securonix

Unified Defense SaaS Admin Training



securonix

Overview

Total Duration: ~12 hours

Format: Self-Paced Learning with Simulations and Knowledge Checks

Assessment: Online Examinations and Knowledge Checks

Credentials Included: Unified Defense SIEM (UDS) - Cyber Defense Admin (included)

Audience: SIEM Administrators

Platform Version: Securonix Unified Defense SIEM (UDS)

Description

The Unified Defense SIEM Unified Learning Path – Analyst & Administrator provides a comprehensive, end-to-end enablement journey covering both administrative and analyst responsibilities on the Securonix Unified Defense SIEM (UDS) platform. This learning path consolidates platform fundamentals, administrative deployment and data onboarding, analyst operations, analytics and content configuration, and incident investigation and response into a single cohesive syllabus.

Learners begin by establishing foundational knowledge of Securonix history, terminology, and platform architecture. The course then progresses through core administrative functions including Hub deployment, management, and data onboarding to ensure reliable data ingestion and enrichment. Analyst-focused content follows, emphasizing Spotter searches, dashboards, reporting, analytics configuration, and threat modeling. The learning path concludes with incident investigation and response workflows, including collaboration, automation, and real-world analyst methodologies.

Simulations and hands-on labs are embedded throughout the learning path to reinforce practical skills required to deploy, administer, operate, tune, and respond effectively using the Securonix Unified Defense SIEM platform.

© Copyright Securonix 2025. All Rights Reserved.

securonix

Course Topics

Module 1: UDS Admin Fundamentals

- History of Securonix
- Core administrative terminology
- Fundamental UDS architecture and major components

Module 2: Hub Deployment and Management

- Hub overview, functionality, and underlying services
- Hub deployment models, sizing, and distribution strategies
- Installation prerequisites, installation, and validation
- Hub troubleshooting, management, and operational best practices

Module 3: Data Onboarding and Ingestion

- Securonix event priority and data onboarding workflow
- Data types, onboarding order, and discovery queues
- User data enrichment, identities, and peer groups
- Activity data ingestion definition, scheduling, and management
- Custom data sources and data dictionary usage
- Windows log collection using NXLog and additional platform considerations

Module 4: UDS Analyst Fundamentals and Operations

- Securonix fundamentals terminology and platform navigation
- Spotter fundamentals and advanced Spotter searches
- Indexes, data exploration, and data insights
- Dashboard development and customization
- Reporting fundamentals and report creation

Module 5: Content Management and Analytics Configuration

- Content management terminology and analytics architecture
- Policy development lifecycle and validation considerations
- Rule-based analytics configuration
- Entity behavior monitoring and behavior profile establishment
- Behavior-based analytics configuration

© Copyright Securonix 2025. All Rights Reserved.

- Threat model and multi-stage analytics configuration

Module 6: Incident Management and Response

- Incident management fundamentals and cyber defense considerations
- Incident and case management workflows
- Incident Management dashboard usage
- On-demand incident creation
- Incident response automation and SOAR integration
- Analyst investigation methodologies and threat hunting techniques

Course Objectives

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

- Understand the evolution, architecture, and core components of the Securonix Unified Defense SIEM platform
- Demonstrate familiarity with administrative and analyst terminology used across the UDS platform
- Deploy, configure, validate, and manage Securonix Hub infrastructure to support resilient data collection
- Design and implement effective data onboarding strategies, including user enrichment and custom data sources
- Navigate and operate the UDS environment to support day-to-day security operations
- Perform effective Spotter searches and leverage indexes, dashboards, reports, and data insights
- Design, tune, and manage rule-based and behavior-based analytics aligned to organizational risk objectives
- Configure and maintain threat models and multi-stage detections
- Apply analytics lifecycle management and validation best practices
- Investigate, prioritize, and respond to security incidents using structured, repeatable methodologies
- Leverage workflows, dashboards, and SOAR automation to improve investigation and response efficiency
- Apply real-world analyst best practices through threat investigation and hunting scenarios

© Copyright Securonix 2025. All Rights Reserved.

securonix

Simulations

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

- Navigating the UDS administrative and analyst interfaces
- Reviewing UDS architecture and data flow
- Installing, validating, and managing Hub infrastructure
- Onboarding data sources and enriching identities
- Configuring NXLog and validating log ingestion
- Performing basic and advanced Spotter searches
- Creating dashboards and reports
- Discovering, tuning, and validating analytics policies
- Building policy-based and behavior-based threat models
- Creating on-demand incidents
- Conducting step-by-step threat investigations and threat hunting exercisesSimulations and hands-on labs are provided throughout the learning path to reinforce real-world skills, including exercises.

© Copyright Securonix 2025. All Rights Reserved.

securonix

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

- Prior exposure to SIEM platforms or SOC operations
- Entry-level security or IT administration experience
- SANS 504 Incident Handling, GSEC, CISSP, GCIH, or GCIA.

Technical Requirements

- Laptop/Desktop - Mac OS or Windows.
- Reliable Internet connection (LAN/Wi-Fi).

© Copyright Securonix 2025. All Rights Reserved.