corelight

Training brief

Corelight on-demand training: Gold

SERVICE OVERVIEW

Corelight Gold Training is an elite, three-day immersive program designed to transform security teams into network detection experts. Delivered virtually and at your own pace, this "Gold" tier offering provides hands-on instruction from world-class Corelight experts. The course is specifically engineered for incident responders, threat hunters, and penetration testers to help them realize the full potential of Zeek®, Suricata, and the Corelight platform. By blending deep-dive architectural knowledge with interactive Capture the Flag (CTF) exercises, this training ensures your organization can extract maximum intelligence from your network traffic.

DELIVERABLE DESCRIPTION

- **Comprehensive course modules:** Access to in-depth training content spanning from foundational Network Traffic Analysis (NTA) to advanced detection engineering
- **Hands-on CTF exercises:** Multiple real-world Capture the Flag scenarios designed to test skills against live attack simulations and protocol analysis
- **Technical deep dives:** Detailed guides on log structures (conn, dns, http, ssl, etc.), API integration, and Fleet Manager orchestration
- **Specialized frameworks:** Access to the Corelight Threat Hunting Guide and instruction on leveraging the MITRE ATT&CK® matrix with Corelight data

ENGAGEMENT PRE-REQUISITES

- **Participant skillset:** Students should be comfortable with networking protocols (IP, TCP, UDP, DNS, HTTP) and standard Security Operations Center (SOC) workflows
- **Familiarity:** Designed for those who may be new to Zeek but are experienced in security operations; no prior Corelight-specific experience is required

SERVICE ENGAGEMENT PROCESS

- The Gold Training is delivered virtually, allowing for a flexible yet rigorous learning path. The curriculum is structured to move from administrative foundations to expert-level hunting

CURRICULUM

Day 1: Deployment & management foundations

- **Corelight Fundamentals:** Introduction to NTA and NDR using current, real-world incident use cases
- **Architecture & visibility:** Discussing network segments, TAP/SPAN configurations, and hardware vs. virtual/cloud sensor throughput
- **Administrative mastery:** Hands-on with the diagnostic shell, REST API for SIEM integration, and deploying/managing sensors at scale via Fleet Manager

Day 2: Data intelligence & integration

- **Suricata integration:** Contrasting Zeek and Suricata roles, rule structure, and uploading rulesets
- **The Zeek progression:** Mapping the path from introductory user to deep expert/developer
- **Deep dive into Logs:** Granular analysis of essential logs including conn, kerberos, ntlm, x509, and dpd
- **Advanced collections:** Exploring encrypted traffic and Command & Control (C2) inference packages

Day 3: Advanced operations & detection engineering

- **Incident response:** Conducting protocol logging and file extraction investigations using only network data
- **Threat hunting:** Using the MITRE ATT&CK® matrix to hunt across months of DNS, SMB, and SSH data
- **Detection engineering:** The "art" of transforming raw traffic into intelligence. Covers custom Zeek scripts, YARA signatures, and the intelligence/input frameworks for business context

TERMS AND ASSUMPTIONS

- **Service scope:** Includes three days of virtual, interactive learning led by Corelight experts, featuring customizable sessions for team-specific needs
- **Access:** Delivered virtually as an on-demand, self-paced, or instructor-led offering (as specified by the Gold tier parameters)
- **Corelight advantage:** Training is built on the "open-core" philosophy, leveraging the expertise of the original creators of Zeek
- **Customer responsibilities:** Participants must meet the prerequisite networking knowledge to ensure the depth of the "Gold" curriculum can be fully absorbed

corelight

To learn more about Corelight training, please visit

https://corelight.com/support/training

info@corelight.com | 888-547-9497