COURSE OUTLINE

# DNS for Security Practitioners

**Intensive and Interactive** – Led by an authorized instructor, this vendor-agnostic training course provides relevant information on how DNS is abused, presented in a format that is easy to understand and digest for today's security practitioners. Several types of activities are used in the course to reinforce topics and increase knowledge retention, including questions from the instructor, demos, group discussions, and case studies.

| | |
|---|---|
| **Course Description** | Understand how DNS is abused by attackers to compromise network security, and the techniques to mitigate those risks. Learn how attacks are executed through case studies and protocol analysis, gain deep understanding of the attacker's mind set, and design defense strategies that strike at the core of DNS-based exploits and tactics. |
| **Target Audience** | This training course is intended for professionals working or intending to work in the information security area. This course is ideal for Cyber Security Specialists, Security Analysts, Security Engineers, Security Operations Manager, and Security Architects. |
| **Duration** | 1 day |
| **Learning Style** | Lecture, demo, and group discussions and activities |
| **Available Modalities** | Instructor-led, Virtual Instructor-led, On-Demand |
| **Prerequisites** | Attendees should have at least two years' experience working in information security or a related field and a basic understanding of networking. |
| **Training Credits** | 10 |
| **Course Topics** | • Protocol Review<br>• DNS and Malware<br>• Lookalike Domains and DGA<br>• Exfiltration and Behavioral Analysis<br>• DNS Hijacking and Encrypted DNS<br>• Cache Poisoning and DNSSEC<br>• Defense Strategies<br>• Best Practices |

20210709

Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com

COURSE OUTLINE

# DNS for Security Practitioners

## Topics in Detail

1. Protocol Review
   - DHCP
   - DNS
   - IPAM
2. DNS and Malware
   - Malware and DNS
   - Command and Control
   - Case Study: WannaCry
   - Case Study: Black KingDom
   - DNS Tunneling
   - Case Study: InvisiMole
3. Lookalike Domains and DGA
   - Lookalike Domains
   - RPZ
   - DGA
   - Case Study: Zloader
   - Defense Options
4. Exfiltration and Behavioral Analysis
   - Data Exfiltration
   - Case Study: AlinaPOS
   - Newly Observed Domains
   - Behavioral Analysis
5. DNS Hijacking and Encrypted DNS
   - Client Hijacking
   - Case Study: Win32.QHOST
   - Case Study: Dridex
   - Domain Hijacking
   - Case Study: FOX-IT
   - Mitigation
   - Encrypted DNS
   - Case Study: GodLUA
6. Cache Poisoning and DNSSEC
   - Cache Poisoning
   - Probability of Success
   - Case Study: The Kaminsky
   - Case Study: SadDNS
   - DNSSEC
7. Defense Strategies
   - Attack and Defense Overview
   - Incorporating DDI and SIEM
   - Pyramid of Pain
   - MITRE ATT&CK
   - DNS Views
8. Best Practices
   - Summary of threats and defenses
   - Best practices

Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com