## OVERVIEW

### Course Level:

Intermediate

### Format:

Instructor-Led

### Prerequisite Knowledge:

Completing the following Arbor Security Academy on-demand courses is recommended:

- Introduction to DDoS
- Getting Started with Arbor Sightline and TMS

### Target Audience:

Network operations personnel, security staff responsible for the monitoring and/or mitigation of network anomalies.

### Duration:

24 course hours

# Arbor Sightline/TMS DDOS Detection and Mitigation User Course

## Course Description

Designed for Network Administrators and Security Analysts, this course will cover how to use Sightline reporting and DoS alerts to analyze malicious traffic. Based on that analysis, you will then orchestrate an appropriate response using BGP routing, Sightline mitigation tools, or Threat Mitigation System (TMS) standard or advanced countermeasures. Finally, you will learn how to monitor the effectiveness of the mitigation and make appropriate changes. The course depends heavily on hands-on learn-by-doing exercises to build your skills and confidence to act when a DDoS attack befalls your own network.

## Course Objectives

- Identify the common DDoS attack methods and characteristics
- Exercise key anomaly detection methods available in Arbor Sightline
- Formulate strategies to mitigate anomalous hostile traffic
- Create and apply attack mitigations using Arbor Sightline with or without TMS appliances and determine the effectiveness of the mitigation

## Course Syllabus

### Module 1: Introduction to Sightline

- Sightline architecture overview
- Understand Sightline data collection
- Using Sightline for traffic visibility and analysis

### Module 2: DDOS Overview

- Describe and understand DDOS threats
- Introduction to DOS Alerts and its representation in Sightline

### Module 3: Host Anomaly Detection

- Anomaly detection and classification by Sightline
- Understand Host Detection and all its misuse types

### Module 4: Profiled Anomaly Detection

- Understand router and network profiled detection

### Module 5: Interpreting Anomaly Alerts

- Learn to analyze DOS alerts
- Understand how to gather DOS alert statistics

### Module 6: Anomaly Mitigation

- Identify different mitigation methods available with Sightline
- Understand how each mitigation method work
- Learn how to launch a mitigation from an alert

### Module 7: TMS Mitigation Workflow

- Manage TMS mitigations
- Learn how to work with Sample Packets
- Understand to differentiate between block and drop
- Understand TMS mitigation health monitoring

### Module 8: Volumetric Attacks

- Learn how to identify volumetric attacks
- Learn how to configure and use traffic filters
- Understand how countermeasures like zombie detection work

### Module 9: State/Stack Attacks

- Learn how to identify stack targeting attacks
- Use TCP SYN Authentication with its different modes
- Learn how to limit and monitor TCP connection usage

### Module 10: Application Layer Attacks

- Learn how to block generic application layer attacks
- Learn to perform more specific blocking like for HTTP and DNS

### Module 11: Enhancing Mitigations

- Leverage scoping on countermeasures
- Understand Arbor Cloud Signaling
- Learn how to use mitigation templates
- Understand auto mitigation functionalities

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_083_EN-2001 10/2020