OVERVIEW

Course Level:

Intermediate

Format:

Instructor-Led

Course Code:

SP-TRAIN-ESSENTIALS

Target Audience:

Security administrators, network operations personnel, and staff responsible for monitoring network traffic, mitigating DDoS attacks and ensuring peak performance of the Arbor SP deployment.

Duration:

40 course hours, 4.0 CEUs

Arbor SP Essentials Course

Course Description

This five-day course focuses on using Arbor SP for both network visibility and availability protection. The goal of the course is to build the attendee's confidence by providing hands-on experience in using Arbor SP to observe traffic characteristics of their network and to identify and mitigate DDoS (Distributed Denial of Service) attacks. Fundamental TMS countermeasures and mitigation workflow are introduced.

Course Objectives

- Navigate the SP UI (User Interface)
- Use system status and monitoring to analyze deployment health
- Use network status and related reports to verifying network operation
- Create managed objects, analyze associated traffic reports, and configure anomaly detection settings
- Differentiate anomalies that are DDoS attacks from non-attack occurrences
- Mitigate DDoS attacks using flowspec filters and blackhole routes
- Mitigate DDoS attacks using specific TMS countermeasures - flow filters, TCP SYN Authentication and Zombie Detection
- Maintain the SP deployment with system tuning, configuration management, and backup/restore of databases

Course Syllabus

Module 1: Technical Review

- Describe Arbor SP's system architecture and overall functionality
- Explain the traffic visibility and analysis capabilities of Arbor SP
- Explain SP's DDoS detection and mitigation capabilities

Module 2: Surveying Your Deployment

- Use SP tools to check the status of the SP deployment
- Use SP tools to check the status of SP appliances
- Use SP tools to check alert activity and ongoing alerts

Module 3: Verifying Your Network

- Analyze the health of the network and monitored routers
- Identify the network boundary
- Describe interface classification
- Configure interface auto-configuration rules

Module 4: Interpreting Network Reports

- Use reports to pull data from the network boundary
- Build Explore Traffic queries for custom multiple-filter reports
- Create custom Wizard reports

Module 5: Creating Managed Objects

- Describe the use of managed objects in SP
- Describe managed object traffic counting methods
- Configure managed objects
- Configure managed object children

Module 6: Interpreting Managed Object Reports

- Describe network and local boundaries
- Explain managed object boundary-based counting
- Apply managed object reporting

Module 7: Configuring Anomaly Detection

- Identify the impact of DDoS attacks
- Describe how SP detects and classifies anomalies
- Configure host detection settings
- Configure profiled router detection settings
- Configure profiled network detection settings
- Activate and configure Fingerprints

Module 8: Interpreting Anomaly Alerts

- Monitor alert activity in your deployment
- Interpret how an anomaly alert is presented
- Analyze an anomaly to identify possible DoS attacks

Module 9: Mitigating Attacks Using SP

- Employ SP mitigation methods

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

TCI_080_EN-1801 04/2018