corelight

Training from the Corelight cyber security experts

Overview

Now you can tap Corelight's expertise to help your organization discover the powerful advantages of Zeek & Suricata. Whether you're just getting to know Zeek or Suricata or you're an expert optimizing your Corelight deployment, we can help.

While thousands of organizations around the world use Zeek®, no one knows Zeek better than Corelight. Our founders created the open-source project and have led the effort to extend, improve, and scale it over the last 25 years.

With Zeek's focus on evidence-based protocol logs, fusing Zeek logs with Suricata IDS on Corelight Sensors is a force multiplier for your security team. Improve analyst performance, reduce analysis time and quickly pivot between Zeek and Suricata logs on the same Corelight Sensor.

We offer four great options to get started:

TRAINING OFFERINGS

Free Video Training	Visit Corelight on YouTube for an overview of Zeek's and Suricata's power. Understand Corelight and Zeek network traffic analysis better and learn how it can make you more effective. https://www.youtube.com/channel/UC3nsuVl5AO7z-Qu-VTn8JQg
Foundational Training	1.5 hours of Corelight foundational knowledge available free to all Corelight customers. Ask your TAM to get enrolled.
One Day Virtual or Onsite Course	For incident responders and threat hunters new to Zeek & Suricata, this training balances lectures and lab exercises to take skills to the next level.

TRAINING OFFERINGS (*continued*)

Three Day Virtual or Onsite Course	This in-depth course takes individuals or teams with minimal knowledge of Zeek & Suricata through sensor deployment and use, with an emphasis on real-world data structure. Day one is more administrative-focused. Days two and three are analyst/security operations-focused.
Silver Customer Academy On-Demand Training	Hosted on Corelight's Learning Management System, the Silver edition recordings are for individuals and teams that require on demand training or need sustainment training on demand or self-paced. Content for the silver edition is from our one day training.
Gold Customer Academy On-Demand Training	Hosted on Corelight's Learning Management System, the Gold edition recordings include everything from the Silver edition but take it much further—deep dives, additional labs, scripting and more. It's designed for individuals and teams that require on training or need sustainment training on demand or self-paced. Content for the gold edition is from our three day training.
Custom Training	We offer various custom training: Zeek scripting, SPCAP into Wireshark, Suricata rule writing, advanced threat hunting and more. Let us know what you want to learn more of.

Examples of the topics we'll cover

- Introduction to Zeek
- Introduction to Suricata
- Common protocols used by attackers
- How to pivot between Zeek and Suricata logs and use fused logs for faster analysis
- How to detect and search for threats in your network
- Investigate different use cases from MITRE ATT&CK®
- How to search for malicious activity going back months or years

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