corelight

Training brief

Corelight Investigator Foundational Training Service datasheet

SERVICE OVERVIEW

Corelight's Investigator Foundational Training Service is a one-day, instructor-led course designed to equip up to 20 participants with essential skills to operate Corelight's Investigator Network Detection and Response (NDR) platform. This training covers the fundamentals of Zeek®, Suricata, and Investigator's machine learning and log search capabilities, focusing on sensor administration, threat detection, and threat hunting. Delivered virtually, the course empowers your team to leverage Investigator effectively, aligning with your security objectives.

DELIVERABLE DESCRIPTION

- **Training materials:** Comprehensive slide decks, reference guides, and resources covering Zeek, Suricata, SmartPCAP, Investigator administration, machine learning models, and threat hunting use cases
- **Practical exercises:** Guided exercises within Investigator, including log search and detection analysis, to apply concepts like threat hunting and dashboard monitoring
- **Course completion certificate:** Issued to participants upon successful completion of the one-day training. This certificate acknowledges participation and is not an industry certification
- **Knowledge transfer summary:** A concise summary of key concepts, exercise outcomes, and additional resources for continued learning

ENGAGEMENT PRE-REQUISITES

- **Participant readiness:** Attendees should have basic familiarity with network security concepts; no prior Corelight or Investigator experience is required
- **Technical requirements:** Provide participants with access to a computer with a stable internet connection, web browser, and virtual lab environment access (provided by Corelight)
- **Stakeholder coordination:** Designate a point of contact to coordinate scheduling, participant lists, and logistical details

SERVICE ENGAGEMENT PROCESS

- **Scheduling:** A Corelight network security trainer coordinates with your team to confirm scheduling, participant details, and delivery logistics for the virtual training

CURRICULUM:

- **Module 1: Admin, configuration, security & detections**
  - Covers initial admin login, sensor configuration, and user setup
  - Introduces monitoring, detection capabilities, and dashboard utilization within Investigator
- **Module 2: Writing LogScale queries & hands-on labs**
  - A comprehensive roadmap for mastering Zeek data analysis in LogScale, progressing from foundational log structures to advanced behavioral modeling and query optimization
- **Module 3: Getting started with Corelight**
  - Explores data types for network monitoring, comparing Zeek data to traditional logs
  - Highlights advantages of Corelight sensors over open-source tools
  - Introduces Suricata integration, SmartPCAP, and an overview of the Investigator platform

- **Module 4: Machine learning models**
  - Explains the scope and use of machine learning models in Investigator
  - Compares ML-driven analysis with manual methods and highlights benefits for incident response
- **Module 4: Log search use case: Threat hunting & hands-on labs**
  - Demonstrates log search functionality in Investigator for threat hunting
  - Guides participants in identifying attack methods through practical exercises
- **Course wrap-up:** Reviews key takeaways, collects participant feedback, and provides resources for ongoing learning

TERMS AND ASSUMPTIONS

- **Service scope:** Includes a one-day, instructor-led foundational training for up to 20 participants, delivered as a dedicated offering, with practical exercises and comprehensive materials
- **Delivery:** Available as virtual or on-site (SKU specific)
- **Validity:** The service is valid for one year from the date of purchase
- **Customer responsibilities:** Provide participant details, ensure technical requirements are met for virtual delivery, and coordinate scheduling
- **Limitations:** The service is non-exchangeable for other Corelight services or products.

corelight

To learn more about Corelight training, please visit

https://corelight.com/support/training

info@corelight.com | 888-547-9497