

Implementing Juniper Networks Secure Analytics (IJSA)

Duration: 3 Days Course Code: JUN_IJSA

Overview:

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

Target Audience:

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

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 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.

- • 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).
- • 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.

Prerequisites:

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

Content:

Day 1	• Configuring Log Activity	• Offense Investigation
Course Introduction	LAB 2: Log Activity	LAB 6: Configure the Offense Manager
Product Overview	Day 2	Day 3
• Overview of the JSA Series Device	Network Activity	JSA Reporting
• Hardware	• Network Activity Overview	• Reporting Functionality
• Collection	• Configuring Network Activity	• Reporting Interface
• Operational Flow	LAB 3: Network Activity	LAB 7: Reporting
Initial Configuration	Assets and Vulnerability Assessment	Configuring Junos Devices for Use with JSA
• A New Installation	• Asset Interface	• Collecting Junos Events
• Administration Console	• Vulnerability Assessment	• Collecting Junos Flows
• Platform Configuration	• Vulnerability Scanners	LAB 8: Configuring Junos Devices for JSA
• Deployment Editor	LAB 4: Assets and Vulnerability Assessment	Basic Tuning and Troubleshooting
LAB 1: Initial Configuration	Rules	• Basic Tuning
Architecture	• Rules	• Troubleshooting
• Processing Log Activity	• Configure Rules and Building Blocks	Appendix A: High Availability
• Processing Network Activity	LAB 5: Rules	• High Availability
• JSA Deployment Options	Offense Manager	• Configuring High Availability
Log Activity	• Offense Manager	
• Log Activity Overview	• Offense Manager Configuration	

Additional Information:

Delegates will receive e-kit courseware.

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK