Updated on 11/14/2025

Register

SentinelOne Training

3 days (21 hours)

Overview

SentinelOne is a modern cybersecurity platform designed to protect workstations, servers, and cloud environments using behavioral analysis and Storyline. This unified EDR and XDR technology automatically detects, analyzes, and remediates threats while providing complete visibility into information system activity.

Our SentinelOne training will teach you how to deploy agents, configure policies, perform advanced investigations, leverage threat intelligence, and integrate SIEM/SOAR.

You will learn how to automate your workflows, optimize your security posture, and effectively monitor your environments.

After completing this training, you will be able to administer the platform, investigate complex incidents, automate responses, and build an operational runbook.

Like all our training courses, this one will introduce you to the latest stable version of SentinelOne available.

Objectives

- Understand the architecture of SentinelOne.
- Deploy and configure agents.
- Analyze and investigate incidents.
- Leverage Threat Intelligence and IOCs.
- Monitor and automate security.

Target audience

- System administrators
- SOC analysts
- Cybersecurity engineers

Prerequisites

- Basic knowledge of cybersecurity
- Knowledge of Windows/Linux

SentinelOne training

[Day 1 - Morning]

SentinelOne architecture and fundamentals

- Understanding the SentinelOne Singularity platform: EDR, XDR, behavioral AI
- How the behavioral engine and Storyline work
- Solution structure: agents, console, groups, policies
- Key components: visibility, detection, autonomous response
- Best practices for getting started and tenant organization
- Hands-on workshop: Guided exploration of the console and initial activity analysis.

[Day 1 - Afternoon]

Agent deployment and configuration

- Windows/macOS/Linux deployment methods
- Management of enrollment tokens and protection modes
- Creating and configuring security policies
- Exclusion management and contextual rules
- Integrated controls: Device Control, firewall, network
- Hands-on workshop: Agent deployment + creation of a targeted policy.

Initial diagnostics and event analysis

- Types of events: alerts, incidents, suspicious behavior
- Reading enriched data via Deep Visibility
- Process tree and behavior analysis
- Rapid identification of potential threats and risks
- Use of filters and advanced searches
- Hands-on workshop: Diagnosis of a suspicious event and guided analysis.

[Day 2 - Morning]

Advanced investigation

- Complete exploration of the storyline
- Reconstruction of the attack chain
- Correlation of events and key indicators
- Integrated MITRE ATT&CK analysis
- Detection of lateral movements and advanced compromises
- Hands-on workshop: Comprehensive investigation of a complex incident.

[Day 2 - Afternoon]

Incident response and remediation

- Automated rollback mechanisms
- Quarantine, network isolation, and targeted deletion
- Large-scale incident management
- Manual response vs. automated response
- Rapid containment strategies
- Hands-on workshop: Implementing a comprehensive remediation strategy.

Threat intelligence and IOC

- Role of Threat Intelligence in SentinelOne
- Working with IOCs: hash, IP, domain, URL
- Automatic enrichment and reputation
- Custom indicator lists
- Proactive detection using behavioral signals
- Hands-on workshop: Adding and using IOCs in the platform.

[Day 3 - Morning]

Monitoring, alerting, and reporting

- Building custom dashboards
- Analysis of attack trends and anomalies
- Creating targeted alerts
- Automated reports for SOC/CISO teams
- Performance indicators and detection quality
- Hands-on workshop: Creating an operational dashboard for SOC.

[Day 3 - Afternoon]

SIEM/SOAR integration and automation

- Connection to a SIEM: Splunk, Elastic, Sentinel
- SOAR scenarios: Cortex, Phantom, Shuffle
- Using the SentinelOne API
- Webhooks, automation, and enhancements
- Building an automated SecOps workflow
- Hands-on workshop: SentinelOne/SIEM integration + automated alerting.

Maintenance, governance, and hardening

- Agent lifecycle management
- Configuration hardening strategies
- Log management, storage, and compliance
- Governance: roles, permissions, audits
- Production checklist and best practices
- Hands-on workshop: Creating a SentinelOne operations runbook.

Target companies

This training is intended for both individuals and companies, large or small, wishing to train their teams in new advanced IT technology or to acquire specific business knowledge or modern methods.

Positioning at the start of training

The positioning at the start of the training course complies with Qualiopi quality criteria. Once they have finalized their registration, learners receive a self-assessment questionnaire that allows us to assess their estimated level of proficiency in different types of technologies, as well as their expectations and personal objectives for the upcoming training course, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could be problematic for the monitoring and smooth running of the training session.

Teaching methods

Practical training: 60% practical, 40% theory. Training materials distributed in digital format to all participants.

Organization

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

Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been correctly acquired.

Certification

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