

# Implementing Juniper Networks Secure Analytics (IJSA)

Engineering Simplicity

## COURSE LEVEL

Implementing Juniper Networks Secure Analytics is an introductory-level course

## 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.

## COURSE 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.

## 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.

## ASSOCIATED CERTIFICATION

N/A

## RELEVANT JUNIPER PRODUCT

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

## RECOMMENDED NEXT COURSE

N/A

## CONTACT INFORMATION

[Contact Juniper Education Services](#)

## OBJECTIVES(contd)

- 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

### Day 1

<b>1</b>	<b>COURSE INTRODUCTION</b>
<b>2</b>	<b>Product Overview</b> <ul style="list-style-type: none"> <li>• Overview of the JSA Series Device</li> <li>• Hardware</li> <li>• Collection</li> <li>• Operational Flow</li> </ul>
<b>3</b>	<b>Initial Configuration</b> <ul style="list-style-type: none"> <li>• A New Installation</li> <li>• Administration Console</li> <li>• Platform Configuration</li> <li>• Deployment Editor</li> </ul> <b>LAB 1: Initial Configuration</b>

<b>4</b>	<b>Architecture</b> <ul style="list-style-type: none"> <li>• Processing Log Activity</li> <li>• Processing Network Activity</li> <li>• JSA Deployment Options</li> </ul>
<b>5</b>	<b>Log Activity</b> <ul style="list-style-type: none"> <li>• Log Activity Overview</li> <li>• Configuring Log Activity</li> </ul> <b>LAB 2: Log Activity</b>

### Day 2

<b>6</b>	<b>Network Activity</b> <ul style="list-style-type: none"> <li>• Network Activity Overview</li> <li>• Configuring Network Activity</li> </ul> <b>LAB 3: Network Activity</b>
<b>7</b>	<b>Assets and Vulnerability Assessment</b> <ul style="list-style-type: none"> <li>• Asset Interface</li> <li>• Vulnerability Assessment</li> <li>• Vulnerability Scanners</li> </ul> <b>LAB 4: Assets and Vulnerability Assessment</b>

<b>8</b>	<b>Rules</b> <ul style="list-style-type: none"> <li>• Rules</li> <li>• Configure Rules and Building Blocks</li> </ul> <b>LAB 5: Rules</b>
<b>9</b>	<b>Offense Manager</b> <ul style="list-style-type: none"> <li>• Offense Manager</li> <li>• Offense Manager Configuration</li> <li>• Offense Investigation</li> </ul> <b>LAB 6: Configure the Offense Manager</b>

## Day 3

10

### JSA Reporting

- Reporting Functionality
- Reporting Interface

#### LAB 7: Reporting

12

### Configuring Junos Devices for Use with JSA

- Collecting Junos Events
- Collecting Junos Flows

#### LAB 8: Configuring Junos Devices for JSA

11

### Basic Tuning and Troubleshooting

- Basic Tuning
- Troubleshooting

### Appendix A: High Availability

- High Availability
- Configuring High Availability