



Unified Defense SIEM Analyst Training: Fundamentals

Securonix Training





Overview

Duration: 1 hour

Format: Self-Paced Learning

Exam format: Online Examination

Audience: Security Analysts and Incident Responders

Platform Version: 6.4 or UDS

Description

The Securonix Analyst course provides analysts with the skills needed to prioritize and respond to use case objectives. Starting with security alert analysis that effectively uses Securonix features to provide user and environmental context and continuing to achieve a wider visibility of entity behavior. Analysts will obtain the ability to determine use case alignment to business objectives and optimizations available to respond to alerts effectively.

Course Topics

1. The History Of Securonix
2. Securonix Terminology
3. UDS Overview
4. Getting Started

Course Objectives

- Understanding Content Management Terminology.
- Review Securonix's fundamental terminology, SaaS Architecture, and components of the enrichment framework.
- Configure the Securonix Unified Defense SIEM (UDS) in a way that aligns with an organization's objectives and offerings to internal or external customers.



Simulations

Simulations of our hands-on labs are provided to reinforce the skills needed to successfully deploy and manage a Securonix Unified Defense SIEM (UDS) Platform.

1. Fundamentals: Configuring Baseline View
2. Fundamentals: Configuring Tenant Baseline
3. Fundamentals: Access Control - Roles, Users and Groups

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 Unified Defense SIEM Platform and functionality from 100 online courses, Industry SIEM analyst training, and certifications.
- Basic understanding of business use case objectives and data source requirements in your environment.

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).