

### **Enterprise Computing Solutions - Education Services**

## **TRAINING OFFERING**

You can reach us at:

Arrow Enterprise Computing Solutions Ltd, Part 1st Floor, Suite 1D/1, Central House, Otley Road, Harrogate, HG3 1UG

Email: educationteam.ecs.uk@arrow.com

Phone: 0870 251 1000



# Implementing Juniper Networks Secure Analytics (IJSA)

CODE: LENGTH: PRICE:

JUN IJSA 24 Hours (3 days) £2,395.00

#### **Description**

Duration: 3 days

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 Related Juniper Product:

- Network Management
- JSA Series
- STRM Series
- · Instructor-Led Training

#### **Objectives**

- · 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.
- · 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**

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

#### **Programme**

Day 1 Course Introduction Product Overview • Overview of the JSA Series Device • Hardware • Collection • Operational Flow Initial Configuration • A New Installation • Administration Console • Platform Configuration • Deployment Editor LAB 1: Initial Configuration Architecture • Processing Log Activity • Processing Network Activity • JSA Deployment Options Log Activity • Log Activity Overview • Configuring Log Activity LAB 2: Log Activity Day 2 Network Activity

- Network Activity Overview Configuring Network Activity LAB 3: Network Activity Assets and Vulnerability Assessment
- Asset Interface Vulnerability Assessment Vulnerability Scanners LAB 4: Assets and Vulnerability Assessment Rules Rules
- Configure Rules and Building Blocks LAB 5: Rules Offense Manager Offense Manager Offense Manager Configuration
- Offense Investigation LAB 6: Configure the Offense Manager Day 3 JSA Reporting Reporting Functionality
- Reporting Interface LAB 7: Reporting Configuring Junos Devices for Use with JSA Collecting Junos Events
- Collecting Junos Flows LAB 8: Configuring Junos Devices for JSA Basic Tuning and Troubleshooting Basic Tuning
- Troubleshooting Appendix A: High Availability High Availability Configuring High Availability

#### **Session Dates**

On request. Please Contact Us

#### **Additional Information**

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