



Course No: (TWI-JUN-CSTRM)

Length: 2 days

About this Course

This two-day course discusses the configuration of Juniper Networks Security Threat Response Manager (STRM) in a typical network environment. Key topics include deploying an STRM device in the network, configuring flows, running reports, and troubleshooting. This course is based on STRM software 2008.3. Through demonstrations and hands-on labs, students will gain experience in configuring, testing, and troubleshooting the STRM device.

Objectives

After successfully completing this course, you should be able to:

- Define STRM and its basic functionality;
- Define the STRM functional architecture;
- Interpret the correlation of flow and event data;
- Configure STRM by reviewing and editing global views and sentries;
- Navigate the STRM Dashboard and Event Viewer;
- Access the Network Surveillance interface;
- Access the Flow Viewer interface;
- Access the Offense Manager interface;
- Specify STRM's asset management and vulnerability assessment functionality;
- Use STRM's reporting functionality;
- Explain the purpose and structure of STRM rules;
- List basic tuning methodology; and
- Identify the basic information for maintaining and troubleshooting STRM.

Intended Audience

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

Course Level

This is an introductory-level course.

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.

twine networks



Course Contents

Day1

Chapter 1: Course Introduction

Chapter 2: Product Overview

- STRM Overview
- Hardware
- Collection
- Operational Flow

Chapter 3: Initial Configuration

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

Chapter 4: Architecture

- Event Flow
- Network Flow
- The STRM Device Architecture

Chapter 5: Dashboard, Event Viewer, and Flow Viewer

- The Dashboard
- Event Viewer
- Rules
- Flow Viewer
- Lab 2: Configure the STRM Dashboard, Event Viewer, and Flow Viewer

twine networks



Day 2

Chapter 6: Network Surveillance

- Network Surveillance
- Views Configuration
- Sentries
- Lab 3: Network Surveillance

Chapter 7: Assets and Vulnerability Assessment

- Assets Interface
- Vulnerability Assessment
- Vulnerability Scanners

Chapter 8: Offense Manager

- Offense Manager
- Network Anomaly
- Lab 4: Offense Manager

Chapter 9: STRM Device Reports

- Reporting Functionality
- Reporting Interface
- Lab 5: Reports

Chapter 10: Basic Tuning and Troubleshooting

- Basic Tuning
- Troubleshooting

twine networks

103 Robyn Street | Jukskei Park | 2188 | Johannesburg | South Africa | Tel: +27(0)123 642 515 | 0861 000 250 (SA only)
E-mail: knowledge@twine-networks.com | Company Registration No.: 2005/011816/23

www.twine-networks.com