

3.10.3 Fighting Player Direction

Problem: Forcing scenarios back to your plan
Solution: Follow player interest and adapt objectives accordingly

3.10.4 Providing Too Much Information

Problem: Answering questions players could figure out
Solution: Turn statements into questions; let players teach each other

3.11 The Lazy IM Mindset

3.11.1 Core Beliefs

- **Players are experts:** They know more collectively than you do individually
- **Questions > Answers:** Discovery beats delivery for learning
- **Scenarios emerge:** Best content comes from group collaboration
- **Mistakes are features:** Uncertainty creates teaching moments
- **Less is more:** Minimal prep allows maximum adaptation

3.11.2 Session Success Metrics

A successful lazy IM session:

- ☐ Players contribute most of the technical content
- ☐ Group makes meaningful discoveries together
- ☐ Everyone participates in problem-solving
- ☐ Learning emerges from collaboration, not lecture
- ☐ IM asks more questions than they answer

3.12 Practical Application

3.12.1 Your First Lazy Session

1. **Choose familiar Malmon:** Start with GaboonGrabber or FakeBat
2. **Minimal prep:** Use the 5-minute method
3. **Trust the process:** Let players drive content discovery
4. **Ask questions:** When in doubt, turn it into a discovery prompt
5. **Embrace uncertainty:** Use "I don't know" as a facilitation tool

3.12.2 Building Lazy IM Skills

- **Practice question patterns:** Make them automatic responses
- **Record sessions:** Notice when you provide vs. facilitate discovery
- **Debrief with players:** Ask what worked for their learning
- **Connect with other IMs:** Share lazy techniques and experiences
- **Embrace the philosophy:** Less preparation really does create better sessions

The lazy IM approach transforms cybersecurity education from information delivery to collaborative discovery, creating more engaging, authentic, and effective learning experiences.

Chapter 4

Session Preparation: Using Scenario Cards

4.1 IM Preparation Quick Reference

4.2 Transforming M&M Sessions Through Rich Narrative

The M&M Scenario Card system represents a fundamental evolution in cybersecurity education facilitation, transforming sessions from technical exercises into compelling, human-centered learning experiences. This security training platform approach provides comprehensive professional context while leaving technical content to emerge from player expertise, enabling better improvisation and more meaningful learning through incident response tabletop exercise methodologies.

4.2.1 The Integration Philosophy

4.2.1.1 Enhancing, Not Replacing

Scenario cards build upon the proven M&M framework for gamified incident response training:

- **Core mechanics remain unchanged:** Role-based investigation, type effectiveness, evolution triggers
- **Lazy IM philosophy enhanced:** Rich backstories enable better improvisation and adaptation for security professional development
- **Question-driven discovery improved:** Compelling scenarios generate more meaningful questions for collaborative learning cybersecurity

- **Player expertise leveraged:** Realistic organizational contexts connect to professional experience in team-based security training

4.2.1.2 From Technical to Human-Centered

Traditional Approach: *"Your organization has been compromised by Gaboon-Grabber. Begin investigating."*

Scenario Card Approach: *"MedTech Solutions is 72 hours from their biggest client go-live ever. St. Mary's Hospital is depending on the new EMR system Monday morning. During the final push yesterday, IT staff received 'critical security updates' that seemed legitimate given the project pressure. Now systems are failing and the project timeline is at risk."*

The Transformation:

- **Immediate stakes:** Players understand what matters and why
- **Compelling timeline:** Pressure creates natural urgency without artificial constraints
- **Realistic context:** Professional experience connects to scenario elements
- **Rich investigation:** Multiple paths and stakeholder perspectives drive discovery

4.2.2 Example Scenario Card

Here's a complete scenario card to demonstrate the structure:

This single card provides everything needed for a rich, 90-minute session: compelling professional context, realistic stakeholder dynamics, and natural investigation paths that connect to participants' real expertise.

4.3 The New IM 30-Minute Scenario Card Preparation

4.3.1 First-Time Facilitator Complete Prep Using Scenario Cards

4.3.1.1 Minutes 1-5: Essential Materials Preparation

Core Game Materials:

- ☐ Malmon cards for chosen scenario
- ☐ Role cards or reference sheets
- ☐ Dice (physical d20s work better than apps)
- ☐ Network Security Status tracker
- ☐ Blank paper for notes and diagrams

4.3.1.2 Minutes 6-10: Scenario Card Selection

Choose Based on Group and Learning Objectives:

```
High-tech group → Technology/Healthcare scenario cards
Mixed group → Healthcare/Financial scenario cards
Business-focused → Manufacturing/Financial scenario cards
Academic → Municipal/Research scenario cards
```

Scenario card categories with built-in professional context:

- **GaboonGrabber Cards:** Social engineering, trust exploitation, deadline pressure
- **WannaCry Cards:** Network propagation, multi-site coordination, rapid response
- **Stuxnet Cards:** Critical infrastructure, sophisticated threats, geopolitical context

4.3.2 Scenario Card Examples by Industry

Here are snippet previews showing how different industries and contexts create varied challenges:

Each card provides complete context: Hook, Pressure, NPCs, Secrets, Villain Plan

4.3.2.1 Minutes 11-15: NPC Development and Context Mastery

Master your scenario card's stakeholders:

Primary NPC Understanding:

- **Role and responsibilities:** What they manage day-to-day
- **Core concerns:** What keeps them awake at night
- **Success criteria:** What a "win" looks like for them
- **Constraints:** Why they can't just "shut everything down"

Stakeholder Dynamics:

- **Competing priorities:** Security vs. Operations vs. Compliance
- **Time pressures:** Real deadlines creating authentic urgency
- **Information flow:** Who reports to whom in crisis
- **Decision authority:** Who ultimately makes the call

4.3.2.2 Minutes 16-20: Hook Mastery and Opening Preparation

Internalize your scenario's hook:

Professional Context Elements:

- **Industry situation:** Context players will immediately recognize
- **Time pressure:** Specific business deadline creating urgency

- **Vulnerability creation:** Why security was compromised under pressure
- **Current symptoms:** What's happening NOW that demands response

Practice Opening Delivery:

- **"[Organization] is [timeframe] from [critical deadline]..."**
- **"During [pressure situation], [stakeholder] approved [security compromise]..."**
- **"Now [symptoms] are appearing..."**
- **"What would worry you most in this situation?"**

4.3.2.3 Minutes 21-25: Context-Driven Question Development

Prepare scenario-specific questions:

Context Integration Questions:

- *"Given [organization's situation], what would worry you most?"*
- *"In [industry context], who would feel this pressure first?"*
- *"How would [primary stakeholder] be thinking about this?"*
- *"What makes this timing particularly problematic?"*

Stakeholder Perspective Questions:

- *"What would [IT Director] be concerned about right now?"*
- *"How would [Business Sponsor] want this handled?"*
- *"What would success look like from [stakeholder] perspective?"*

Professional Reality Questions:

- *"How would you handle [competing pressures] in your organization?"*
- *"What would this response look like in your real workplace?"*
- *"Who would you need to coordinate with for this approach?"*

4.3.2.4 Minutes 26-30: Contingency Planning

Backup Plans:

- **Alternative Malmon:** If chosen one doesn't resonate with group
- **Simplified scenario:** If group struggles with complexity
- **Extended scenario:** If group moves faster than expected
- **Time management:** Strategies for running long or short

Emergency Protocols:

- **Silent group:** Prepared icebreaker questions
- **Dominated discussion:** Techniques for balanced participation
- **Technical disputes:** Facilitation methods for conflicting expertise
- **Technology failure:** Pen-and-paper alternatives

4.4 The Experienced IM 5-Minute Scenario Card Preparation

4.4.1 Streamlined Workflow for Regular Facilitators

4.4.1.1 Minute 1: Scenario Card Selection

- Choose card based on group expertise and learning objectives
- Consider industry match and stakeholder complexity
- Have backup card from different context ready

4.4.1.2 Minute 2: Secrets and Clues Preparation

Using the Sly Flourish secrets and clues methodology (see Sly Flourish Principles):

- **Identify core secret:** Why did this attack succeed in this organization?
- **Scatter 3-4 clues:** Evidence discoverable through different investigation paths
- **Plan revelation:** How will each role naturally uncover clues through their expertise?

4.4.1.3 Minute 3: NPC Motivation Review

- Quick scan of primary stakeholder concerns and constraints
- Identify key stakeholder conflicts and competing priorities
- Review why normal security processes were bypassed

4.4.1.4 Minute 4: Hook Internalization

- Practice opening hook delivery connecting context to symptoms
- Understand why this attack is happening NOW
- Prepare transition from hook to investigation questions

4.4.1.5 Minute 5: Pressure Timeline Understanding

- Review business deadline and why it can't move
- Understand escalation stages if threat evolves
- Prepare authentic urgency without rushing facilitation

4.4.1.6 Final Steps: Question Preparation and Setup

- Prepare context-driven discovery questions
- Materials check: scenario card, dice, tracking sheets
- Mental transition to facilitator mode

4.4.2 When to Spend More Time

Extend preparation for:

- **Unfamiliar groups:** Need more stakeholder dynamic contingency planning
- **New scenario cards:** Require deeper professional context review
- **High-stakes sessions:** Conference workshops, executive audiences
- **Complex stakeholder dynamics:** Multi-authority or regulatory scenarios

Stick to 5 minutes for:

- **Regular groups:** Known professional backgrounds and dynamics
- **Familiar scenario cards:** Comfortable with context and stakeholders
- **Standard sessions:** Normal learning objectives and complexity
- **Confident facilitation:** Experience with context-driven questioning

4.5 Malmon Selection Decision Trees

4.5.1 Based on Group Composition

4.5.1.1 High Technical Expertise Groups

```
Experienced SOC analysts, security engineers, incident responders

Recommended Malmons:
- Stuxnet (if industrial experience present)
- Noodle RAT (advanced persistence concepts)
- LockBit (complex ransomware operations)
- WannaCry (network propagation mechanics)

Avoid:
- GaboonGrabber (too basic)
- FakeBat (obvious techniques)
```

4.5.1.2 Mixed Expertise Groups

```
Combination of technical and business professionals

Recommended Malmons:
- GaboonGrabber (clear concepts, good learning progression)
- Raspberry Robin (tangible USB infection vector)
- GhOst RAT (classic remote access techniques)
- WireLurker (cross-platform concepts)

Focus on:
- Clear type effectiveness
```

```
- Collaborative learning opportunities
- Business impact discussions
```

4.5.1.3 Business-Focused Groups

```
Managers, compliance, risk management, executives

Recommended Malmons:
- FakeBat (clear deception, business impact)
- GaboonGrabber (social engineering focus)
- LockBit (business continuity implications)
- Code Red (historical context, business lessons)

Emphasize:
- Business impact and decision-making
- Communication and coordination
- Risk management perspectives
```

4.5.2 Based on Learning Objectives

4.5.2.1 Technical Skill Development

- **WannaCry:** Network propagation and patching
- **Stuxnet:** Advanced evasion and attribution
- **Noodle RAT:** Fileless techniques and persistence
- **Poison Ivy:** Classic RAT capabilities

4.5.2.2 Incident Response Process

- **GaboonGrabber:** Full IR lifecycle
- **Raspberry Robin:** Containment and forensics
- **Gh0st RAT:** Coordination and communication
- **LockBit:** Business continuity and recovery

4.5.2.3 Threat Intelligence and Attribution

- **Stuxnet:** Nation-state analysis
- **Gh0st RAT:** APT group characteristics
- **LitterDrifter:** Geopolitical context
- **Noodle RAT:** Campaign tracking

4.6 Organization Context Templates

4.6.1 Quick Context Generator

4.6.1.1 Healthcare Organizations

- **Stakes:** Patient safety, HIPAA compliance, operational continuity

- **Critical assets:** EMR systems, patient data, medical devices
- **Vulnerabilities:** Legacy systems, user convenience, interconnected devices
- **Constraints:** Cannot disrupt patient care, strict privacy requirements

4.6.1.2 Financial Services

- **Stakes:** Customer trust, regulatory compliance, financial stability
- **Critical assets:** Transaction systems, customer data, trading platforms
- **Vulnerabilities:** High-value targets, complex integrations, mobile access
- **Constraints:** Regulatory reporting, availability requirements, fraud prevention

4.6.1.3 Manufacturing/Industrial

- **Stakes:** Production continuity, worker safety, competitive advantage
- **Critical assets:** Control systems, proprietary processes, supply chain data
- **Vulnerabilities:** Air-gapped networks, legacy systems, remote monitoring
- **Constraints:** Safety systems, production schedules, physical security

4.6.1.4 Technology Companies

- **Stakes:** Intellectual property, customer data, service availability
- **Critical assets:** Source code, customer databases, cloud infrastructure
- **Vulnerabilities:** Developer tools, cloud misconfigurations, supply chain
- **Constraints:** Rapid development cycles, distributed workforce, scalability

4.6.2 Collaborative Context Creation

4.6.2.1 Group-Driven Approach

Instead of pre-selecting, let the group decide:

- *"What kind of organization are you protecting today?"*
- *"What would be devastating if compromised?"*
- *"What makes your organization unique or challenging to secure?"*

Benefits:

- Immediate investment in scenario
- Authentic expertise application
- Natural constraints and considerations
- Real-world relevance

4.7 Core Integration Points

4.7.1 Integration with Role-Based Investigation

4.7.1.1 Enhanced Role Clarity

Scenario cards provide organizational context that makes roles immediately meaningful:

Detective Role:

- **Traditional:** "Investigate the compromise"
- **With Scenario Cards:** "Sarah (IT Director) needs to understand what happened during the project crunch - interview staff, analyze logs, determine attack timeline"

Protector Role:

- **Traditional:** "Identify systems to protect"
- **With Scenario Cards:** "Critical hospital systems go live Monday - determine what's at risk, implement containment without disrupting patient care"

Communicator Role:

- **Traditional:** "Coordinate team response"
- **With Scenario Cards:** "Hospital CIO is calling hourly demanding updates - manage stakeholder communication while coordinating technical response"

4.7.1.2 Natural Investigation Paths

NPCs and organizational context create realistic investigation opportunities:

- **Staff interviews** reveal social engineering vectors and organizational pressures
- **System dependencies** show critical assets and business impact priorities
- **Timeline pressures** create realistic constraints on investigation thoroughness
- **Stakeholder concerns** drive investigation priorities and communication needs

4.7.2 Integration with Question-Driven Discovery

4.7.2.1 Enhanced Question Frameworks

Scenario cards provide rich context for more meaningful discovery questions:

Discovery Phase Questions:

- *"Given the pressure [organization] was under, what would make [specific stakeholder] click on suspicious emails?"*

- *"How would [business deadline] affect normal security awareness and procedures?"*
- *"What organizational factors would make this attack particularly effective at this time?"*

Investigation Phase Questions:

- *"If [critical deadline] is missed, what are the real consequences for [specific stakeholders]?"*
- *"How would [regulatory requirement] affect your investigation approach and evidence collection?"*
- *"What would [key customer/partner] do if they knew about this security incident?"*

Response Phase Questions:

- *"Given [specific organizational constraint], what response options are actually feasible?"*
- *"How would you manage [stakeholder conflict] while responding to this cybersecurity threat?"*
- *"What communication strategy maintains [key relationship] during incident response?"*

4.8 Contingency Planning

4.8.1 Alternative Scenarios

4.8.1.1 Backup Malmon Strategy

Always have 2-3 Malmons prepared:

- **Primary choice:** Based on group and objectives
- **Simpler backup:** If group struggles with complexity
- **Complex alternative:** If group advances quickly

4.8.1.2 Time Management Alternatives

Running Long (Extra 30+ minutes):

- Extended investigation phase
- Multiple evolution scenarios
- Advanced response techniques
- Detailed debrief and lessons learned

Running Short (30+ minutes remaining):

- Accelerated discovery phase
- Combined investigation/response
- Quick evolution challenge
- Rapid debrief with key takeaways

Severe Time Constraints (Under 60 minutes):

- Single-round scenario
- Focus on one aspect (discovery or response)
- Mini-session with core concepts
- Promise follow-up session

4.8.2 Group Dynamic Challenges

4.8.2.1 Silent Group Protocol

- **Structured icebreakers:** "Share one cybersecurity concern"
- **Direct questions:** Address individuals by name and role
- **Collaborative tasks:** Force interaction through shared problems
- **Lower stakes:** Reduce pressure with hypothetical scenarios

4.8.2.2 Dominated Discussion Management

- **Rotation systems:** Ensure everyone speaks before anyone speaks twice
- **Role-specific questions:** Direct questions to quiet participants
- **Private coaching:** Brief sidebar with dominant speaker
- **Structural solutions:** Break into smaller groups

4.8.2.3 Technical Knowledge Gaps

- **Peer teaching:** Connect experts with learners
- **Simplified scenarios:** Reduce technical complexity
- **Common sense focus:** Emphasize logical thinking over technical knowledge
- **Learning opportunities:** Frame gaps as discovery moments

4.8.3 Emergency Protocols

4.8.3.1 Technology Failures

- **Backup methods:** Paper alternatives for all digital tools
- **Simple substitutions:** Use coin flips instead of dice apps
- **Manual tracking:** Paper Network Security Status tracker
- **Continue regardless:** Don't let technology stop the session

4.8.3.2 Participant Issues

- **Late arrivals:** Quick integration techniques
- **Early departures:** Graceful role transitions
- **Disruptive behavior:** Professional de-escalation
- **Medical/personal emergencies:** Session pause and support protocols

4.8.3.3 Facilitator Challenges

- **Knowledge gaps:** Redirect to group expertise
- **Time pressure:** Flexible scenario adaptation
- **Group conflict:** Neutral facilitation techniques
- **Personal stress:** Breathing techniques and perspective

4.9 Pre-Session Checklist

4.9.1 24 Hours Before

☐ Confirm participant count and experience levels
☐ Review chosen Malmon technical details
☐ Prepare physical materials
☐ Confirm room setup and technology
☐ Review emergency contact information

4.9.2 1 Hour Before

☐ Room setup and materials arrangement
☐ Technology testing (if used)
☐ Personal preparation and mindset
☐ Final scenario review
☐ Contingency plan review

4.9.3 10 Minutes Before

☐ Participant greeting and informal assessment
☐ Final materials check
☐ Mental transition to facilitator mode
☐ Energy level and room atmosphere check
☐ Begin informal relationship building

4.10 Example: Following the Method in Practice

Let's walk through using this method to prepare for a session with a mixed-expertise group.

4.10.1 Group Context

You have 5 participants: an IT manager, a software developer, a compliance officer, a network admin, and a project manager. They work in different organizations but all deal with healthcare technology.

4.10.2 Following the Preparation Activities

4.10.2.1 Activity 1: Scenario Card Selection

Your thinking: *Mixed group with healthcare focus. GaboonGrabber healthcare scenario will resonate - social engineering they can all relate to, technical depth for IT folks, business pressure for managers.*

Your choice: GaboonGrabber "MedTech Solutions" scenario card **Backup:** WannaCry hospital scenario (if they want more technical network focus)

4.10.2.2 Activity 2: NPC Motivation and Context Review

From the scenario card, you understand:

Sarah (IT Director): Under massive pressure to deliver hospital EMR system on time. Monday go-live cannot be delayed - hospital staff trained, old system being decommissioned. She's been cutting corners on security approvals because "the project absolutely cannot fail."

Dr. Martinez (Hospital CIO): Depending on MedTech to deliver Monday. If EMR isn't ready, hospital operations could be severely disrupted. Patient safety is her primary concern, but she needs the new system.

Mike (MedTech CEO): This contract makes or breaks the company. If St. Mary's cancels, MedTech loses credibility and probably goes under. He's been pushing everyone to "do whatever it takes."

Competing priorities: Security vs. delivery timeline vs. patient safety vs. business survival.

4.10.2.3 Activity 3: Hook Internalization and Opening

Your opening: *"MedTech Solutions is 72 hours from their biggest client go-live ever. St. Mary's Hospital has trained 200 staff members and is shutting down their old EMR system Sunday night. The new system absolutely must work Monday morning for patient safety. Yesterday, during the final integration push, IT staff received 'critical security updates' from what looked like Microsoft. Under pressure to keep the project on track, they approved the updates immediately. Now systems are running 30% slower and help desk is getting calls about pop-ups. What would worry you most in this situation?"*

4.10.2.4 Activity 4: Pressure Timeline and Evolution Planning

Business deadline: Monday morning hospital go-live - immovable because:

- 200 hospital staff already trained on new system
- Old EMR being decommissioned Sunday night
- Patient care depends on working system Monday

If threat evolves:

- Stage 1: Performance issues (current)
- Stage 2: Data exfiltration and system corruption
- Stage 3: Complete system failure Sunday night, hospital cannot treat patients Monday

4.10.2.5 Activity 5: Question Preparation and Materials Setup

Your prepared questions:

- *"Given the project pressure MedTech was under, what would make IT staff click on security updates without proper verification?"*
- *"If this system fails Monday morning, what happens to patient care at St. Mary's?"*
- *"How would you balance cybersecurity response with the absolute need to have systems working in 72 hours?"*
- *"What would Sarah (IT Director) be most afraid of - the cyberattack or missing the deadline?"*

Materials ready: GaboonGrabber malmon card, scenario card, dice, whiteboard markers, participant name tags.

4.10.3 What This Preparation Achieves

Immediate engagement: Players understand the stakes before you even explain the technical threat.

Professional relevance: Everyone has experienced project pressure and stakeholder conflicts.

Natural investigation paths:

- IT Manager: "I need to understand what these updates actually did"
- Developer: "How do we fix this without breaking the go-live?"
- Compliance Officer: "What are our reporting requirements if patient data is at risk?"
- Network Admin: "I want to trace what network connections these updates made"
- Project Manager: "How do we coordinate response while maintaining the timeline?"

Rich facilitation opportunities: You can represent Sarah's desperation, Dr. Martinez's patient safety concerns, and Mike's business survival fears to create realistic tension and decision-making pressure.

Multiple learning outcomes: Social engineering awareness, incident response coordination, business-security balance, stakeholder management under pressure.

4.10.4 During the Session

Your job becomes easy because the scenario card provides:

- Context players immediately understand
- Stakeholders you can role-play naturally
- Business pressure that creates realistic urgency
- Multiple investigation angles for different expertise
- Authentic decision-making dilemmas

Instead of lecturing about GaboonGrabber techniques, you ask: *"Given what you've found, what would worry you about this 'security update' from Sarah's perspective?"*

Players discover the technical details while you facilitate the human drama.

4.11 Post-Preparation Mindset

4.11.1 Confidence Building

Remember:

- **Preparation is foundation, not script:** Be ready to adapt
- **Players provide content:** Your job is facilitation, not information delivery
- **Mistakes are learning:** Both for you and participants
- **Questions > answers:** When in doubt, ask the group
- **Success is participation:** Everyone contributing meaningfully

4.11.2 Session Success Indicators

A well-prepared session typically includes:

☐ All participants contribute meaningfully
☐ Technical discussions emerge naturally from group expertise
☐ Questions drive discovery more than explanations
☐ Group makes collaborative decisions
☐ Learning happens through practice, not lecture
☐ Everyone leaves with applicable insights

4.12 Practical Integration Workflows

4.12.1 Scenario Card Selection Process

4.12.1.1 Matching Cards to Groups

Step 1: Assess Group Composition

- **Experience Level:** Beginner → GaboonGrabber scenarios; Advanced → Stuxnet scenarios
- **Professional Background:** Healthcare → Medical scenarios; Finance → Banking scenarios
- **Learning Objectives:** Social engineering → Trojan scenarios; Network security → Worm scenarios

Step 2: Review Adaptation Notes Each scenario card includes specific guidance for:

- **High-expertise groups:** Additional complexity and advanced concepts
- **Beginner groups:** Simplification strategies and concept focus
- **Time constraints:** Compression options and priority elements

Step 3: Customize for Context

- **Industry familiarity:** Adapt organizational details to match group experience
- **Current events:** Connect scenario timing to relevant news or industry trends
- **Group interests:** Emphasize aspects that align with participant professional concerns

4.12.2 Troubleshooting Integration Challenges

4.12.2.1 When Scenario Cards Feel Overwhelming

Simplification Strategies - Focus on Core Elements:

- **Hook:** Why this is happening now
- **Pressure:** What creates urgency
- **NPCs:** 2-3 key stakeholders maximum
- **Secrets:** 1-2 organizational factors that enabled attack

Adaptation Approach:

- Use scenario cards as inspiration rather than rigid scripts
- Select elements that serve your learning objectives
- Ignore complexity that doesn't add value for your specific group
- Trust the "lazy IM" philosophy - good enough preparation with rich context beats perfect preparation with rigid structure

4.12.2.2 When Group Doesn't Connect to Scenario Context

Quick Adaptation Techniques:

- **Industry Swap:** Change from healthcare to technology, finance to manufacturing
- **Scale Adjustment:** Adjust organization size and complexity
- **Stakeholder Modification:** Replace NPCs with roles familiar to your group

- **Context Simplification:** Focus on universal business pressures rather than industry-specific details

Collaborative Fixes:

- Ask group to suggest organizational context they find more relevant
- Let participants modify NPCs to match their professional experience
- Encourage group to adapt scenario elements during session
- Use "yes, and…" techniques to incorporate participant suggestions

The goal of scenario card preparation is confident flexibility - ready for anything while attached to nothing. Scenario cards enhance the "lazy IM" philosophy by providing rich context that enables better improvisation, not rigid scripts that constrain adaptation.

Chapter 5

Comprehensive Scenario Types Guide

5.1 IM Quick Reference: All Session Types

This chapter provides a unified overview of every session format available in our cybersecurity education framework, helping you choose the right approach for your group and goals through our security training platform that supports both incident response training and security professional development.

5.1.1 Decision Matrix: Choosing Session Type

Group Type	Time Available	Learning Goal	Recommended Approach
Mixed expertise, educational setting	2+ hours	Understanding cybersecurity evolution	**Historical Foundation**
Advanced technical team	90 minutes	Current practical skills	**Contemporary Standard**
Leadership/business focus	90-120 minutes	Strategic decision-making	**Contemporary with Business Focus**
New to cybersecurity	90 minutes	Basic incident response	**Standard Contemporary (Beginner Malmons)**

Group Type	Time Available	Learning Goal	Recommended Approach
Expert-dominated group	2+ hours	Collaborative learning	**Historical Foundation**
Training/certification	60-90 minutes	Specific current techniques	**Contemporary Focused**

5.2 Session Type Categories

5.2.1 1. Standard Contemporary Sessions

5.2.1.1 Core Format

- **Duration:** 90-120 minutes
- **Technology Context:** Current platforms, tools, and threats
- **Malmons:** Any contemporary malmon (GaboonGrabber, WannaCry, Raspberry Robin, etc.)
- **Scenario Cards:** Multiple organizational contexts per malmon

5.2.1.2 Session Structure

1. **Setup** (15 min) - Introductions, role assignment, context setting
2. **Investigation** (30-45 min) - Collaborative threat analysis and discovery
3. **Response** (30-45 min) - Coordinated containment and mitigation
4. **Debrief** (15 min) - Learning synthesis and real-world application

5.2.1.3 When to Use

Perfect for:

- Groups wanting immediate practical skills
- Limited time availability
- Focus on current cybersecurity challenges
- Professional development and training

Avoid when:

- Group wants historical perspective
- Significant time available for deeper exploration
- Educational setting focused on evolution and learning

5.2.1.4 IM Preparation (10 minutes)

- Choose appropriate malmon for group expertise level

- Select scenario card matching group's industry/context
- Review Network Security Status tracking approach
- Prepare role assignments based on group backgrounds

5.2.1.5 Success Indicators

- Effective team coordination and communication
- Appropriate use of current cybersecurity tools and techniques
- Realistic business decision-making under pressure
- Learning that applies directly to participants' current work

5.2.2 2. Legacy Malmon Sessions

5.2.2.1 Two Distinct Approaches Available

5.2.3 2A. Historical Foundation Sessions

5.2.3.1 Core Format

- **Duration:** 2+ hours for full exploration
- **Technology Context:** Authentic period technology (2001-2010)
- **Malmons:** Code Red, Stuxnet, Gh0st RAT, Poison Ivy
- **Learning Goal:** Understanding cybersecurity evolution through collaborative discovery

5.2.3.2 Session Structure

1. **Historical Context** (15 min) - Period technology and security assumptions
2. **Authentic Historical Investigation** (45 min) - Response using only period tools/knowledge
3. **Collaborative Modernization** (30 min) - Team discovery of evolution to current threats
4. **Learning Synthesis** (15 min) - Pattern recognition and current application insights

5.2.3.3 When to Use

Perfect for:

- Educational settings and training programs
- Groups with diverse expertise levels
- Time available for extended learning exploration
- Expert-dominated groups needing collaborative focus
- Understanding how cybersecurity knowledge developed

Avoid when:

- Immediate practical skills needed

- Limited time (less than 2 hours)
- Group focused only on current challenges
- Advanced technical audience wanting cutting-edge techniques

5.2.3.4 IM Preparation (20 minutes)

- Research historical technology context thoroughly
- Prepare period-appropriate organizational scenarios
- Plan modernization discovery questions
- Ready to enforce historical limitations strictly

5.2.3.5 Success Indicators

- Authentic surprise at historical security assumptions
- Collaborative discovery of evolution patterns
- "Aha moments" about how threats have developed
- Enhanced understanding of current threats through historical perspective
- Strong team collaboration across expertise levels

5.2.4 2B. Contemporary Legacy Sessions

5.2.4.1 Core Format

- **Duration:** 90-120 minutes
- **Technology Context:** Modern technology with evolved versions of historical threats
- **Malmons:** Modern versions (Cloud Infrastructure Attack, Smart Grid Sabotage, etc.)
- **Learning Goal:** Understanding how classic attack patterns manifest today

5.2.4.2 Session Structure

1. **Evolutionary Context** (5 min) - Connection to historical threat
2. **Contemporary Response** (75 min) - Standard modern incident response
3. **Historical Comparison** (15 min) - Brief evolution discussion in debrief

5.2.4.3 When to Use

Perfect for:

- Groups wanting both current skills and historical perspective
- Standard time constraints with added learning value
- Understanding persistent attack patterns across time
- Advanced groups appreciating threat evolution

5.2.4.4 IM Preparation (15 minutes)

- Understand connection between historical and contemporary versions
- Prepare brief evolutionary context explanation
- Plan debrief comparison questions
- Focus on persistent attack patterns

5.2.5 3. Specialized Session Formats

5.2.5.1 3A. Business Leadership Sessions

5.2.5.2 Core Adaptations

- **Focus:** Strategic decision-making and organizational implications
- **Language:** Executive-appropriate terminology and concepts
- **Decisions:** Board-level choices with enterprise-wide impact
- **NPCs:** C-level executives, board members, regulatory agencies

5.2.5.3 Key Modifications

- Emphasize strategic coordination over technical details
- Focus on policy implications and precedent-setting
- Include interagency and international coordination
- Measure success by strategic contribution, not just incident resolution

5.2.5.4 Example Session Types

- **Stuxnet Strategic Response:** Nation-state attack requiring federal coordination
- **WannaCry Executive Crisis:** Healthcare system-wide ransomware impact
- **Supply Chain Compromise:** Enterprise vendor relationship crisis

5.2.5.5 3B. Technical Deep-Dive Sessions

5.2.5.6 Core Adaptations

- **Focus:** Advanced technical analysis and cutting-edge response techniques
- **Complexity:** Multi-stage attacks with sophisticated evasion techniques
- **Tools:** Advanced threat hunting, forensic analysis, custom defensive measures
- **Challenge Level:** Nation-state capabilities and zero-day exploitation

5.2.5.7 Key Modifications

- Increased technical complexity and realism
- Advanced MITRE ATT&CK technique mapping
- Custom tool development and advanced forensics
- Focus on threat intelligence and attribution

5.2.5.8 3C. Industry-Specific Sessions

5.2.5.9 Healthcare Focus

- **Regulatory Context:** HIPAA, patient safety, medical device security
- **Critical Systems:** Electronic health records, patient monitoring, surgical systems
- **Stakeholders:** Patients, medical staff, regulatory agencies, insurance

5.2.5.10 Financial Services Focus

- **Regulatory Context:** SOX, PCI DSS, banking regulations, market oversight
- **Critical Systems:** Trading platforms, payment processing, customer accounts
- **Stakeholders:** Customers, regulators, market participants, law enforcement

5.2.5.11 Critical Infrastructure Focus

- **Regulatory Context:** NERC CIP, national security, public safety
- **Critical Systems:** Power generation, water treatment, transportation
- **Stakeholders:** Government agencies, public safety, national security

5.2.6 4. Problem-Focused Sessions

5.2.6.1 4A. Expert-Dominated Groups

- **Challenge:** Senior participants overwhelming others
- **Solution:** Historical context to level playing field
- **Technique:** Uncomfortable role assignments requiring collaboration
- **Goal:** Collaborative learning despite expertise imbalances

5.2.6.2 4B. Silent/Disengaged Groups

- **Challenge:** Participants reluctant to contribute
- **Solution:** Structured discovery questions and role validation
- **Technique:** Small wins building to larger contributions
- **Goal:** Active engagement from all participants

5.2.6.3 4C. Lost/Overwhelmed Groups

- **Challenge:** Participants feeling out of their depth
- **Solution:** Simplified scenarios with strong IM guidance
- **Technique:** Breaking complex problems into manageable steps
- **Goal:** Confidence building through achievable success

5.3 Scenario Card System

5.3.1 Understanding Scenario Cards

Each malmon can be encountered through multiple **scenario cards** that provide different organizational contexts while maintaining consistent core threat behavior.

5.3.1.1 Scenario Card Components

- **Organization:** Specific company/agency context with realistic constraints
- **Stakes:** What's at risk (data, operations, reputation, compliance)
- **Hook:** Compelling opening situation drawing players into the incident
- **NPCs:** Period and context-appropriate characters with specific expertise
- **Secrets:** Hidden information revealed through investigation
- **Adaptation Notes:** Guidance for different group expertise levels

5.3.1.2 Organizational Context Variations

Healthcare: MedTech Solutions (200 employees)

- **Constraints:** Patient safety, HIPAA compliance, medical device security
- **Stakes:** Patient data, medical device integrity, regulatory compliance
- **NPCs:** Medical staff, IT support, compliance officers, patient advocates

Financial Services: Regional Credit Union (50,000 members)

- **Constraints:** Financial regulations, real-time transactions, customer trust
- **Stakes:** Customer financial data, transaction integrity, regulatory standing
- **NPCs:** Financial officers, IT security, regulators, customer service

Education: University Technology Services (15,000 students)

- **Constraints:** Academic freedom, limited budget, diverse user base
- **Stakes:** Student data, research integrity, operational continuity
- **NPCs:** IT staff, faculty, students, administrators

Small Business: Local Marketing Agency (25 employees)

- **Constraints:** Limited resources, personal relationships, survival-level decisions
- **Stakes:** Client data, business survival, personal liability
- **NPCs:** Business owner, freelance IT, key clients, family members

5.3.2 Choosing Scenario Cards

5.3.2.1 Match Group Context

- **Industry Experience:** Choose scenarios familiar to participants
- **Organizational Size:** Match complexity to group's professional experience
- **Regulatory Environment:** Use familiar compliance and legal frameworks
- **Technical Sophistication:** Align with group's technical capabilities

5.3.2.2 Contrast for Learning

- **Different Industry:** Expose participants to unfamiliar constraints
- **Different Scale:** Help understand how organizational size affects incident response
- **Different Stakes:** Explore various business impact scenarios
- **Different Resources:** Experience resource-constrained vs. well-resourced response

---

5.4 Session Planning Framework

5.4.1 Pre-Session Decision Process

5.4.1.1 Step 1: Group Assessment (5 minutes)

- **Expertise Levels:** Technical backgrounds and cybersecurity experience
- **Industry Experience:** Professional contexts and regulatory familiarity
- **Learning Goals:** Immediate skills vs. broader understanding
- **Time Constraints:** Available session duration and follow-up possibilities

5.4.1.2 Step 2: Session Type Selection (2 minutes)

- **Historical Foundation:** Educational focus, diverse expertise, extended time
- **Contemporary Standard:** Practical skills, limited time, current challenges
- **Specialized Format:** Leadership group, technical deep-dive, industry-specific needs

5.4.1.3 Step 3: Malmon and Scenario Selection (3 minutes)

- **Complexity Match:** Align threat sophistication with group capabilities
- **Context Relevance:** Choose organizational scenario matching group experience

- **Learning Objectives:** Select threats supporting specific learning goals

5.4.1.4 Step 4: Preparation Focus (Variable)

- **Historical Foundation:** Research period context, prepare evolution questions
- **Contemporary:** Review current techniques, select appropriate tools/references

- **Specialized:** Adapt language, stakes, and decision complexity for audience

5.4.2 Session Execution Guidelines

5.4.2.1 Opening Phase Best Practices

- **Energy Setting:** Establish collaborative, learning-focused environment
- **Expectation Management:** Explain session type and learning approach
- **Role Assignment:** Match roles to backgrounds while encouraging stretch growth
- **Context Clarity:** Ensure everyone understands organizational and threat context

5.4.2.2 Investigation Phase Best Practices

- **Question-Driven Discovery:** Guide learning through questions, not exposition
- **Collaborative Building:** Help participants build on each other's insights
- **Progressive Revelation:** Introduce complexity gradually based on team readiness
- **Role Validation:** Ensure each participant contributes unique value

5.4.2.3 Response Phase Best Practices

- **Realistic Constraints:** Maintain organizational limitations and resource availability
- **Coordinated Action:** Require team collaboration for success
- **Adaptive Challenge:** Allow threat evolution based on team actions
- **Success Recognition:** Acknowledge effective teamwork and creative solutions

5.4.2.4 Debrief Phase Best Practices

- **Learning Synthesis:** Help participants connect session experience to real-world application
- **Pattern Recognition:** Highlight transferable principles and techniques

- **Honest Reflection:** Encourage discussion of challenges and improvement opportunities
- **Future Application:** Connect learning to participants' current professional contexts

---

5.5 Advanced IM Techniques

5.5.1 Managing Mixed Groups

5.5.1.1 Expertise Balancing

- **Historical Context:** Use unfamiliar contexts to reduce expertise advantages
- **Role Rotation:** Give experts unfamiliar roles requiring new skill development
- **Collaborative Requirements:** Structure success to require diverse perspectives
- **Learning Focus:** Emphasize discovery over demonstration of existing knowledge

5.5.1.2 Engagement Strategies

- **Validated Contribution:** Ensure every participant contributes unique value
- **Progressive Challenge:** Start accessible, build complexity based on team success
- **Peer Learning:** Structure opportunities for participants to teach each other
- **Success Sharing:** Celebrate team achievements over individual brilliance

5.5.2 Adapting Session Complexity

5.5.2.1 Scaling Up for Advanced Groups

- **Multi-Stage Attacks:** Complex, coordinated threats requiring sustained response
- **Advanced Techniques:** Cutting-edge attack methods and defensive capabilities
- **Strategic Implications:** Enterprise-wide and industry-wide impact considerations
- **International Coordination:** Multi-agency and international response requirements

5.5.2.2 Scaling Down for Beginners

- **Clear Progression:** Obvious attack stages with distinct response phases

- **Guided Discovery:** More IM support for investigation and analysis
- **Simplified Decisions:** Fewer variables and clearer choice consequences
- **Success Reinforcement:** Frequent positive feedback and achievement recognition

5.5.3 Real-Time Adaptation

5.5.3.1 Reading Group Dynamics

- **Engagement Indicators:** Participation levels, question quality, collaborative behavior
- **Difficulty Calibration:** Signs of being overwhelmed vs. underchallenged
- **Learning Progress:** Understanding development and insight generation
- **Energy Management:** Maintaining focus and enthusiasm throughout session

5.5.3.2 Mid-Session Adjustments

- **Complexity Modification:** Adding or reducing challenge based on team performance
- **Role Rebalancing:** Addressing participation imbalances or role mismatches
- **Pacing Adjustment:** Speeding up or slowing down based on group processing
- **Learning Support:** Providing additional guidance or clarification as needed

---

5.6 Success Metrics by Session Type

5.6.1 Standard Contemporary Sessions

5.6.1.1 Technical Success Indicators

- Appropriate use of current cybersecurity tools and techniques
- Realistic decision-making within organizational constraints

- Effective team coordination and communication
- Business-aware technical choices

5.6.1.2 Learning Success Indicators

- Direct application insights for participants' current work
- Enhanced understanding of team-based incident response
- Improved confidence in cybersecurity decision-making

- Recognition of cross-functional collaboration importance

5.6.2 Historical Foundation Sessions

5.6.2.1 Historical Understanding Indicators

- Authentic surprise at historical security assumptions
- Understanding of period technology limitations
- Recognition of security knowledge evolution
- Appreciation for historical cybersecurity pioneers

5.6.2.2 Evolution Learning Indicators

- Collaborative discovery of threat development patterns
- Connection between historical and current threats
- Insight into defensive capability advancement
- Understanding of persistent attack principles

5.6.3 Business Leadership Sessions

5.6.3.1 Strategic Decision Indicators

- Appropriate escalation and coordination decisions
- Understanding of policy and precedent implications
- Effective interagency and stakeholder coordination
- Strategic risk assessment and management

5.6.3.2 Organizational Impact Indicators

- Recognition of enterprise-wide incident implications
- Appropriate governance and communication decisions
- Understanding of regulatory and legal considerations
- Long-term organizational resilience planning

5.6.4 Technical Deep-Dive Sessions

5.6.4.1 Advanced Technical Indicators

- Sophisticated threat analysis and attribution
- Advanced tool usage and custom solution development
- Complex multi-stage attack understanding
- Cutting-edge defensive technique application

5.6.4.2 Professional Development Indicators

- Enhanced threat hunting and forensic capabilities
- Improved understanding of advanced persistent threats
- Development of technical leadership skills

- Contribution to cybersecurity knowledge advancement

5.7 Quick Reference Cards

5.7.1 Session Type Quick Selection

Need immediate practical skills + limited time + current focus: → Standard Contemporary Session

Want to understand cybersecurity evolution + have extended time + diverse group: → Historical Foundation Session

Need current skills with historical perspective + standard time: → Contemporary Legacy Session

Working with senior leadership + strategic focus + enterprise implications: → Business Leadership Session

Advanced technical team + cutting-edge challenges + deep technical focus: → Technical Deep-Dive Session

Expert-dominated group + need collaboration + extended time available: → Historical Foundation Session

5.7.2 Preparation Time Investment

- **Standard Contemporary:** 10 minutes
- **Historical Foundation:** 20 minutes

- **Contemporary Legacy:** 15 minutes
- **Business Leadership:** 15 minutes
- **Technical Deep-Dive:** 20 minutes
- **Problem-Focused:** 15 minutes + specific technique research

5.7.3 Common Session Planning Mistakes

Choosing Historical Foundation for time-constrained groups → Requires minimum 2 hours for effective learning

Using advanced technical scenarios with business-focused groups → Alienates non-technical participants and misses learning goals

Selecting familiar organizational contexts for all sessions → Limits learning about cybersecurity challenges in different industries

Assuming expertise level without group assessment → Results in inappropriate challenge level and poor learning outcomes

Mixing session types without clear transition → Confuses participants and dilutes learning effectiveness

This comprehensive guide ensures you can select and execute the most effective session type for any group while maximizing learning outcomes and participant engagement.

Chapter 6

Malmon System Mastery

6.1 Understanding the Complete Framework

As an Incident Master within our cybersecurity education framework, your mastery of the Malmon system enables you to create rich, educational experiences that teach genuine cybersecurity concepts through engaging gameplay and security awareness training. You don't need to be a malware analysis expert, but you do need to understand how the system works and how to use it effectively for collaborative learning cybersecurity that supports security professional development.

Legacy and Contemporary Threat Education: Your toolkit includes both historical threats that shaped cybersecurity (Code Red 2001, Stuxnet 2010, Ghost RAT 2008, Poison Ivy 2005) and current attacks (GaboonGrabber, LockBit, FakeBat, WannaCry). This range helps teams understand threat evolution - how techniques developed over time, why certain defenses exist, and how past lessons apply to modern challenges.

6.1.1 The Type System in Practice

6.1.1.1 Core Type Relationships

Trojan Types:

- **Strengths:** Deception, social engineering, appearing legitimate
- **Weaknesses:** Behavioral analysis, user education, runtime monitoring
- **Learning Focus:** Social engineering awareness, detection techniques
- **IM Application:** Emphasize human factors and user training

Worm Types:

- **Strengths:** Network propagation, automatic spreading, speed

- **Weaknesses:** Network segmentation, patch management, traffic monitoring
- **Learning Focus:** Network security, vulnerability management
- **IM Application:** Emphasize infrastructure protection and rapid response

Ransomware Types:

- **Strengths:** Business disruption, encryption, payment pressure
- **Weaknesses:** Backup systems, business continuity, network isolation
- **Learning Focus:** Business impact, recovery planning
- **IM Application:** Emphasize organizational resilience and stakeholder management

Rootkit Types:

- **Strengths:** Stealth, system-level access, persistence
- **Weaknesses:** Forensic analysis, integrity checking, advanced detection
- **Learning Focus:** Advanced threats, forensic techniques
- **IM Application:** Emphasize sophisticated detection and investigation

APT Types:

- **Strengths:** Patience, sophistication, strategic objectives
- **Weaknesses:** Threat intelligence, behavioral analysis, long-term monitoring
- **Learning Focus:** Strategic threats, attribution, intelligence
- **IM Application:** Emphasize strategic thinking and advanced coordination

Infostealer Types:

- **Strengths:** Data collection, credential harvesting, stealth
- **Weaknesses:** Encryption, access controls, data loss prevention
- **Learning Focus:** Data protection, access management
- **IM Application:** Emphasize data security and privacy protection

6.1.1.2 Type Effectiveness Reference for IMs

Use this comprehensive chart to understand security control effectiveness and guide team discussions:

6.1.1.3 Using Type Effectiveness for Learning

Super Effective Relationships (+3 Bonus): When teams use approaches that directly counter a Malmon's primary strengths:

- **Behavioral analysis vs. Trojans:** Teaches importance of runtime monitoring
- **Network isolation vs. Worms:** Demonstrates network segmentation value

- **Backup systems vs. Ransomware:** Shows business continuity importance

Not Effective Relationships (-2 Penalty): When teams use approaches that don't address the Malmon's characteristics:

- **Signature detection vs. Zero-day APTs:** Teaches limitations of known-bad approaches
- **Network controls vs. USB Worms:** Shows importance of physical security
- **Antivirus vs. Living-off-the-land techniques:** Demonstrates behavioral analysis needs

IM Facilitation Strategy: Use type effectiveness to guide learning without lecturing:

- *"How well do you think that approach would work against this type of threat?"*
- *"What might make this particular threat resistant to that strategy?"*
- *"Based on what we know about this Malmon's characteristics, what approaches might be most effective?"*

6.1.2 Evolution Mechanics for Learning

6.1.2.1 Understanding Evolution Triggers

Time Pressure Evolution:

- **Trigger:** Teams take too long to identify or respond
- **Learning Goal:** Emphasizes importance of rapid incident response
- **IM Application:** Use time pressure to create urgency and decision-making practice

Failed Containment Evolution:

- **Trigger:** Teams use ineffective approaches against Malmon type
- **Learning Goal:** Teaches importance of matching strategy to threat characteristics
- **IM Application:** Let teams experience consequences of mismatched responses

Environmental Evolution:

- **Trigger:** Organizational vulnerabilities enable threat advancement
- **Learning Goal:** Shows how security posture affects incident outcomes
- **IM Application:** Connect organizational preparedness to incident success

6.1.2.2 Managing Evolution During Sessions

Evolution as Learning Tool: When Malmons evolve, use it as a teaching moment:

- *"Your initial approach didn't account for this threat's [characteristic] - how does that change your strategy?"*
- *"What would have prevented this evolution?"*
- *"How do you adapt when threats become more sophisticated during response?"*

Preventing Unwanted Evolution: When teams are learning well but struggling with complexity:

- Adjust dice modifiers to reflect good collaboration
- Allow type effectiveness bonuses for creative approaches
- Focus on learning objectives over strict mechanical adherence

Evolution Recovery: When evolution creates too much complexity:

- *"Let's focus on the most critical aspect of this evolved threat"*
- *"What's your priority now that the situation has become more complex?"*
- *"How do you manage when incidents escalate beyond initial expectations?"*

6.1.3 Malmon Selection for Different Learning Goals

6.1.3.1 For Fundamental Concepts (New Teams)

GaboonGrabber (Trojan/Stealth):

- **Learning Goals:** Basic incident response, social engineering awareness, team coordination
- **Why It Works:** Clear type characteristics, straightforward investigation path, multiple role contributions
- **IM Focus:** Emphasize collaboration, basic cybersecurity concepts, role specialization

Code Red (Worm):

- **Learning Goals:** Network security basics, vulnerability management, rapid response
- **Why It Works:** Simple propagation mechanism, clear containment strategies, historical context
- **IM Focus:** Network concepts, patch management, infrastructure protection

6.1.3.2 For Intermediate Concepts (Experienced Teams)

WannaCry (Worm/Ransomware):

- **Learning Goals:** Complex threats, business impact, global coordination

- **Why It Works:** Multiple threat vectors, significant real-world impact, policy implications
- **IM Focus:** Multi-vector response, business continuity, international cooperation

Raspberry Robin (Worm/APT):

- **Learning Goals:** Physical/digital convergence, living-off-the-land techniques, policy effectiveness
- **Why It Works:** USB propagation teaches physical security, legitimate tool abuse shows detection challenges
- **IM Focus:** Physical security integration, behavioral analysis, user education

6.1.3.3 For Advanced Concepts (Expert Teams)

Stuxnet (APT/Rootkit Legendary):

- **Learning Goals:** Nation-state threats, attribution, strategic implications
- **Why It Works:** Sophisticated technical and political elements, attribution challenges, policy implications
- **IM Focus:** Strategic thinking, attribution analysis, policy coordination

LockBit (Ransomware/Criminal):

- **Learning Goals:** Criminal organizations, ransomware-as-a-service, law enforcement coordination
- **Why It Works:** Modern threat landscape, business model analysis, international cooperation
- **IM Focus:** Criminal threat analysis, business impact, law enforcement integration

6.1.4 Regional Variants and Customization

6.1.4.1 Industry-Specific Adaptations

Healthcare Variants:

- **Focus:** Patient safety, HIPAA compliance, clinical system integration
- **Modifications:** Add patient care continuity pressures, regulatory notification requirements
- **Learning Goals:** Healthcare-specific risk assessment, compliance coordination

Financial Variants:

- **Focus:** Transaction processing, PCI-DSS compliance, market stability
- **Modifications:** Include trading system impacts, regulatory reporting, customer notification
- **Learning Goals:** Financial sector risk management, regulatory coordination

Critical Infrastructure Variants:

- **Focus:** Physical world impact, safety systems, national security
- **Modifications:** Add SCADA/ICS elements, safety considerations, government coordination
- **Learning Goals:** Infrastructure protection, public safety, strategic threats

6.1.4.2 Geographic Adaptations

Regulatory Environment Customization:

- **GDPR Regions:** Add data protection authority notification, individual rights considerations
- **Different Legal Systems:** Modify law enforcement coordination, legal evidence requirements
- **Cultural Considerations:** Adapt communication styles, authority relationships, social factors

6.1.5 Advanced Malmon Mechanics

6.1.5.1 Hybrid Types and Complex Interactions

Multi-Type Malmons: Some Malmons combine characteristics from multiple types:

- **WannaCry (Worm/Ransomware):** Network propagation + data encryption
- **Stuxnet (APT/Rootkit):** Strategic patience + deep system access
- **Raspberry Robin (Worm/APT):** Physical propagation + sophisticated persistence

IM Application:

- Teach teams to recognize multiple threat characteristics
- Guide development of multi-faceted response strategies
- Emphasize complexity of real-world threats

6.1.5.2 Legendary Malmons

Special Characteristics:

- **Unprecedented capabilities:** Multiple zero-days, novel techniques
- **Historical significance:** Changed cybersecurity practices and policies
- **Strategic implications:** Nation-state operations, infrastructure impacts
- **Attribution complexity:** Advanced investigation and intelligence requirements

Facilitation Approach:

- Reserve for expert teams ready for strategic-level thinking

- Emphasize historical context and lessons learned
- Include policy and strategic response discussions
- Connect to current threat landscape and future implications

6.1.6 Building Scenario Complexity

6.1.6.1 Layered Threat Introduction

Basic Scenario Structure:

1. **Single Malmon:** Focus on core concepts and team coordination
2. **Evolution Challenge:** Add complexity through threat advancement
3. **Multi-Vector:** Introduce related threats or coordinated campaigns
4. **Strategic Context:** Include attribution, policy, and long-term implications

Progressive Complexity Management:

- Start simple and add complexity based on team capability
- Use evolution mechanics to introduce new challenges gradually
- Allow teams to master basic concepts before adding advanced elements
- Maintain focus on learning objectives over mechanical complexity

6.1.6.2 Environmental Factors

Organizational Maturity Levels:

- **Basic:** Limited security tools, minimal incident response capability
- **Intermediate:** Standard security controls, established IR processes
- **Advanced:** Sophisticated security operations, threat hunting capabilities
- **Expert:** Strategic threat intelligence, advanced coordination capabilities

Resource Constraints:

- **Limited Budget:** Emphasize cost-effective approaches and prioritization
- **Small Team:** Focus on coordination and external resource utilization
- **Time Pressure:** Practice rapid decision-making and communication
- **Limited Expertise:** Emphasize collaboration and knowledge sharing

6.1.7 Malmon Creation and Customization

6.1.7.1 Adapting Existing Malmons

Difficulty Adjustment:

- **Simplify for New Teams:** Reduce evolution complexity, provide more guidance
- **Enhance for Experts:** Add attribution elements, policy implications, strategic context
- **Industry Customization:** Modify technical details and business impact for specific sectors

- **Regional Adaptation:** Adjust regulatory and cultural elements for different contexts

Learning Objective Alignment:

- **Communication Focus:** Choose Malmons that require significant stakeholder coordination
- **Technical Focus:** Select threats that emphasize specific technical skills
- **Strategic Focus:** Use Malmons with policy, attribution, or long-term implications
- **Crisis Management:** Pick scenarios that test coordination and resource allocation

6.1.7.2 Community Contribution

Documenting New Variants:

- **Technical Accuracy:** Base on real malware analysis and threat intelligence
- **Educational Value:** Ensure clear learning objectives and type relationships
- **Facilitation Guidance:** Include IM notes, question prompts, and common challenges
- **Community Review:** Validate with other IMs and subject matter experts

Sharing Innovations:

- **Novel Techniques:** Document new facilitation approaches and question strategies
- **Successful Adaptations:** Share industry or regional customizations that work well
- **Challenge Solutions:** Contribute solutions to common facilitation difficulties
- **Assessment Methods:** Share evaluation techniques and learning measurement approaches

6.1.8 Assessment and Continuous Improvement

6.1.8.1 Evaluating Malmon Effectiveness

Learning Outcome Measures:

- **Concept Understanding:** Do participants grasp key cybersecurity concepts?
- **Collaboration Quality:** How well do teams coordinate and share knowledge?
- **Real-World Application:** Can participants connect learning to their work context?

- **Engagement Level:** Are participants actively involved and motivated?

Adaptation Indicators:

- **Too Simple:** Teams solve quickly without significant discussion or learning
- **Too Complex:** Teams become overwhelmed and disengage from learning
- **Misaligned:** Scenario doesn't match group's learning needs or experience level
- **Technical Mismatch:** Malmon characteristics don't fit organizational context

6.1.8.2 Iterative Improvement Process

Session Reflection:

- **What worked well:** Which Malmon characteristics created good learning opportunities?
- **What was challenging:** Where did complexity interfere with learning objectives?
- **Participant Feedback:** What aspects were most and least valuable for learning?
- **Facilitation Insights:** What questions and techniques were most effective?

Community Learning:

- **Share Experiences:** Contribute insights to community knowledge base
- **Learn from Others:** Adopt successful techniques and adaptations from other IMs
- **Collaborative Development:** Work with other IMs to improve Malmon designs
- **Research Integration:** Incorporate findings from educational research and assessment

The Malmon system provides a flexible, scalable framework for cybersecurity education. Your mastery of this system enables you to create powerful learning experiences that adapt to your participants' needs while maintaining educational rigor and real-world relevance.

Chapter 7

Role-Based Team Facilitation for Gamified Incident Response Training

7.1 The Power of Role-Based Collaboration

Managing a six-role *Malware & Monsters* team requires understanding both the unique contributions each role brings and how to orchestrate their collaboration for maximum learning impact. Your job as Incident Master is to ensure every role has meaningful opportunities to contribute while maintaining productive team dynamics.

7.1.1 Understanding Role Dynamics

7.1.1.1 Role Specialization Benefits

Why Roles Matter:

- **Focused Expertise:** Each role approaches problems from a distinct perspective
- **Comprehensive Coverage:** Six roles ensure all aspects of incident response are addressed
- **Natural Division of Labor:** Teams self-organize around role-based responsibilities
- **Learning Amplification:** Different perspectives create richer understanding

Avoiding Role Rigidity:

- Roles are lenses for contribution, not rigid job descriptions

- Encourage cross-role collaboration and knowledge sharing
- Allow expertise to transcend role boundaries when appropriate
- Focus on team success rather than individual role performance

7.1.1.2 Team Composition Strategies

For 4-Player Teams: Essential Core:

- Detective (investigation and analysis)
- Protector (containment and security)
- Tracker (monitoring and data flow)
- Communicator (coordination and stakeholder management)

Optional Additions:

- Add Crisis Manager for complex coordination scenarios
- Add Threat Hunter for advanced threat analysis

For 5-Player Teams: Recommended Configuration:

- Core four roles plus Crisis Manager for coordination-heavy scenarios
- Core four roles plus Threat Hunter for technically complex threats
- Allow team to choose based on interests and scenario requirements

For 6-Player Teams: Full Role Coverage: All six roles provide maximum perspective diversity and learning opportunities

7.1.2 Role Modifier System

7.1.2.1 Understanding Player Role Modifiers

Each incident response role provides specific mechanical modifiers - or bonuses - that players can apply to relevant actions during sessions. These modifiers reinforce role identity while providing concrete gameplay benefits for specialization.

Detective Modifiers:

Understanding Detective Modifiers in Practice:

+3 Forensic Analysis represents the Detective's mastery of digital evidence examination. When a Detective player attempts forensic analysis, this substantial bonus reflects their ability to efficiently parse complex log files, correlate timestamps across multiple systems, and extract meaningful intelligence from technical artifacts. For the IM, this means Detective actions involving evidence analysis should almost always succeed when using appropriate tools and methods. Use this bonus when players examine system logs, analyze malware samples, reconstruct attack timelines, or investigate digital crime scenes. The high bonus acknowledges that forensic analysis is the Detective's core competency.

+2 Pattern Recognition captures the Detective's trained eye for spotting anomalies others miss. This moderate bonus applies when connecting seemingly unrelated events, identifying recurring attack signatures, or recognizing

behavioral patterns in system activity. For the IM, grant this bonus when players attempt to link disparate clues, spot unusual network behavior, or identify attack patterns across multiple incidents. This skill helps Detectives excel at seeing the bigger picture and making connections that drive investigations forward.

+1 Documentation reflects the Detective's methodical approach to maintaining investigation records. While less exciting than active analysis, proper documentation is crucial for incident response success. Apply this bonus when players create incident reports, develop indicators of compromise (IoCs), maintain evidence chains, or produce documentation for legal proceedings. For the IM, this bonus ensures that Detective players can reliably produce high-quality documentation that supports team coordination and post-incident analysis.

Protector Modifiers:

Understanding Protector Modifiers in Practice:

+3 Containment Actions represents the Protector's expertise in rapidly stopping threats from spreading. This high bonus reflects their ability to quickly isolate compromised systems, deploy emergency security controls, and implement protective measures under pressure. For the IM, this means Protector actions focused on immediate threat containment should succeed reliably, especially when using established security tools and procedures. Use this bonus when players attempt to quarantine infected systems, block malicious network traffic, disable compromised accounts, or deploy emergency security controls. The substantial bonus acknowledges that containment is the Protector's primary responsibility during active incidents.

+2 Damage Assessment captures the Protector's skill at evaluating the extent of system compromise. This moderate bonus applies when determining how far an attack has spread, assessing data integrity, or understanding the scope of security control failures. For the IM, grant this bonus when players investigate which systems are affected, evaluate the effectiveness of existing security measures, or determine the extent of data exposure. This skill helps Protectors make informed decisions about containment priorities and resource allocation.

+1 Recovery Planning reflects the Protector's methodical approach to system restoration. While containment is urgent, recovery planning requires careful consideration of business continuity and security requirements. Apply this bonus when players develop restoration strategies, validate backup integrity, coordinate system recovery timelines, or design secure rebuild procedures. For the IM, this bonus ensures that Protector players can reliably develop recovery plans that balance security with business needs, supporting the organization's return to normal operations.

Tracker Modifiers:

Understanding Tracker Modifiers in Practice:

+3 Network Analysis represents the Tracker's mastery of network traffic examination and data flow understanding. This substantial bonus reflects their ability to efficiently monitor network communications, map connection relationships between systems, and track how data moves through the organization's infrastructure. For the IM, this means Tracker actions involving network investigation should succeed reliably when using appropriate monitoring tools and techniques. Use this bonus when players analyze network logs, trace connection patterns, monitor data transfers, or investigate lateral movement pathways. The high bonus acknowledges that network analysis is the Tracker's core specialty and primary contribution to incident response.

+2 Behavioral Detection captures the Tracker's skill at recognizing unusual patterns in network activity that might indicate compromise. This moderate bonus applies when identifying anomalous data transfers, detecting unusual communication patterns, or spotting indicators of system compromise through traffic analysis. For the IM, grant this bonus when players attempt to identify suspicious network behavior, detect data exfiltration attempts, spot unusual connection patterns, or recognize signs of lateral movement. This skill helps Trackers excel at finding threats that might otherwise go unnoticed in network traffic.

+1 Communication Monitoring reflects the Tracker's systematic approach to detecting and blocking malicious external communications. This bonus applies to identifying command-and-control channels, mapping threat actor infrastructure, and coordinating network-based countermeasures. Apply this bonus when players work to detect C2 communications, identify external threat infrastructure, coordinate with network security tools to block malicious connections, or develop network-based indicators for threat hunting. For the IM, this bonus ensures that Tracker players can reliably identify and help disrupt external threat actor communications.

Communicator Modifiers:

Understanding Communicator Modifiers in Practice:

+3 Stakeholder Management represents the Communicator's expertise in coordinating with diverse organizational stakeholders during crisis situations. This substantial bonus reflects their ability to effectively brief executive leadership, manage user communications, and serve as liaison between technical teams and business units. For the IM, this means Communicator actions involving stakeholder coordination should succeed reliably, especially when using established communication channels and protocols. Use this bonus when players conduct executive briefings, coordinate with affected user communities, manage vendor relationships during incidents, or facilitate communication between technical and business teams. The high bonus acknowledges that stakeholder management is the Communicator's primary strength and critical for organizational incident response.

+2 Business Impact Assessment captures the Communicator's skill at evalu-

ating the organizational implications of security incidents. This moderate bonus applies when assessing financial impacts, understanding operational disruptions, or prioritizing response activities based on business criticality. For the IM, grant this bonus when players attempt to quantify incident impacts, assess business continuity risks, evaluate regulatory implications, or help prioritize recovery efforts based on business needs. This skill helps Communicators ensure that technical response activities align with organizational priorities and business requirements.

+1 Crisis Communication reflects the Communicator's systematic approach to managing information flow during security incidents. This bonus applies to coordinating external communications, managing regulatory notifications, and ensuring appropriate crisis communication protocols are followed. Apply this bonus when players coordinate with legal teams, manage media relations, handle regulatory reporting requirements, or develop public communications about security incidents. For the IM, this bonus ensures that Communicator players can reliably navigate the complex external communication requirements that accompany significant security incidents.

Crisis Manager Modifiers:

Understanding Crisis Manager Modifiers in Practice:

+3 Team Coordination represents the Crisis Manager's mastery of organizing and directing incident response teams under pressure. This substantial bonus reflects their ability to effectively allocate resources, establish clear priorities across multiple teams, and develop strategic response plans that maximize overall team effectiveness. For the IM, this means Crisis Manager actions involving team organization and strategic planning should succeed reliably, especially when coordinating complex multi-team responses. Use this bonus when players coordinate team assignments, establish incident response priorities, allocate resources across competing needs, or develop comprehensive response strategies. The high bonus acknowledges that team coordination is the Crisis Manager's primary responsibility and most critical contribution to incident response success.

+2 Multi-track Management captures the Crisis Manager's skill at handling parallel response efforts and managing complex interdependencies. This moderate bonus applies when coordinating simultaneous response activities, managing dependencies between different workstreams, or ensuring comprehensive coverage of all incident aspects. For the IM, grant this bonus when players attempt to coordinate parallel investigation and containment efforts, manage dependencies between different response activities, ensure comprehensive incident coverage, or balance competing response priorities. This skill helps Crisis Managers excel at maintaining oversight of complex, multi-faceted incident responses.

+1 Timeline Management reflects the Crisis Manager's systematic approach to balancing speed and quality in incident response. This bonus applies to establishing realistic response timelines, coordinating time-sensitive activities, and

optimizing the balance between urgency and thoroughness. Apply this bonus when players work to establish incident response timelines, coordinate time-critical response activities, balance immediate needs with long-term recovery, or ensure response activities are completed within business requirements. For the IM, this bonus ensures that Crisis Manager players can reliably develop and maintain response timelines that meet both technical and business needs.

Threat Hunter Modifiers:

Understanding Threat Hunter Modifiers in Practice:

+3 Proactive Investigation represents the Threat Hunter's mastery of hypothesis-driven threat discovery and advanced persistent threat detection. This substantial bonus reflects their ability to hunt for hidden threats using systematic analysis, search for indicators of sophisticated attacks, and uncover malicious activities that standard security tools miss. For the IM, this means Threat Hunter actions involving proactive threat discovery should succeed reliably, especially when using advanced hunting techniques and tools. Use this bonus when players conduct hypothesis-driven hunting, search for advanced persistent threats, investigate potential threat actor presence, or look for hidden indicators of compromise. The high bonus acknowledges that proactive investigation is the Threat Hunter's unique strength and primary contribution to comprehensive incident response.

+2 Advanced Technique Recognition captures the Threat Hunter's skill at identifying sophisticated attack methods and understanding complex adversary tradecraft. This moderate bonus applies when recognizing advanced attack techniques, understanding sophisticated threat actor tactics, or identifying indicators of state-sponsored or advanced criminal activity. For the IM, grant this bonus when players attempt to identify advanced attack techniques, recognize sophisticated threat actor tradecraft, understand complex attack chains, or assess the sophistication level of observed threats. This skill helps Threat Hunters excel at understanding the most challenging and sophisticated threats facing the organization.

+1 Intelligence Development reflects the Threat Hunter's systematic approach to creating actionable threat intelligence from incident artifacts and attack patterns. This bonus applies to developing hunting hypotheses, creating threat intelligence products, and producing intelligence that improves organizational defenses. Apply this bonus when players work to develop threat intelligence from incident findings, create hunting hypotheses for future investigations, produce threat assessments, or develop indicators and signatures for improved detection. For the IM, this bonus ensures that Threat Hunter players can reliably transform their investigations into actionable intelligence that strengthens the organization's security posture.

7.1.2.2 Facilitating Role Modifiers

When to Apply Bonuses:

- Player actions clearly align with role specialization
- Demonstrates relevant real-world knowledge or experience

- Coordinates effectively with teammates using role expertise
- Approaches problems from role-appropriate perspective

How to Communicate Bonuses:

Instead of: *"Roll a d20"* Try: *"As the Detective, you get +3 for forensic analysis. Roll a d20 and add 3."*

Instead of: *"That's a 15, you succeed"*
Try: *"With your Tracker bonus for network analysis, that 12 becomes a 15. You successfully identify the C2 traffic."*

Encouraging Role Identity:

- Verbally acknowledge when players demonstrate role expertise
- Ask role-specific questions that leverage bonuses: *"Tracker, what network patterns concern you most?"*
- Create situations where each role's bonuses provide clear advantages
- Celebrate successful collaboration that combines multiple role bonuses

7.1.2.3 Team Bonus Synergies

Direct Support (+2 additional): When one player's action directly enables another's specialization:

- Detective provides forensic evidence → Protector configures targeted security controls
- Tracker identifies data flows → Threat Hunter investigates hidden connections
- Crisis Manager coordinates timeline → All roles benefit from clear priorities

Team Coordination (+3 additional): When multiple players coordinate using their role bonuses:

- Detective + Tracker collaborate on comprehensive attack timeline
- Protector + Crisis Manager coordinate systematic containment strategy
- Communicator + all roles manage complex stakeholder response

Perfect Teamwork (Automatic Success): When entire team demonstrates role coordination:

- Each role contributes unique perspective using appropriate bonuses
- Actions build logically using role specializations
- Real-world expertise drives decision-making through role lenses

7.1.2.4 Common Modifier Mistakes to Avoid

Over-Restriction:

- Don't prevent players from taking actions outside their role
- Allow expertise to transcend role boundaries when appropriate
- Focus on bonus enhancement, not action limitation

Under-Recognition:

- Don't forget to apply bonuses when players demonstrate role expertise
- Acknowledge role contributions even for failed rolls
- Use bonuses to reinforce successful role-playing

Inconsistent Application:

- Apply bonuses consistently across all roles and players
- Document which bonuses you've used to maintain fairness
- Adjust difficulty considering team's cumulative bonus potential

7.1.2.5 Role Reference Cards for Incident Masters

Use these quick reference cards during gameplay to understand each role's focus areas and provide appropriate challenges and opportunities.

7.1.3 Roll Difficulty Framework

7.1.3.1 Understanding When to Call for Rolls vs. Automatic Success

As an Incident Master, one of your most important decisions is when to require dice rolls versus granting automatic success. This framework helps you make consistent, fair decisions that maintain engagement while rewarding knowledge and collaboration.

7.1.3.2 Difficulty Levels and Target Numbers

7.1.3.2.1 Easy Tasks (Target: 8+)

Success Rate: ~85% - builds confidence and momentum
When to Use: Standard procedures with appropriate tools and expertise

Specific Examples:

- Detective analyzing Windows Event Logs for Process Creation events
- Protector deploying standard antivirus tools on infected systems
- Tracker monitoring network traffic with familiar SIEM tools
- Communicator providing routine incident updates to executive leadership
- Crisis Manager coordinating response activities using established protocols
- Threat Hunter searching for known indicators of compromise

7.1.3.2.2 Medium Tasks (Target: 12+)

Success Rate: ~60% - creates meaningful challenge and uncertainty
When to Use: Complex analysis, coordination requiring expertise, or time pressure situations

Specific Examples:

- Detective reverse-engineering unknown malware samples to understand capabilities
- Protector implementing novel security controls under crisis conditions
- Tracker identifying sophisticated C2 communications using advanced techniques
- Communicator managing crisis communications with multiple external parties
- Crisis Manager coordinating response across multiple business units with conflicting priorities
- Threat Hunter developing custom hunting queries for zero-day threats

7.1.3.2.3 Hard Tasks (Target: 16+)

Success Rate: ~35% - requires exceptional expertise or perfect teamwork
When to Use: Cutting-edge techniques, high-stakes decisions, significant obstacles

Specific Examples:

- Detective developing attribution analysis for state-sponsored attack campaigns
- Protector designing custom containment strategies for novel attack vectors
- Tracker analyzing encrypted or obfuscated command and control infrastructure
- Communicator managing organization-wide crisis with regulatory and media attention
- Crisis Manager coordinating international incident response with law enforcement
- Threat Hunter predicting threat actor next moves based on tactical intelligence

7.1.3.3 Automatic Success Criteria (No Roll Required)

Grant automatic success when players demonstrate:

Clear Role Expertise:

- Actions clearly within role specialization with demonstrated knowledge
- Real-world cybersecurity knowledge and best practices applied appropriately
- Creative approaches that directly address threat-specific vulnerabilities

Effective Team Collaboration:

- Well-coordinated team efforts with logical planning and clear execution steps
- Each role contributing unique perspective that builds on others' work
- Communication and coordination that reflects real incident response practices

Appropriate Tools and Procedures:

- Standard procedures executed with proper tools and clear understanding
- Solutions that demonstrate understanding of threat characteristics
- Approaches that leverage organizational capabilities effectively

7.1.3.4 IM Decision Making Guidelines

Call for Dice Rolls When:

- **Uncertain outcomes:** Player demonstrates knowledge but success depends on external factors
- **Time pressure:** Standard procedures complicated by crisis conditions or tight deadlines
- **Novel situations:** Creative solutions that haven't been tried before in this context
- **High stakes:** Critical decisions where failure has significant consequences
- **Learning opportunities:** Moments where uncertainty creates valuable team discussion

Grant Automatic Success When:

- **Clear expertise:** Player demonstrates specific, relevant cybersecurity knowledge through role lens
- **Appropriate tools:** Standard procedures with proper tools and clear understanding of their use
- **Excellent teamwork:** Well-coordinated efforts that leverage multiple roles' bonuses effectively
- **Type advantage:** Approaches that directly exploit Malmon weaknesses or use role strengths
- **Good planning:** Logical, well-thought-out approaches with clear execution steps

7.1.3.5 Practical Decision Examples

Automatic Success Example: *Player says: "As the Detective, I'll examine the Windows Event Logs for Process Creation events around 10:30 AM when users reported the suspicious behavior, focusing on any processes spawned from unusual parent processes or locations."*

IM Response: *"That's exactly the right approach with the right tools. You find several suspicious PowerShell processes spawned from Word documents -*

automatic success."

Medium Roll Example: *Player says: "I want to try reverse-engineering this malware sample to understand what data it's trying to steal."*

IM Response: *"That's complex analysis under time pressure. Roll d20 and add your Detective bonus for forensic analysis - you need 12 or higher."*

Team Coordination Automatic Success: *Team collaborates: "Detective will analyze the logs while Tracker monitors network traffic, Protector prepares containment measures, and Communicator notifies stakeholders about potential data exposure."*

IM Response: *"Perfect coordination using each role's strengths with clear procedures - automatic success for the whole team."*

7.1.4 Role-Specific Facilitation Techniques

7.1.4.1 Detective (Cyber Sleuth) Facilitation

Encouraging Detective Contributions:

- *"What patterns do you notice that others might miss?"*
- *"How would you piece together the timeline of this attack?"*
- *"What evidence would help confirm or rule out your hypothesis?"*
- *"What questions would a digital forensics investigator ask here?"*

When Detectives Dominate:

- *"That's great analysis, Detective [Name] - how might other roles use this information?"*
- *"Let's hear how this evidence looks from different role perspectives."*
- *"What would the Protector want to know about these findings?"*

When Detectives Withdraw:

- *"We need the Detective's analytical perspective here."*
- *"What patterns or anomalies stand out to you in this scenario?"*
- *"How would you approach investigating this if it happened at your organization?"*

Detective Learning Objectives:

- Pattern recognition and evidence analysis
- Timeline construction and attack progression
- Digital forensics concepts and methodologies
- Connection between evidence and response decisions

7.1.4.2 Protector (Digital Guardian) Facilitation

Encouraging Protector Contributions:

- *"What immediate protective actions would you consider?"*
- *"How would you prevent this attack from causing more damage?"*
- *"What security controls could have prevented this situation?"*
- *"What's your assessment of current system security posture?"*

When Protectors Rush to Action:

- *"That's a good protective instinct - what information would help you choose the best approach?"*
- *"How would you coordinate with other team members before implementing that control?"*
- *"What might go wrong if you acted immediately without more analysis?"*

When Protectors Are Passive:

- *"The systems are under active attack - what's your protective response?"*
- *"How would you limit damage while the investigation continues?"*
- *"What would worry you most about the current security posture?"*

Protector Learning Objectives:

- Containment strategy development and implementation
- Security control selection and deployment
- Risk assessment and damage limitation
- Balance between protection and business continuity

7.1.4.3 Tracker (Data Whisperer) Facilitation

Encouraging Tracker Contributions:

- *"What network activity patterns concern you?"*
- *"How would you trace the data flow in this attack?"*
- *"What monitoring would help you understand the scope of compromise?"*
- *"Where would you look for signs of data exfiltration?"*

When Trackers Get Lost in Technical Details:

- *"That's detailed network analysis - what does it tell us about the attacker's objectives?"*
- *"How would you explain these network patterns to non-technical team members?"*
- *"What decisions does this network intelligence support?"*

When Trackers Can't Contribute:

- *"Even without deep network expertise, what would concern you about data movement?"*
- *"What questions would you ask about how information flows through the organization?"*
- *"How would you determine if sensitive data was at risk?"*

Tracker Learning Objectives:

- Network behavior analysis and anomaly detection
- Data flow understanding and protection strategies
- Communication pattern recognition
- Integration of network intelligence with incident response

7.1.4.4 Communicator (People Whisperer) Facilitation

Encouraging Communicator Contributions:

- *"Who needs to know about this situation and what do they need to know?"*
- *"How would you explain this technical situation to organizational leadership?"*
- *"What stakeholder concerns would you anticipate with this type of incident?"*
- *"How would you coordinate response with different organizational departments?"*

When Communicators Focus Only on External Relations:

- *"How does stakeholder management inform our technical response strategy?"*
- *"What business requirements should guide our containment approach?"*
- *"How would you gather information from users to support the investigation?"*

When Communicators Feel Left Out of Technical Discussion:

- *"The business impact perspective is crucial here - what concerns you most?"*
- *"How would you assess the organizational implications of what we're discovering?"*
- *"What questions would executive leadership ask about this situation?"*

Communicator Learning Objectives:

- Stakeholder management and crisis communication
- Business impact assessment and risk communication
- Coordination between technical and business teams
- Translation of technical concepts for diverse audiences

7.1.4.5 Crisis Manager (Chaos Wrangler) Facilitation

Encouraging Crisis Manager Contributions:

- *"How would you coordinate all these different response activities?"*
- *"What priorities would you set for the team's next actions?"*
- *"How would you allocate resources across these different response needs?"*
- *"What dependencies and constraints affect our response timeline?"*

When Crisis Managers Micromanage:

- *"That's good strategic thinking - how would you empower each role to contribute their expertise?"*
- *"What information do you need from other roles to make coordination decisions?"*
- *"How would you balance centralized coordination with distributed expertise?"*

When Crisis Managers Are Overwhelmed:

- *"Let's break this complex situation into manageable pieces - what are the key priorities?"*
- *"What would help you organize these different response activities?"*
- *"How would you approach coordinating this type of incident in your organization?"*

Crisis Manager Learning Objectives:

- Incident coordination and resource allocation
- Strategic decision-making under pressure
- Team leadership and cross-functional collaboration
- Integration of technical response with business continuity

7.1.4.6 Threat Hunter (Pattern Seeker) Facilitation

Encouraging Threat Hunter Contributions:

- *"What aren't we seeing that might still be hidden in the environment?"*
- *"How would you proactively search for related threats or compromise?"*
- *"What hypotheses would you test about additional attacker activities?"*
- *"What intelligence would help predict the attacker's next moves?"*

When Threat Hunters Go Off on Tangents:

- *"That's interesting threat intelligence - how does it inform our current incident response?"*
- *"What's the most actionable insight from your analysis for our immediate situation?"*
- *"How would you prioritize these different threat possibilities?"*

When Threat Hunters Can't Find Hidden Threats:

- *"What questions would you ask to determine if there are other threats we haven't discovered?"*
- *"How would you validate that we've found all the attacker activities?"*
- *"What would make you confident that the threat has been fully contained?"*

Threat Hunter Learning Objectives:

- Proactive threat discovery and hypothesis testing
- Threat intelligence analysis and application
- Advanced investigation techniques and tools

- Strategic thinking about adversary behavior and motivation

7.1.5 Managing Role Interactions

7.1.5.1 Natural Role Partnerships

Detective + Threat Hunter Synergy:

- **Complementary Analysis:** Detective provides evidence, Threat Hunter develops hypotheses
- **Facilitation Approach:** *"How do the Detective's findings support the Threat Hunter's theory about additional threats?"*
- **Learning Opportunity:** Evidence-based investigation combined with proactive threat discovery

Protector + Crisis Manager Synergy:

- **Implementation Coordination:** Protector provides technical solutions, Crisis Manager coordinates deployment
- **Facilitation Approach:** *"How would you coordinate the Protector's containment strategy across the organization?"*
- **Learning Opportunity:** Technical security controls integrated with strategic incident management

Tracker + Communicator Synergy:

- **Intelligence and Impact:** Tracker provides technical details, Communicator assesses business implications
- **Facilitation Approach:** *"How do the Tracker's network findings affect the Communicator's stakeholder management strategy?"*
- **Learning Opportunity:** Technical network analysis connected to business impact assessment

7.1.5.2 Managing Role Conflicts

When Roles Disagree on Priorities: Common Scenario: Protector wants immediate containment, Detective wants more investigation time

Facilitation Approach:

- *"Both perspectives have merit - what are the trade-offs of each approach?"*
- *"How might we address both the Protector's urgency and the Detective's need for evidence?"*
- *"What would help you decide between immediate action and continued analysis?"*
- *"How would you resolve this tension in a real incident?"*

When Roles Have Overlapping Interests: Common Scenario: Multiple roles want to investigate the same aspect

Facilitation Approach:

- *"Let's leverage different role perspectives on this issue - Detective, focus on evidence; Threat Hunter, look for related threats."*
- *"How would each role approach this investigation differently?"*
- *"What unique insights can each role contribute to understanding this aspect?"*

7.1.5.3 Ensuring Balanced Participation

When Some Roles Dominate: Identification Signs:

- One or two roles providing most responses
- Other team members becoming passive
- Technical discussions excluding business-focused roles

Intervention Strategies:

- *"Let's hear from roles we haven't heard from yet."*
- *"[Quiet Role], what questions would someone in your position ask?"*
- *"How would this situation look from different role perspectives?"*
- *"What would worry each role most about this scenario?"*

When Some Roles Withdraw: Identification Signs:

- Minimal participation from specific roles
- "I don't know enough about this" responses
- Deferring to more technical roles

Intervention Strategies:

- *"Every role brings valuable perspective - what would concern you about this situation?"*
- *"You don't need deep technical knowledge - what does your role's perspective suggest?"*
- *"How would someone in your position typically respond to this type of incident?"*
- *"What questions would you ask if this happened at your organization?"*

7.1.6 Advanced Team Management Techniques

7.1.6.1 Rotating Leadership

Technique: Give different roles team leadership during different phases

Implementation:

- **Discovery Phase:** Detective leads investigation coordination
- **Investigation Phase:** Crisis Manager leads resource allocation and prioritization
- **Response Phase:** Protector leads containment strategy development

Benefits:

- Every role experiences leadership responsibility
- Team appreciates different leadership styles and perspectives
- More comprehensive understanding of incident response coordination

7.1.6.2 Cross-Role Teaching

Technique: Have roles explain their perspective to others

Implementation:

- *"Detective, help the Communicator understand what these technical findings mean for stakeholder messaging."*
- *"Protector, explain to the Crisis Manager what resources you'd need for this containment strategy."*
- *"Tracker, walk the team through what this network analysis tells us about the attack progression."*

Benefits:

- Develops communication and teaching skills
- Builds empathy and understanding between roles
- Creates shared vocabulary and understanding

7.1.6.3 Role Switching

Technique: Temporarily have team members consider other role perspectives

Implementation:

- *"Everyone think like a Communicator for a moment - what would worry you about this situation?"*
- *"If you were the Protector, what immediate actions would you consider?"*
- *"From a Crisis Manager perspective, how would you prioritize these different response activities?"*

Benefits:

- Develops appreciation for different role challenges
- Builds more well-rounded incident response thinking
- Encourages collaborative rather than siloed approaches

7.1.7 Assessment and Learning Objectives

7.1.7.1 Team Effectiveness Indicators

Successful Role Integration:

- All roles contribute meaningfully to investigation and response
- Team leverages different role perspectives to develop comprehensive strategies
- Roles collaborate rather than compete for contribution opportunities

- Team demonstrates understanding of how different cybersecurity functions work together

Communication Quality:

- Roles explain their perspectives clearly to others
- Team builds on each other's contributions rather than working in isolation
- Technical concepts are made accessible to business-focused roles
- Business implications inform technical decision-making

Strategic Thinking:

- Team balances immediate response needs with thorough investigation
- Roles coordinate their activities for maximum effectiveness
- Team considers both technical and business aspects of incident response
- Strategic decisions reflect input from multiple role perspectives

7.1.7.2 Individual Role Development

Role Mastery Indicators:

- Consistent contribution of role-appropriate insights and perspectives
- Ability to explain role's value to other team members
- Development of role-specific skills and knowledge
- Growing confidence in role-based contributions

Cross-Role Understanding:

- Appreciation for other roles' contributions and challenges
- Ability to collaborate effectively with all other roles
- Understanding of how role fits into broader incident response strategy
- Development of communication skills across different expertise areas

Remember: Your goal is not perfect role execution, but collaborative learning that builds understanding of how diverse cybersecurity perspectives work together to create effective incident response. Focus on facilitating meaningful contributions from every role while building appreciation for the value of collaborative cybersecurity work.

Chapter 8

Managing the Progression System

8.1 Understanding Player Development

As an Incident Master, you play a crucial role in recognizing, encouraging, and validating the cybersecurity expertise that participants develop through *Malware & Monsters* sessions. The progression system isn't just about tracking achievements—it's about creating meaningful pathways for professional growth and community contribution.

8.1.1 Recognizing Skill Development

8.1.1.1 During-Session Observation

Detective Skill Indicators:

- **Pattern Recognition:** Connects seemingly unrelated clues into coherent attack narratives
- **Evidence Analysis:** Systematically examines artifacts and draws logical conclusions
- **Timeline Construction:** Builds accurate chronologies of attack progression
- **Question Development:** Asks probing questions that reveal important insights

Protector Skill Indicators:

- **Strategic Containment:** Selects appropriate security controls based on threat characteristics
- **System Thinking:** Understands how security measures affect overall organizational operations

- **Risk Assessment:** Evaluates trade-offs between security and business continuity
- **Implementation Planning:** Develops realistic approaches for deploying security measures

Tracker Skill Indicators:

- **Network Awareness:** Understands data flows and communication patterns
- **Behavioral Analysis:** Recognizes anomalous activities and unusual patterns
- **Monitoring Strategy:** Develops effective approaches for detecting ongoing threats
- **Technical Integration:** Connects network security with broader incident response

Communicator Skill Indicators:

- **Stakeholder Management:** Effectively coordinates with diverse organizational roles
- **Technical Translation:** Explains complex cybersecurity concepts in accessible language
- **Crisis Communication:** Manages information flow during high-stress situations
- **Business Alignment:** Connects technical security decisions to organizational objectives

Crisis Manager Skill Indicators:

- **Strategic Coordination:** Orchestrates complex, multi-faceted response efforts
- **Resource Allocation:** Makes effective decisions about time, personnel, and tool deployment
- **Priority Management:** Balances competing demands and urgent requirements
- **Team Leadership:** Guides collaborative decision-making and maintains team effectiveness

Threat Hunter Skill Indicators:

- **Proactive Investigation:** Seeks out threats before they trigger alerts
- **Hypothesis Development:** Creates and tests theories about threat activity
- **Intelligence Integration:** Uses external information to guide investigation priorities
- **Advanced Analysis:** Discovers sophisticated threats and evasion techniques

8.1.1.2 Growth Trajectory Patterns

Novice to Competent (Sessions 1-5):

- Building confidence in role-specific contributions
- Learning to collaborate effectively with other roles
- Developing basic understanding of cybersecurity concepts
- Starting to ask insightful questions about threats and responses

Competent to Proficient (Sessions 6-15):

- Taking initiative in role-specific investigations
- Helping newer participants understand concepts and techniques
- Contributing unique insights based on growing expertise
- Beginning to see connections between different types of threats and responses

Proficient to Expert (Sessions 16+):

- Leading complex investigations and response coordination
- Mentoring other participants and sharing knowledge effectively
- Contributing to community knowledge through innovative techniques
- Taking on facilitation or community leadership responsibilities

8.1.2 The Badge System Implementation

8.1.2.1 Badge Assessment Criteria

Network Security Badge - "Guardian of Digital Highways"

Evidence Requirements:

- Successfully leads containment of 5+ Worm-type Malmons using network-based approaches
- Demonstrates understanding of network segmentation, traffic analysis, and lateral movement
- Shows ability to coordinate network security with other security domains
- Contributes insights about network architecture and monitoring strategies

Assessment Methods:

- **Direct Observation:** IM notes network-focused contributions during sessions
- **Peer Recognition:** Other participants acknowledge network security leadership
- **Knowledge Demonstration:** Explains network security concepts to less experienced participants
- **Innovation:** Develops or shares novel network security techniques or insights

Documentation:

```
Badge: Network Security
Participant: [Name]
Sessions: [List of relevant sessions]
Evidence:
- Led WannaCry containment using network isolation (Session #12)
- Explained lateral movement concepts to new participants (Session #15)
- Developed network monitoring checklist adopted by local community (Session #18)
Assessment: Demonstrates comprehensive network security understanding and leadership
Awarded: [Date]
Assessor: [IM Name]
```

Human Factors Badge - "Defender Against Social Engineering"

Figure 8.1: Human Factors Badge - Earned State

Evidence Requirements:

- Successfully counters 5+ social engineering or phishing-based attacks
- Develops effective security awareness training programs or materials
- Demonstrates excellent crisis communication during high-stress incidents
- Shows ability to translate technical security concepts for non-technical audiences

Assessment Methods:

- **Communication Excellence:** Consistently manages stakeholder expectations during incidents
- **Training Development:** Creates or improves security awareness materials
- **Social Engineering Defense:** Recognizes and counters human-targeted attacks
- **Crisis Leadership:** Maintains calm, clear communication under pressure

---

Endpoint Security Badge - "Protector of Digital Workstations"

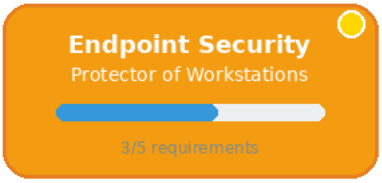

Figure 8.2: Endpoint Security Badge - Progress State

Evidence Requirements:

- Successfully contains 5+ Trojan or Rootkit-type Malmons using host-based approaches
- Masters behavioral analysis and system monitoring techniques
- Leads system recovery and hardening efforts post-incident
- Develops comprehensive endpoint protection strategies

Assessment Methods:

- **Host Analysis:** Demonstrates proficiency with system-level threat detection
- **Malware Analysis:** Shows understanding of endpoint threat behaviors and capabilities
- **Recovery Leadership:** Successfully guides system restoration and hardening
- **Prevention Strategy:** Develops proactive endpoint security measures

---

Data Protection Badge - "Guardian of Digital Assets"

Figure 8.3: Data Protection Badge - Pending State

Evidence Requirements:

- Successfully defends against 5+ Ransomware or Infostealer-type Malmons
- Implements and tests effective backup and recovery strategies
- Demonstrates data loss prevention techniques and controls
- Leads data breach response and notification processes

Assessment Methods:

- **Data Security:** Shows mastery of encryption, classification, and handling procedures
- **Backup Strategy:** Develops and validates comprehensive data protection plans
- **Breach Response:** Manages data incident investigation and compliance requirements
- **Prevention Systems:** Implements effective data loss prevention controls

---

Critical Infrastructure Security Badge - "Protector of Essential Systems"

Figure 8.4: Critical Infrastructure Badge - Progress State

Evidence Requirements:

- Successfully defends against 3+ industrial control system or infrastructure threats
- Understands operational technology (OT) security principles and risks
- Coordinates effective IT/OT security integration efforts
- Develops business continuity and disaster recovery plans

Assessment Methods:

- **OT Security:** Demonstrates understanding of industrial control system protection
- **Integration Leadership:** Successfully bridges IT and operational technology security
- **Continuity Planning:** Develops comprehensive business continuity strategies
- **Critical Systems:** Shows expertise in protecting essential infrastructure

---

Governance and Compliance Badge - "Navigator of Regulatory Requirements"

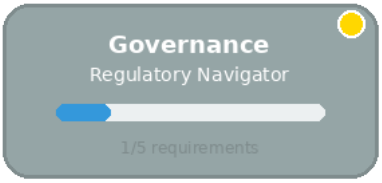

Figure 8.5: Governance Badge - Pending State

Evidence Requirements:

- Successfully manages compliance aspects of 5+ security incidents
- Demonstrates thorough understanding of relevant regulatory frameworks
- Leads compliance reporting and documentation efforts
- Develops risk management and governance programs

Assessment Methods:

- **Regulatory Knowledge:** Shows mastery of applicable compliance frameworks (GDPR, HIPAA, SOX, etc.)
- **Risk Management:** Develops comprehensive risk assessment and management strategies

- **Documentation Excellence:** Creates thorough incident reports and compliance documentation
- **Governance Leadership:** Builds effective security governance and policy programs

8.1.2.2 Badge States and Visual Reference

Each badge has three visual states that IMs should recognize:

- **EARNED (Green):** Player has completed all requirements and demonstrated sustained competency
- **PROGRESS (Yellow):** Player is actively working toward requirements with documented evidence
- **PENDING (Gray):** Badge not yet pursued or early-stage interest indicated

8.1.2.3 Cross-Role Badge Development

Advanced Badges Requiring Multiple Role Experience:

Crisis Leadership Badge:

- Must demonstrate competence in at least 3 different roles
- Successfully coordinates response to level threats
- Shows ability to adapt leadership style to different team compositions

- Mentors other participants in role development and team coordination

Community Educator Badge:

- Effectively teaches cybersecurity concepts to participants with diverse backgrounds
- Develops or adapts scenarios for specific learning objectives
- Contributes to community knowledge through documentation or presentation
- Demonstrates ability to connect game mechanics to real-world applications

8.1.2.4 Badge Validation Process

Community-Based Assessment:

- **Self-Assessment:** Participants reflect on their growth and contributions
- **Peer Feedback:** Other participants provide input on observed skills and contributions
- **IM Evaluation:** Incident Masters assess demonstrated competencies during sessions
- **Portfolio Development:** Participants document their learning journey and contributions

Quality Assurance:

- **Multiple Session Evidence:** Badges require demonstration across multiple sessions and contexts
- **Community Review:** Local communities validate badge awards through peer discussion
- **Continuous Learning:** Badge holders commit to ongoing skill development and community contribution
- **Mentorship Responsibility:** Badge recipients support other participants' learning and development

8.1.3 Elite Specialization Tracks

8.1.3.1 APT Specialist Development

Prerequisites:

- Network Security, Endpoint Security, and Data Protection badges
- Demonstrated experience with level threat scenarios
- Active contribution to threat intelligence and attribution discussions
- Mentorship of other participants in advanced threat analysis

Development Pathway:

- **Advanced Threat Analysis:** Lead investigation of nation-state level threats
- **Attribution Methodology:** Develop expertise in connecting threats to specific actors

- **Intelligence Integration:** Use external threat intelligence to guide response strategies
- **Strategic Assessment:** Understand geopolitical and strategic implications of advanced threats

Assessment Criteria:

- Successfully leads response to 3+ APT-level scenarios
- Demonstrates understanding of advanced threat actor tactics and motivations
- Contributes original analysis or insights about sophisticated threat campaigns
- Shows ability to coordinate response across organizational and national boundaries

8.1.3.2 Global Incident Commander Track

Prerequisites:

- Crisis Manager experience with complex, multi-stakeholder scenarios
- Demonstrated leadership in cross-organizational coordination exercises
- Experience with regulatory, legal, and policy aspects of major incidents
- Strong communication and diplomatic skills for international cooperation

Development Opportunities:

- **Multi-Organization Scenarios:** Lead response efforts involving multiple organizations
- **Regulatory Coordination:** Navigate complex compliance and reporting requirements
- **Media Management:** Handle public communication during high-profile incidents
- **International Cooperation:** Coordinate with government agencies and international partners

8.1.4 Supporting Individual Development Plans

8.1.4.1 Assessment and Goal Setting

Quarterly Development Reviews:

- **Self-Reflection:** What cybersecurity areas interest you most?
- **Skill Assessment:** Where do you feel confident, and where do you want to grow?
- **Goal Setting:** What specific capabilities do you want to develop?
- **Community Contribution:** How do you want to help other participants learn?

Individual Development Planning:

```
Participant: [Name]
Current Role Focus: [Primary role, secondary interests]
Experience Level: [Novice/Competent/Proficient/Expert]

Skill Development Goals:

- Technical: [Specific cybersecurity knowledge areas]
- Collaboration: [Team coordination and communication objectives]
- Leadership: [Mentorship and community contribution goals]

Badge Progression Plan:

- Next Badge Target: [Specific badge and timeline]
- Evidence Requirements: [What needs to be demonstrated]
- Learning Activities: [Sessions, mentorship, community contribution]

Community Involvement:

- Mentorship: [Who you're learning from, who you're helping]
- Contributions: [How you're adding to community knowledge]
- Leadership: [What community responsibilities you're taking on]
```

8.1.4.2 Mentorship and Peer Learning

Facilitating Mentor Relationships:

- **Expert-Novice Pairing:** Connect experienced participants with newcomers
- **Cross-Role Learning:** Encourage participants to explore different role perspectives
- **Community Introductions:** Help participants connect with others who share their interests
- **Recognition Opportunities:** Highlight when participants help others learn effectively

Community Learning Opportunities:

- **Practice Sessions:** Additional opportunities to practice skills between formal sessions
- **Knowledge Sharing:** Informal discussions about real-world cybersecurity experiences
- **Innovation Labs:** Groups focused on developing new techniques or approaches

8.1.5 Organizational Integration

8.1.5.1 Connecting Progression to Professional Development

Performance Review Integration:

- **Skill Documentation:** How progression demonstrates cybersecurity competency development
- **Leadership Evidence:** Examples of mentorship, teaching, and community contribution
- **Innovation Contribution:** Novel techniques or insights developed through participation
- **Professional Network:** Relationships built through community participation

Career Advancement Support:

- **Portfolio Development:** Documenting cybersecurity learning and achievement
- **Reference Networks:** Connections with other cybersecurity professionals
- **Conference Opportunities:** Speaking about collaborative learning experiences
- **Certification Connections:** How progression supports formal cybersecurity certification

8.1.5.2 Team Capability Assessment

Organizational Skill Mapping:

- **Role Coverage:** What incident response capabilities exist within the organization
- **Experience Distribution:** How cybersecurity expertise is distributed across the team
- **Development Priorities:** What skills would most benefit organizational security
- **Succession Planning:** Who can take on additional responsibilities as they develop

Training Integration:

- **Skill Gap Analysis:** What capabilities are missing or need strengthening
- **Development Planning:** How Malware & Monsters supports broader training objectives
- **Budget Justification:** Return on investment for collaborative learning programs
- **Vendor Coordination:** How community learning complements commercial training

Remember: The progression system serves learning, not the other way around.

Focus on recognizing and supporting genuine skill development and community contribution rather than checking boxes or accumulating achievements. The goal is building cybersecurity expertise and community, with progression recognition as a supportive framework for that growth.

Chapter 9

Containment Mechanics

9.1 Facilitating Strategic Response Decisions

The containment phase of *Malware & Monsters* sessions transforms theoretical cybersecurity knowledge into practical decision-making skills. As an Incident Master, your role is to guide teams through the complex process of selecting appropriate response strategies while maintaining the educational focus that makes these decisions meaningful learning experiences.

9.1.1 Understanding Type Effectiveness in Practice

9.1.1.1 Beyond Rock-Paper-Scissors

While the type effectiveness system provides structure, avoid presenting it as a simple matching game. Real cybersecurity requires nuanced thinking about context, resources, and organizational constraints.

9.1.1.2 IM Reference: Type Effectiveness Chart

Use this chart to guide discussions about security control effectiveness, but encourage teams to think beyond simple type matching:

Effective Facilitation:

- *"Given that this is a Trojan-type threat, what approaches might be most effective?"*
- *"How does knowing the threat type inform your strategy, but what other factors matter?"*
- *"What would make a typically effective approach fail in this specific situation?"*

Avoid Oversimplification:

- Don't present type effectiveness as automatic success or failure
- Help teams understand why certain approaches work better against specific threats
- Encourage discussion of real-world constraints and complications

9.1.1.3 Guiding Type-Based Thinking

Discovery Questions:

- *"What does knowing this threat type tell us about how to respond?"*
- *"What vulnerabilities would this type of threat typically have?"*
- *"How might this threat try to evade standard containment approaches?"*

Strategic Questions:

- *"How do we match our available resources to this threat's weaknesses?"*
- *"What would happen if our first approach doesn't work?"*
- *"How do we balance speed with thoroughness given this threat type?"*

Learning Questions:

- *"Why would [specific approach] be particularly effective against this type?"*
- *"What would make this threat harder to contain than others?"*
- *"How does understanding threat types improve real-world incident response?"*

9.1.2 Facilitating Security Control Selection

9.1.2.1 Moving Beyond Tool Lists

Help teams think strategically about security controls rather than simply matching tools to threats.

Framework Questions:

- *"What needs to happen to stop this threat from achieving its objectives?"*
- *"How do we address both immediate containment and long-term prevention?"*
- *"What combination of technical and non-technical controls would be most effective?"*

Context Integration:

- *"How do organizational constraints affect your containment options?"*
- *"What would different stakeholders need to know about your containment approach?"*
- *"How do you balance containment speed with business continuity?"*

9.1.2.2 Common Security Controls and Facilitation Approaches

Signature Detection:

- *Strengths:* Effective against known threats, fast implementation
- *IM Questions: "When would signature-based detection be your best first response?"*
- *Learning Focus:* Limitations of signature-based approaches, need for behavioral analysis

Network Isolation:

- *Strengths:* Immediate containment, prevents spread
- *IM Questions: "What are the business implications of isolating these systems?"*
- *Learning Focus:* Balance between containment and operational continuity

Behavioral Analysis:

- *Strengths:* Effective against novel threats, reveals attack patterns
- *IM Questions: "How would you detect malicious behavior without clear signatures?"*
- *Learning Focus:* Advanced detection techniques, human analysis skills

Backup and Recovery:

- *Strengths:* Restores operations, reduces ransomware impact
- *IM Questions: "How do you ensure backups aren't also compromised?"*
- *Learning Focus:* Business continuity planning, backup verification

Threat Intelligence:

- *Strengths:* Provides context, enables proactive defense
- *IM Questions: "How would external intelligence change your response strategy?"*
- *Learning Focus:* Intelligence integration, attribution and context

9.1.3 Managing Collaborative Decision-Making

9.1.3.1 Encouraging Team Coordination

Role Integration Questions:

- *"How does each role's perspective inform the containment strategy?"*
- *"What would [specific role] be most concerned about with this approach?"*
- *"How do we ensure all expertise is represented in our decision?"*

Resource Allocation:

- *"Who takes the lead on each aspect of the containment effort?"*
- *"How do you coordinate timing between different containment activities?"*
- *"What communication is needed between team members during implementation?"*

Risk Assessment:

- *"What could go wrong with this containment approach?"*

- *"How do you balance aggressive containment with operational stability?"*
- *"What's your backup plan if the primary approach fails?"*

9.1.3.2 Managing Disagreement

When Team Members Propose Different Approaches:

- *"Both strategies have merit—what are the trade-offs?"*
- *"How might we test which approach would work better in this situation?"*
- *"What additional information would help you choose between these options?"*
- *"In what circumstances would each approach be most appropriate?"*

Facilitating Compromise:

- *"How might you combine elements of both approaches?"*
- *"What would a phased implementation look like?"*
- *"How do you address the concerns raised about each option?"*

9.1.4 Using Dice Mechanics Meaningfully

9.1.4.1 When to Roll Dice

- **Uncertain outcomes:** When approach effectiveness depends on factors beyond team control
- **Time pressure:** When teams need to act with incomplete information
- **Environmental factors:** When organizational context affects success likelihood
- **Learning opportunities:** When exploring "what if" scenarios adds educational value

9.1.4.2 When NOT to Roll Dice

- **Clear expertise:** When teams demonstrate solid understanding and appropriate approach
- **Collaborative success:** When team coordination and communication are excellent
- **Learning moments:** When the process is more valuable than the outcome
- **Technical accuracy:** When teams apply correct cybersecurity principles

9.1.4.3 Making Dice Results Educational

Success with High Rolls:

- *"Your containment approach worked well—what made it effective?"*
- *"How would you explain your success to other teams facing similar threats?"*
- *"What did you learn that you can apply to future incidents?"*

Failure with Low Rolls:

- *"The approach was sound, but implementation faced challenges—what would you try next?"*
- *"Real incidents sometimes don't go as planned—how do you adapt when good strategies face obstacles?"*
- *"What would you do differently knowing what you know now?"*

Partial Success:

- *"You made progress but didn't fully contain the threat—how do you build on what worked?"*
- *"What aspects of your approach were most effective, and what needs adjustment?"*
- *"How do you communicate partial success to stakeholders while planning next steps?"*

9.1.5 Network Security Status Three-Track System

The comprehensive Network Security Status tracking system measures incident response success across three critical dimensions, providing realistic feedback that reflects the complexity of actual cybersecurity incidents.

9.1.5.1 Understanding the Three Tracks

Network Security Track (0-100) - **Measures:** Technical security posture and system integrity - **Starts at:** 100 (optimal security state) - **Decreases when:** Malware spreads, vulnerabilities exploited, security controls fail - **Increases when:** Threats contained, vulnerabilities patched, security enhanced

IR Effectiveness Track (0-100) - **Measures:** Team coordination and incident response quality - **Starts at:** 100 (optimal team performance) - **Decreases when:** Poor coordination, investigation stalls, communication breaks down - **Increases when:** Good teamwork, effective investigation, clear communication

Business Operations Track (0-100) - **Measures:** Operational continuity and stakeholder confidence - **Starts at:** 100 (normal business operations) - **Decreases when:** Systems offline, stakeholder panic, regulatory scrutiny - **Increases when:** Service restored, confidence rebuilt, stakeholders informed

9.1.5.2 Track Interactions and Dependencies

The tracks influence each other realistically:

Poor IR Effectiveness impacts Network Security: - Delayed response allows more damage - Miscommunication leads to incomplete containment - *IM Questions: "How is the team's coordination affecting your ability to contain this threat?"*

Network Security problems impact Business Operations: - System outages disrupt operations - Data breaches damage stakeholder confidence - *IM Questions: "How do these technical issues affect business continuity?"*

Business pressure affects IR Effectiveness: - Stakeholder pressure rushes decisions - Resource constraints limit response options - *IM Questions: "How is business pressure influencing your response strategy?"*

9.1.5.3 Practical Track Adjustment Guidelines

Network Security Track Adjustments:

Decrease (-5 to -25): - Malware spreads to additional systems (-10) - Critical vulnerability discovered (-15) - Security control bypassed or fails (-20) - Threat evolves to new stage (-25)

Increase (+5 to +20): - Successful threat containment (+15) - Vulnerabilities patched effectively (+10) - Security controls strengthened (+20) - Complete threat elimination (+25)

IR Effectiveness Track Adjustments:

Decrease (-5 to -20): - Team roles conflict or duplicate effort (-10) - Investigation goes off-track (-15) - Poor communication between roles (-20) - Key information missed or ignored (-25)

Increase (+5 to +20): - Excellent role coordination (+15) - Breakthrough investigation discovery (+20) - Clear, effective communication (+10) - Collaborative problem-solving (+25)

Business Operations Track Adjustments:

Decrease (-5 to -30): - Critical systems go offline (-20) - Stakeholder confidence lost (-15) - Regulatory scrutiny begins (-25) - Public disclosure of incident (-30)

Increase (+5 to +25): - Systems restored to operation (+20) - Stakeholder confidence rebuilt (+15) - Proactive communication success (+10) - Regulatory compliance maintained (+25)

9.1.5.4 Using Tracks for Educational Discussion

When Network Security is low but IR Effectiveness is high: - *"Your team is working well together despite the technical challenges—how does good coordination help in difficult situations?"* - *"What would excellent teamwork accomplish that individual expertise might miss?"*

When Business Operations drops significantly: - *"Stakeholders are feeling the impact—how do you balance technical response with business communication?"* - *"What would help restore confidence while you're still working on the technical problems?"*

When all tracks move together: - *"Notice how your decisions affect multiple aspects of the organization—what does this teach about incident response complexity?"*

9.1.5.5 Track-Specific Facilitation Questions

Network Security Focus: - *"What would improve the technical security posture right now?"* - *"How do you prevent this threat from causing additional damage?"* - *"What technical controls would be most effective here?"*

IR Effectiveness Focus: - *"How is the team working together—what's helping or hindering coordination?"* - *"What communication would improve team effectiveness?"* - *"How are different perspectives contributing to better decision-making?"*

Business Operations Focus: - *"What are the business implications of your technical decisions?"* - *"How do you maintain stakeholder confidence during response activities?"* - *"What would different organizational roles need to know about the current situation?"*

9.1.5.6 Final Track Scores and Success Assessment

Excellent Success (All tracks 80+): - *"Outstanding incident response—what made this team so effective across all dimensions?"* - *"How would you share your approach with other organizations?"*

Mixed Success (Tracks vary significantly): - *"You succeeded in some areas while facing challenges in others—what does this teach about incident response complexity?"* - *"How would you balance competing priorities differently in future incidents?"*

Learning Success (Low scores but good process): - *"This was a challenging scenario that tested your skills—what did you learn that will help in future incidents?"* - *"How does experiencing realistic incident complexity prepare you for actual cybersecurity work?"*

9.1.6 Advanced Containment Scenarios

9.1.6.1 Multi-Vector Threats

When Malmons Combine Types:

- *"How does addressing a worm/ransomware hybrid differ from dealing with each type separately?"*
- *"What containment strategies work against threats with multiple attack vectors?"*
- *"How do you prioritize response when facing complex, multi-faceted attacks?"*

9.1.6.2 Evolution During Containment

When Threats Adapt to Response:

- *"The malware is adapting to your containment efforts—how does this change your strategy?"*
- *"What would cause a threat to evolve during your response, and how do you prevent it?"*
- *"How do you balance thorough containment with speed when threats are actively evolving?"*

9.1.6.3 Resource Constraints

When Perfect Solutions Aren't Available:

- *"Your ideal containment approach isn't possible with current resources—what's your alternative?"*
- *"How do you achieve effective containment when you can't implement your preferred strategy?"*
- *"What creative approaches might work when standard containment methods aren't available?"*

9.1.7 Environmental Factors in Containment

9.1.7.1 Organizational Context

Different Industries, Different Constraints:

- **Healthcare:** *"How does patient safety affect your containment priorities?"*
- **Financial:** *"What regulatory requirements influence your response timeline?"*
- **Manufacturing:** *"How do you balance cybersecurity response with production continuity?"*
- **Education:** *"What unique challenges do BYOD policies create for containment?"*

Organizational Maturity:

- **Advanced Security:** *"How do sophisticated monitoring capabilities change your containment options?"*
- **Basic Security:** *"What containment strategies work when you have limited security infrastructure?"*
- **Hybrid Environments:** *"How do you coordinate containment across cloud and on-premises systems?"*

9.1.7.2 Technical Environment

Network Architecture:

- *"How does your network segmentation affect containment strategy?"*
- *"What containment options do air-gapped systems provide or limit?"*
- *"How do you leverage existing security architecture for containment?"*

Technology Stack:

- *"How do the specific technologies in your environment influence containment approaches?"*
- *"What unique containment challenges do legacy systems create?"*
- *"How do you adapt general containment principles to your specific technology environment?"*

9.1.8 Assessment and Learning Integration

9.1.8.1 Evaluating Containment Effectiveness

Process Assessment:

- *"How well did the team coordinate different containment activities?"*
- *"What communication strategies supported effective containment decision-making?"*
- *"How did role specialization contribute to containment success?"*

Strategic Assessment:

- *"How effectively did the team match containment strategies to threat characteristics?"*
- *"What demonstrated understanding of type effectiveness and environmental factors?"*
- *"How well did the team balance speed, thoroughness, and business continuity?"*

Learning Assessment:

- *"What cybersecurity concepts did the containment phase reinforce or teach?"*
- *"How did hands-on containment decision-making enhance understanding?"*
- *"What insights about real-world incident response emerged from the containment experience?"*

9.1.8.2 Post-Containment Reflection

Strategic Questions:

- *"What made your containment approach effective (or what would you improve)?"*
- *"How did understanding threat types influence your strategy selection?"*
- *"What role did team coordination play in containment success?"*

Learning Questions:

- *"What did this containment experience teach you about cybersecurity defense?"*
- *"How would you explain your containment strategy to others facing similar threats?"*
- *"What insights from this simulation apply to real-world incident response?"*

Application Questions:

- *"How would you adapt this containment approach for your actual work environment?"*
- *"What containment capabilities would you want to develop in your organization?"*
- *"How does this experience change your thinking about cybersecurity preparedness?"*

9.1.9 Building Containment Expertise

9.1.9.1 For New Teams

- Focus on fundamental containment concepts rather than complex technical details
- Emphasize collaborative decision-making and role coordination
- Use automatic successes for good teamwork and logical approaches
- Connect containment decisions to basic cybersecurity principles

9.1.9.2 For Experienced Teams

- Explore sophisticated containment strategies and advanced technical approaches
- Include organizational constraints and business continuity considerations
- Challenge teams with resource limitations and environmental complexities
- Connect containment success to strategic cybersecurity planning

9.1.9.3 For Expert Teams

- Introduce multi-stakeholder coordination and cross-organizational response
- Explore innovation in containment techniques and creative problem-solving
- Include policy and regulatory implications of containment decisions
- Connect containment expertise to community knowledge sharing and mentorship

9.1.10 IM Guide: Containment Success Validation

9.1.10.1 Using the Containment Success Criteria

Teams assess their containment effectiveness using four levels: Complete, Effective, Partial, and Failure. Each level has specific, observable criteria that you

can validate during gameplay.

Your Role as IM:

- **Observe during gameplay:** Note when teams meet specific success criteria
- **Validate objectively:** Use the criteria checklists to provide concrete feedback
- **Focus on learning:** Emphasize improvement and understanding over "winning"
- **Provide examples:** Give specific instances of what teams did well or could improve

9.1.10.2 Validation Guidelines by Success Level

Complete Containment Validation: Look for teams that demonstrate:

- **Technical precision:** Can explain exactly how they stopped malicious activity
- **Comprehensive coverage:** All aspects addressed (persistence, communication, spread, recovery)
- **Role coordination:** Every available role contributed meaningfully
- **Documentation mindset:** Show awareness of lessons learned and intelligence value
- **Stakeholder thinking:** Consider business impact and communication needs

Effective Containment Validation: Teams show:

- **Core competency:** Successfully address primary threats
- **Most roles engaged:** 4+ roles participating effectively
- **Appropriate controls:** Generally correct security control selections
- **Basic coordination:** Good team communication and coordination
- **Recovery focus:** Understand importance of system restoration

Partial Containment Validation: Teams demonstrate:

- **Some success:** Eventually neutralize threat despite challenges
- **Limited coordination:** 2-3 roles working together effectively
- **Mixed decisions:** Some good choices, some suboptimal approaches
- **Learning awareness:** Recognize areas for improvement
- **Basic understanding:** Show grasp of fundamental concepts

Failure as Learning Experience: Frame failures positively:

- **Learning opportunity:** Complex scenarios provide valuable insights
- **Realistic outcomes:** Real incidents sometimes have poor outcomes initially
- **Skill development:** Identify specific areas for team growth
- **Resilience building:** Emphasize iteration and improvement

9.1.10.3 IM Validation Process

During Sessions:

1. **Take notes:** Record specific examples of criteria being met
2. **Don't interrupt:** Allow natural team coordination to develop
3. **Ask clarifying questions:** Help teams articulate their reasoning
4. **Encourage participation:** Ensure all roles have opportunities to contribute

At Session End:

5. **Review criteria together:** Go through the checklist with the team
6. **Provide specific examples:** "You achieved Complete Containment because…"
7. **Identify improvements:** "To reach the next level, consider…"
8. **Connect to learning:** "This experience teaches us…"

9.1.10.4 Sample IM Feedback Scripts

Complete Containment: *"Excellent work! You achieved Complete Containment. Specifically, I observed the Detective identifying all persistence mechanisms, the Protector successfully blocking C2 communications, the Tracker confirming no lateral movement, and the Communicator managing stakeholder notifications effectively. Your team coordination using each role's strengths was particularly impressive."*

Effective Containment: *"Great job achieving Effective Containment. You successfully stopped the threat and restored core systems. The area for growth is intelligence generation - you focused effectively on immediate containment but could develop more threat intelligence for future defense."*

Partial Containment: *"This was a challenging scenario that provided valuable learning. You achieved Partial Containment - the threat was eventually stopped. The key learning opportunity is role coordination. Try having the Crisis Manager actively coordinate between roles rather than working independently."*

Learning from Failure: *"This scenario demonstrated the complexity of real cybersecurity incidents. While the malmon achieved its objectives, your team gained important insights about threat assessment and response prioritization. In actual incidents, these lessons are exactly what make teams more effective over time."*

9.1.10.5 Common IM Validation Mistakes to Avoid

Being Too Generous:

- Don't award higher success levels just to make teams feel good
- Require actual demonstration of criteria, not just discussion
- Use specific examples to justify your assessment

Being Too Harsh:

- Remember that learning is the primary objective
- Celebrate partial successes and improvement
- Focus on constructive feedback rather than criticism

Missing Role Contributions:

- Actively look for ways each role contributed
- Ask quiet players about their perspective
- Ensure all roles have opportunities to demonstrate expertise

Ignoring Process:

- Success isn't just about outcomes - process matters too
- Good teamwork with poor results can still be valuable learning
- Poor teamwork with good results misses collaboration lessons

Remember: Containment mechanics serve learning objectives, not game complexity. The goal is developing strategic thinking about cybersecurity defense, not mastering game rules. Focus on helping teams understand how to match response strategies to threats while considering real-world constraints and organizational objectives.

Chapter 10

Technical Foundation for Incident Masters

10.1 The Right Level of Technical Knowledge

As an Incident Master facilitating cybersecurity education through our security training platform, you need enough technical understanding to ask good questions and recognize when participants are on productive learning paths—but you don't need to be the most technically knowledgeable person in the room. Your participants provide the expertise; you facilitate its sharing through security awareness training methodologies that promote cybersecurity skills development via gamified incident response training experiences.

10.1.1 Essential Cybersecurity Concepts

10.1.1.1 Core Malware Categories

Understanding Without Expertise:

Trojans: Malware disguised as legitimate software

- *Key insight:* Deception is the primary attack vector
- *IM questions: "What made this seem legitimate to users?"*
- *Learning focus:* Social engineering awareness and behavioral detection

Worms: Self-replicating malware that spreads through networks

- *Key insight:* Network propagation without user interaction
- *IM questions: "How might this spread so quickly through our network?"*
- *Learning focus:* Network segmentation and vulnerability management

Ransomware: Malware that encrypts data and demands payment

- *Key insight:* Business disruption through data unavailability
- *IM questions: "What would this mean for business operations?"*
- *Learning focus:* Business continuity and backup strategies

Rootkits: Malware that hides deep in system software

- *Key insight:* Stealth and persistence are primary goals
- *IM questions: "How would you detect something designed to be invisible?"*
- *Learning focus:* Advanced detection and forensic analysis

APTs: Advanced Persistent Threats with sophisticated, long-term objectives

- *Key insight:* Patient, well-resourced attackers with strategic goals
- *IM questions: "What would motivate someone to invest this much effort?"*
- *Learning focus:* Threat intelligence and strategic defense

10.1.1.2 Attack Lifecycle Understanding

Using MITRE ATT&CK as Framework:

Initial Access: How attackers first get into systems

- *IM application: "How might this attack have started?"*
- *Common methods:* Email, web vulnerabilities, removable media

Execution: How malware runs on target systems

- *IM application: "What needed to happen for this malware to activate?"*
- *Key concept:* User interaction vs. automatic execution

Persistence: How threats maintain access through restarts and updates

- *IM application: "How would this survive if we rebooted infected systems?"*
- *Learning opportunity:* System hardening and monitoring

Privilege Escalation: How attackers gain higher-level access

- *IM application: "What would this enable the attacker to do next?"*
- *Security principle:* Least privilege and access controls

Defense Evasion: How threats avoid detection

- *IM application: "Why didn't our security tools catch this?"*
- *Learning focus:* Behavioral analysis and advanced detection

Discovery: How attackers learn about target environments

- *IM application: "What information would be valuable to the attacker?"*
- *Defensive insight:* Network segmentation and monitoring

Lateral Movement: How threats spread through networks

- *IM application: "Where might this go next?"*
- *Prevention strategy:* Network segmentation and access controls

Collection: How attackers gather target data

- *IM application: "What data would be most valuable to steal?"*
- *Protection approach:* Data classification and access monitoring

Exfiltration: How stolen data leaves the organization

- *IM application: "How would we detect data leaving our network?"*
- *Technical control:* Data loss prevention and network monitoring

Impact: How attacks achieve their objectives

- *IM application: "What's the ultimate goal of this attack?"*
- *Business perspective:* Risk assessment and impact analysis

10.1.2 Technical Concepts You Should Understand

10.1.2.1 Network Security Basics

What You Need to Know:

- **Network segmentation:** Dividing networks to limit threat spread
- **Firewalls:** Controlling traffic between network segments
- **Monitoring:** Watching network traffic for unusual patterns
- **Air gaps:** Physical separation of critical systems from networks

How to Use This Knowledge:

- Guide discussions about containment strategies
- Ask questions about network architecture and defense
- Help teams think about lateral movement and propagation
- Connect technical controls to business protection

10.1.2.2 Endpoint Security Fundamentals

What You Need to Know:

- **Antivirus/Anti-malware:** Signature-based detection of known threats
- **Behavioral analysis:** Monitoring for unusual system behavior
- **System integrity:** Ensuring systems haven't been modified maliciously
- **Patch management:** Keeping software updated to fix vulnerabilities

How to Use This Knowledge:

- Guide discussions about detection and prevention
- Ask questions about why security tools might fail
- Help teams understand the limitations of different approaches
- Connect endpoint security to user behavior and training

10.1.2.3 Data Protection Concepts

What You Need to Know:

- **Encryption:** Protecting data so it's unreadable without proper keys
- **Backup systems:** Maintaining copies of important data for recovery
- **Access controls:** Limiting who can access what data
- **Data loss prevention:** Monitoring and controlling data movement

How to Use This Knowledge:

- Guide discussions about ransomware response and data protection
- Ask questions about data value and protection priorities
- Help teams think about recovery and business continuity
- Connect data protection to regulatory and compliance requirements

10.1.3 MITRE ATT&CK as Your Facilitation Framework

10.1.3.1 Using ATT&CK Without Deep Technical Knowledge

As a Question Framework: Instead of needing to know all techniques, use ATT&CK categories to structure your questions:

Initial Access Questions:

- *"How might this attack have started?"*
- *"What would make users vulnerable to this approach?"*
- *"How could we prevent this type of initial compromise?"*

Persistence Questions:

- *"How would this maintain access if we restarted systems?"*
- *"What would we need to do to completely remove this threat?"*
- *"How would we detect if this came back after removal?"*

Defense Evasion Questions:

- *"Why didn't our existing security tools detect this?"*
- *"What would make this difficult to find?"*
- *"How might the attacker try to hide their activities?"*

10.1.3.2 ATT&CK for Session Structure

Discovery Phase: Focus on Initial Access and Execution

- Help teams understand how the attack began
- Guide discussion of attack vectors and user interaction
- Connect to prevention and user education opportunities

Investigation Phase: Explore Persistence, Privilege Escalation, and Discovery

- Guide analysis of how the attack progressed
- Help teams understand the full scope of compromise
- Connect to containment and damage assessment strategies

Response Phase: Address Defense Evasion, Collection, and Impact

- Guide development of response strategies
- Help teams think about preventing future similar attacks
- Connect to business continuity and recovery planning

10.1.4 Handling Technical Knowledge Gaps

10.1.4.1 When You Don't Know the Answer

Redirect to the Group:

- *"That's a great technical question—who here has experience with that?"*
- *"How would someone with [relevant expertise] think about this?"*
- *"What would you do to find out more about that technical detail?"*

Focus on Learning Objectives:

- *"The important thing for our learning is understanding [concept]—how does this technical detail help with that?"*
- *"We're focusing on [learning goal]—how does this connect to that objective?"*

Acknowledge and Move Forward:

- *"I don't know the technical details, but let's think about what this means for our response strategy."*
- *"That's beyond my expertise—what matters for our decision-making is [relevant concept]."*

10.1.4.2 Leveraging Participant Expertise

Expert Identification:

- *"Who here has worked with [relevant technology/situation]?"*
- *"What's your experience been with [relevant concept]?"*
- *"How does this compare to what you've seen in your work?"*

Teaching Moments:

- *"Can you help the rest of us understand how [technical concept] works?"*
- *"What would someone new to this field need to know about [topic]?"*
- *"How would you explain [concept] to a non-technical stakeholder?"*

Collaborative Problem-Solving:

- *"How would you combine [Expert A's] insight with [Expert B's] approach?"*
- *"What questions would you ask to build on what [Name] just shared?"*
- *"How do these different perspectives help us understand the bigger picture?"*

10.1.5 Emergency Technical Protocols

10.1.5.1 When Technical Discussion Goes Too Deep

Refocus on Learning Objectives:

- *"This is great technical detail—how does it inform our team's next steps?"*
- *"What decisions does this technical analysis help us make?"*
- *"How would you explain the importance of this to the rest of the organization?"*

Time Management:

- *"We have [X] minutes left in this phase—what's our priority?"*
- *"Let's capture this insight and think about how it affects our overall approach."*
- *"What's the most important takeaway from this technical discussion?"*

10.1.5.2 When You're Technically Wrong

Acknowledge and Learn:

- *"Thanks for the correction—what does that mean for our scenario?"*
- *"I appreciate you setting that straight—how does the accurate information change our approach?"*
- *"That's why having experts in the room is so valuable—what should we do with this better understanding?"*

Model Learning:

- *"I learned something new—how does this new information affect our thinking?"*
- *"That's a good reminder that I'm here to facilitate, not be the technical expert."*
- *"What other assumptions should we question based on this correction?"*

10.1.6 Building Your Technical Foundation

10.1.6.1 Continuous Learning Approach

Learn from Every Session:

- Pay attention to technical concepts that participants explain
- Note areas where your questions could be more informed
- Ask participants to recommend resources for learning specific topics
- Build your understanding gradually rather than trying to learn everything at once

Focus on Conceptual Understanding:

- Understand the "why" behind security concepts rather than technical implementation details

- Learn how different security domains connect to each other
- Develop intuition about what questions lead to productive learning
- Build knowledge of how technical concepts relate to business objectives

Community Learning:

- Connect with other Incident Masters to share knowledge and experiences
- Participate in cybersecurity communities to stay current with trends
- Attend conferences and training focused on cybersecurity education rather than just technical skills
- Read case studies and incident reports to understand real-world attack patterns

10.1.6.2 Recommended Learning Resources

For Fundamental Concepts:

- NIST Cybersecurity Framework for understanding security functions
- SANS Institute resources for practical cybersecurity knowledge
- Cybersecurity industry reports for understanding current threat landscape
- Case studies of major incidents for learning attack patterns and response strategies

For Attack Understanding:

- MITRE ATT&CK framework documentation and training materials
- Vendor threat intelligence reports for understanding attack trends
- Academic research on cybersecurity incidents and response
- Government publications on cybersecurity best practices

For Facilitation Skills:

- Adult learning theory and educational research
- Facilitation guides and training programs
- Community of practice resources for peer learning
- Feedback and reflection tools for continuous improvement

10.1.7 The Growth Mindset

10.1.7.1 Embracing Your Learning Edge

Technical Growth Through Facilitation:

Every session teaches you something new about cybersecurity. Your role puts you in contact with diverse expertise and perspectives, making you a better-informed facilitator over time.

Teaching Others to Teach:

As you become more comfortable with technical concepts, you can help participants become better at sharing their knowledge with others—a valuable skill in cybersecurity collaboration.

Building Community Expertise:

Your growing technical understanding, combined with your facilitation skills, positions you to contribute to community knowledge and help other Incident Masters develop their capabilities.

Remember: Your technical knowledge serves your facilitation, not the other way around. Stay curious, ask good questions, and trust that the combination of your facilitation skills and your participants' expertise creates powerful security professional development experiences through our innovative incident response tabletop exercise methodology.

Chapter 11

Running Sessions: Thorough Guide

11.1 Session Overview and Timing

A complete Malware & Monsters session follows this structure:

- **Setup Phase**
- **Round 1 (Discovery)**
- **Round 2 (Investigation)**
- **Round 3 (Response)**
- **Closing**

This chapter provides thorough guidance for confident session management.

11.2 The Opening: Foundation for Success

11.2.1 Welcome and Energy Setting

11.2.1.1 Your Opening Script

"Welcome everyone! I'm [Name] and for the next couple of hours, you're going to become an incident response team facing a real cybersecurity crisis. This isn't a lecture - you'll be the experts solving problems together."

"Before we dive into the emergency, let's see what expertise we're working with."

11.2.1.2 Energy Assessment

Quickly read the room:

- **High energy:** Move faster, dive into action
- **Low energy:** Use more icebreaking, build excitement gradually
- **Mixed energy:** Address different levels individually
- **Nervous energy:** Provide reassurance and clear structure

11.2.2 Expertise Discovery and Team Chemistry

11.2.2.1 The Expertise Round

"Let's go around quickly - first name and one thing you know about computers or cybersecurity. This could be work experience, personal projects, something you've read, or just common sense."

Facilitation Notes:

- **Time limit:** 30-45 seconds per person maximum
- **Encourage breadth:** "Technical and non-technical insights are both valuable"
- **Take mental notes:** Who has what expertise for later role assignment
- **Build confidence:** "Great background" or "That's exactly the perspective we need"

Sample Participant Responses and Your Reactions:

- *"I work in IT support"* → *"Perfect - you see problems first-hand"*
- *"I'm curious about cybersecurity"* → *"Curiosity and fresh thinking are incredibly valuable"*
- *"I develop software"* → *"Great - you understand how systems work"*
- *"I handle compliance"* → *"Essential perspective - business impact matters"*

11.2.3 Collaborative Role Assignment

11.2.3.1 Role Assignment Script

"Based on what you've shared, I'll suggest roles for our incident response team. Feel free to speak up if you'd prefer something different:"

Assignment Logic:

- **IT/Technical background** → Detective or Protector
- **Network/Infrastructure** → Tracker
- **Business/Management** → Communicator
- **Security experience** → Crisis Manager
- **Analytical mindset** → Threat Hunter

11.2.3.2 Role Introduction (Brief)

"Let me quickly explain what each role brings to incident response:"

- **Detective:** *"You find clues and analyze evidence"*
- **Protector:** *"You secure systems and stop threats"*

- **Tracker:** *"You follow data flows and monitor networks"*
- **Communicator:** *"You handle stakeholders and coordinate response"*
- **Crisis Manager:** *"You manage the overall incident response"*
- **Threat Hunter:** *"You proactively search for hidden threats"*

Group Confirmation: *"Any adjustments to these assignments?"*

11.2.4 Character Development and Context Setting

11.2.4.1 Character Creation

"Now develop your character around your real name and role. Think about:"

- *"What's your work obsession or quirk?"*
- *"Why do you care about protecting this organization?"*
- *"What would devastate you if it were compromised?"*

Facilitation During Character Creation:

- **Move around the room:** Available for quiet consultation
- **Encourage fun:** *"Lean into the stereotypes - they're based in truth"*
- **Provide prompts:** Use role-specific questions for stuck participants
- **Manage time:** *"One more minute for character development"*

11.2.4.2 In-Character Introductions

This is where the magic happens. Fun and laughs are important to break the ice and get players engaged. So if they don't make it fun themselves during the introduction, try and do ask questions to their role's stereotypes in order to make them and the other players laugh.

"The emergency alarm just went off. You're all rushing to the situation room. Introduce yourselves as your characters - 30 seconds each."

Sample Character Introductions:

- *"I'm Sarah, IT Support. I've been watching logs like Netflix for two years, and something's been bothering me since yesterday."*
- *"Marcus, Systems Admin. These servers are my children, and someone's been messing with them."*

Your Response: Build energy and acknowledge each character

- *"I love the protective instinct, Marcus"*
- *"Sarah, your pattern recognition is exactly what we need"*

11.3 Round 1: Discovery Phase

11.3.1 Phase Setup

11.3.1.1 Crisis Presentation Script

"Here's the situation at [Organization Name]. You've been called in because:"

Present 2-3 clear symptoms:

- *"Multiple users across all locations report computers running 30% slower since yesterday"*
- *"Help desk received 5 calls about unexpected pop-ups appearing"*
- *"One user mentioned receiving a 'critical software update' email yesterday afternoon"*

11.3.1.2 Stakes and Pressure

"Your critical systems are affected. [Specific organizational stakes]. The clock is ticking."

Initial Status Setting:

- *"Network Security Status starts at 100"*
- *"Each of you gets 2 actions this round"*
- *"Your goal: figure out what you're dealing with"*

11.3.2 Individual Investigation

11.3.2.1 Action Facilitation

"Each role investigates from their expertise area. [Role name], what's your first move?"

Detective Actions:

- **Prompt:** *"Sarah, your pattern-recognition instincts are tingling. What do you investigate first?"*
- **Follow-up:** *"What would worry you most in those logs?"*
- **Success guidance:** Help them find evidence that leads to Malmon identification

Protector Actions:

- **Prompt:** *"Marcus, someone's attacking your systems. What's your defensive instinct?"*
- **Follow-up:** *"What would you check to see how they're hiding?"*
- **Success guidance:** Guide toward understanding attack techniques

Tracker Actions:

- **Prompt:** *"Alex, you're seeing unusual trains on your network subway map. What do you track first?"*
- **Follow-up:** *"What would suspicious outbound traffic look like here?"*
- **Success guidance:** Help discover data exfiltration or command & control

Communicator Actions:

- **Prompt:** *"Jamie, you need to understand the human side. Who do you talk to first?"*
- **Follow-up:** *"What questions help you understand how this attack succeeded?"*
- **Success guidance:** Reveal social engineering or user compromise

Crisis Manager Actions:

- **Prompt:** *"Taylor, you're seeing the big picture. What's your first priority?"*
- **Follow-up:** *"How do you coordinate the team's efforts?"*
- **Success guidance:** Help organize team response and resource allocation

Threat Hunter Actions:

- **Prompt:** *"Riley, you're looking for what others missed. Where do you hunt first?"*
- **Follow-up:** *"What signs suggest there's more than meets the eye?"*
- **Success guidance:** Help discover hidden persistence or additional threats

11.3.2.2 Real-Time Facilitation Notes

- **Dice rolls:** Use for uncertain outcomes, not obvious successes
- **Build on expertise:** When players demonstrate real knowledge, auto-succeed
- **Guide toward Malmon:** Help discoveries point to your chosen threat
- **Time management:** *"Two more minutes for individual actions"*
- **Energy monitoring:** If energy drops, inject urgency or stakes

11.3.3 Knowledge Sharing

11.3.3.1 Structured Information Exchange

"Excellent investigation work. Now share your findings - what story do your discoveries tell together?"

Facilitation Sequence:

1. **Detective reports first:** Sets foundation with evidence
2. **Protector adds technical details:** How the attack works
3. **Tracker provides network perspective:** What's happening with data
4. **Communicator explains human factor:** How the attack succeeded

5. **Crisis Manager synthesizes:** Big picture assessment
6. **Threat Hunter reveals hidden elements:** What others missed

11.3.3.2 Pattern Recognition Guidance

Help the group connect dots without providing answers:

- *"Interesting - fake software updates AND process injection. What does that combination suggest?"*
- *"So we have social engineering AND technical evasion. What kind of threat does both?"*
- *"The timing and sophistication level - what does that tell us about our adversary?"*

11.3.3.3 Collaborative Building Techniques

- **Yes, and...** *"Yes, that's exactly right, and what does that mean for…"*
- **Connect expertise:** *"Jamie's social engineering insight connects to what Sarah found in the logs"*
- **Build tension:** *"This is more sophisticated than a random attack"*

11.3.4 Malmon Identification

11.3.4.1 The Revelation Moment

"Based on your investigation, you're dealing with a specific type of threat. Given the evidence - social engineering, process injection, data exfiltration - what kind of Malmon matches this pattern?"

Guide toward correct identification:

- **If they struggle:** *"Think about the combination of deception and technical sophistication"*
- **If they're close:** *"Yes, that's exactly the right family of threats"*
- **If they're off-track:** *"What about the [key evidence] suggests something different?"*

11.3.4.2 Malmon Card Reveal

"Exactly right. Meet your adversary…"

[Reveal Malmon card with dramatic flair]

"This is [Malmon Name], a [Type] that specializes in [primary ability]. You've identified the threat, but it's already been active for [time period]. What's your assessment?"

Network Security Status Update:

- Calculate changes based on group performance
- Announce new status: *"Network Security Status is now [number]"*

- Build urgency: *"The threat is established but not yet evolved"*

11.4 Round 2: Investigation Phase

11.4.1 Phase Transition

11.4.1.1 Escalation Script

"Now that you know what you're facing, you need to understand the full scope of [Malmon Name]'s infiltration. The threat is active and could evolve if not contained quickly."

New Objectives:

- *"Assess the complete impact"*
- *"Understand the attack progression"*
- *"Identify vulnerabilities that enabled success"*
- *"Prepare for potential evolution"*

11.4.2 Impact Assessment

11.4.2.1 Role-Specific Deep Dives

Each role investigates different aspects of the compromise:

Detective: Evidence Analysis
"Sarah, now that you know it's [Malmon Name], what evidence would confirm its full capabilities?"

- Guide toward forensic indicators
- Help discover timeline and progression
- Reveal attack vector details

Protector: Damage Assessment
"Marcus, how many systems are affected and what's been compromised?"

- Guide toward scope of infection
- Help identify vulnerable systems
- Reveal defensive failures

Tracker: Data Flow Analysis
"Alex, what data is being stolen and where is it going?"

- Guide toward exfiltration patterns
- Help identify command & control
- Reveal network compromise

Communicator: Human Factor Analysis
"Jamie, how did this attack succeed and who was targeted?"

- Guide toward social engineering analysis

- Help identify user education gaps
- Reveal organizational vulnerabilities

Crisis Manager: Organizational Impact
"Taylor, what's the business impact and what resources do we need?"

- Guide toward operational assessment
- Help identify recovery requirements
- Reveal stakeholder concerns

Threat Hunter: Hidden Threats
"Riley, what else might be lurking that we haven't found yet?"

- Guide toward additional persistence
- Help identify lateral movement
- Reveal potential additional threats

11.4.3 Attack Vector Analysis

11.4.3.1 Collaborative Mapping

"Let's map how [Malmon Name] got in and spread through our environment."

Facilitation Techniques:

- **Use whiteboard:** Visual mapping of attack progression
- **Build timeline:** When did each phase occur?
- **Identify decision points:** Where could this have been stopped?
- **Connect to type effectiveness:** How does [Malmon Type] exploit weaknesses?

11.4.3.2 Vulnerability Assessment

"What enabled this attack to succeed?"

Guide discussion toward:

- Technical vulnerabilities (unpatched systems, weak configurations)
- Process gaps (inadequate training, poor procedures)
- Human factors (social engineering susceptibility)
- Environmental issues (network segmentation, monitoring gaps)

11.4.4 Evolution Threat

11.4.4.1 The Escalation Moment

"Just as you're getting a handle on the situation, your monitoring tools alert you: [Malmon Name] is attempting to evolve. It's trying to [specific evolution behavior based on Malmon card]."

Critical Decision Point: *"Do you focus on containing what you've found, or continue investigating to understand the complete scope? This decision affects your response options."*

Facilitation Notes:

- Let group debate naturally
- Both choices have consequences
- Their decision affects Round 3 difficulty
- Build tension around time pressure

11.5 Round 3: Response Phase

11.5.1 Phase Transition

11.5.1.1 Action Phase Setup

"Time for coordinated response. Based on your investigation, how does the team counter [Malmon Name]?"

Response Objectives:

- *"Stop ongoing damage"*
- *"Prevent evolution/spread"*
- *"Begin recovery operations"*
- *"Coordinate stakeholder communications"*

11.5.2 Strategy Coordination

11.5.2.1 Team Planning Session

"Plan your coordinated response. Remember [Malmon Name]'s type weaknesses: [specific weaknesses from card]."

Facilitation Focus:

- **Encourage type advantage usage:** *"How can you exploit its weakness to [vulnerability]?"*
- **Coordinate actions:** *"How do your individual actions support each other?"*
- **Address constraints:** *"What real-world limitations affect your response?"*
- **Build on expertise:** *"Given your experience, what would work best?"*

11.5.2.2 Strategy Validation

Help group assess their plan:

- *"What could go wrong with this approach?"*
- *"What would [Malmon Name] do to counter your strategy?"*

- *"How does this plan address all the evidence you found?"*

11.5.3 Implementation

11.5.3.1 Coordinated Action Execution

Each player executes their response strategy:

Action Resolution:

- **Use dice for uncertain outcomes**
- **Apply type effectiveness bonuses/penalties**
- **Reward creative solutions**
- **Build on collaborative efforts**

11.5.3.2 Malmon Counter-Actions

"[Malmon Name] fights back using [specific abilities from card]."

- Use Malmon's abilities to create challenges
- Don't make it impossible, make it interesting
- Reward good strategy and teamwork
- Build dramatic tension

11.5.3.3 Real-Time Network Security Status Updates

Track and announce changes:

- *"Good coordination - Network Security Status improves to [number]"*
- *"The attack is being contained but [complication]"*
- *"Excellent use of [type advantage] - major progress"*

11.5.4 Resolution

11.5.4.1 Outcome Determination

Based on team coordination and strategy effectiveness:

Complete Victory (80+ Security Status): *"Outstanding work. [Malmon Name] has been completely contained with minimal impact. Your coordinated response and use of type advantages was textbook incident response."*

Partial Victory (60-79 Security Status): *"Good work under pressure. The threat is contained, though some damage occurred. You've learned valuable lessons about [specific insights]."*

Pyrrhic Victory (40-59 Security Status): *"The threat is stopped, but at significant cost. This scenario highlights the importance of [key lessons] for future incidents."*

11.5.4.2 Evolution Outcomes

If Malmon evolved during the scenario:

"[Malmon Name] successfully evolved into [next form], demonstrating how threats escalate when not quickly contained. However, your response prevented [worse outcome]."

11.6 Session Transitions and Pacing

11.6.1 Maintaining Energy Throughout

11.6.1.1 Energy Monitoring Checklist

- **High engagement:** Players actively discussing, building on each other's ideas
- **Medium engagement:** Some participation, but needs encouragement
- **Low engagement:** Minimal discussion, blank stares, checking phones

11.6.1.2 Energy Management Techniques

For Low Energy:

- *"What's the worst-case scenario here?"*
- *"Who would be panicking right now besides us?"*
- *"What would happen if we're wrong about this?"*
- Inject urgency and stakes

For Overwhelming Complexity:

- *"Let's step back to the big picture"*
- *"What's the most important thing to focus on right now?"*
- *"If you had to pick one action, what would it be?"*

11.6.2 Time Management Strategies

11.6.2.1 Running Ahead of Schedule

- **Extend investigation phases:** Deeper technical discussions
- **Add complexity:** Multiple attack vectors or evolution
- **Enhanced debrief:** More detailed lessons learned
- **Advanced scenarios:** What happens next week/month?

11.6.2.2 Running Behind Schedule

- **Accelerate discovery:** Provide more direct guidance
- **Combine phases:** Investigation and response together
- **Focus on key learning:** Hit main educational objectives
- **Efficient resolution:** Quick but satisfying conclusion

11.6.2.3 Real-Time Adjustments

- **10 minutes over:** Normal, just note for next time
- **15 minutes over:** Start condensing remaining phases
- **20+ minutes over:** Emergency time management protocols

11.6.3 Participant Management

11.6.3.1 Encouraging Quiet Participants

- **Direct, gentle questions:** *"Alex, what's your network perspective on this?"*
- **Role-specific prompts:** *"As our Communicator, how would you handle this?"*
- **Expertise validation:** *"Given your [background], what would you try?"*
- **Lower stakes questions:** *"What's your gut feeling about this situation?"*

11.6.3.2 Managing Dominant Participants

- **Redirect without dismissing:** *"That's valuable insight. Let's hear other perspectives."*
- **Role assignments:** *"Can you help facilitate others' contributions?"*
- **Structured turns:** *"Let's go around and hear from everyone."*
- **Private sidebar:** Brief, respectful conversation about balance

11.6.3.3 Handling Technical Disputes

- **Acknowledge both sides:** *"Both approaches have merit"*
- **Focus on scenario:** *"In our specific situation, which would work better?"*
- **Use time pressure:** *"Given our constraints, what's the fastest effective solution?"*
- **Learn from disagreement:** *"This is exactly the kind of discussion incident response teams have"*

11.7 Closing Strong

11.7.1 Session Wrap-up

11.7.1.1 Immediate Debrief

"Quick debrief - what's one thing that surprised you about this incident?" "What's one technique you could use in your real work?" "What would you want to learn more about?"

11.7.1.2 MalDex Entry Creation

"Let's capture this for the community:"

- **Incident name:** Group creates memorable name
- **Key learnings:** Most important insights
- **Effective techniques:** What worked well
- **Future applications:** How to use these skills

11.7.1.3 Community Connection

"You're now part of the Malware & Monsters community. Here's how to stay connected…"

- Contact information sharing
- Follow-up resources
- Future session opportunities
- Contribution possibilities

11.7.2 Success Indicators

A successful session typically includes:

☐ Everyone contributed meaningfully to the investigation
☐ Technical discussions emerged from group expertise
☐ Questions drove more discovery than explanations
☐ Group made collaborative decisions under pressure
☐ Players connected game concepts to real-world applications
☐ Energy remained high throughout all phases
☐ Participants want to play again or facilitate sessions

11.8 Common Real-Time Challenges

11.8.1 When Nobody Knows Technical Details

- **Common sense redirect:** *"Using logic, what would worry you about this?"*
- **Analogy method:** *"Think of this like [familiar comparison]"*
- **Role-playing approach:** *"You don't need technical expertise - as [role], what concerns you?"*
- **Collaborative building:** *"Let's think through this together"*

11.8.2 When Sessions Go Off-Script

- **Follow player interest:** Their direction often leads to better learning
- **Maintain objectives:** Guide back to key concepts when possible
- **Improvise confidently:** Trust that engagement leads to education
- **Document insights:** Capture unexpected learning for future sessions

11.8.3 When Technical Accuracy is Questioned

- **Redirect to group:** *"Who here has experience with this?"*
- **Focus on learning:** *"What can we learn from this discussion?"*
- **Acknowledge limits:** *"I'm not an expert in this area - let's explore together"*
- **Use uncertainty:** *"This is exactly the kind of uncertainty incident responders face"*

The key to successful session management is confident flexibility - ready for anything while maintaining focus on collaborative learning and practical skill development.

Chapter 12

Practical Facilitation Techniques

12.1 The Question Arsenal

Effective facilitation depends on asking the right questions at the right time. This chapter provides a comprehensive toolkit of questions, techniques, and responses for real-time session management.

12.1.1 Universal Discovery Questions

12.1.1.1 Opening Investigation Questions

These work for any Malmon and expertise level:

- *"What's the first thing that would seem unusual here?"*
- *"Who in your organization would typically notice these problems first?"*
- *"What pattern suggests this isn't a normal technical issue?"*
- *"Based on your experience, what would worry you most about this situation?"*
- *"What would be your first instinct when hearing these symptoms?"*
- *"How would this compare to problems you've seen before?"*

12.1.1.2 Evidence Analysis Questions

When players find clues but need to interpret them:

- *"What does this evidence tell us about our adversary?"*
- *"How does this connect to what we found earlier?"*
- *"What would someone with malicious intent do with this access?"*
- *"If you were the attacker, what would your next move be?"*

- *"What's the significance of the timing here?"*
- *"What does the sophistication level suggest?"*

12.1.1.3 Pattern Recognition Questions

Help groups connect disparate clues:

- *"What's the common thread between these different findings?"*
- *"How do these pieces fit together into a single story?"*
- *"What type of threat typically combines these techniques?"*
- *"What does the combination of [A] and [B] usually indicate?"*
- *"If this is all connected, what would that mean?"*

12.1.2 Investigation Phase Question Bank

12.1.2.1 Impact Assessment Questions

For understanding scope and damage:

- *"What's the worst-case scenario if this continues unchecked?"*
- *"What would be most valuable to an attacker in this environment?"*
- *"How would this affect your organization's core mission?"*
- *"What regulatory or compliance implications are you seeing?"*
- *"Who would be most affected if this data is compromised?"*
- *"What systems absolutely cannot be taken offline?"*

12.1.2.2 Technical Deep-Dive Questions

When groups need to explore technical aspects:

- *"What tools would help you investigate this further?"*
- *"How would you typically approach this type of analysis?"*
- *"What indicators would confirm your suspicions?"*
- *"What would you need to prove this theory?"*
- *"How would you test whether [solution] would work?"*
- *"What's the technical explanation for what we're seeing?"*

12.1.2.3 Attack Vector Questions

For understanding how threats succeeded:

- *"How might this have gotten past your existing defenses?"*
- *"What vulnerabilities enabled this attack?"*
- *"Why would this technique be effective in this environment?"*
- *"What would have had to happen for this to succeed?"*
- *"How could this have been prevented?"*
- *"What assumptions did the attacker make about your environment?"*

12.1.3 Response Phase Question Bank

12.1.3.1 Strategy Development Questions

For coordinating team responses:

- *"What's your biggest constraint in responding to this?"*
- *"How would you prioritize your response actions?"*
- *"What could go wrong with this approach?"*
- *"How do we balance speed with thoroughness?"*
- *"What resources would you need to implement this?"*
- *"How would you coordinate this in your real organization?"*

12.1.3.2 Risk Assessment Questions

For evaluating response options:

- *"What's the risk of taking this action versus not taking it?"*
- *"What collateral damage might this response cause?"*
- *"How do we minimize disruption while containing the threat?"*
- *"What happens if this response fails?"*
- *"How do we maintain business operations during response?"*
- *"What stakeholders need to be informed about this decision?"*

12.1.3.3 Coordination Questions

For managing team dynamics during crisis:

- *"How do your individual actions support the overall strategy?"*
- *"Who needs to know what, and when?"*
- *"How do we ensure we're not working against each other?"*
- *"What communication is essential versus what creates noise?"*
- *"How do we track progress across all response activities?"*
- *"What decisions require team consensus versus individual expertise?"*

12.2 Managing Group Dynamics

12.2.1 Encouraging Quiet Participants

12.2.1.1 Direct Engagement Techniques

- **Role-specific questions:** *"As our [role], what's your perspective on this?"*
- **Expertise validation:** *"Given your background in [area], what would you try?"*
- **Opinion seeking:** *"What's your gut feeling about this situation?"*
- **Experience mining:** *"Have you seen anything similar in your work?"*

12.2.1.2 Indirect Inclusion Methods

- **Turn to neighbor:** *"Discuss with the person next to you, then we'll hear thoughts"*
- **Written first:** *"Jot down your thoughts, then we'll share"*
- **Choice offering:** *"Here are three options - which appeals to you and why?"*
- **Build on others:** *"What would you add to what [name] just said?"*

12.2.1.3 Confidence Building Approaches

- **Lower stakes questions:** *"What questions would you want to ask about this?"*
- **Common sense focus:** *"Even without technical expertise, what seems off here?"*
- **Future thinking:** *"What would you want to learn more about after this?"*
- **Validation offering:** *"That's exactly the kind of thinking we need"*

12.2.2 Managing Dominant Participants

12.2.2.1 Gentle Redirection Techniques

- **Acknowledge then redirect:** *"That's valuable insight. Let's hear other perspectives."*
- **Time boxing:** *"Thanks for that detail. In the interest of time, let's hear from others."*
- **Role switching:** *"Can you help facilitate input from the rest of the team?"*
- **Question redirection:** *"What questions does that raise for others?"*

12.2.2.2 Structural Solutions

- **Rotation systems:** *"Let's go around and hear one thought from everyone"*
- **Role assignments:** Give dominant participants teaching or coordination roles
- **Small groups:** Break into pairs or triads for discussion
- **Written contributions:** Have everyone write thoughts before verbal sharing

12.2.2.3 Private Conversation Approaches

During natural breaks:

- *"Your expertise is really valuable. Can you help me draw out others' insights too?"*
- *"I notice you have a lot to contribute. How can we make space for everyone?"*

- *"Would you mind holding back a bit so we can encourage others to participate?"*

12.2.3 Building Psychological Safety

12.2.3.1 Creating Safe Learning Environment

- **Normalize uncertainty:** *"Not knowing is normal in incident response"*
- **Validate attempts:** *"Good thinking" even when answers aren't perfect
- **Share your own uncertainty:** *"I don't know that either - let's figure it out together"*
- **Reframe mistakes:** *"That's exactly the kind of question real incident responders ask"*

12.2.3.2 Encouraging Risk-Taking

- **Model vulnerability:** *"I'm not sure about this either"*
- **Celebrate attempts:** *"I appreciate you thinking out loud"*
- **Use hypotheticals:** *"What if we tried…"* instead of *"We should…"*
- **Focus on learning:** *"What can we learn from this approach?"*

12.3 Handling Technical Knowledge Gaps

12.3.1 When Nobody Knows the Answer

12.3.1.1 The Progressive Revelation Technique

Step 1: Simplify the Question *Original:* "How would you detect advanced persistent threats?" *Simplified:* "How would you notice something that's trying to hide in your network?"

Step 2: Provide Context Clues *"Think about it this way - if someone was living in your house secretly, what might give them away?"*

Step 3: Multiple Choice Framework *"Would you be more concerned about: A) New files appearing, B) Unusual network traffic, or C) Strange user behavior?"*

Step 4: Collaborative Discovery *"Let's think through this together. What would be the signs?"*

Step 5: Direct Teaching (Last Resort) *"This is a great learning moment. Security professionals typically look for…"*

12.3.1.2 Common Sense Bridge Technique

- **Start with logic:** *"Using common sense, what would worry you?"*
- **Use analogies:** *"This is like [familiar situation]"*
- **Focus on impact:** *"What would be the business consequences?"*

- **Ask about feelings:** *"What makes you uncomfortable about this situation?"*

12.3.2 When Information is Incorrect

12.3.2.1 Gentle Correction Methods

- **Question back:** *"Can you walk me through that reasoning?"*
- **Seek clarification:** *"Help me understand how that would work"*
- **Offer alternatives:** *"What about this other possibility?"*
- **Group validation:** *"What do others think about that approach?"*

12.3.2.2 Learning from Errors

- **Explore the thinking:** *"That's interesting logic - let's see where it leads"*
- **Compare approaches:** *"How does that compare to [alternative]?"*
- **Real-world check:** *"How would that work in your actual environment?"*
- **Use as teaching moment:** *"This highlights an important distinction…"*

12.3.3 Bridging Expertise Gaps

12.3.3.1 Expert-to-Beginner Translation

When experts use complex terminology:

- *"Can you explain that in terms [beginner] would understand?"*
- *"What's the business impact of what you just described?"*
- *"How would you explain that to your CEO?"*
- *"What's the simple version of that concept?"*

12.3.3.2 Encouraging Peer Teaching

- *"[Expert], can you help the team understand [concept]?"*
- *"Who here can break down what [complex thing] means?"*
- *"Let's have [expert] teach us about [topic]"*
- *"Can someone translate that technical detail for the group?"*

12.4 Reading the Room and Adapting

12.4.1 Energy Level Assessment

12.4.1.1 High Engagement Indicators

- Active discussion and debate
- Building on each other's ideas
- Asking clarifying questions
- Leaning forward, eye contact
- Time seems to pass quickly

Response: Maintain pace, dive deeper into technical details, encourage debate

12.4.1.2 Medium Engagement Indicators

- Some participation with prompting
- Polite attention but limited initiative
- Following along but not contributing
- Checking time occasionally

Response: Inject urgency, ask direct questions, change pace or approach

12.4.1.3 Low Engagement Indicators

- Minimal response to questions
- Checking phones or laptops
- Side conversations
- Slumped posture, wandering attention
- Frequent time checking

Response: Emergency engagement protocols, break activity, refocus on stakes

12.4.2 Adaptive Difficulty Management

12.4.2.1 Increasing Difficulty Mid-Session

When group advances quickly:

- Add complexity to scenarios
- Introduce multiple attack vectors
- Explore advanced techniques
- Challenge assumptions
- Add time pressure

12.4.2.2 Decreasing Difficulty Mid-Session

When group struggles:

- Simplify terminology
- Provide more guidance
- Focus on core concepts
- Use more analogies
- Reduce scope

12.4.2.3 Real-Time Assessment Questions

- *"How are we doing on complexity level?"*
- *"Should we dive deeper or move on?"*
- *"Is this hitting the right level of challenge?"*
- *"What would be most valuable to explore further?"*

12.4.3 Cultural and Communication Adaptation

12.4.3.1 Diverse Group Management

- **Check understanding:** *"Does this make sense to everyone?"*
- **Invite perspectives:** *"How would this work in your organization/country?"*
- **Cultural sensitivity:** Be aware of different communication styles
- **Language barriers:** Use simple, clear language and check comprehension

12.4.3.2 Mixed Experience Levels

- **Expert involvement:** *"Can you help others understand this concept?"*
- **Beginner inclusion:** *"What questions does this raise for you?"*
- **Experience sharing:** *"Who's dealt with something similar?"*
- **Learning partnerships:** Pair experts with beginners

12.5 Advanced Facilitation Techniques

12.5.1 Building Dramatic Tension

12.5.1.1 Escalation Techniques

- **Time pressure:** *"You have 10 minutes before the attack spreads"*
- **Stakes raising:** *"Customer data is being stolen right now"*
- **Complication introduction:** *"Just as you think you have it contained…"*
- **Choice consequences:** *"This decision will determine whether…"*

12.5.1.2 Suspense Building

- **Cliffhanger moments:** End phases with unresolved tension
- **Gradual revelation:** Release information piece by piece
- **Multiple threats:** Suggest additional hidden dangers
- **Personal stakes:** Connect to character motivations

12.5.2 Improvisation and Adaptation

12.5.2.1 When Scenarios Go Sideways

- **Follow player interest:** Their direction often leads to better learning
- **Incorporate unexpected elements:** Use player contributions to evolve scenario
- **Maintain core objectives:** Guide back to key learning goals
- **Document insights:** Capture unexpected discoveries for future sessions

12.5.2.2 Creative Problem-Solving Encouragement

- **Yes, and...** Build on creative suggestions

- **What if...** Explore unconventional approaches
- **Challenge assumptions:** *"What if the obvious answer is wrong?"*
- **Encourage experimentation:** *"Let's try that and see what happens"*

12.5.3 Seamless Transition Management

12.5.3.1 Between Phases

- **Energy maintenance:** Keep momentum between rounds
- **Clear objectives:** Make new goals explicit
- **Stakes evolution:** Escalate tension appropriately
- **Progress acknowledgment:** Celebrate discoveries and progress

12.5.3.2 Between Activities

- **Smooth handoffs:** Connect current activity to next
- **Participation shifts:** Ensure everyone stays engaged
- **Focus management:** Help group shift attention smoothly
- **Time awareness:** Keep group informed of schedule

12.6 Emergency Facilitation Protocols

12.6.1 When Groups Get Completely Stuck

12.6.1.1 Circuit Breaker Techniques

- **Change perspective:** *"Let's approach this from a different angle"*
- **Lower stakes:** *"What if resources were unlimited?"*
- **Role switch:** *"What would [different role] do here?"*
- **Break it down:** *"What's the simplest first step?"*

12.6.1.2 Reset Strategies

- **Step back:** *"Let's recap what we know for certain"*
- **Refocus:** *"What's the most important thing to figure out right now?"*
- **Simplify:** *"If you had to pick just one action, what would it be?"*
- **Time jump:** *"Fast forward - what does success look like?"*

12.6.2 When Conflict Arises

12.6.2.1 Technical Disagreements

- **Acknowledge both sides:** *"Both approaches have merit"*
- **Focus on context:** *"In our specific situation, which would work better?"*
- **Use constraints:** *"Given our time/resource limits, what's most practical?"*
- **Learn from disagreement:** *"This is exactly what real teams debate"*

12.6.2.2 Personality Conflicts

- **Redirect to task:** *"Let's focus on solving the incident"*
- **Acknowledge emotions:** *"I can see this is important to both of you"*
- **Use roles:** *"From your role perspective, what would you recommend?"*
- **Private intervention:** Brief sidebar conversations if needed

12.6.3 When Technology Fails

12.6.3.1 Backup Facilitation Methods

- **Paper alternatives:** Have analog versions of all digital tools
- **Verbal tracking:** Use group memory for status tracking
- **Whiteboard substitution:** Visual tools for complex scenarios
- **Continue regardless:** Don't let technology stop learning

12.7 Success Indicators and Troubleshooting

12.7.1 Session Success Metrics

12.7.1.1 Engagement Indicators

☐ Everyone contributes meaningfully
☐ Questions generate more discussion than answers
☐ Players build on each other's ideas
☐ Time feels like it passes quickly
☐ Group wants to continue or play again

12.7.1.2 Learning Indicators

☐ Technical concepts emerge from group discussion
☐ Players connect game concepts to real work
☐ Misconceptions get corrected through peer interaction
☐ New insights emerge from collaboration
☐ Confidence in cybersecurity concepts increases

12.7.2 Common Problems and Solutions

12.7.2.1 Problem: Group Won't Engage

Solutions:

- Lower stakes questions
- Direct individual attention
- Change physical arrangement
- Inject urgency or humor
- Break into smaller groups

12.7.2.2 Problem: Too Much Technical Detail

Solutions:

- Redirect to big picture
- Ask about business impact
- Use time pressure to prioritize
- Focus on decisions rather than details
- Acknowledge expertise but maintain pace

12.7.2.3 Problem: Not Enough Technical Depth

Solutions:

- Ask follow-up questions
- Encourage expert elaboration
- Dive into specific techniques
- Explore alternative approaches
- Connect to real-world tools and methods

12.7.2.4 Problem: Time Management Issues

Solutions:

- Flexible scenario adaptation
- Priority-based decision making
- Efficient transition techniques
- Strategic time allocation
- Emergency pacing protocols

12.8 Scenario Card Preparation Method

12.8.1 The 5-Minute Scenario Card Prep

Most experienced IMs can prepare for any session using scenario cards in just 5 minutes:

12.8.1.1 Minute 1: Card Selection (60 seconds)

- Choose based on group expertise and industry context
- Quick scan: Hook, Pressure, NPCs, Secrets, Villain Plan

12.8.1.2 Minute 2: NPC Motivation Review (60 seconds)

- Identify primary stakeholder (IT Director, Hospital CIO, etc.)
- Understand their immediate concerns and constraints
- Note competing priorities and pressure sources

12.8.1.3 Minute 3: Hook Internalization (60 seconds)

- Understand WHY this attack is happening NOW
- Connect to realistic business pressures and deadlines
- Prepare opening hook: "Organization X is 72 hours from critical deadline Y..."

12.8.1.4 Minute 4: Pressure Timeline Review (60 seconds)

- Understand business deadline and consequences
- Map escalation stages if threat evolves
- Balance urgency with realistic response time

12.8.1.5 Minute 5: Question Preparation (60 seconds)

- Prepare context-driven discovery questions
- Focus on stakeholder perspectives: "What would worry you most?"
- Trust scenario card details, facilitate discovery over lecturing

12.8.2 Why Scenario Cards Work

Rich Context Pre-Built: - Organizational situations participants recognize professionally
- Authentic business constraints and stakeholder pressures - Realistic technical vulnerabilities and attack progression

95% Content Reuse: - Core technical content identical across scenarios - Only organizational details change (company names, deadlines, NPCs) - Allows focus on facilitation rather than content generation

Professional Authenticity: - Industry-specific pressure situations - Realistic stakeholder dynamics and competing priorities - Natural investigation starting points and discovery paths

12.8.3 Emergency Shortcuts

2-Minute Panic Prep: - Grab most familiar scenario card - Read hook and primary stakeholder motivation
- Trust the card, ask context questions, let them discover

1-Minute Crisis Prep: - Pick any scenario card - Read the hook aloud as written - Ask: "What would worry you most in this situation?"

Key Principle: Scenario cards contain everything needed. Your job is facilitation, not expertise demonstration.

The key to practical facilitation is building a toolkit of responses that become automatic, allowing you to focus on reading the group and adapting to their needs in real-time.

Chapter 13

Session Management

13.1 The Art of Orchestrating Collaborative Learning

Effective session management balances structure with flexibility, ensuring that learning objectives are met while adapting to the unique dynamics and expertise of each group. Your role is to create and maintain an environment where collaborative discovery can flourish.

13.1.1 Pre-Session Setup

13.1.1.1 Essential Preparation

Digital Resources:

- **Reference Materials:** Type effectiveness chart, role descriptions, emergency protocols
- **Backup Plans:** Printed materials in case of technology failure
- **Time Management:** Visible timer or clock for phase management
- **Documentation Tools:** Capture insights and lessons learned

13.1.1.2 Group Assessment and Adaptation

Rapid Expertise Assessment:

As participants arrive, gather information about their backgrounds:

- *"What brings you here today?"*
- *"What's your experience level with incident response?"*
- *"Are there specific learning goals you hope to achieve?"*
- *"Any particular cybersecurity challenges you're facing at work?"*

Adaptation Indicators:

- **High Expertise Group:** Focus on complex scenarios, advanced concepts, innovation opportunities
- **Mixed Expertise Group:** Leverage peer teaching, emphasize collaboration over individual performance
- **Low Expertise Group:** Emphasize concept learning, provide more guidance and structure
- **Organizational Team:** Connect learning to specific workplace challenges and opportunities

13.1.2 Opening and Character Creation

13.1.2.1 Creating Psychological Safety

Set Collaborative Expectations:

- *"This is a learning environment where questions and mistakes are valuable."*
- *"Everyone brings knowledge and perspective that contributes to our collective understanding."*
- *"We succeed as a team, not as individuals competing against each other."*
- *"The goal is learning together, not demonstrating expertise or getting everything right."*

Address Common Concerns:

- *"You don't need to be a cybersecurity expert to contribute meaningfully."*
- *"Technical knowledge helps, but problem-solving and collaboration skills are equally valuable."*
- *"We'll learn from each other's experience and perspectives throughout the session."*

13.1.2.2 Skills Discovery and Role Assignment

Structured Sharing Process:

Have each participant briefly share (45 seconds each):

- Name and background
- Connection to cybersecurity (professional, academic, personal interest)
- One thing they know about computers, security, or technology
- What they hope to learn or contribute

Collaborative Role Selection: Based on interests and team needs:

- *"Based on what everyone shared, let's think about how to build a strong incident response team."*
- *"Which roles appeal to you based on your interests and experience?"*
- *"How can we ensure all key perspectives are represented?"*
- *"Remember, roles are starting points - your expertise can contribute across all areas."*

13.1.2.3 Character Development

Individual Reflection: Participants develop their character using prompts:

- Keep your real first name
- Build a personality around your chosen role
- Think about what motivates your character
- Consider how your real experience informs your character

Brief Introductions: Each participant introduces their character in 20-30 seconds:

- Name and role
- One character trait or quirk
- What drives them to protect their organization
- How they approach cybersecurity challenges

13.1.3 Round Management

13.1.3.1 Discovery Phase Management

Phase Introduction:

- Present initial symptoms clearly and concisely
- Establish the learning objective: identify the specific threat
- Remind team of available time and individual action allocation
- Encourage role-based investigation approaches

Individual Investigation:
Your Role During This Time:

- **Circulate and Listen:** Move around table, listen to discussions, gauge engagement
- **Ask Clarifying Questions:** Help participants think through their role's perspective
- **Provide Guidance When Stuck:** Offer gentle prompts without providing answers
- **Monitor Time:** Give time warnings as needed but focus on learning; you don't want to break off an engaging conversation where everybody partakes and learn just for the mere sake of progress.

Effective Circulation Questions:

- *"What would someone in your role typically investigate first?"*
- *"What patterns or anomalies stand out to you?"*
- *"How would you approach this if it happened at your organization?"*
- *"What questions would your role ask about these symptoms?"*

Knowledge Sharing:
Facilitate Structured Sharing:

- Go around table, giving each role 90 seconds to share findings

- Ask follow-up questions that connect different perspectives
- Help team see patterns and connections across different investigations
- Build toward collective understanding without forcing conclusions

Effective Facilitation Questions:

- *"How do these different findings connect?"*
- *"What patterns emerge when we look at all perspectives together?"*
- *"What questions remain after hearing everyone's investigation?"*
- *"What type of threat explains all these different symptoms?"*

Malmon Identification: Guide Collaborative Conclusion:

- Help team synthesize their investigations into threat identification
- Validate their reasoning and analysis process
- Reveal Malmon card and confirm their assessment
- Briefly discuss type effectiveness and what it means for response

13.1.3.2 Investigation Phase Management

Phase Transition:

- Acknowledge successful discovery work
- Present evolution pressure or additional complications
- Establish phase objective: understand scope and plan response
- Maintain urgency while allowing thorough analysis

Impact Assessment: Key Areas to Explore:

- What systems and data are affected or at risk?
- How has the attack progressed since initial compromise?
- What are the business and operational implications?
- What vulnerabilities enabled this attack to succeed?

Facilitation Focus:

- Keep discussions tied to actionable intelligence
- Help team balance thoroughness with time pressure
- Connect technical findings to business impact
- Encourage cross-role collaboration and information sharing

Attack Vector Analysis: Guide Deeper Understanding:

- How did the attack succeed initially?
- What would have prevented this compromise?
- What does this reveal about organizational security posture?
- How might similar attacks be prevented in the future?

Evolution Assessment: Create Urgency for Response:

- Present signs of potential threat evolution or escalation
- Help team understand time pressure for effective response

- Connect investigation findings to response strategy needs
- Transition focus from understanding to action planning

13.1.3.3 Response Phase Management

Strategy Development: Facilitate Collaborative Planning:

- Help team choose approaches based on Malmon type effectiveness
- Encourage role-based contribution to strategy development
- Address resource constraints and organizational realities
- Build consensus around coordinated response approach

Key Questions:

- *"Given what we know about this threat type, what approaches would be most effective?"*
- *"How would you coordinate different response activities?"*
- *"What could go wrong with this approach, and how would you address those risks?"*
- *"How does this response strategy address both immediate threats and long-term prevention?"*

Implementation:
Manage Action Resolution:

- Help team execute their strategy through role-based actions
- Use dice mechanics when outcomes are uncertain
- Apply type effectiveness bonuses and penalties appropriately
- Maintain tension while rewarding good collaboration and planning

Resolution:
Wrap Up the Incident:

- Determine final outcome based on team performance and decisions
- Acknowledge effective strategies and collaboration
- Connect results to learning objectives and real-world applications
- Set up post-session reflection and documentation

13.1.4 Time Management Strategies

13.1.4.1 When Phases Run Long

Early Intervention:

- *"We are almost out of time for this phase - what's our key priority?"*
- *"Let's focus on the most important decision we need to make."*
- *"What's the essential information we need before moving to the next phase?"*

Late Intervention:

- *"Time to wrap up - what's our main conclusion?"*
- *"What's the most important takeaway from this phase?"*
- *"We'll carry forward [key insight] as we move to the next phase."*

13.1.4.2 When Phases Run Short

Depth Questions:

- *"What might we be missing if we move too quickly?"*
- *"What are the implications of this decision?"*
- *"How would different approaches change our outcomes?"*
- *"What would worry you most about our current understanding?"*

Extension Activities:

- Cross-role consultation and knowledge sharing
- Alternative scenario exploration
- Strategic thinking about prevention and improvement
- Connection to real-world organizational challenges

13.1.5 Energy and Engagement Management

13.1.5.1 Maintaining High Energy

Technique Rotation:

- **Discussion:** Collaborative problem-solving and knowledge sharing
- **Action:** Individual investigation and strategy implementation
- **Reflection:** Analysis of decisions and learning capture
- **Movement:** Physical position changes, role consultations

Engagement Indicators:

- Active participation from all roles
- Building on each other's contributions
- Questions and curiosity about the scenario
- Connection to real-world experience and challenges

13.1.5.2 Addressing Low Energy

Immediate Interventions:

- *"What's at stake if we don't solve this problem?"*
- *"How would you explain the urgency to your organization's leadership?"*
- *"What would make this attack particularly dangerous?"*
- Brief physical movement or position change

Systemic Adjustments:

- Reduce complexity and focus on core learning objectives

- Increase role-based structure and guidance
- Add collaborative elements and team consultation
- Connect more directly to participants' real-world experience

13.1.6 Managing Different Group Types

13.1.6.1 High-Expertise Groups

Characteristics: Deep technical knowledge, may find scenarios too simple
Management Approach:

- Add complexity and advanced concepts
- Focus on innovation and technique development
- Encourage mentoring and knowledge sharing
- Connect to cutting-edge threats and responses

Effective Questions:

- *"What additional complications might arise in real incidents?"*
- *"How would you improve on standard response approaches?"*
- *"What would you do differently based on your experience?"*
- *"How would you teach this concept to less experienced colleagues?"*

13.1.6.2 Mixed-Experience Groups

Characteristics: Varying levels of technical knowledge and experience
Management Approach:

- Facilitate peer teaching and learning
- Ensure all participants can contribute meaningfully
- Balance technical depth with accessible concepts
- Use experienced participants as teaching resources

Effective Questions:

- *"How would you explain this to someone new to cybersecurity?"*
- *"What questions would someone without technical background ask?"*
- *"How do different experience levels contribute to understanding this threat?"*
- *"What can we learn from each other's different perspectives?"*

13.1.6.3 Low-Experience Groups

Characteristics: Limited cybersecurity background, may feel intimidated
Management Approach:

- Emphasize concept learning over technical details
- Provide more structure and guidance
- Celebrate insights and logical thinking
- Connect to everyday technology experience

Effective Questions:

- *"What would common sense suggest in this situation?"*
- *"How is this similar to technology problems you've encountered?"*
- *"What would worry you if this happened to your personal computer?"*
- *"What questions would you ask if you were responsible for fixing this?"*

13.1.6.4 Organizational Teams

Characteristics: Work together regularly, want applicable insights
Management Approach:

- Connect learning directly to organizational challenges
- Address specific workplace constraints and opportunities
- Encourage discussion of implementation and application
- Support team development and relationship building

Effective Questions:

- *"How would this scenario play out in your specific environment?"*
- *"What organizational factors would help or hinder this response?"*
- *"How could you apply these insights to improve your current security posture?"*
- *"What would you need to implement these approaches at work?"*

13.1.7 Post-Session Wrap-Up (5 minutes)

13.1.7.1 Learning Capture

Structured Reflection:

- What surprised you most about this scenario?
- Which response techniques were most effective?
- How does this connect to your real-world experience?
- What would you do differently in a similar situation?

MalDex Documentation:

- Key insights about the Malmon's behavior and weaknesses
- Effective response strategies discovered during the session
- Lessons learned about team coordination and collaboration
- Recommendations for other teams facing similar threats

13.1.7.2 Community Connection

Next Steps:

- Information about additional learning opportunities
- Connection to local cybersecurity communities
- Resources for continued skill development
- Opportunities to contribute to community knowledge

Feedback Collection:

- What worked well in this session?
- What could be improved for future sessions?
- Interest in additional scenarios or advanced challenges
- Suggestions for community development and growth

Remember: Effective session management creates the conditions for collaborative learning while adapting to the unique needs and dynamics of each group. Focus on maintaining engagement, ensuring meaningful participation from all roles, and connecting learning to real-world applications and challenges.

Chapter 14

Advanced Troubleshooting and Session Recovery

14.1 Complex Facilitation Challenges

14.1.1 The "Mixed Expertise Crisis"

Scenario: Team has both cybersecurity experts and complete newcomers, creating tension between depth and accessibility.

Symptoms:

- Experts getting frustrated with "basic" explanations
- Newcomers withdrawing from technical discussions
- Discussion splitting into separate conversations
- Learning objectives not being met for any participant

Recovery Strategy:

1. **Acknowledge the challenge:** *"We have a great mix of experience levels—let's use that as a strength."*
2. **Reframe expert role:** *"[Expert names], help us understand this from a teaching perspective—how would you explain this to someone new to the field?"*
3. **Empower newcomers:** *"[Newcomer names], your questions help everyone learn—what would you want to know about this?"*
4. **Bridge building:** *"How can we combine [Expert's] technical insight with [Newcomer's] fresh perspective?"*

Prevention for Future:

- Set expectations during character creation about peer teaching
- Explicitly assign mentorship roles to experienced participants

- Use "explain it like I'm new" as a regular facilitation technique
- Create structured opportunities for knowledge sharing

14.1.2 The "Analysis Paralysis Spiral"

Scenario: Team gets stuck in endless technical debate without reaching decisions or making progress.

Symptoms:

- Same technical points debated repeatedly
- No clear decision-making process
- Time running out with minimal progress
- Participants expressing frustration with lack of direction

Emergency Intervention:

1. **Pattern interrupt:** *"I'm noticing we've been exploring this technical detail for a while—let's step back."*
2. **Decision forcing:** *"In a real incident, you'd need to act with incomplete information. What would you decide right now?"*
3. **Criteria establishment:** *"What factors should guide this decision? What matters most?"*
4. **Time boxing:** *"Let's take 3 minutes to reach a conclusion, then move forward with our best judgment."*

Underlying Issues to Address:

- Unclear decision-making authority within the team
- Perfectionism preventing action under uncertainty
- Lack of incident response experience with time pressure
- Over-emphasis on technical correctness vs. practical response

14.1.3 The "Personality Conflict Explosion"

Scenario: Strong personalities clash over approaches, creating tension that disrupts learning for everyone.

Symptoms:

- Personal criticism rather than idea-focused discussion
- Participants taking sides in conflicts
- Defensive responses and escalating emotions
- Learning completely overshadowed by interpersonal dynamics

Immediate De-escalation:

1. **Stop the action:** *"Let's pause for a moment and take a breath."*
2. **Reframe to learning:** *"We're here to learn from each other—both perspectives have value."*

3. **Redirect to scenario:** *"How would this disagreement be handled in a real incident response team?"*
4. **Reset expectations:** *"Let's focus on collaborative problem-solving rather than being right."*

Structural Changes:

- Break into smaller subgroups temporarily
- Assign specific roles that channel personalities productively
- Use written reflection before verbal discussion
- Focus on shared objectives and common ground

14.1.4 The "Technical Overreach Problem"

Scenario: Participants want to explore technical details that are beyond the scope of the learning objectives or IM expertise.

Symptoms:

- Deep technical discussions that exclude some participants
- Requests for specific technical information IM doesn't have
- Session becoming too advanced for intended learning level
- Focus shifting away from collaborative learning to technical training

Response Framework:

1. **Acknowledge value:** *"This is clearly an important technical concept."*
2. **Clarify scope:** *"For our learning objectives today, we're focusing on [specific concept]."*
3. **Redirect:** *"How does this technical detail inform our collaborative response strategy?"*
4. **Offer follow-up:** *"This seems like a great topic for deeper exploration after our session."*

Boundary Management:

- Use learning objectives as guardrails for scope
- Differentiate between facilitation and technical training
- Encourage peer learning and resource sharing outside formal session
- Connect participants with appropriate technical resources

14.2 Advanced Group Dynamics

14.2.1 Managing Dominant Personalities

14.2.1.1 The "Expert Who Knows Everything"

Challenge: Participant with extensive expertise answering all questions and providing all solutions.

Intervention Strategies:

- **Role assignment:** *"[Name], take on the coaching role—help others discover these insights."*
- **Question redirection:** *"[Name], what questions would help us think through this problem?"*
- **Peer teaching:** *"[Name], what would someone new to this field need to understand first?"*
- **Delayed gratification:** *"[Name], hold that insight for a moment—let's see what others discover first."*

14.2.1.2 The "Silent Participant"

Challenge: Team member who contributes minimally to discussion despite apparent engagement.

Gentle Engagement Techniques:

- **Direct inclusion:** *"[Name], what's your perspective on this approach?"*
- **Role-specific questions:** *"[Name], from the [role] viewpoint, what would concern you?"*
- **Written reflection:** Use quick written exercises before group discussion
- **Small group work:** Break into pairs or triads for initial discussion

14.2.1.3 The "Perfectionist Paralysis"

Challenge: Participant who needs complete information before making any decisions.

Progressive Action Building:

- **Hypothesis testing:** *"What would you try first, even if you're not completely sure?"*
- **Scenario pressure:** *"In a real incident, what would you do with the information you have now?"*
- **Risk assessment:** *"What's the risk of waiting for more information vs. acting now?"*
- **Incremental decisions:** Break large decisions into smaller, manageable choices

14.2.2 Cultural and Communication Challenges

14.2.2.1 Cross-Cultural Facilitation

Different Communication Styles:

- **Direct vs. Indirect:** Some cultures prefer explicit statements while others use subtle implications
- **Hierarchy Awareness:** Some participants may defer to perceived authority figures

- **Risk Tolerance:** Cultural differences in comfort with uncertainty and ambiguity
- **Time Orientation:** Different approaches to time management and deadline pressure

Adaptive Strategies:

- **Multiple Communication Channels:** Use verbal, written, and visual approaches
- **Explicit Permission:** Clearly invite participation from all cultural backgrounds
- **Cultural Bridge Building:** Help participants understand different communication styles
- **Flexible Pacing:** Adapt time expectations to accommodate different processing styles

14.2.2.2 Language and Technical Barriers

When English is a Second Language:

- Use simpler vocabulary when possible without losing meaning
- Allow extra processing time for complex concepts
- Encourage peer translation and explanation
- Provide visual aids and written summaries

When Technical Jargon Creates Barriers:

- Define technical terms when first introduced
- Use analogies and real-world examples
- Encourage questions about unfamiliar concepts
- Create a "jargon-free zone" for initial discussions

14.3 Technology and Equipment Failures

14.3.1 Digital Tool Failures

14.3.1.1 When Presentation Technology Fails

Backup Strategies:

- **Paper materials:** Always have key references printed
- **Participant devices:** Use phones/laptops to access materials
- **Analog alternatives:** Whiteboard/flipchart for tracking and notes
- **Pure discussion:** Run session as structured conversation

Rapid Adaptation Techniques:

1. **Acknowledge quickly:** *"Technology isn't cooperating—let's adapt."*
2. **Enlist help:** *"Can someone access the materials on their device?"*
3. **Simplify approach:** Focus on core concepts without digital aids

4. **Maintain energy:** Don't let technical problems derail learning momentum

14.3.1.2 When Internet Access is Lost

Offline Facilitation Strategies:

- Use printed Malmon cards and reference materials
- Focus on conceptual discussions rather than real-time research
- Leverage participant experience and knowledge sharing
- Create hypothetical scenarios based on group expertise

14.3.2 Physical Environment Challenges

14.3.2.1 Noise and Distraction Management

Common Issues:

- Construction or maintenance noise
- Interruptions from other activities
- Uncomfortable temperature or lighting
- Inadequate space for group size

Adaptive Responses:

- **Acknowledge impact:** *"This noise is distracting—let's adjust our approach."*
- **Break and relocate:** Move to different space if possible
- **Modify activities:** Use more interactive, engaging techniques to maintain focus
- **Shorter segments:** Break complex discussions into smaller chunks

14.3.2.2 Group Size Problems

Too Many Participants (8+):

- Break into smaller subgroups for detailed work
- Use structured reporting back from subgroups
- Assign specific roles to manage participation
- Focus on concepts rather than detailed technical work

Too Few Participants (2-3):

- Adapt scenarios to smaller team size
- Have participants play multiple roles
- Focus on in-depth exploration rather than broad coverage
- Use more coaching and mentoring approach

14.4 Learning Objective Misalignment

14.4.1 When Sessions Go Off-Track

14.4.1.1 Content Drift

Problem: Discussion moves away from intended learning objectives toward unrelated topics.

Course Correction:

1. **Acknowledge value:** *"This is clearly important to the group."*
2. **Check relevance:** *"How does this connect to our main learning objective?"*
3. **Parking lot:** *"Let's capture this topic for discussion after our session."*
4. **Redirect:** *"For our main objective today, let's focus on…"*

14.4.1.2 Scope Creep

Problem: Team wants to explore concepts beyond what can be covered effectively in available time.

Boundary Management:

1. **Realistic assessment:** *"We have [X] time remaining—what's most important to cover?"*
2. **Priority setting:** *"If you could take away one key insight today, what would it be?"*
3. **Future planning:** *"This seems like excellent material for a follow-up session."*
4. **Core focus:** *"Let's make sure we accomplish our main objective before exploring additional topics."*

14.4.2 Assessment and Adjustment

14.4.2.1 Real-Time Learning Check

Mid-Session Assessment Questions:

- *"What's been most valuable so far?"*
- *"What questions are still unresolved for you?"*
- *"How well are we meeting your learning expectations?"*
- *"What would make the remaining time most valuable?"*

Adjustment Strategies:

- **Pace modification:** Speed up or slow down based on group needs
- **Depth adjustment:** Go deeper or broader depending on interest and understanding
- **Method variation:** Switch between discussion, hands-on work, and reflection

- **Objective refinement:** Modify learning goals based on emerging group needs

14.5 Post-Session Recovery and Learning

14.5.1 When Sessions Don't Go Well

14.5.1.1 Immediate Post-Session Actions

For Participants:

1. **Acknowledge challenges:** *"That session had some bumps—what did we learn despite the difficulties?"*
2. **Extract value:** *"What insights did you gain that you can apply in your work?"*
3. **Future improvement:** *"What would make a future session even more valuable?"*
4. **Maintain relationships:** *"Thank you for your patience as we worked through those challenges together."*

For Yourself as IM:

1. **Honest reflection:** What went well? What would you change?
2. **Learning identification:** What did you learn about facilitation from this experience?
3. **Community connection:** Share experiences with other IMs for support and learning
4. **Skill development:** Identify specific areas for improvement and practice

14.5.1.2 Transforming Difficult Experiences into Learning

Participant Follow-Up:

- Send summary of key insights despite challenges
- Provide additional resources related to topics that emerged
- Invite feedback for continuous improvement
- Offer opportunities for future sessions with lessons applied

Community Sharing:

- Document lessons learned for other facilitators
- Contribute to troubleshooting knowledge base
- Share successful recovery techniques with IM community
- Help improve frameworks and materials based on real experience

14.5.2 Building Resilience

14.5.2.1 Developing Adaptive Expertise

Core Facilitation Skills:

- **Flexibility:** Ability to change approach based on emerging needs
- **Emotional regulation:** Managing your own reactions under pressure
- **Group reading:** Sensing group energy, engagement, and dynamics
- **Recovery orientation:** Focusing on learning from setbacks rather than avoiding them

Advanced Capabilities:

- **Cultural sensitivity:** Adapting to diverse communication styles and preferences
- **Conflict resolution:** Helping groups work through disagreements constructively
- **Learning design:** Modifying activities in real-time to optimize learning outcomes
- **Community building:** Creating connections that extend beyond individual sessions

14.5.2.2 Self-Care and Sustainability

Managing Facilitation Stress:

- **Preparation boundaries:** Avoid over-preparing as anxiety management
- **Performance pressure:** Focus on learning facilitation rather than perfect execution
- **Imposter syndrome:** Remember that your role is facilitation, not expertise demonstration
- **Continuous learning:** View every session as professional development opportunity

Building Support Networks:

- **Peer connections:** Regular contact with other IMs for support and learning
- **Mentorship relationships:** Both receiving guidance and providing it to newcomers
- **Community involvement:** Active participation in IM community development
- **Professional development:** Ongoing skill building in facilitation and cybersecurity

14.5.3 Continuous Improvement

14.5.3.1 Session Documentation

What to Track:

- **Group composition:** Experience levels, roles, organizational contexts
- **Challenges encountered:** Specific problems and how they were addressed

- **Successful techniques:** Approaches that worked particularly well
- **Learning outcomes:** What participants gained from the experience

How to Use Documentation:

- **Pattern recognition:** Identify recurring challenges and successful approaches
- **Preparation improvement:** Better pre-session planning based on experience
- **Community contribution:** Share insights that help other facilitators
- **Personal growth:** Track your development as a facilitator over time

14.5.3.2 Feedback Integration

Participant Feedback:

- **Immediate reaction:** Quick pulse check at session end
- **Reflection feedback:** Follow-up after participants have time to process
- **Specific suggestions:** Concrete ideas for improvement
- **Learning validation:** Confirmation of what was most valuable

Peer Feedback:

- **Co-facilitation opportunities:** Learning from observing and being observed
- **IM community input:** Sharing challenges and solutions with peers
- **Mentorship guidance:** Regular check-ins with more experienced facilitators
- **Cross-pollination:** Learning from facilitators in other domains

Remember: Every challenging session teaches valuable lessons about facilitation, group dynamics, and cybersecurity education. The goal is not perfect sessions, but continuous learning and improvement in service of collaborative cybersecurity education.

Chapter 15

Advanced Scenarios

15.1 Beyond Basic Incident Response

Once teams have mastered fundamental Malmon encounters and collaborative response techniques, advanced scenarios provide opportunities to tackle complex, multi-faceted cybersecurity challenges that mirror the sophistication of real-world threats. These scenarios test not just technical knowledge, but strategic thinking, coordination under pressure, and adaptive problem-solving.

15.1.1 Characteristics of Advanced Scenarios

15.1.1.1 Multi-Vector Attacks

Coordinated Threat Campaigns:

- Multiple Malmons deployed simultaneously with different objectives
- Attacks that span multiple attack vectors (email, web, USB, supply chain)
- Threat actors using diversified techniques to achieve strategic goals
- Requires teams to coordinate response across multiple concurrent threats

Example: Healthcare Hybrid Campaign

- **Initial Vector:** Spear-phishing emails targeting administrative staff (GaboonGrabber)
- **Secondary Vector:** USB-based propagation through medical device maintenance (Raspberry Robin)
- **Final Payload:** Ransomware deployment targeting patient data systems (LockBit)
- **Learning Objectives:** Multi-domain coordination, priority setting, resource allocation

15.1.1.1.1 Multi-Vector ATT&CK Analysis

Raspberry Robin Analysis (Secondary Vector):

LockBit Analysis (Final Payload):

15.1.1.2 Evolving Threat Landscapes

Dynamic Adaptation Scenarios:

- Malmons that evolve based on defensive responses
- Threat actors adapting tactics in real-time during incidents
- Scenarios where initial containment strategies trigger escalation
- Long-term campaigns that require sustained response over multiple sessions

Example: Nation-State Evolution Chain

- **Phase 1:** Reconnaissance and initial access (Stuxnet-style APT)
- **Phase 2:** Lateral movement and intelligence gathering
- **Phase 3:** Sabotage attempt triggers defensive response
- **Phase 4:** Threat actor adaptation and counter-response
- **Learning Objectives:** Strategic patience, attribution analysis, escalation management

15.1.1.3 Cross-Organizational Incidents

Supply Chain and Partnership Scenarios:

- Attacks that affect multiple organizations simultaneously
- Vendor compromises that impact customer organizations
- Information sharing and coordination between organizations
- Regulatory and legal implications of cross-organizational incidents

Example: Cloud Service Provider Compromise

- **Scenario Setup:** Critical cloud service used by multiple organizations is compromised
- **Team Challenge:** Coordinate response while maintaining business operations
- **External Coordination:** Share information with other affected organizations
- **Learning Objectives:** Third-party risk management, information sharing protocols

15.1.2 Industry-Specific Advanced Scenarios

15.1.2.1 Healthcare Sector Challenges

Critical Infrastructure Considerations:

- Patient safety implications of cybersecurity incidents
- Coordination between IT and clinical staff during response

- HIPAA compliance requirements during emergency response
- Medical device security and operational technology integration

Advanced Healthcare Scenario: "Code Blue Cyber"

- **Setup:** Ransomware targets both IT systems and connected medical devices
- **Complication:** Attack occurs during peak patient care hours
- **Stakeholders:** IT staff, clinical teams, hospital administration, regulatory bodies
- **Unique Challenges:** Patient safety takes precedence over standard incident response procedures
- **Learning Objectives:** Healthcare-specific prioritization, regulatory compliance under pressure

15.1.2.2 Financial Services Complexity

Regulatory and Market Implications:

- Real-time transaction processing during incidents
- Market confidence and customer communication
- Multi-jurisdictional regulatory requirements
- Coordination with law enforcement and financial regulators

Advanced Financial Scenario: "Market Manipulation"

- **Setup:** APT campaign targeting high-frequency trading systems
- **Complication:** Attack designed to manipulate market prices
- **Stakeholders:** Trading floor, risk management, regulators, law enforcement
- **Unique Challenges:** Distinguishing between attack effects and market volatility
- **Learning Objectives:** Financial crime investigation, market impact assessment

15.1.2.3 Critical Infrastructure Protection

Physical/Cyber Convergence:

- Operational technology and information technology integration
- Safety system implications of cybersecurity incidents
- Coordination with emergency services and government agencies
- Public safety and national security considerations

Advanced Infrastructure Scenario: "Grid Down"

- **Setup:** Stuxnet-variant targeting electrical grid control systems
- **Complication:** Attack causes rolling blackouts affecting multiple states
- **Stakeholders:** Utility operators, emergency services, government agencies, media

- **Unique Challenges:** Physical safety implications of cyber incident response
- **Learning Objectives:** Critical infrastructure protection, public-private coordination

15.1.3 Time-Pressure Scenarios

15.1.3.1 Crisis Timeline Management

Compressed Decision-Making:

- Incidents with immediate public safety implications
- Media attention and public scrutiny during response
- Regulatory notification deadlines during active incidents
- Coordinating response while managing external pressure

High-Pressure Scenario: "Zero Hour"

- **Setup:** Ransomware with 4-hour deadline targeting hospital systems
- **Time Constraint:** Must maintain patient care while responding to threat
- **Media Element:** Local news coverage adds public pressure
- **Learning Objectives:** Decision-making under extreme pressure, stakeholder management

15.1.3.2 Marathon Incidents

Sustained Response Operations:

- Multi-week incidents requiring team endurance and rotation
- Evolving threats that require adaptive long-term strategies
- Resource management and team sustainability
- Maintaining response effectiveness over extended periods

Extended Scenario: "The Long Game"

- **Setup:** Nation-state APT with 6-month operation timeline
- **Format:** Multiple connected sessions spanning weeks
- **Evolution:** Threat adapts based on team responses between sessions
- **Learning Objectives:** Strategic patience, long-term incident management

15.1.4 Competitive Advanced Scenarios

15.1.4.1 Red Team vs Blue Team Evolutions

Dynamic Adversary Simulation:

- Red team adapts tactics based on blue team responses
- Multiple rounds with escalating sophistication
- Real-time threat actor decision-making

- Authentic pressure of adapting adversaries

Advanced Red/Blue: "Adaptive Adversary"

- **Round 1:** Red team deploys initial Malmon (30 minutes)
- **Round 2:** Blue team responds, Red team adapts (30 minutes)
- **Round 3:** Escalated tactics based on defensive effectiveness (30 minutes)
- **Debrief:** Analysis of adaptation strategies and defensive effectiveness

15.1.4.2 Multi-Organization Championships

Coordinated Response Competitions:

- Teams representing different organizations must coordinate
- Information sharing protocols under competitive pressure
- Balancing organizational interests with collective security
- Simulating real-world industry cooperation during major incidents

Championship Format: "Global Response"

- **Setup:** International incident affecting multiple countries/organizations
- **Teams:** Each represents different organization (government, private sector, international)
- **Challenge:** Balance individual organizational response with collective coordination
- **Scoring:** Both individual effectiveness and collaborative success

15.1.5 Scenario Design Principles

15.1.5.1 Authentic Complexity

Real-World Fidelity:

- Based on actual incident patterns and threat actor behaviors
- Include authentic stakeholder pressures and constraints
- Incorporate real regulatory and business requirements
- Use actual threat intelligence and attack techniques

Managed Complexity:

- Complex enough to challenge advanced teams
- Structured to maintain learning focus
- Scalable based on team capability and available time
- Clear learning objectives despite scenario complexity

15.1.5.2 Adaptive Facilitation

Dynamic Scenario Adjustment:

- Modify complexity based on team performance
- Introduce additional challenges if teams handle initial scenario easily

- Provide additional support if complexity overwhelms learning
- Balance challenge with achievable success

Multiple Success Paths:

- No single "correct" solution to scenario challenges
- Reward creative and innovative approaches
- Recognize different valid strategic choices
- Focus on learning process rather than predetermined outcomes

15.1.6 Facilitation Techniques for Advanced Scenarios

15.1.6.1 Managing Increased Complexity

Information Management:

- Provide information gradually to prevent overwhelming teams
- Use multiple information sources (reports, briefings, intelligence updates)
- Allow teams to request specific information based on their investigation priorities
- Balance realism with manageable information flow

Stakeholder Simulation:

- Introduce external pressures through simulated stakeholder demands
- Create tension between different organizational priorities
- Simulate media pressure and public scrutiny
- Include regulatory and legal considerations in decision-making

Time Management:

- Use realistic time pressure without preventing learning
- Allow for breaks and team consultation during complex scenarios
- Extend session time when warranted by scenario complexity
- Balance urgency with opportunity for reflection and learning

15.1.6.2 Supporting Advanced Learning

Strategic Thinking Development:

- Ask questions that require long-term thinking and planning
- Encourage teams to consider second and third-order effects
- Guide discussion of strategic trade-offs and resource allocation
- Help teams balance immediate response with long-term resilience

Cross-Functional Coordination:

- Simulate coordination with departments outside cybersecurity
- Include business stakeholders, legal teams, and executive leadership
- Practice communication with external agencies and partners
- Develop skills in translating technical findings into business language

Innovation Encouragement:

- Reward creative approaches to complex problems
- Encourage teams to develop novel techniques and strategies
- Support experimentation with different response approaches
- Celebrate learning from failed approaches and adaptive thinking

15.1.7 Assessment and Learning Objectives

15.1.7.1 Advanced Competency Indicators

Strategic Leadership:

- Ability to coordinate complex, multi-team responses
- Strategic thinking about long-term implications and recovery
- Effective communication with diverse stakeholders under pressure
- Innovation in response techniques and coordination approaches

Advanced Technical Integration:

- Understanding of complex attack techniques and defense strategies
- Ability to coordinate technical and business response elements
- Integration of threat intelligence with tactical response decisions
- Advanced threat hunting and analysis capabilities

Organizational Resilience:

- Development of organizational learning and improvement capabilities
- Integration of incident response with business continuity planning
- Building relationships and processes that support ongoing security
- Contributing to industry-wide security improvement through information sharing

15.1.7.2 Reflection and Improvement

Comprehensive After-Action Reviews:

- Analysis of decision-making processes under complex conditions
- Evaluation of coordination effectiveness across teams and organizations
- Assessment of learning objectives achievement despite scenario complexity
- Identification of skills and knowledge gaps revealed by advanced challenges

Community Contribution:

- Documentation of innovative techniques discovered during advanced scenarios
- Sharing of lessons learned with broader Incident Master community
- Development of new scenario concepts based on advanced scenario experiences
- Contribution to advanced facilitator training and development

15.1.8 Building Advanced Scenario Capabilities

15.1.8.1 Facilitator Development

Advanced Facilitation Skills:

- Managing complex multi-stakeholder scenarios
- Adapting scenarios in real-time based on team performance
- Balancing realism with learning objectives in complex situations
- Supporting team learning during high-pressure, complex scenarios

Subject Matter Expertise:

- Developing deeper understanding of specific industry challenges
- Building knowledge of advanced attack techniques and threat actor behaviors
- Understanding of strategic cybersecurity planning and organizational resilience
- Knowledge of cross-organizational coordination and information sharing

15.1.8.2 Community Innovation

Scenario Development Collaboration:

- Working with industry experts to develop authentic advanced scenarios
- Testing and refining scenarios through community feedback
- Adapting scenarios for different organizational contexts and learning objectives
- Contributing to repository of advanced scenarios for community use

Research and Improvement:

- Evaluating effectiveness of advanced scenarios for learning objectives
- Researching best practices for complex scenario facilitation
- Contributing to academic and industry understanding of cybersecurity education
- Developing metrics and assessment approaches for advanced learning outcomes

Advanced scenarios represent the cutting edge of collaborative cybersecurity learning, preparing teams for the complex, high-stakes incidents they may face in their professional careers while building the strategic thinking and coordination skills necessary for cybersecurity leadership.

Chapter 16

Community Tournaments

16.1 Organizing Competitive Learning Events

Community tournaments amplify the collaborative learning power of Malware & Monsters by bringing together multiple teams, creating opportunities for knowledge sharing, healthy competition, and community building. As an Incident Master, organizing tournaments requires balancing competitive excitement with educational objectives.

16.1.1 Tournament Design Philosophy

16.1.1.1 Educational Competition

Primary Goals:

- **Accelerate Learning:** Competition pressure enhances skill development
- **Knowledge Sharing:** Teams learn from observing other approaches
- **Community Building:** Events create lasting professional relationships
- **Innovation Catalyst:** Competition drives creative problem-solving

Secondary Benefits:

- **Skill Assessment:** Teams can gauge their development progress
- **Technique Refinement:** Repeated practice improves response capabilities
- **Professional Networking:** Career advancement through community connections
- **Organizational Recognition:** Showcase cybersecurity team capabilities

16.1.1.2 Competitive Formats

16.1.2 Speed Response Tournaments

16.1.2.1 Event Structure

- **Timeline:** 2-4 hours for local events, full day for regional championships
- **Team Size:** 4-6 participants per team
- **Number of Teams:** 4-12 teams for optimal interaction
- **Scenario Complexity:** Intermediate level Malmons for consistent challenge

16.1.2.2 Competition Rules

Scenario Selection:

- All teams face identical Malmon and organizational context
- Intermediate complexity ( ) for fair comparison
- Well-tested scenarios with predictable flow and clear success criteria

Timing Structure:

- **Setup:** 15 minutes for team formation and rules explanation
- **Session Time:** 60 minutes compressed
- **Scoring Period:** 10 minutes for completion assessment
- **Debrief:** 15 minutes sharing insights across teams

Success Criteria:

- **Malmon Identification:** Correct type and threat assessment (25 points)
- **Team Coordination:** Effective role specialization and collaboration (25 points)
- **Response Strategy:** Appropriate containment approach for Malmon type (25 points)
- **Time Efficiency:** Bonus points for early completion without sacrificing quality (25 points)
- **Network Security Status:** Final organizational health score (bonus multiplier)

16.1.2.3 Facilitation Approach

Pre-Competition Preparation:

- **Scenario Testing:** Run through with practice team to identify timing issues
- **Scoring Clarity:** Ensure all teams understand evaluation criteria
- **Judge Training:** Brief evaluators on consistent assessment methods
- **Backup Plans:** Prepare for technical difficulties or timing problems

During Competition Management:

- **Simultaneous Sessions:** All teams run identical scenarios concurrently
- **Observation Protocol:** Judges take minimal notes without disrupting teams
- **Time Management:** Clear warnings at 45 and 55 minute marks
- **Fair Play Monitoring:** Ensure no team has unfair advantages or information

Post-Competition Activities:

- **Rapid Scoring:** Results available within 30 minutes of completion
- **Approach Sharing:** Winning teams explain their strategies briefly
- **Innovation Recognition:** Acknowledge creative solutions regardless of speed
- **Learning Synthesis:** Facilitate discussion of lessons learned across teams

16.1.3 Perfect Response Competitions

16.1.3.1 Event Structure

Timeline: 3-6 hours for thorough analysis and strategy development **Emphasis:** Quality and completeness over speed **Challenge Level:** Advanced scenarios requiring sophisticated coordination

16.1.3.2 Competition Criteria

Perfection Standards:

- **Zero Network Degradation:** Maintain Security Status above 95 throughout session
- **Complete Analysis:** Full Malmon characterization and attribution
- **Comprehensive Strategy:** Prevention plan addressing root causes
- **Stakeholder Management:** Effective communication with all affected parties
- **Documentation Quality:** Professional incident report suitable for executive review

Evaluation Dimensions:

- **Technical Excellence:** Depth and accuracy of threat analysis (30 points)
- **Strategic Thinking:** Long-term prevention and improvement planning (25 points)
- **Coordination Mastery:** Seamless team collaboration and role integration (25 points)
- **Communication Effectiveness:** Clear stakeholder management and documentation (20 points)

16.1.3.3 Advanced Facilitation Techniques

Complexity Management:

- **Layered Scenarios:** Additional complications introduced based on team progress
- **Stakeholder Simulation:** IM plays executive, legal, or media roles requiring team interaction
- **Real-Time Intelligence:** New information provided throughout session based on team decisions
- **Resource Constraints:** Limited tools or personnel to increase realism

16.1.4 Red Team vs Blue Team Battles

16.1.4.1 Dynamic Competition Format

Structure: Two teams alternate between attacker and defender roles **Session Length:** 90-120 minutes for full attack/defense cycle **Learning Objective:** Understanding both offensive and defensive perspectives

16.1.4.2 Role Assignment

Red Team Responsibilities:

- **Attack Planning:** Design realistic attack progression using chosen Malmon
- **Execution Simulation:** Implement attack phases with IM facilitation
- **Adaptation Strategy:** Modify approach based on Blue Team defensive responses
- **Learning Documentation:** Capture insights about defensive effectiveness

Blue Team Responsibilities:

- **Detection Implementation:** Identify attack indicators and threat progression
- **Response Coordination:** Implement containment and recovery strategies
- **Adaptation Management:** Adjust approach based on Red Team evolution
- **Resilience Building:** Develop improvements to prevent future similar attacks

16.1.4.3 Facilitation Challenges

Balancing Realism with Learning:

- **Attack Constraints:** Ensure Red Team approaches remain realistic and educational
- **Defensive Capabilities:** Provide Blue Team with appropriate tools and information
- **Time Management:** Balance thorough analysis with dynamic interaction

- **Fairness Assurance:** Prevent either team from having unfair advantages

Managing Competitive Dynamics:

- **Constructive Competition:** Emphasize learning over winning
- **Knowledge Sharing:** Encourage explanation of approaches and techniques
- **Mutual Respect:** Maintain collaborative learning environment despite competition
- **Debrief Integration:** Facilitate discussion of insights from both perspectives

16.1.5 Multi-Organization Championships

16.1.5.1 Scaling Tournament Complexity

Participant Scope: Teams from multiple organizations, industries, or regions **Event Duration:** Full-day or multi-day events with various competition formats **Coordination Requirements:** Advanced planning and resource management

16.1.5.2 Event Planning Considerations

Logistical Complexity:

- **Venue Requirements:** Space for multiple simultaneous sessions
- **Technology Needs:** Reliable network, presentation capabilities, backup systems
- **Catering Coordination:** Meals and breaks that support networking
- **Material Preparation:** Sufficient supplies and backup materials for all teams

Stakeholder Management:

- **Organizational Representatives:** Coordination with participating organizations
- **Sponsor Relations:** Acknowledgment and integration of supporting organizations
- **Media Management:** Public relations and community visibility
- **Volunteer Coordination:** Additional facilitators, judges, and support staff

16.1.5.3 Advanced Competition Formats

Industry-Specific Championships:

- **Healthcare Cybersecurity Cup:** Scenarios focused on medical environment challenges
- **Financial Services Challenge:** Banking and payment system specific threats

- **Critical Infrastructure Defense:** Power, water, transportation sector scenarios
- **Government Security Olympics:** Public sector and national security focused competitions

International Competitions:

- **Cultural Adaptation:** Scenarios relevant to different regulatory and cultural contexts
- **Language Accessibility:** Translation and interpretation support
- **Time Zone Coordination:** Scheduling across global participants
- **Technology Infrastructure:** Reliable international connectivity and platform access

16.1.6 Assessment and Recognition Systems

16.1.6.1 Scoring Methodologies

Objective Measures:

- **Time to Identification:** Speed of correct Malmon type determination
- **Response Effectiveness:** Appropriateness of containment strategies for threat type
- **Network Security Maintenance:** Final organizational health status
- **Coordination Quality:** Observable teamwork and role specialization

Subjective Evaluation:

- **Innovation Recognition:** Creative approaches to novel challenges
- **Communication Excellence:** Stakeholder management and documentation quality
- **Learning Demonstration:** Evidence of skill development and knowledge sharing
- **Sportsmanship Assessment:** Collaborative behavior and community contribution

16.1.6.2 Recognition Categories

Team Awards:

- **Overall Champions:** Highest combined scores across multiple evaluation criteria
- **Speed Response Leaders:** Fastest effective containment with quality maintenance
- **Perfect Response Masters:** Highest precision and thoroughness in analysis
- **Innovation Recognition:** Most creative and effective novel approaches
- **Collaboration Excellence:** Best demonstration of team coordination and communication

Individual Recognition:

- **Role Excellence Awards:** Outstanding performance in specific incident response roles
- **Cross-Functional Leadership:** Exceptional coordination across multiple team functions
- **Technical Innovation:** Individual contributions to technique development
- **Community Building:** Outstanding support for other teams and participants

Organizational Honors:

- **Program Development:** Organizations with outstanding internal training programs
- **Community Support:** Significant contribution to community events and resources
- **Innovation Leadership:** Organizations driving advancement in collaborative learning
- **Diversity and Inclusion:** Exceptional efforts to build inclusive cybersecurity communities

16.1.7 Tournament Facilitation Best Practices

16.1.7.1 Pre-Event Preparation

Scenario Development:

- **Testing and Refinement:** Multiple practice runs with feedback incorporation
- **Difficulty Calibration:** Appropriate challenge level for expected participant experience
- **Backup Scenarios:** Alternative options for timing or technical difficulties
- **Judge Training:** Consistent evaluation criteria and application methods

Participant Communication:

- **Clear Expectations:** Rules, evaluation criteria, and event logistics
- **Preparation Guidance:** Recommended background knowledge and team formation advice
- **Technology Requirements:** Platform access, connectivity needs, backup plans
- **Schedule Communication:** Detailed timeline with breaks and networking opportunities

16.1.7.2 During Event Management

Dynamic Adaptation:

- **Real-Time Adjustment:** Modify timing or complexity based on participant progress
- **Technical Support:** Rapid response to connectivity or platform issues
- **Energy Management:** Monitor participant engagement and adjust activities
- **Fair Play Monitoring:** Ensure consistent application of rules and evaluation

Learning Enhancement:

- **Cross-Team Observation:** Opportunities for teams to learn from each other
- **Expert Commentary:** Insights from experienced practitioners and researchers
- **Technique Sharing:** Structured time for approach explanation and discussion
- **Innovation Highlighting:** Recognition of creative solutions and novel approaches

16.1.7.3 Post-Event Activities

Immediate Debrief:

- **Results Presentation:** Clear explanation of evaluation and recognition decisions
- **Approach Sharing:** Winning teams explain their strategies and techniques
- **Learning Synthesis:** Group discussion of insights and lessons learned
- **Network Building:** Structured time for professional connection and follow-up

Follow-Up Engagement:

- **Documentation Sharing:** Tournament insights and innovative approaches
- **Community Integration:** Connection of participants to ongoing learning opportunities
- **Improvement Feedback:** Participant input for future event enhancement
- **Relationship Maintenance:** Ongoing communication and collaboration support

16.1.8 Building Sustainable Tournament Programs

16.1.8.1 Community Development

Local Chapter Support:

- **Facilitator Training:** Development of local tournament organization capabilities

- **Resource Sharing:** Templates, scenarios, and best practices distribution
- **Mentorship Networks:** Connection of new organizers with experienced facilitators
- **Quality Assurance:** Standards and guidelines for consistent community experiences

Regional Coordination:

- **Event Calendaring:** Coordination to avoid conflicts and enable progression
- **Resource Pooling:** Shared development of scenarios and evaluation materials
- **Judge Training:** Consistent evaluation standards across multiple events
- **Champion Development:** Pathways for advancement from local to regional to national competition

16.1.8.2 Long-Term Sustainability

Financial Models:

- **Sponsorship Development:** Corporate and organizational support for events
- **Participant Fees:** Reasonable cost structures that support event quality
- **Volunteer Recognition:** Acknowledgment and development opportunities for community contributors
- **Resource Efficiency:** Streamlined processes that minimize organizer burden

Innovation and Growth:

- **Format Evolution:** Continuous improvement based on participant feedback and learning research
- **Technology Integration:** Platform development and enhancement for better participant experience
- **Research Collaboration:** Partnership with academic institutions for effectiveness studies
- **Global Expansion:** Sustainable models for international growth and cultural adaptation

16.1.9 Educational Impact Measurement

16.1.9.1 Learning Assessment

Skill Development Tracking:

- **Pre/Post Tournament Assessment:** Measurement of participant capability improvement
- **Longitudinal Studies:** Career advancement and professional development correlation

- **Competency Validation:** External recognition of skills developed through competition
- **Knowledge Retention:** Long-term application of tournament learning in professional settings

Community Impact Evaluation:

- **Network Formation:** Professional relationship development and collaboration increase
- **Knowledge Dissemination:** Spread of techniques and approaches across organizations
- **Innovation Acceleration:** Rate of technique development and community contribution
- **Industry Advancement:** Contribution to overall cybersecurity capability improvement

16.1.9.2 Continuous Improvement

Feedback Integration:

- **Participant Surveys:** Comprehensive evaluation of experience and learning outcomes
- **Facilitator Development:** Training and support based on event management experience
- **Format Refinement:** Ongoing improvement of competition structures and evaluation methods
- **Community Evolution:** Adaptation to changing cybersecurity landscape and learning needs

Research and Development:

- **Academic Partnership:** Collaboration with educational institutions for effectiveness research
- **Industry Validation:** Corporate feedback on skill development and professional application
- **Innovation Documentation:** Capture and sharing of community-developed improvements
- **Global Best Practices:** International exchange of successful tournament models and approaches

Tournament organization provides Incident Masters with opportunities to build community, accelerate learning, and contribute to the advancement of collaborative cybersecurity education. Through thoughtful design and careful facilitation, tournaments create lasting value for participants, organizations, and the broader cybersecurity community.

Chapter 17

Malmon Reference

Note: This PDF version includes basic malmon cards only. For detailed facilitation guidance, visit the online IM Handbook.

17.1 Current Malmons

17.2 Legacy Malmons

Historical threats that shaped cybersecurity - adapted for modern learning.

Chapter 18

Quick Reference

18.1 Emergency Protocols

Chapter 19

Emergency Facilitation Protocols

19.1 When Teams Get Stuck

19.1.1 The "Analysis Paralysis" Problem

Symptoms: Team spends excessive time debating technical details without making progress
Emergency Response:

1. **Redirect to decisions:** *"That's great analysis - what does this tell us about our next steps?"*
2. **Time pressure:** *"We have X minutes left in this phase - what's our priority?"*
3. **Role focus:** *"How does this technical detail help each role contribute?"*
4. **Action orientation:** *"What would you do with this information in a real incident?"*

19.1.2 The "Knowledge Vacuum" Problem

Symptoms: Team lacks expertise in the technical area being explored
Emergency Response:

1. **Common sense pivot:** *"Let's step back from technical details - what would common sense suggest?"*
2. **Analogy approach:** *"How is this similar to something you do understand?"*
3. **Role-based thinking:** *"From your role's perspective, what would concern you most?"*

4. **Multiple choice:** *"Which of these options seems most logical: A, B, or C?"*

19.1.3 The "Dominant Player" Problem

Symptoms: One person providing all answers while others stay silent
Emergency Response:

1. **Acknowledge and redirect:** *"Thanks [Name] - let's hear other perspectives on this"*
2. **Role-specific questions:** *"[Other Name], from the [Role] perspective, what would you add?"*
3. **Build on contributions:** *"Can someone expand on what [Name] just shared?"*
4. **Divide the work:** *"[Name], focus on X while [Other] explores Y"*

19.2 When Sessions Lose Energy

19.2.1 The "Low Engagement" Crisis

Symptoms: Short responses, minimal discussion, checking phones
Emergency Response:

1. **Raise stakes:** *"What's the worst-case scenario if we don't solve this?"*
2. **Personal investment:** *"Who would be affected if this attack succeeds?"*
3. **Competition element:** *"Other teams have solved this faster - what are we missing?"*
4. **Break and regroup:** Brief 2-minute stretch/discussion break

19.2.2 The "Technical Overwhelm" Problem

Symptoms: Non-technical participants withdrawing from discussion
Emergency Response:

1. **Refocus on roles:** *"Every role has something valuable to contribute here"*
2. **Business impact:** *"What would this mean for the organization?"*
3. **Human factors:** *"How would users react to this situation?"*
4. **Communication focus:** *"How would you explain this to management?"*

19.3 When Conflicts Arise

19.3.1 The "Approach Disagreement" Situation

Symptoms: Team members advocating for conflicting response strategies
Emergency Response:

1. **Acknowledge all perspectives:** *"Both approaches have merit - let's explore each"*
2. **Criteria discussion:** *"What factors should guide our decision?"*
3. **Risk assessment:** *"What could go wrong with each approach?"*
4. **Hybrid solutions:** *"How might we combine elements of both ideas?"*

19.3.2 The "Expertise Challenge" Problem

Symptoms: Participants questioning each other's technical knowledge
Emergency Response:

1. **Redirect to learning:** *"This is a great discussion - what can we learn from both perspectives?"*
2. **Focus on scenario:** *"In our specific situation, which approach fits better?"*
3. **Collaborative synthesis:** *"How do we build on everyone's insights?"*
4. **Real-world reality:** *"In actual incidents, teams often have different views - how do you resolve this?"*

19.4 Technical Difficulties

19.4.1 When Game Mechanics Break Down

Symptoms: Dice rolls producing unrealistic results, type effectiveness confusion
Emergency Response:

1. **Story over mechanics:** *"What would realistically happen in this situation?"*
2. **Group consensus:** *"What does the team think makes most sense?"*
3. **Learning focus:** *"The important thing is what we're learning, not the dice"*
4. **Simplify:** Reduce mechanical complexity and focus on collaboration

19.4.2 When Technology Fails

Symptoms: Presentation equipment, network issues, digital materials unavailable
Emergency Response:

1. **Paper backup:** Have printed key materials (type chart, role descriptions)
2. **Analog approach:** Use whiteboard/flipchart for tracking
3. **Participant devices:** Ask participants to access materials on phones/laptops
4. **Pure discussion:** Run session as structured discussion without digital aids

19.5 Time Management Crises

19.5.1 When Phases Run Long

Symptoms: Discovery or Investigation phases consuming too much time
Emergency Response:

1. **Rapid summary:** *"Let's quickly summarize what we know so far"*
2. **Key decisions:** *"What's the most important decision we need to make?"*
3. **Time boxing:** *"We have 5 minutes to reach a conclusion"*
4. **Carry forward:** *"We'll continue this investigation in the next phase"*

19.5.2 When Teams Move Too Fast

Symptoms: Teams rushing through phases without adequate discussion
Emergency Response:

1. **Depth questions:** *"What might we be missing if we move too quickly?"*
2. **Consequence exploration:** *"What happens if we're wrong about this?"*
3. **Role consultation:** *"Has everyone contributed their perspective?"*
4. **Learning check:** *"What have we learned that we can apply elsewhere?"*

19.6 Participant Management

19.6.1 The "Expert Overwhelm" Problem

Symptoms: Participants with deep expertise getting frustrated with simplified scenarios
Emergency Response:

1. **Complexity acknowledgment:** *"In real situations, this would involve X, Y, Z - for learning purposes we're focusing on A"*
2. **Mentorship role:** *"Help others understand the concepts you're familiar with"*
3. **Advanced challenges:** *"What additional complications might we face?"*
4. **Teaching moments:** *"Share a real-world example of how this plays out"*

19.6.2 The "Novice Anxiety" Problem

Symptoms: New participants feeling intimidated or unable to contribute
Emergency Response:

1. **Value affirmation:** *"Your perspective as someone new to this is really valuable"*
2. **Common sense validation:** *"What does your intuition tell you about this?"*
3. **Question encouragement:** *"What would you want to know if this happened at your workplace?"*

4. **Role focus:** *"Your role brings a unique viewpoint that we need"*

19.7 Session Recovery Strategies

19.7.1 The "Complete Restart" Protocol

When to use: Session has fundamentally broken down, multiple problems occurring
Steps:

1. **Pause and acknowledge:** *"Let's take a step back and regroup"*
2. **Learning focus:** *"What have we discovered so far that's valuable?"*
3. **Simplified restart:** Return to basic scenario with reduced complexity
4. **Success orientation:** Focus on collaboration and learning rather than game completion

19.7.2 The "Pivot to Discussion" Protocol

When to use: Game mechanics aren't working but group engagement is strong
Steps:

1. **Transition announcement:** *"Let's shift to a structured discussion about this scenario"*
2. **Question framework:** Use discovery/investigation/response questions without mechanics
3. **Experience sharing:** *"Who has dealt with similar situations?"*
4. **Learning synthesis:** *"What would you do differently in a real incident?"*

19.8 Post-Crisis Learning

19.8.1 Immediate Recovery

- **Acknowledge the challenge:** Don't pretend problems didn't happen
- **Focus on learning:** What did we learn despite the difficulties?
- **Participant feedback:** Quick check on how people are feeling
- **Adjust expectations:** Set realistic goals for remainder of session

19.8.2 Session Debrief Enhancement

When sessions have significant challenges:

- **Process discussion:** What made facilitation difficult?
- **Adaptation strategies:** How did we overcome obstacles?
- **Improvement ideas:** What would work better next time?
- **Resilience celebration:** How did the team handle adversity?

19.8.3 Facilitator Self-Care

- **Normalize difficulties:** Even experienced facilitators face challenges
- **Learning mindset:** Every difficult session teaches valuable lessons
- **Community support:** Share experiences with other facilitators
- **Skill development:** Identify specific areas for improvement

19.9 Prevention Strategies

19.9.1 Pre-Session Risk Assessment

- **Group composition:** Mix of experience levels and personalities
- **Technical readiness:** Equipment, materials, backup plans
- **Time management:** Realistic pacing for group size and complexity
- **Energy management:** Room setup, break planning, engagement strategies

19.9.2 Early Warning Systems

- **Engagement monitoring:** Watch for withdrawal, frustration, confusion
- **Time tracking:** Keep phases moving without rushing learning
- **Energy assessment:** Adjust activities based on group energy levels
- **Conflict detection:** Address disagreements before they escalate

19.9.3 Adaptive Facilitation

- **Multiple approaches:** Be ready to change tactics based on group needs
- **Flexible objectives:** Prioritize learning over perfect game execution
- **Participant empowerment:** Let group expertise drive content when possible
- **Recovery preparation:** Always have simplified backup approaches ready

Remember: The goal is collaborative learning, not perfect session execution. When challenges arise, focus on maintaining the learning environment and participant engagement rather than following the planned structure exactly.

19.10 Role Cards Reference

Chapter 20

Role Cards Reference for Incident Masters

This appendix provides complete role cards for all six incident response roles. Use these during facilitation to understand each role's strengths, focus areas, modifiers, and roleplay guidance. These are identical to the cards in the Players Handbook for easy cross-reference.

20.1 Complete Role Cards Overview

20.1.1 Detective (Cyber Sleuth)

20.1.2 Protector (Digital Guardian)

20.1.3 Tracker (Network Analyst)

20.1.4 Communicator (Stakeholder Liaison)

20.1.5 Crisis Manager (Incident Commander)

20.1.6 Threat Hunter (Proactive Defender)

20.2 IM Quick Reference: Role Strengths & Modifiers

20.2.1 Role Modifier Quick Reference Table

Role	+3 Bonus	+2 Bonus	+1 Bonus
Detective	Forensic Analysis	Pattern Recognition	Documentation
Protector	Containment	Security Architecture	Business Continuity
Tracker	Network Analysis	Data Tracking	Infrastructure Mapping
Communicator	Stakeholder Management	Crisis Communication	Compliance
Crisis Manager	Coordination	Strategic Planning	Escalation Management
Threat Hunter	Threat Detection	Intelligence Analysis	Attack Prediction

20.2.2 Role Strengths at a Glance

- **Detective:** Pattern recognition, evidence analysis, timeline construction
- **Protector:** Containment, security architecture, business continuity

- **Tracker:** Network analysis, data flow tracking, infrastructure mapping
- **Communicator:** Stakeholder management, crisis communication, compliance
- **Crisis Manager:** Coordination, strategic planning, resource allocation
- **Threat Hunter:** Advanced detection, intelligence analysis, attack prediction

20.3 Facilitation Tips by Role

20.3.1 Encouraging Balanced Participation

When Roles Dominate:

- **Detective dominating:** *"Great analysis - how might other roles use this evidence?"*
- **Protector rushing:** *"What do other roles need to know before we contain?"*
- **Tracker getting technical:** *"How does this network data impact our response strategy?"*
- **Communicator over-managing:** *"What do the technical roles need to investigate first?"*
- **Crisis Manager micro-managing:** *"Let's hear the specialist perspectives before coordinating."*
- **Threat Hunter rabbit-holing:** *"What immediate threats need the team's attention now?"*

When Roles Withdraw:

- **Detective quiet:** *"What patterns or anomalies stand out to you here?"*
- **Protector passive:** *"How would you protect our critical systems right now?"*
- **Tracker disconnected:** *"What network activity concerns you most?"*
- **Communicator silent:** *"Who needs to know about these developments?"*
- **Crisis Manager absent:** *"How should we prioritize these response activities?"*
- **Threat Hunter unfocused:** *"What aren't we seeing that we should be looking for?"*

20.3.2 Role-Specific Questions to Ask

Detective Activation:

- *"What story do these clues tell you?"*
- *"What patterns does this remind you of?"*
- *"How would you build a timeline of this attack?"*

Protector Activation:

- *"What's your biggest security concern right now?"*
- *"How do we stop this from spreading?"*
- *"What systems need immediate protection?"*

Tracker Activation:

- *"Where is this data going?"*
- *"What network activity looks suspicious?"*
- *"How is this threat moving through our systems?"*

Communicator Activation:

- *"Who needs to know about this development?"*
- *"How would you explain this to executive leadership?"*
- *"What are the business implications?"*

Crisis Manager Activation:

- *"How should we prioritize these response activities?"*
- *"What resources do we need to coordinate?"*
- *"What's our overall strategy here?"*

Threat Hunter Activation:

- *"What else might be hiding that we haven't found?"*
- *"What would a sophisticated attacker do next?"*
- *"What intelligence can help us get ahead of this threat?"*

20.4 Team Composition Guidelines

20.4.1 For 4-Player Teams

Essential Core:

- Detective (investigation and analysis)
- Protector (containment and security)
- Communicator (stakeholder management)
- Crisis Manager (coordination)

Alternative Configurations:

- Replace Crisis Manager with Tracker for network-heavy scenarios
- Replace Crisis Manager with Threat Hunter for sophisticated threats

20.4.2 For 5-Player Teams

Recommended Additions:

- Core four + Tracker for network-focused incidents
- Core four + Threat Hunter for APT scenarios
- Allow team to choose based on interests and scenario type

20.4.3 For 6-Player Teams

Full Coverage: All six roles provide maximum perspective diversity and comprehensive incident response coverage.

20.4.4 For Teams with Role Overlap

Managing Multiple Players in Same Role:

- Assign specialized focus areas (junior/senior, different systems)
- Create complementary responsibilities (analysis vs. communication)
- Use geographical or departmental divisions
- Emphasize different aspects of the role's capabilities

This reference ensures IMs can quickly understand each role's mechanical benefits, behavioral tendencies, and optimal activation strategies for balanced, engaging facilitation.