DNS Guardian Description and Operation

TRAINING SUMMARY

Overview:

Via hands-on training, the participants will acquire the knowledge to configure and use DNS Guardian.

Objectives:

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

- Configure DNS Guardian
- Manage the Guardian Cache
- Manage Domain and Client lists with Client Query Filtering (CQF)
- Understand, Detect, and Mitigate DNS Attacks

- **SOLIDserver Software Version:** 8.x
- **Course Type:** Instructor-led (on-site, remote)
- **Duration:** 18 hours (spread over 3 or 4 days)
- **Optional eLearning:** DNS Security Threats (1 hour)
- **Audience:** System, Network, and Security Administrators
- **Prerequisites:** Attend the SOLIDserver DDI Administrator or DNS Administrator Course
- **Certification:** yes (optional)

COURSE CONTENT

Module 1: DNS Guardian Description and Operation

- DNS Guardian Description
- DNS Blast Series Description
- Configuring DNS Guardian
- Connecting to the DNS Guardian CLI

Module 2: Cache Management and Client Query Filtering

- Managing the Guardian Cache
- Enabling Traffic Filtering using CQF
- Using Tags with CQF
- Logging DNS Queries and Responses

Module 3: Adaptive Security in Motion

- Monitoring DNS Guardian Performance using Analytics and Statistics
- Managing Monitored Clients
- Using Triggers to Automate the Detection of Attacks in Real Time
- Using Rescue Mode and SERVFAIL Diff to Mitigate Attacks on Recursive DNS
- Enabling Logging when Arming Triggers

Module 4: Use Cases Analysis

- Understand, Detect and Mitigate the following DNS Attacks:
  - DNS Tunneling
  - Data Exfiltration
  - Denial of Service Attacks
- Explore Best Practices to help Monitor the State of the DNS Server

Module 5: Going Further

- Guardian Support on Authoritative DNS Servers
- DNS over TLS (DoT)
- DNS over HTTPS (DoH)
- Integration with Cisco Umbrella

efficient iP™

As one of the world's fastest growing DDI vendors, EfficientIP helps organizations drive business efficiency through agile, secure and reliable network infrastructures. Our unified management framework for DNS-DHCP-IPAM (DDI) and network configurations ensures end-to-end visibility, consistency control and advanced automation. Additionally, our unique 360° DNS security solution protects data confidentiality and application access from anywhere at any time. Companies rely on us to help control the risks and reduce the complexity of challenges they face with modern key IT initiatives such as cloud applications, virtualization, and mobility. Institutions across a variety of industries and government sectors worldwide rely on our offerings to assure business continuity, reduce operating costs and increase the management efficiency of their network and security teams.

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
3 HarbourFront Place, Level 11
HarbourFront Tower 2, Singapore 099254
+65 6678 7752