Syllabus: 301 Enterprise DFIR

Live Workshop

2-Day Live Workshop Provided by Blue Cape Security, LLC

Instructor: Markus Schober Founder, Blue Cape Security

Description

This two-day intensive workshop is designed to immerse participants in a hands-on DFIR (Digital Forensics and Incident Response) investigation of a realistic multi-system ransomware attack. Beginning with essential DFIR concepts and an overview of the investigation scenario, attendees will delve into effective incident response methodologies through a comprehensive, end-to-end DFIR investigation.

Participants will engage in various aspects of the initial triage using SIEM, threat hunting tools, and data collection techniques. These processes will facilitate the detailed examination and analysis of forensic artifacts. The digital forensics segment will provide in-depth training in email and web browser analysis while uncovering attack techniques commonly observed in real-world ransomware cases. Advanced log and memory analysis, along with the creation of a super timeline, will further equip participants with effective and advanced incident analysis skills.

By the end of the workshop, attendees will have gained practical expertise to manage and resolve enterprise-level security breaches with confidence, ready to handle real-world incidents effectively.

Requirements

- Stable internet connection and RDP client required to access the lab environment.
- Dedicated, cloud based lab environment will be provided for each student.
- Basic understanding of IT security and digital forensic concepts.
- Familiarity with virtualization and command line terminals.

Audience

- This workshop is designed for intermediate-level security professionals who are involved in various roles related to SOC monitoring, incident response, forensics, and IT security within an enterprise environment.
- Roles include, but is not limited to: SOC analysts, DFIR professionals, Threat Hunters, IT administrators, System engineers, IT managers, Red Teamers, etc.

Course Agenda

DFIR Overview and Methodology	• **DFIR Fundamentals and Processes**: Introduction to key concepts and standard processes in Digital Forensics and Incident Response. • **Tools and Best Practices**: Overview of essential tools and industry best practices for effective DFIR.
Anatomy of Ransomware Attacks	• Current Trends and Threat Landscape: Insights into the latest ransomware trends and the cyber threat landscape. • Lifecycle of Ransomware Attacks: Step-by-step examination of how ransomware attacks unfold. • Access Broker Model: Understanding the role of access brokers in ransomware operations. • Common Tactics and Techniques: Identification of the typical tactics and techniques used in ransomware attacks.
Case Introduction	• Ransomware Case Scenario: Introduction to the ransomware case study. • Initial Alert and Information: Overview of the initial indicators and information received.
SIEM Log Analysis	• Splunk and Event Logs: Introduction to using Splunk for event log analysis. • Detecting Malicious Activity: Identifying malicious files and events such as command-and-control traffic, process executions, PowerShell payloads, scheduled tasks, and more. • Incident Scoping: Determining the extent of the incident. • Malicious Network Traffic: Identification and analysis of suspicious network activity.

Threat Hunting and Analysis	• Remote Forensics with Velociraptor: Conducting remote forensic analysis and threat hunting at scale. • Evidence Collection**:** Establishing evidence of compromise across multiple systems.
Data Collection	• Data Collection Techniques**:** Applying various methods to collect live response data.

Digital Forensics	• Memory and Disk Artifact Analysis: Examination of key forensic artifacts from memory and disk.
	• Email and Web Browser Artifacts: Analyzing email and browser data for signs of compromise.
	• Ransomware Tools and Malware: Investigation of ransomware tools and associated malware.
	• Attack Techniques Identification: Recognizing and analyzing attack techniques, including:
	  o Payload delivery and initial access
	  o Persistence mechanisms
	  o Privilege escalation
	  o Reconnaissance and discovery
	  o Defense evasion
	  o Credential access
	  o Lateral movement
	  o Data exfiltration
	  o Ransomware execution

Advanced Analysis Techniques	• Malware Detection with Yara**:** Using Yara rules for identifying malware. • Log Analysis with Sigma**:** Employing Sigma rules for log analysis. • Rapid Event Log Analysis**:** Techniques for quickly analyzing event logs including logon events and timelines. • Super Timeline**:** Generating and analyzing comprehensive timelines with Plaso and Timesketch.
Ransomware and Extortion	• Aftermath of Ransomware Attacks**:** Understanding the consequences and impact of ransomware incidents. • Extortion Schemes and Tactics**:** Learning about the extortion techniques used by attackers.