Training Course on Incident Response Automation and Orchestration

Professional Development Training Course Outline

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

Course Introduction

In today’s evolving threat landscape, cybersecurity teams are overwhelmed with alerts and repetitive manual tasks. To combat sophisticated attacks at scale, organizations are turning to Security Orchestration, Automation, and Response (SOAR). Training Course on Incident Response Automation and Orchestration (SOAR) equips IT and cybersecurity professionals with the critical skills and tools to automate threat detection, streamline response workflows, and enhance operational efficiency across security operations centers (SOCs).

This hands-on training combines real-world case studies, practical labs, and AI-driven automation techniques to build deep technical expertise in integrating SIEMs, threat intelligence platforms, playbooks, and response workflows. Participants will learn how to build, customize, and operationalize SOAR platforms like Splunk SOAR, Palo Alto Cortex XSOAR, and IBM Resilient. From alert triage to incident containment, this course delivers the future of automated incident response.

Programme Curriculum

Training Course on Incident Response Automation and Orchestration

Introduction

In today’s evolving threat landscape, cybersecurity teams are overwhelmed with alerts and repetitive manual tasks. To combat sophisticated attacks at scale, organizations are turning to Security Orchestration, Automation, and Response (SOAR). Training Course on Incident Response Automation and Orchestration (SOAR) equips IT and cybersecurity professionals with the critical skills and tools to automate threat detection, streamline response workflows, and enhance operational efficiency across security operations centers (SOCs).

This hands-on training combines real-world case studies, practical labs, and AI-driven automation techniques to build deep technical expertise in integrating SIEMs, threat intelligence platforms, playbooks, and response workflows. Participants

will learn how to build, customize, and operationalize SOAR platforms like Splunk SOAR, Palo Alto Cortex XSOAR, and IBM Resilient. From alert triage to incident containment, this course delivers the future of automated incident response.

Course Objectives

1. Understand SOAR architecture, capabilities, and core components.
2. Design and deploy custom automated playbooks for incident response.
3. Integrate SOAR with SIEM, EDR, and threat intelligence platforms.
4. Implement AI-driven alert triage and contextual enrichment.
5. Build end-to-end workflows for phishing, malware, and insider threats.
6. Conduct root cause analysis and post-incident reporting using SOAR.
7. Apply machine learning to detect anomalies and reduce false positives.
8. Ensure compliance and audit readiness with automated evidence collection.
9. Operationalize threat intelligence feeds within automated workflows.
10. Troubleshoot and optimize SOAR integrations for scalability.
11. Automate response to ransomware, DDoS, and privilege escalation attacks.
12. Evaluate ROI and KPIs of SOAR implementation.
13. Develop strategic blueprints for enterprise-wide SOAR adoption.

Target Audiences

1. SOC Analysts (Tier 1, 2, and 3)
2. Cybersecurity Engineers
3. Incident Response Managers
4. Security Architects
5. Threat Intelligence Analysts
6. Compliance and Risk Officers
7. DevSecOps Teams
8. IT Operations Leaders

Course Duration: 5 days

Course Modules

Module 1: Introduction to SOAR and Its Strategic Value

- What is SOAR? Architecture and ecosystem
- Market landscape: SOAR vs SIEM vs SIEM-SOAR fusion
- Key benefits: Speed, scale, and consistency
- Core components: Automation engine, orchestration, case management
- Risk reduction and ROI metrics
- **Case Study**: Automating phishing triage in a Fortune 500 company

Module 2: Designing and Implementing SOAR Playbooks

- Introduction to playbook logic and automation paths
- Visual builders vs script-based automation
- Common use cases: Phishing, malware, insider threats
- Input/output configurations and triggers
- Best practices in modular design
- **Case Study**: Custom malware containment playbook at a national bank

Module 3: Integration with SIEM, EDR & Threat Intelligence

- Ingesting data from Splunk, QRadar, CrowdStrike, etc.

- Connecting threat feeds (AlienVault, MISP, Anomali)
- Normalization, correlation, and data enrichment
- Automating IOC lookups and enrichment
- Troubleshooting integration failures
- **Case Study**: Unified response system integrating SOAR and SIEM at a healthcare provider

Module 4: Alert Triage, Enrichment & Prioritization

- Event deduplication and clustering techniques
- Natural Language Processing (NLP) in alert analysis
- Contextual threat scoring models
- Auto-prioritization based on severity and asset value
- Reducing analyst fatigue and false positives
- **Case Study**: NLP-enhanced triage workflow for financial fraud detection

Module 5: Threat Containment and Automated Remediation

- Trigger-based containment strategies
- API-driven remediation actions (block IP, disable accounts, etc.)
- Automation vs Human-in-the-Loop decisioning
- Integration with ITSM systems for escalation
- Post-remediation verification and closure
- **Case Study**: Real-time ransomware containment via XSOAR

Module 6: Compliance Automation and Reporting

- Generating automated incident reports
- Ensuring evidence chain for legal and audit review
- SOAR dashboards for compliance frameworks (HIPAA, PCI-DSS, GDPR)
- Alert-to-resolution timelines and SLA tracking
- Reducing manual documentation burden
- **Case Study**: Automated GDPR reporting using SOAR in a telecom firm

Module 7: Advanced Analytics and AI in SOAR

- Behavior analytics and anomaly detection
- Machine learning models for response decisioning
- Predictive analytics for incident forecasting
- Visualizing threat trends with dashboards
- AI-based prioritization and threat mapping
- **Case Study**: Using AI to predict insider threat attacks in a tech company

Module 8: Enterprise-Level SOAR Deployment and Scalability

- Multi-tenant architecture considerations
- Role-based access controls and policy enforcement
- Managing cross-department workflows
- Scaling SOAR across global SOCs
- Measuring success: KPIs, ROI, and continuous optimization
- **Case Study**: Global SOAR deployment at a multinational conglomerate

Training Methodology

- Live Instructor-Led Sessions
- Hands-on Labs using Real SOAR Platforms
- Interactive Playbook Building Workshops

- Scenario-Based Learning with Case Studies
- Group Activities and Role-Based Simulations
- Post-Training Assessment and Certification Exam

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org 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
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Physical	$0

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

Register Online Now

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