Threat hunting and Incident response tactics and procedures have evolved rapidly over the past several years. You can no longer afford to use antiquated incident response and threat hunting techniques that fail to properly identify compromised systems. The key is to constantly look for attacks that get past security systems, and to catch intrusions in progress, rather than after attackers have completed their objectives and done worse damage to the organization.

Incident Response Training

Incident Response Team

Part I: Preparing for the Inevitable Incident

In this part, our goal is to provide you with high-level incident response perspective and guidance that are useful to build an IR team and prepare for incident response. We begin by sharing our experiences from two real-world incidents. Then we discuss incident response management, including defining the IR process, investigation lifecycle, remediation, information tracking, and what you need to build a successful IR team.
Finally, we cover steps you can take to prepare your infrastructure, your organization, and the IR team.

Module 1: Real-World Incidents	What Constitutes an Incident? What Is Incident Response? Why Should You Care About Incident Response? Case Studies Case Study #1: Show Me the Money Case Study #2: Certificate of Authenticity Concept of the Attack Lifecycle
Module 2: IR Management Handbook	What Is a Computer Security Incident? What Are the Goals of Incident Response? Who Is Involved in the IR Process? Finding IR Talent The Incident Response Process Initial Response Investigation Remediation Tracking of Significant Investigative Information Reporting
Module 3: Pre-Incident Preparation	Preparing the Organization for Incident Response Identifying Risk Policies That Promote a Successful IR Working with Outsourced IT Thoughts on Global Infrastructure Issues Educating Users on Host-Based Security Preparing the IR Team Defining the Mission Communication Procedures Deliverables Resources for the IR Team Preparing the Infrastructure for Incident Response Computing Device Configuration Network Configuration

Part II: Incident Detection and Characterization

The actions you take when you first detect an incident will have great consequence on the outcome of the investigation. Part II covers investigative tips and techniques that contribute to a successful incident response. We discuss checklists, case notes, development of leads, creating indicators of compromise, and determining the scope of the incident.

Module 4: Getting the Investigation Started on the Right Foot	Collecting Initial Facts Checklists Maintenance of Case Notes Building an Attack Timeline Understanding Investigative Priorities What Are Elements of Proof? Setting Expectations with Management
Module 5: Initial Development of Leads	Defining Leads of Value Acting on Leads Turning Leads into Indicators The Lifecycle of Indicator Generation Resolving Internal Leads Resolving External Leads
Module 6: Discovering the Scope of the Incident	What Should I Do? Examining Initial Data Gathering and Reviewing Preliminary Evidence Determining a Course of Action Customer Data Loss Scenario Customer Data Loss—Scoping Gone Wrong Automated Clearing House (ACH) Fraud Scenario ACH Fraud—Scoping Gone Wrong

Part III: Data Collection

Each incident you work on will require the collection and preservation of information. In this part, we discuss collecting data from both running and offline systems, the network, and from enterprise services. Data sources include memory, hard drives, network packet captures, and log files.

Module 7: Live Data Collection	When to Perform a Live Response Selecting a Live Response Tool What to Collect Collection Best Practices Live Data Collection on Microsoft Windows Systems Prebuilt Toolkits Do It Yourself Memory Collection Live Data Collection on Unix-Based Systems Live Response Toolkits Memory Collection
Module 8: Forensic Duplication	Forensic Image Formats Complete Disk Image Partition Image Logical Image Image Integrity Traditional Duplication Hardware Write Blockers Image Creation Tools Live System Duplication Duplication of Enterprise Assets Duplication of Virtual Machines
Module 9: Network Evidence	The Case for Network Monitoring Types of Network Monitoring Event-Based Alert Monitoring Header and Full Packet Logging Statistical Modeling Setting Up a Network Monitoring System Choosing Appropriate Hardware Installation of a Pre-built Distribution Deploying the Network Sensor Evaluating Your Network Monitor Network Data Analysis Data Theft Scenario Webshell Reconnaissance Scenario Other Network Analysis Tools Collect Logs Generated from Network Events

Module 10: Enterprise Services	Network Infrastructure Services DHCP DNS Enterprise Management Applications Antivirus Software, Antivirus Quarantine Web Servers Apache HTTP Server Microsoft Internet Information Services (IIS) Database Servers Microsoft SQL MySQL Oracle

Part IV: Data Analysis

After you collect data, the next step is to perform analysis. In this part, we discuss general analysis approaches and then dive into specific operating systems. We cover Microsoft Windows and Apple OS X. We also include a chapter on malware triage, primarily focusing on the Windows platform. Lastly, we discuss report writing and provide a sample report template.

Module 11: Analysis Methodology	Define Objectives Know Your Data Where Is Data Stored? What's Available? Access Your Data Analyze Your Data Outline an Approach Select Methods Evaluate Results
Module 12: Investigating Windows Systems	NTFS and File System Analysis The Master File Table INDX Attributes Change Logs Volume Shadow Copies File System Redirector Prefetch Event Logs Scheduled Tasks Creating Tasks with the "at" Command Creating Tasks with the schtasks Command The Windows Registry Registry Analysis Tools Other Artifacts of Interactive Sessions LNK Files Jump Lists The Recycle Bin Memory Forensics Memory Analysis Alternative Persistence Mechanisms Startup Folders Recurring Tasks System Binary Modification DLL Load-Order Hijacking Review: Answering Common Investigative Questions
Module 13: Investigating Applications	What Is Application Data? Where Is Application Data Stored? Windows

	OS X Linux General Investigation Methods Web Browsers Internet Explorer Google Chrome Mozilla Firefox E-Mail Clients Web E-Mail Microsoft Outlook for Windows Apple Mail Microsoft Outlook for Mac Instant Message Clients
Module 14: Malware Triage	Malware Handling Safety Documentation Distribution Accessing Malicious Sites Triage Environment Setting Up a Virtual Environment Static Analysis What Is That File? Portable Executable Files Dynamic Analysis Automated Dynamic Analysis: Sandboxes Manual Dynamic Analysis
Module 15: Report Writing	Why Write Reports? Reporting Standards Report Style and Formatting Report Content and Organization Quality Assurance

Part V: Remediation

Remediation is the end goal of any incident response—returning the organization back to a normal state. In this part, we introduce remediation concepts, including a seven-step remediation process. Then we apply those concepts to one of the real-world scenarios from Chapter 1 as part of a remediation case study.

Module 16: Remediation Introduction	Basic Concepts Remediation Pre-Checks Form the Remediation Team When to Create the Remediation Team Assigning a Remediation Owner Members of the Remediation Team Determine the Timing of the Remediation Develop and Implement Remediation Posturing Actions Implications of Alerting the Attacker Develop and Implement Incident Containment Actions Develop the Eradication Action Plan Determine Eradication Event Timing and Execute Eradication Plan Develop Strategic Recommendations Document the Lessons Learned Putting It All Together Common Mistakes That Lead to Remediation Failure
Module 17: Remediation Case Study	Remediation Plan for Case Study #1: Show Me the Money Select the Team Determine Remediation Timing Contain the Incident Posture the Environment Eradicate the Attacker Set the Strategic Direction

Notes

- There'll be slides for the covered modules
- All attendance should bring their own laptop as there'll be lots of hands-on exercises during the training.