Defending Your Network With Arbor Sightline & TMS

Course Description
This course focuses on using Arbor Sightline & TMS for protection from availability threats such as volumetric, state-exhaustion, and application-layer Distributed Denial of Service (DDoS) attacks.

The goal of the course is to build your confidence to mitigate hostile DDoS attacks by providing hands-on experience in using Arbor Sightline & TMS to identify and mitigate malicious DDoS traffic. You will learn about the different types of DDoS attacks and how to use Arbor Sightline & TMS to monitor and analyze traffic. Then through hands-on lab exercises, you will experience different types of DDoS attacks and use Arbor Sightline & TMS to mitigate the malicious traffic that is targeting the servers you are assigned to protect.

Course Objectives
• Use Arbor Sightline to differentiate hostile attack traffic from anomalous but safe network traffic
• Describe the characteristics of volumetric, state-exhaustion, and application layer DDoS attacks
• Configure BGP blackhole routing, BGP flow specification, and BGP traffic diversion to a TMS node to mitigate DDoS attack traffic
• Apply TMS-defined countermeasures to mitigate DDoS threats

OVERVIEW

Course Level:
Intermediate

Format:
Instructor-Led Training

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:
Security or Network Operations Center professionals, Security Engineers, Network Engineers

Duration:
16 course hours
Course Syllabus

Module 1: Detecting DDoS Attacks
- Describe how Sightline detects network anomalies
- Identify the impact of DDoS attacks
- Searching for and analyzing a DoS Host Alert
- Lab: Analyzing Sightline DoS Host Alerts

Module 2: Identifying and Mitigating Volumetric DDoS Attacks
- Describe the characteristics and impact of a volumetric attack
- List and describe the techniques available in Sightline to drop or block malicious traffic
- Use Sightline to launch a blackhole mitigation and a flow specification mitigation
- Launch a TMS mitigation using appropriate countermeasures and filter lists to mitigate a volumetric attack
- Lab: Mitigate a DDoS Attack Using BGP Blackhole Routing
- Lab: Start a BGP Flow Specification Mitigation
- Lab: Use Arbor TMS to Mitigate a Flood

Module 3: Protecting Against State-exhaustion DDoS Attacks
- Describe the characteristics and impact of a TCP state-exhaustion attack
- Use the TMS to launch and monitor a mitigation
- Identify and use countermeasures to best protect against a TCP state-exhaustion attack
- Lab: Mitigating a SYN Flood

Module 4: Application-layer DDoS Attacks
- Describe the characteristics and impact of application-layer attacks
- Choose the appropriate TMS countermeasures to protect against a specific application-layer attack
- Lab: Mitigating an Application-Layer Attack
- Lab: Mitigate a DNS-based DDoS Attack

Module 5: Using the Remaining TMS Countermeasures
- Additional TMS Mitigation Settings
- Scoping
- More TMS Countermeasures
- Lab: Test Your Skill - Mitigate an Unknown Attack