COURSE TABLE OF CONTENTS

CSLS training course: master the features of Stormshield Log Supervisor

OEM: Stormshield • Code: NT-CSLS

COURSE DESCRIPTION

During the Certified Stormshield Log Supervisor (CSLS) course, trainees will learn how to operate and configure the SLS solution. At the end of this course, they are expected to know how to view activity on their networks, analyze logs and customize dashboards, reports and alarm rules. Trainees will also learn how to automate incident response using SOAR.The Stormshield CSLS certification attests to the acquisition of these skills.

AUDIENCE PROFILE

- IT managers, network administrators and IT technicians.

PREREQUISITES

- This course is reserved for candidates who have passed the CSNA exam within the three years prior to the CSLS course. The hardware requirements to follow this training session remotely are:
- Latest version of a web browser: Chrome or Firefox with JavaScript installed to enable access to the CyberRange platform for practical exercises (only these browsers are supported),
- A working webcam and permissions to install the videoconferencing application,
- Internet access of at least 2 Mbps,
- A second monitor of at least 22 inches is recommended.

COURSE OBJECTIVES

By the end of this course, participants will be able to:

- configure SLS, users and their privileges
- configure the secure forwarding of logs from SNS firewalls to SLS
- perform targeted searches
- generate custom and context-based dashboards
- configure the automatic generation of custom reports
- automate incident identification and reporting
- analyze security incidents based on logs
- automate incident investigation actions with SOAR

COURSE OUTLINE

Module 1: Course Outline

- Individual introduction of trainees

Installing, operating and maintaining SLS

- Configuration of the various types of log storage
- Management of user authentication and their privileges

- Secure forwarding of logs from SNS firewalls to SLS
- Simple searches

Advanced searches

- Aggregation
- Multi-criteria
- Labels
- Macros
- Lists
- Enrichment through external data

- Display of search results
- Search template, creation of searches based on variable criteria

Getting started with the dashboards

- Presentation and customization of pre-configured dashboards
- Creating new dashboards

Reports

- Using pre-configured Stormshield reports
- Creating new custom reports
- Scheduling and sending reports

Alarm rules

- Creating alarm rules
- Tracking and processing alarms

SOAR

- Overview
- Integration with security tools
- Playbook configuration
- Study of results