Updated on 30/09/2025

Sign up

TryHackMe SAL1 Certification Training

ALL-IN-ONE : EXAM INCLUDED IN PRICE

5 days (35 hours)

Presentation

TryHackMe SAL1 is a practical certification dedicated to security operations centers (SOC). It validates the skills of a Junior SOC Analyst in triaging, investigating and responding to incidents in a simulated environment.

Our TryHackMe SAL1 training course will enable you to master log collection and normalization, alert detection and enrichment, SIEM investigation and incident response.

You'll learn to use practical tools to analyze traffic, identify indicators of compromise (IOCs), automate tasks via scripts and produce actionable incident reports.

You'll be able to conduct full investigations, automate repetitive actions and prepare to pass the SAL1 exam. The course includes a full mock exam to put you in real-life certification conditions.

Like all our training courses, this one is based on the latest version of official TryHackMe content, and takes a resolutely practical and operational approach.

Objectives

- Understand the role and missions of a Level 1 SOC Analyst
- Master the use of a SIEM to sort and enrich alerts
- Detect threats using Threat Intelligence and IOCs
- Conduct incident response and write clear reports
- Prepare effectively for the SAL1 exam via a mock exam

Target audience

- Junior SOC analysts
- Security technicians
- IT/OPS teams

Prerequisites

- Basic knowledge of networks and systems
- Notions of log analysis

TryHackMe SAL1 training program

[Day 1 - Morning]

SOC fundamentals and context

- Role of an SOC Analyst: missions, scope and interactions
- Incident cycle: detection, triage, escalation, remediation
- Overview of SOC tools: SIEM, EDR, NDR, ticketing
- Essential network reminders
- Practical workshop: Getting to grips with the environment and triaging simple alerts.

[Day 1 - Afternoon]

Log collection and standardization

- Log sources: endpoints, network, applications, cloud
- Common formats : Syslog, CEF, JSON, key fields
- Standardization and enrichment
- Data quality: noise, duplication, event prioritization
- Practical workshop: Ingestion and parsing of log sets in a demo SIEM.

Investigation tools and workflow

- SIEM searches: filters, correlations, aggregations
- Pivoting and timeline: IP, user, host, application
- Evidence preservation and chain of custody
- Hypothesis-driven investigation methodology
- Practical workshop: Conducting a mini-investigation and producing a short report.

[Day 2 - Morning]

Threat detection and use cases

- Signatures vs. behavioral detection (UEBA, rules)
- Use cases: phishing, brute force, exfiltration, lateral movements
- Writing and tuning rules (reducing false positives)
- Detection dashboards and KPIs
- Practical workshop: Creating and testing alert rules in the SIEM.

[Day 2 - Afternoon]

Malware triage and basic forensics

- Static vs. dynamic analysis: principles and limitations
- Collection of endpoint artifacts (processes, persistence, services)
- Infection indicators: IOC files, network, registry
- Good sandbox practices and manipulation security
- Practical workshop: Sorting a suspicious binary and extracting IOCs.

Threat Intelligence and enrichment

- IT sources (open-source, commercial) and SOC integration
- IOC & TTP: use and operational limits
- Enrichment playbooks
- Threat prioritization and MITRE ATT&CK mapping
- Practical workshop: Enriching alerts and qualifying severity with Threat Intelligence.

[Day 3 - Morning]

Incident response and escalation

- Escalation process: criteria, channels, responsibilities
- Containment, eradication, recovery: strategies and pitfalls
- Operational communication and reporting in times of crisis
- Tabletop exercises and RACI roles
- Practical workshop: Simulation of an incident with escalation phases.

[Day 3 - Afternoon]

Cloud monitoring and log security

- Cloud specificities and native logs
- Typical detections: compromised keys, IAM drift
- Centralization and retention of cloud logs
- Compliance constraints and environment segmentation
- Practical workshop: Investigating anomalous cloud events.

Network forensics and traffic capture

- Capture tools (tcpdump, Wireshark): filters and playback
- HTTP/DNS/TLS flow reconstruction and inspection
- Detection of exfiltration and non-standard channels
- Linking network traffic to application logs
- Practical workshop: pcap trace analysis and IOC extraction.

[Day 4 - Morning]

Automation and orchestration

- SOAR concepts: playbooks, jobs, automated actions
- Use cases: enrichment, blocking, quarantines
- SIEM - SOAR - ITSM chain and traceability
- Measuring effectiveness: MTTR, false positives, coverage
- Practical workshop: Creating a simple automation playbook.

[Day 4 - Afternoon]

Languages and scripts useful to the analyst

- Python/PowerShell scripts for sorting and extraction
- API-based enrichment automation
- Best practices in secure scripting
- Error handling and rollback
- Practical workshop: Writing an alert enrichment script.

Vulnerability management and correlation

- Vulnerability vs. incident: SOC complementarities
- Integrating Vulnerability Scans into SIEM
- Vulnerability-event correlation and risk prioritization
- Remediation strategies and communication
- Practical workshop: Cross-referencing scans and alerts to prioritize.

[Day 5 - Morning]

Reporting and continuous improvement

- Writing a readable report for technical and business users
- SOC KPIs: SLI/SLO, MTTR, false positive rate
- Post-mortem and feedback
- Building a catalog of playbooks and runbooks
- Practical workshop: Producing a complete post-incident report.

[Day 5 - Afternoon]

Putting skills into production

- From lab to workstation: SOC integration checklist
- Operational continuity, documentation and handover
- Open-source tools and complementary certification paths
- Progression plan for a Junior SOC
- Practical workshop: Building an integration and skills enhancement plan.

SAL1 exam preparation

- Structure and expectations of the SAL1 exam
- Time management and prioritization strategies
- Review checklist: SIEM, logs, IOC, TTP, cloud, scripts
- Good writing practices and quality of deliverables
- Practical workshop: Mock exam + correction

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced IT technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the forthcoming training course, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical training: 60% hands-on, 40% theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Certification

A certificate will be awarded to each trainee who has completed the entire course.