CSLS COURSE OUTLINE

Certified Stormshield Log Supervisor (NT-CSLS)

STORMSHIELD SAS training organization

Introduction

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.

Target audience

IT managers, network administrators and IT technicians.

Learning methods

The structure of the course alternates between theory and practical exercises in online courses, including interaction with an instructor via videoconferencing and over the Airbus CyberRange platform for practical exercises.

Courseware is provided to trainees and consists of course content and practical exercises (labs) in English. Trainees are given access to a full-scale technical environment so that they can put into practice what they learn during the course.

In order for trainees to keep their knowledge up to date, all updated versions of courseware will be available in PDF on our platform **https://institute.stormshield.eu** for three years. L

Aims of this course

At the end of the course, trainees are expected to know how to:

- configure SLS, users and their privileges
- configure the secure forwarding of logs from SNS firewalls and SES agents 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

Venue and duration

Stormshield conducts onsite training sessions. The schedule of when these sessions are held can be found on the **Stormshield website**.

We can also conduct in-company training for groups of at least five trainees.

Each session is open to a maximum of eight trainees.

The duration of the CSLS course is 14 hours over two consecutive 7-hour days.

Registration

All registration requests must be sent to a Stormshield training center (STC) distributor or to Stormshield's training department (**training@stormshield.eu**). Registrations are confirmed only upon receipt of the order form.

Our general sales terms and conditions are available at **https://www.stormshield.com/standard-terms-conditions-sale-service/**

Facilities for trainees with disabilities

Our course facilities are equipped to accommodate and cater to individuals with disabilities. However, a prior assessment of the nature of the disability is necessary. To ensure that we anticipate trainees' needs and make the necessary arrangements, we ask that they inform our training department of their requirements via e-mail at **referent-handicap-formation@stormshield.eu** as soon as they get in touch.

Cost

The public price is €1890 before tax.

Trainees are given two attempts at the CSLS certification to validate what they learned.

Requirements and hardware specifications

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.

Detailed training program

- 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 and SES agents 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

Certification exam

To obtain certification, trainees must complete a 1-hour online exam containing 40 questions.

The minimum score required to obtain the certification is 70%.

Access to the exam automatically opens the day after the end of the course on the https://institute.stormshield.eu platform and remains open for three weeks. If trainees fail their first attempt or are unable to sit for the exam within this time frame, they will be entitled to a second and final attempt, which will open with immediate effect for an additional week.