TPS
Threat Protection System with aGalaxy

Instructs Network Operations, Development Operations, Network Security, and Architects on implementing an effective threat protection system for A10 ACOS deployments in data center environment.

Objectives

Students learn to:

- Deploy a Threat Protection System in different topologies
- Use aGalaxy to orchestrate TPS devices
- Monitor traffic and detect attacks
- Configure and apply mitigation strategies against the following DDoS attacks:
  - volumetric
  - protocol
  - reflection
  - resource
- Configure a Zero-day Attack ¨Pattern Recognition (ZAPR) solution
- Generate reports
- Examine network traffic at the packet level

Class Structure

- Classroom Discussion 50%
- Lab Exercises 50%

Prerequisites

- OSI reference model
- Network topology and administration

Audience

- Network Operations (NetOps)

- Development Operations (DevOps)
- Network Security (NetSec)
- Architects (Arch)

Outline

- Overview
  - Types of DDoS Attacks
  - Mitigation Strategies
- Configuration
  - Components of A10 Threat Protection System
  - Deployment Topologies
- Attack Detection
  - Zones
  - Monitoring Traffic
  - Zone Escalation Process
  - Zone Operational Modes
  - Traffic Baseline
- Attack Mitigation
  - Incident Creation
  - Incident Mitigation
- Traffic Rate Limiting
  - GLIDs
  - Zone-Templates
  - Zone Level Based Mitigation
- Layer 3/4 Security
  - TCP Security Measures
  - UDP Security Measures
  - ICMP Security Measures
- Layer 7 Security
  - DNS Security Measures
  - HTTP Security Measures
  - SSL Security Measures
- ZAPR

- Configuring ZAPR
- Detection 2.0
  - Supported Topologies Workflow
- Reporting and Troubleshooting
  - Reports
  - Packet Capture
  - Packet Debugger