DNS Guardian Administration & Configuration

Training Course

SOLIDserver software version:
8.4

Course type:
Choice of Instructor-led or Self-paced eLearning with hands-on labs

Duration:
Instructor-led: 19 hours (spread over 3 or 4 days)
Self-paced: 12 to 14 hours

Lab access:

Instructor-led: For course duration
Self-paced: 12 hours (over a 15-day period)

Audience:
System and network administrators

Prerequisites:
Completion of SOLIDserver Administration training that includes DNS management

Certifications:
DNS Guardian Administrator
DNS Guardian Advanced Administrator

Training Summary

Overview:

Via the hands-on training, the participants will acquire the knowledge to manage and configure DNS Guardian to detect and protect against threats.

Objectives:

By the end of the course, the students will be able to:

- Describe the function and benefits of DNS Guardian
- Understand how DNS traffic metrics are used in Analytics, Statistics and Triggers
- Configure Triggers and view log entries
- Use CQF for to provide DNS filtering and application access control
- Create and provision lists, rulesets and rules
- Create tags and use them in rules with tagmatch and tagjoin
- Use CQF with DNS Threat Pulse
- Use the Blastcli to access the Guardian Configuration and Cache
- Use the Blastcli to analyze DNS Attacks
- Monitor Guardian performance & statistics
- Use the Rescue Mode and Servfail Diff features
- Understand the benefits of Cache Sharing

Course Content

The course is divided into 3 focus areas.

DNS Guardian Administration

DNS Guardian Introduction
- DNS Guardian Description
- Introduction to Guardian Threat Protection

Introduction to Guardian Management
- Web Interface Overview
- CLI Overview
- Threat Detection in Action

DNS Metrics and Statistics
- DNS Traffic Metrics
- DNS Guardian Statistics
- View Statistics in the Web UI

DNS Guardian Analytics
- View Analytics in the Web UI

DNS Guardian Trigger Overview
- Triggers Overview
- Manage Policies and Triggers
- View Trigger Values in the Log

Trigger Action and Logging
- Trigger Actions
- Trigger Logging

Threat Analysis & Mitigation Data Exfiltration
- Investigate a Data Exfiltration Attack
- Use Triggers as a Countermeasure

Threat Analysis & Mitigation DNS Server Attacks
- Volumetric Attacks
- Stealth / Slow Drip Attacks
- Investigation and Countermeasures

DNS Threat Pulse
- Introduction to CQF and Threat Pulse
- CQF Lists and Rules
- Configure Client Query Filtering with DNS Threat Pulse

DNS Intelligence Center (IC)
- Introduction to DNS Intelligence Center
- Data Collection and Upload
- Investigation of threats and suspicious domains

DNS Client Query Filtering

CQF Lists
- CQF Lists
- Create a List & List Entry

CQF Rules
- CQF Rulesets & Rules
- Create a Ruleset & Rule

Use CQF to Tune Triggers
- False Positive Trigger Actions
- Tune Triggers Using a CQF Rule
- Tune Triggers Using a CQF List

CQF Client Identifiers and Lists
- Filter Using Source Client
- Add a Rule Using a Client List
- List Management
- Client Identifiers
- Lists With Multiple Identifiers

View Client Identifiers
- View Client Identifiers
- Configuring a View Client Identifier

efficient iP

Americas
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

Europe
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes-FRANCE
+33 1 75 84 88 98

Asia
EfficientIP PTE Ltd
60 Paya Lebar Road #11-47
Paya Lebar Square SINGAPORE 409051
+65 6678 7752

CQF Tags
- Add Tags
- Add a List Entry with a Tag

CQF Rules with Threat Pulse
- Tune Threat Pulse using CQF Rules
- Use Tags with Threat Pulse

Application Access Control Using Tags
- Reminder: Rule Definitions
- Use Tage for Application Access Control

Advanced Configuration

BlastCLI
- Blastcli Overview
- Cache Responses
- Cache Dump
- Reset Cache Command
- Cache Analysis

Using BlastCLI to Analyze Triggers
- Sloth DNS Attack Analysis
- DNS Exfiltration Attack Analysis

BlastCLI Statistics
- BlastCLI Statistics
- Client Statistics
- Client Statistics for Invalid Query Attack
- Client Statistics Distribution

Adaptive Security Features
- Rescue Mode
- Servfail Diff

CQF Lists and Rules Configuration
- List & RuleSet Provisioning
- List Statistics

Cache and Client Management
- Cache Sharing
- Cache Management
- Client Management

Other Guardian Features
- Guardian on Authoritative Server
- Guardian with an ECS-Enabled Recursive Server
- Secure DNS Traffic with DoT and DoH
- Transparent DNS Proxy Feature
- TOS/DSCP Marking

efficient iP

Americas
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

Europe
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes-FRANCE
+33 1 75 84 88 98

Asia
EfficientIP PTE Ltd
60 Paya Lebar Road #11-47
Paya Lebar Square SINGAPORE 409051
+65 6678 7752