Arrow ECS Finland Oy - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS Finland Oy, Lars Sonckin kaari 16, 02600 Espoo, Finland

Email: education.ecs.fi@arrow.com
Phone: 0870 251 1000

Implementing Juniper Networks Secure Analytics (IJSA)

CODE:	LENGTH:	PRICE:
JUN_IJSA	24 Hours (3 days)	€2,850.00

Description

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 is an introductory-level 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 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.

Audience

This course is intended for network engineers, support personnel, reseller support, and anyone responsible for implementing the JSA system.

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.

Programme

Overview of the JSA Series Device
Hardware
Collection
Operational Flow

Day 1 **Chapter 1: Course Introduction** **Chapter 2: Product Overview** **Chapter 3: Initial Configuration**
A New Installation
Administration Console
Platform Configuration Processing Log Activity Log Activity Overview
Deployment Editor Processing Network Activity Configuring Log Activity
Lab 1: Initial Configuration JSA Deployment Options Lab 2: Log Activity

Chapter 4: Architecture **Chapter 5: Log Activity** **Day 2** **Chapter 6: Network Activity**
Asset Interface
Network Activity Overview Vulnerability Assessment
Configuring Network Activity Vulnerability Scanners
Lab 3: Network Activity Lab 4: Assets and Vulnerability Assessment

Chapter 7: Assets and Vulnerability Assessment **Chapter 8: Rules**
Offense Manager
Rules Offense Manager Configuration
Configure Rules and Building Blocks Offense Investigation
Lab 5: Rules Lab 6: Configure the Offense Manager

Chapter 9: Offense Manager **Day 3** **Chapter 10: JSA Reporting**
Reporting Functionality
Reporting Interface Basic Tuning
Lab 7: Reporting Troubleshooting

Chapter 11: Basic Tuning and Troubleshooting **Chapter 12: Configuring Junos Devices for Use with JSA**
Collecting Junos Events
Collecting Junos Flows
Lab 8: Configuring Junos Devices for JSA
High Availability
Appendix A: High Availability Configuring High Availability

Session Dates

Aikataulutamme kiinnostuksen mukaan. Ota yhteyttä

Additional Information

This training is also available as onsite training. Please contact us to find out more.