securonix

Unified Defense SIEM Analyst Training

Securonix Training

Overview

Total Duration: ~12 hours
Format: Self-Paced Learning with Simulations and Knowledge Checks
Assessment: Online Examinations and Knowledge Checks
Credential: Unified Defense SIEM (UDS) - Cyber Defense Analyst (included)
Audience: Security Analysts, Incident Responders, Cyber Defense Analysts, Threat Hunters, Content Developers, Administrators
Platform Version: 6.4 or UDS

Description

The Unified Defense SIEM Analyst Training – Complete Learning Path provides a comprehensive, end-to-end enablement journey for analysts working on the Securonix Unified Defense SIEM (UDS) platform. This learning path consolidates foundational knowledge, operational expertise, analytics and content configuration, and incident investigation and response into a single cohesive syllabus.

Learners begin by understanding the origins of Securonix, core terminology, and the UDS platform architecture. The course then progresses into hands-on operational usage, including Spotter searches, indexing, dashboards, reporting, and data insights. Advanced sections focus on UDS analytics architecture, policy development, rule-based and behavior-based analytics, threat modeling, and content lifecycle management. The learning path concludes with a deep dive into Incident Management, covering investigation workflows, collaboration, SOAR automation, and real-world analyst response scenarios.

Throughout the learning path, simulations and hands-on labs reinforce practical skills required to deploy, operate, tune, and respond effectively using the Securonix Unified Defense SIEM platform.

securonix

Topics

Module 1: UDS Analyst Fundamentals

- History of Securonix
- Securonix fundamentals terminology
- Unified Defense SIEM (UDS) overview
- UDS platform architecture and core components
- Getting started with the UDS environment

Module 2: UDS Analyst Operations

- Spotter fundamentals
- Performing basic and advanced Spotter searches
- Indexes and data exploration
- Dashboard development and customization
- Reporting fundamentals and report creation
- Data insights and operational use cases

Module 3: UDS Content Management

- Content management terminology
- UDS analytics architecture
- Common policy configurations and best practices
- Policy development lifecycle and validation considerations
- Rule-based analytics configuration
- Entity behavior monitoring and behavior profile establishment
- Behavior-based analytics configuration
- Threat model configuration and multi-stage analytics

Module 4: UDS Incident Management

- Incident management fundamentals

- Cyber defense considerations
- Incident and case management workflows
- Incident Management dashboard usage
- On-demand incident creation
- Incident Management and SOAR automation
- Analyst investigation methodology and day-in-the-life workflows
- Threat investigation and threat hunting techniques

Learning Objectives

By the end of this learning path, learners will be able to:

- Understand the origins of Securonix and the evolution of the Unified Defense SIEM platform
- Demonstrate familiarity with Securonix fundamentals terminology, SaaS architecture, and core platform components
- Navigate and operate the UDS environment confidently
- Perform effective Spotter searches, including advanced search techniques, to support security monitoring and investigations
- Utilize indexes, dashboards, reports, and data insights to align security operations with organizational objectives
- Understand UDS analytics architecture and apply best practices for analytics and content development
- Design, configure, tune, and manage rule-based and behavior-based analytics
- Monitor entity behavior and establish behavior profiles to improve detection fidelity
- Configure and manage threat models aligned to business and risk objectives
- Apply analytics lifecycle management and validation techniques to maintain high-quality detection content
- Understand Securonix Incident Management terminology and workflows

- Investigate, prioritize, and respond to security incidents using structured, repeatable methodologies
- Leverage Incident Management dashboards, workflows, and SOAR automation to improve response efficiency
- Apply analyst best practices through real-world investigation, threat hunting, and response scenarios

Simulations

Simulations and hands-on labs are provided throughout the learning path to reinforce real-world skills, including:

- Accessing and navigating the UDS environment
- Configuring baseline views and exploring widgets
- Performing basic and advanced Spotter searches
- Creating customized dashboards and reports
- Discovering, tuning, and validating analytics policies
- Reducing risk scores for policy violations
- Creating new policies following lifecycle best practices
- Building multi-stage, policy-based threat models
- Creating on-demand incidents
- Conducting step-by-step threat investigations
- Performing threat hunting activities

Course Requirements

Required Knowledge

The following prerequisites will ensure that trainees receive the best experience.

- Basic understanding of networking and network security
- Basic understanding of SIEM concepts and functionality
- Familiarity with business use case objectives and data source requirements

Recommended Industry Analyst Training and Certifications

- SANS 504 Incident Handling
- GSEC, CISSP, GCIH, or GCIA

Technical Requirements

- Laptop/Desktop - Mac OS or Windows.
- Reliable Internet connection (LAN/Wi-Fi).
- Most current web browser (Google Chrome Recommended).