corelight

Corelight Training

One day course

Delivered onsite or virtually

This course teaches new-to-Corelight incident responders, threat hunters and penetration testers everything they need to know to start using this powerful tool. The course balances lectures and lab exercises while covering the need for network monitoring, how to deploy Corelight Sensors, and the value of Corelight data. The day ends with a Capture the Flag exercise designed to test the skills you've just learned.

COURSE MODULES

Why NTA? Why NDR? **Why Smart PCAP?** **Why Investigator?** **Why Corelight?**	We will cover what Network Traffic Analysis and Network Detection and Response are with examples using current and relevant incidents, intrusions and compromises as use cases. This foundational model will frame the remainder of the course with context and background.
Corelight in Your Network	This interactive module covers common protocols, and data visibility across the network, leading into an overview of SPAN ports, taps, and packet brokers. We end with a walkthrough of exporting.
ETC and C2 Collections from Corelight Research	Corelight's research continues to enhance the visibility above and beyond open-source Zeek®. We'll highlight the latest updates to include the Encrypted Traffic Collection and Command and Control Collection of inference packages.

COURSE MODULES *(continued)*

Use case: Incident Response	Learn how Suricata and Zeek work together to detect, investigate and track threats in real time with Investigator. The power of Zeek, Suricata and Investigator becomes clear when used for incident response investigations. We'll complete a hands-on investigation, including file extraction and protocol logging using only network data.
Capture the Flag Competition	We will apply Corelight data in a variety of scenarios, including internal hosts compromised by malware infections and externally-exposed hosts being compromised. Participants need speed and precision to find artifacts and assemble the attack's storyline and workflow. An instructor is available to answer 1:1 questions and guide students through the challenge questions.

To learn more about Corelight training, please visit **https://www.corelight.com/support/training** or the Corelight website **corelight.com**

corelight

Corelight provides security teams with network evidence so they can protect the world's most critical organizations and companies. On-prem and in the cloud, our open Network Detection and Response platform enhances visibility and analytics, leading to faster investigations and expanded threat hunting. Corelight's global customers include Fortune 500 companies, major government agencies, and large research universities. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek®, the widely-used network security technology.

info@corelight.com | 888-547-9497