Implementing Juniper Networks Secure Analytics (IJSA)

ID IJSA **Prix** US$ 2 400,– (Hors Taxe) **Durée** 3 jours

Pré-requis

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.

Objectifs

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.

Contenu

Day 1

Chapter 1: Course Introduction

Chapter 2: Product Overview

- Overview of the JSA Series Device
- Hardware
- Collection
- Operational Flow

Chapter 3: Initial Configuration

- A New Installation
- Administration Console
- Platform Configuration
- Deployment Editor
- Lab 1: Initial Configuration

Chapter 4: Architecture

- Processing Log Activity
- Processing Network Activity
- JSA Deployment Options

Chapter 5: Log Activity

- Log Activity Overview
- Configuring Log Activity
- Lab 2: Log Activity

Day 2

Chapter 6: Network Activity

- Network Activity Overview
- Configuring Network Activity
- Lab 3: Network Activity

Chapter 7: Assets and Vulnerability Assessment

- Asset Interface
- Vulnerability Assessment
- Vulnerability Scanners
- Lab 4: Assets and Vulnerability Assessment

Chapter 8: Rules

- Rules
- Configure Rules and Building Blocks
- Lab 5: Rules

Chapter 9: Offense Manager

-
- Offense Manager
- Offense Manager Configuration
- Offense Investigation
- Lab 6: Configure the Offense Manager

Day 3

Chapter 10: JSA Reporting

- Reporting Functionality
- Reporting Interface
- Lab 7: Reporting

Chapter 11: Basic Tuning and Troubleshooting

- Basic Tuning
- Troubleshooting

Chapter 12: Configuring Junos Devices for Use with JSA

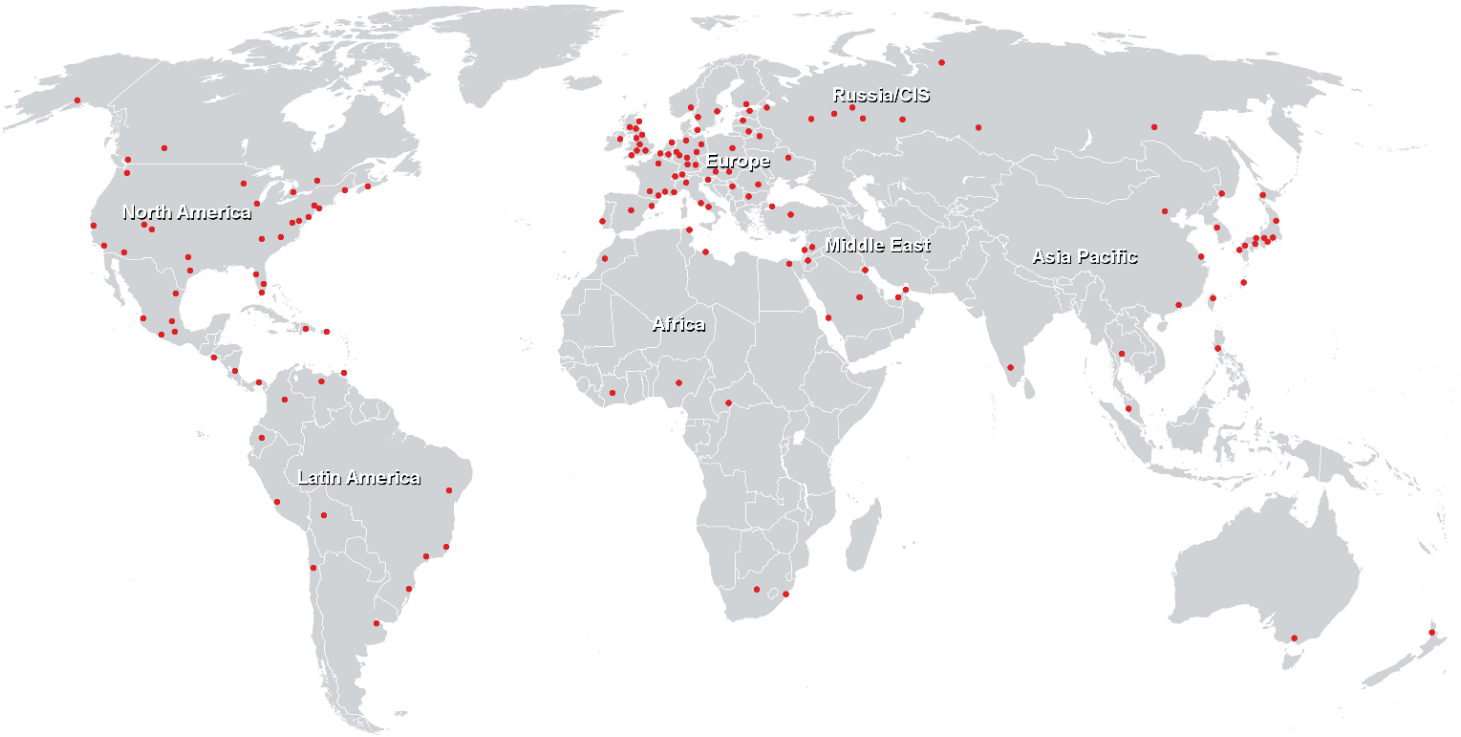
- Collecting Junos Events
- Collecting Junos Flows
- Lab 8: Configuring Junos Devices for JSA

Appendix A: High Availability

- High Availability
- Configuring High Availability

Implementing Juniper Networks Secure Analytics (IJSA)

Centres de formation dans le monde entier



Fast Lane Institute for Knowledge Transfer GmbH

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

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