

Implementing Juniper Networks Secure Analytics (IJSA)

ID IJSA **Price** US \$ 2,400.—(excl. VAT) **Duration** 3 days

Prerequisites

This course assumes that students have basic networking knowledge and experience in the following areas:

- Understanding of TCP/IP operation;
- Understanding of network security concepts; and
- Experience in network security administration.

Course Objectives

After successfully completing this course, you should be able to:

- Describe the JSA system and its basic functionality.
- Describe the hardware used with the JSA system.
- Identify the technology behind the JSA system.
- Identify the JSA system's primary design divisions—display versus detection, and events versus traffic.
- Plan and prepare for a new installation.
- Access the administration console.
- Configure the network hierarchy.
- Configure the automatic update process.
- Access the Deployment Editor.
- Describe the JSA system's internal processes.
- Describe event and flow source configuration.
- List key features of the JSA architecture.
- Describe the JSA system's processing logic.
- Interpret the correlation of flow data and event data.
- List the architectural component that provides each key function.
- Describe Events and explain where they come from.
- Access the Log Activity interface.
- Execute Event searches.
- Describe flows and their origin.
- Configure the Network Activity interface.
- Execute Flow searches.
- Specify the JSA system's Asset Management and Vulnerability Assessment functionality.
- Access the Assets interface.
- View Asset Profile data.
- View Server Discovery.
- Access the Vulnerability Assessment Scan Manager to produce vulnerability assessments (VAs).
- Access vulnerability scanner configuration.
- View vulnerability profiles.

- Describe rules.
- Configure rules.
- Configure Building Blocks (BBs).
- Explain how rules and flows work together.
- Access the Offense Manager interface.
- Understand Offense types.
- Configure Offense actions.
- Navigate the Offense interface.
- Explain the Offense summary screen.
- Search Offenses.
- Use the JSA system's Reporting functionality to produce graphs and reports.
- Navigate the Reporting interface.
- Configure Report Groups.
- Demonstrate Report Branding.
- View Report formats.
- Identify the basic information on maintaining and troubleshooting the JSA system.
- Navigate the JSA dashboard.
- List flow and event troubleshooting steps.
- Access the Event Mapping Tool.
- Configure Event Collection for Junos devices.
- Configure Flow Collection for Junos devices.
- Explain high availability (HA) functionality on a JSA device.

Course Content

This course replaces the CSTRM (Configuring Security Threat Response Manager)

This three-day course discusses the configuration of Juniper Networks JSA Series Secure Analytics (formerly known as Security Threat Response Manager [STRM]) in a typical network environment. Key topics include deploying a JSA Series device in the network, configuring flows, running reports, and troubleshooting.

Through demonstrations and hands-on labs, students will gain experience in configuring, testing, and troubleshooting the JSA Series device. This course uses the Juniper Networks Secure Analytics (JSA) VM virtual appliance for the hands-on component. This course is based on JSA software 2014.2R4.

Implementing Juniper Networks Secure Analytics (IJSa)

Training Centres worldwide



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, <https://www.flane.ch>