Training Course on Digital Forensics and Incident Response Orchestration with SOAR Platforms

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's interconnected world, the sophistication and frequency of cyber threats are escalating at an unprecedented pace. Organizations face a constant barrage of advanced persistent threats (APTs), ransomware attacks, and insider threats, making robust **Digital Forensics and Incident Response (DFIR)** capabilities paramount. Training Course on Digital Forensics and Incident Response Orchestration with SOAR Platforms delves into the critical integration of DFIR with cutting-edge **Security Orchestration, Automation, and Response (SOAR)** platforms, empowering cybersecurity professionals to dramatically improve their **threat detection**, **incident containment**, and **recovery strategies**. Participants will gain hands-on expertise in leveraging automation and orchestration to streamline complex workflows, reduce **mean time to detect (MTTD)** and **mean time to respond (MTTR)**, and build a more resilient **cybersecurity posture**.

The course emphasizes practical, **real-world scenarios** and **case studies**, ensuring that participants not only grasp theoretical concepts but also develop actionable skills. We will explore the entire **incident response lifecycle**, from proactive **threat hunting** and **vulnerability management** to meticulous **digital evidence collection**, **malware analysis**, and **post-incident reporting**. By mastering the power of SOAR, attendees will learn to automate repetitive tasks, orchestrate disparate security tools, and enhance **Security Operations Center (SOC)** efficiency, ultimately transforming reactive incident handling into a proactive, intelligent, and **scalable security operation**. This training is essential for any organization seeking to modernize its cybersecurity defenses and effectively combat evolving cyber adversaries.

Programme Curriculum

Training Course on Digital Forensics and Incident Response Orchestration with SOAR Platforms

Introduction

In today's interconnected world, the sophistication and frequency of cyber threats are escalating at an unprecedented pace. Organizations face a constant barrage of advanced persistent threats (APTs), ransomware attacks, and insider threats, making robust **Digital Forensics and Incident Response (DFIR)** capabilities paramount. Training Course on Digital Forensics and Incident Response Orchestration with SOAR Platforms delves into the critical integration of DFIR with cutting-edge **Security Orchestration, Automation, and Response (SOAR)** platforms, empowering cybersecurity professionals to dramatically improve their **threat detection**, **incident containment**, and **recovery strategies**. Participants will gain hands-on expertise in leveraging automation and orchestration to streamline complex workflows, reduce **mean time to detect (MTTD)** and **mean time to respond (MTTR)**, and build a more resilient **cybersecurity posture**.

The course emphasizes practical, **real-world scenarios** and **case studies**, ensuring that participants not only grasp theoretical concepts but also develop actionable skills. We will explore the entire **incident response lifecycle**, from proactive **threat hunting** and **vulnerability management** to meticulous **digital evidence collection**, **malware analysis**, and **post-incident reporting**. By mastering the power of SOAR, attendees will learn to automate repetitive tasks, orchestrate disparate security tools, and enhance **Security Operations Center (SOC)** efficiency, ultimately transforming reactive incident handling into a proactive, intelligent, and **scalable security operation**. This training is essential for any organization seeking to modernize its cybersecurity defenses and effectively combat evolving cyber adversaries.

Course Duration

5 days

Course Objectives

1. Master the Incident Response Lifecycle and its integration with Digital Forensics methodologies.
2. Implement robust Threat Intelligence mechanisms for proactive threat hunting and early detection.
3. Utilize SOAR Platforms to orchestrate and automate complex incident response playbooks.
4. Conduct advanced Digital Forensics across diverse platforms, including Cloud Forensics and IoT Forensics.
5. Perform comprehensive Malware Analysis (static and dynamic) to understand attack vectors and indicators of compromise (IOCs).
6. Develop effective Incident Containment and Eradication strategies leveraging SOAR automation.
7. Manage and preserve Digital Evidence according to legal and forensic standards, ensuring chain of custody.
8. Analyze Network Traffic and Log Data for suspicious activities and attack pattern recognition .
9. Automate Alert Triage and Incident Prioritization to reduce alert fatigue and focus on critical threats.
10. Integrate diverse Security Tools with SOAR for a unified security ecosystem.
11. Conduct Post-Incident Analysis and generate actionable Lessons Learned for continuous improvement.
12. Develop and customize SOAR Playbooks for various cyberattack scenarios, including ransomware response and data breach remediation.
13. Enhance overall Security Operations Center (SOC) efficiency and scalability through SOAR adoption.

Organizational Benefits

- Significantly reduce Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) through automation and orchestration.
- Proactive threat detection and rapid containment minimize the impact of cyber incidents.
- Automate repetitive tasks, freeing up security analysts for more complex, strategic work.
- Intelligent alert triage and prioritization allow security teams to focus on high-fidelity threats.
- Enforce consistent and repeatable incident response processes through automated playbooks.
- Optimize the use of existing security tools and personnel by integrating them via SOAR.
- Automated data collection and evidence preservation aid in meeting regulatory requirements and generating comprehensive incident reports.
- Leverage threat intelligence and automated responses to prevent future attacks.

Target Audience

1. Security Operations Center (SOC) Analysts.
2. Incident Responderss.
3. Digital Forensic Investigators
4. Cybersecurity Engineers.
5. IT Security Managers.
6. Threat Hunters
7. Network Administrators.
8. Security Architects.

Course Outline

Module 1: Foundations of Digital Forensics and Incident Response (DFIR)

- Introduction to the DFIR lifecycle: Preparation, Identification, Containment, Eradication, Recovery, Post-Incident.
- Key principles of digital forensics: Chain of Custody, Volatility, Anti-forensics.
- Understanding common attack vectors and the MITRE ATT&CK framework.
- Legal and ethical considerations in digital forensics and incident response.
- **Case Study:** Analyzing a simulated phishing attack leading to initial access.

Module 2: Introduction to SOAR Platforms and Automation

- Defining SOAR: Security Orchestration, Automation, and Response.
- Benefits of SOAR in modern SOC environments: efficiency, speed, consistency.
- Components of a SOAR platform: Playbooks, Connectors, Case Management.
- Understanding the difference between orchestration and automation.
- **Case Study:** Automating the initial triage of a suspicious email alert using a SOAR playbook.

Module 3: Digital Evidence Collection and Preservation

- Techniques for acquiring volatile and non-volatile digital evidence.
- Forensic imaging and data carving methodologies.
- Tools and best practices for maintaining the integrity of digital evidence.
- Collecting evidence from various sources: endpoints, networks, cloud environments.
- **Case Study:** Preserving evidence from a compromised Windows server after a suspected intrusion.

Module 4: Network Forensics and Log Analysis

- Analyzing network traffic using tools like Wireshark and network flow data (NetFlow, IPFIX).
- Identifying suspicious network patterns, command and control (C2) traffic, and data exfiltration.
- Correlation of security logs from SIEM, firewalls, and intrusion detection systems (IDS/IPS).
- Utilizing log management for incident detection and investigation.
- **Case Study:** Tracing lateral movement of an attacker by analyzing firewall logs and NetFlow data.

Module 5: Endpoint Forensics and Malware Analysis

- Memory forensics techniques using Volatility Framework and other tools.
- Disk forensics: file system analysis, artifact extraction (MFT, Registry, Prefetch).
- Static and dynamic malware analysis for threat intelligence gathering.
- Identifying persistence mechanisms and anti-forensic techniques.
- **Case Study:** Analyzing memory dumps and disk images from an infected workstation to identify malware and its execution path.

Module 6: Building and Customizing SOAR Playbooks

- Designing effective incident response playbooks for various threat scenarios.
- Leveraging SOAR platform features for conditional logic, data enrichment, and integrations.
- Automating responses for common incidents: phishing, malware infections, unauthorized access.
- Testing and refining SOAR playbooks for optimal performance.
- **Case Study:** Developing a SOAR playbook for automated ransomware containment and eradication, including system isolation and backup restoration.

Module 7: Advanced Incident Response Orchestration

- Integrating SOAR with Threat Intelligence Platforms (TIPs) for enriched context.
- Orchestrating responses across multiple security domains (network, endpoint, cloud).
- Developing custom connectors and integrations for unique security tools.
- Implementing security automation for vulnerability management and compliance.
- **Case Study:** Orchestrating a large-scale data breach response involving cloud environments, multiple endpoints, and external legal counsel notification.

Module 8: Post-Incident Activities and Continuous Improvement

- Conducting post-incident reviews and "lessons learned" sessions.
- Developing comprehensive incident reports for management and legal purposes.
- Utilizing forensic findings to improve security controls and policies.
- Measuring SOAR effectiveness and identifying areas for further automation.
- **Case Study:** A post-mortem analysis of a simulated APT attack, identifying gaps in defenses and recommending improvements based on SOAR automation.

Training Methodology

This course employs a highly interactive and practical training methodology, combining theoretical instruction with extensive hands-on labs and real-world case studies.

- **Instructor-Led Sessions:** Engaging presentations and discussions led by industry experts.

- **Hands-on Labs:** Practical exercises using industry-standard digital forensics tools and a live SOAR platform environment.
- **Real-World Case Studies:** In-depth analysis of actual cyberattack scenarios to apply learned concepts.
- **Simulated Incident Response Drills:** Participants will engage in simulated incidents, acting as incident responders and forensic investigators.
- **Group Discussions and Collaborative Exercises:** Fostering knowledge sharing and problem-solving among participants.
- **Q&A Sessions:** Opportunities for participants to clarify doubts and explore specific challenges.
- **Assessments and Capstone Project:** Evaluating understanding and practical application of skills through quizzes and a comprehensive final project.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to FINESKILL TRAINING CENTER account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500
19 Oct 2026	23 Oct 2026	Physical	$1,500
26 Oct 2026	30 Oct 2026	Physical	$1,500

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com