

Updated on 09/29/2026

Sign Up

Strategy One Training: Creating Dashboards

2 days (14 hours)

Overview

SentinelOne Singularity Endpoint is a platform for protecting endpoints and servers that combines EPP, EDR, behavioral detection, and automated response. It enables you to detect, analyze, and contain threats while centralizing endpoint monitoring from a single console.

Our SentinelOne training course will help you master the essential mechanisms for deployment, administration, and investigation using SentinelOne Singularity Endpoint.

You'll learn how to deploy and configure SentinelOne agents, organize endpoints, define protection policies, and monitor the security status of workstations and servers.

You'll learn to analyze threats with Storyline, apply containment and remediation actions, and then use Deep Visibility to conduct advanced investigations and threat hunting operations.

By the end of the training, you will be able to administer a SentinelOne environment, analyze an attack chain, respond to incidents, and improve visibility into assets using Singularity Network Discovery.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Understand the architecture and key features of SentinelOne Singularity Endpoint
- Deploy, configure, and manage SentinelOne agents on endpoints
- Configure protection policies and monitor the security status of the endpoint fleet
- Analyze threats and attack chains using Storyline
- Conduct investigations and threat hunting operations using Deep Visibility
- Implement containment, remediation, and incident response actions

Target Audience

- System administrator
- Security administrator
- SOC Analyst
- Cybersecurity engineer
- Endpoint Protection Manager

Prerequisites

- General knowledge of Windows, Linux, or macOS system administration
- Understanding of the fundamentals of cybersecurity
- Basic knowledge of malware, network attacks, and incident response

Technical Requirements

- Computer running Windows 11, Linux, or macOS with administrator privileges
- At least 8 GB of RAM; 16 GB recommended for lab exercises
- A modern web browser capable of accessing the SentinelOne Singularity console
- Stable internet connection allowing access to the provided lab environment

SentinelOne Training Agenda

[Day 1 - Morning]

Deployment and Administration of SentinelOne Singularity Endpoint

- Overview of the SentinelOne Singularity platform and positioning of EPP, EDR, and automated response capabilities
- Singularity Endpoint architecture, the role of the management console, and how the SentinelOne agent
- Organizing environments, sites, groups, and endpoints in the management console
- Deployment and management of agents on Windows, macOS, and Linux workstations and servers
- Configuring protection policies, security settings, exclusions, and update strategies
- Hands-on workshop: Getting started with the console, deploying an agent on an endpoint, and applying an appropriate protection policy.

[Day 1 – Afternoon]

Threat detection, analysis, and response

- Understanding Static AI and Behavioral AI detection mechanisms and their use against malware and fileless attacks
- Analyze alerts, events, and indicators of compromise reported by the platform
- Use Storyline to visualize the processes, events, and relationships that make up an attack chain
- Use response actions: process termination, quarantine, remediation, network isolation, and incident resolution
- Understand how Rollback works to restore changes caused by certain attacks and ransomware
- Hands-on workshop: Analyze a detected threat using Storyline, identify its source, and then apply the appropriate containment and remediation actions.

[Day 2 - Morning]

Advanced Investigation and Threat Hunting with Deep Visibility

- Discover Deep Visibility and the telemetry data collected from endpoints
- Build queries to identify suspicious processes, files, network connections, users, and events
- Use contextual information from Storyline to reconstruct the complete sequence of events in an attack
- Identify adversarial techniques and leverage mappings to the MITRE ATT&CK framework
- Implement a threat hunting approach based on indicators, behaviors, and compromise hypotheses
- Hands-on workshop: Conduct an investigation using Deep Visibility, reconstruct an attack chain, and identify potentially compromised endpoints.

[Day 2 - Afternoon]

Advanced operation, monitoring, and securing of the platform

- Manage security policies, exclusions, device controls, and operational settings across the entire infrastructure
- Explore Singularity Network Discovery to identify devices on the network and identify unprotected assets
- Use control and isolation features to limit communication with unauthorized devices
- Monitor agent status, fleet coverage, incidents, and security events from the console
- Explore SentinelOne's integration capabilities with SIEM tools, third-party solutions, and the Singularity ecosystem

- Hands-on workshop: monitor device coverage, identify unprotected devices, and build a comprehensive detection, investigation, and response scenario.

Target Audience

This training is intended for both individuals and companies—large and small—seeking to train their teams on new, advanced IT technology or to acquire specific industry knowledge or modern methodologies.

Assessment at the Start of Training

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency with various types of technologies, as well as their expectations and personal goals for the upcoming training, 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 pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. Training materials distributed in digital format to all participants.

Organization

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

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

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