



## PRODUCT TRAINING

### WORKSHOP: Infoblox Threat Defense Administration

**Course Description** Strengthen your understanding of Infoblox Threat Defense and how it protects organizations from malicious DNS activity, data exfiltration, and endpoint-driven threats. This workshop provides a comprehensive, hands-on learning experience that covers Threat Defense components, DNS forwarding proxies, NIOS-X deployment, policy inspection, endpoint integration, and advanced analytics using Threat Insight. Participants will explore DNS security controls, analyze Threat Defense reports, and apply hands-on labs to detect, inspect, and mitigate threats across hybrid network environments.

<b>Target Audience</b>	Security operators, administrators, SOC analysts, and technical staff responsible for DNS-centric threat detection and protection.
<b>Products Covered</b>	NIOS-X, Infoblox Threat Defense, DNS Forwarding Proxies, Threat Insight analytics
<b>Duration</b>	3 x 4 Hour Sessions <b>OR</b> 2 Days
<b>Learning Style</b>	Lecture, demo, and hands-on labs
<b>Available Modalities</b>	Instructor-led, virtual instructor-led
<b>Certification Exam</b>	No exam
<b>Prerequisites</b>	- If new to security concepts, consider taking DNS Security Associate beforehand.

#### Workshop Content/Agenda

- Exploring Threat Defense
- Setting Up the Lab
- Demystifying NIOS-X
- Examining DNS Forwarding Proxies
- Examining Infoblox Endpoints
- Installing & Managing Infoblox Endpoints
- Examining External Networks & Secondary Network Scopes
- Examining Security Policies, General Settings & Precedence
- Inspecting Policy Rules & Actions
- Configuring Threat Defense Security Policies
- Integrating DNS Forwarding Proxies into Security Policies
- Adding Endpoint Groups to Security Policies
- Intercepting Exfiltration with Threat Insight
- Analyzing Threat Defense Reports
- Examining Discovery Reports
- Using Application Discovery Reports
- Using Web Content Discovery Reports