corelight

## Training brief

# Corelight Education Services training overview

Corelight Education Services offers a comprehensive suite of training programs designed to build mastery across the entire Network Detection and Response (NDR) lifecycle. From initial sensor deployment to advanced detection engineering, these courses provide the technical depth required for modern security operations.

### CORELIGHT FOUNDATIONAL TRAINING

*Three-day, Instructor-led (Virtual or On-site)*

This course is designed to empower up to 20 participants with the skills to effectively operate and leverage Corelight's NDR solution. It delivers expert-led instruction to build proficiency in sensor administration, log analysis, incident response, and threat hunting.

- **Day 1: Corelight fundamentals & deployment foundations**—Covers Network Detection & Response (NDR), architecture & visibility, administrative mastery, scalable operations, and advanced inspection
- **Day 2: Extending & interpreting Corelight data**—Focuses on log analysis deep dive and advanced collections
- **Day 3: Advanced operations & detection engineering**—Covers incident response, threat hunting, and detection engineering
- **Knowledge checks and hands-on labs**—Interactive assessments to validate theoretical comprehension and guided technical exercises to reinforce configuration and operational proficiency
- **Practical validation**—A Capture-the-Flag (CTF) exercise focused on log-based forensic reconstruction

### CORELIGHT INVESTIGATOR FOUNDATIONAL TRAINING

*One-day, Instructor-led (Virtual)*

This course is designed to equip up to 20 participants with essential skills to operate Corelight's Investigator NDR platform. It covers the fundamentals of Zeek®, Suricata, and Investigator's machine learning and log search capabilities.

- **Module 1: Admin, configuration, security & detections**—Covers initial admin login, sensor configuration, user setup, monitoring, and dashboard utilization
- **Module 2: Writing LogScale queries & hands-on labs**—A roadmap for mastering Zeek data analysis in LogScale, from foundational structures to query optimization
- **Module 3: Getting started with Corelight**—Explores data types for network monitoring, advantages over open-source tools, and Suricata/SmartPCAP integration
- **Module 3: Machine learning models**—Explains the scope of machine learning models and their benefits for incident response
- **Module 4: Log search use case: Threat hunting & hands-on labs**—Demonstrates log search functionality and identifies attack methods through practical exercises

### ON-DEMAND TRAINING: GOLD

*Three-day, Self-paced or Virtual*

Our premier on-demand offering is an elite, immersive program designed to transform security teams into network detection experts. It is specifically engineered for incident responders, threat hunters, and penetration testers.

- **Day 1: Deployment & management foundations**—Covers Corelight fundamentals, architecture & visibility, and administrative mastery
- **Day 2: Data intelligence & integration**—Focuses on Suricata integration, the Zeek progression, deep dive into logs, and advanced collections
- **Day 3: Advanced operations & detection engineering**—Covers incident response, threat hunting, and detection engineering
- **Hands-on CTF exercises**—Multiple real-world Capture the Flag scenarios designed to test skills against live attack simulations
- **Corelight advantage**—Built on the "open-core" philosophy, leveraging the expertise of the original creators of Zeek

corelight

To learn more about Corelight training, please visit

**https://corelight.com/support/training**

info@corelight.com | 888-547-9497