CSNTS COURSE OUTLINE

Certified Stormshield Network Troubleshooting &Support (NT-CSNTS)

STORMSHIELD SAS training organization

Introduction

This course comprehensively covers the tools and methods used to gather crucial network data. With such data, issues can be analyzed and fixed effectively in the command line interface (CLI) on Stormshield Network UTM appliances.

This course caters to employees of companies aiming for Stormshield's highest level of partnership, and potential support engineers and expert instructors specializing in our UTM appliances.

Target audience

IT managers, network administrators and IT technicians.

Learning methods

This course can be conducted in two ways: in-person with other trainees in a classroom, or online, in which the instructor uses a combination of videoconferencing tools and the Airbus CyberRange platform. The structure of the course includes both theory and practical exercises.

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

To allow trainees to keep their expertise up to date, all updated versions of courseware are available in PDF for three years on our platform **https://institute.stormshield.eu**.On this platform, trainees will also have access to a virtual environment in which they can operate the appliance and replay lab exercises at their own pace.

Aims of this course

At the end of the course, and after revising the fundamentals, trainees are expected to know:

- the organization of the file system, and the daemons and processes on Stormshield Network appliances
- how to locate, explore and handle the various configuration and log files
- the difference between specific features and anomalies in network and routing configurations
- how to capture network traffic and analyze captures
- how to analyze a security policy, and identify its general directives and special parameters
- how to identify the processes applied to ongoing connections
- how to generate an adapted, comprehensive and usable report to make a diagnosis
- how to configure IPSec VPN tunnel policies, identify enabled mechanisms and diagnose malfunctions on these mechanisms
- how to analyze and debug a high availability configuration

Venue, duration and registration

Stormshield conducts training sessions, either onsite at its offices in Paris, Lille and Lyon, or online.

Our instructors are also equipped to conduct in-company training (onsite or online) for groups of at least five trainees.

The duration of the Troubleshooting and Support course is 28 hours over four consecutive 7-hour days for in-person sessions, or three 7-hour days and two half-days lasting 3.5 hours for the online version.

All registration requests must be sent to a Stormshield training center (STC) distributor or to Stormshield's training department **(training@stormshield.eu**). Each session is open to a maximum of six trainees.

Within the framework of our training courses, it is possible to welcome people with disabilities after evaluation of the nature of the disability. In order to anticipate the needs and study the necessary compensations, it is requested to inform the training department about it before booking a seat.

Cost

The public price of the course is €4000 before tax for 28 hours of course time and two certification attempts online.

Requirements and hardware specifications

Trainees must already be CSNE-certified with a certification that is still valid.

Advanced knowledge of TCP/IP and UNIX shell.

The hardware requirements depend on the format of the session.

In-person:

- Laptop, preferably running in a Windows operating system (physical or virtual with bridged network access) with administrator privileges, on which the following applications are installed: Firefox, PuTTY (or any other SSH client), WinSCP (or an equivalent SCP client), Wireshark, VirtualBox or VMWare equivalent (VMWare Workstation Player or Pro).

Online:

- Web browser: Chrome 50 (or higher) or Firefox 50 (or higher) with Javascript installed to enable access to the CyberRange platform for practical exercises (only these browsers are supported).Trainees must also hold permissions to install plugins that support video calls
- PC with 6 GB of RAM and an i3 processor without hard disk limits
- Internet access of at least 2 Mbps
- A second monitor of at least 22 inches is recommended

Detailed training program

- Individual introduction of trainees
- Introduction to the course
- Operating system and related UNIX commands
    - Shell access and settings

- SSH features
- File system and associated commands
- Directories and associated commands
- System and user environment
- Files and associated commands

- Logs
  - Local logs: location, characteristics, syntax and categories
  - Associated commands
  - Configuration files
  - Logd, logctl, kernel message logs
- Configuration files
  - Directories, structure and general syntax
  - Backups (*.na), decbackup and tar
  - Default configuration
- Objects
  - Object syntax
  - Dynamic and FQDN objects
- Network and routing
  - Network interface settings
  - Bridges and associated commands
  - Routing functions and their priorities
  - Default routes and static routes
  - Gatemon and router objects
  - Dynamic routing
  - Relative commands and showing routes
  - Verbose mode
  - Lab: Network and routing
- Traffic captures and analyses
  - Introduction and tips
  - General syntax and arguments
  - Common filters
  - Commented examples and preparations for effective captures
  - Analyzing traffic with tcpdump (TCP and UDP/icmp traffic)
  - Lab: Network/tcpdump

- ASQ: the various stages of its analysis
  - Step-by-step analysis of network layers
  - Associated commands
  - Global settings
  - Special profiles and settings
  - Asynchronous ASQ: various cases and watermarking
  - ASQ verbose mode
  - Lab: ASQ settings
- ASQ: security policy

- Configuration files and directories, and rule syntax
- Filtering: associated commands
- Filtering: examples of loaded rules (action, inspection level, plugin, PBR, QoS, interfaces and proxy)
- Filtering: translation of groups and lists
- NAT: revision (dynamic NAT, static NAT by port, static NAT/bimap and no NAT)
- NAT: associated commands
- NAT: syntax of loaded rules
- LAB: NAT and filtering

- ASQ: stateful tracking and status tables
  - Protected address table
  - Host table
  - Connection table: examples of connection statuses (NAT, vconn, FTP plugin, async, lite, etc.)
  - LAB: ASQ stateful tracking
- Daemons and processes
  - Lists and roles
  - Supervisor daemon
  - Relative commands
- Eventd: event manager
- IPSec VPN
  - Stormshield Network IKE/IPsec implementation
  - Configuration files
  - Security policy (SPD and SAD)
  - IKE negotiations
  - Negotiations: main mode and aggressive mode
  - ISAKMP and IPsec SAs
  - IKE proposals
  - Specific features: NAT-T, DPD, Keepalive, SharedSA, Policy None and SPD cache
  - Associated commands
  - Analysis of an IPSec-SA
  - Logs
  - “Delete SA” notifications
  - ISAKMP traffic captures and analyses
  - Particularities of dynamic peers
  - Verbose mode and common errors
  - LAB: ISAKMP/IPsec
- PKIs and certificates
  - Recap and global directives
  - CA directory
  - Configuration tips
  - Certificate verification
- High availability

- Overview
- Configuration files
- Relative commands
- Enabling HA and managing network interfaces
- Processes and traffic involved
- Replications/synchronization
- HA events and logs

Certification exam

To obtain certification, trainees must complete a 4-hour online exam containing 60 questions.

The exam consists of a combination of MCQs and open questions on features, settings and advanced troubleshooting methods that must be implemented to provide an exhaustive response to the incident reports that our clients submit.

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 six months. 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 opens automatically and immediately for a week.