corelight

Service briefing datasheet

Corelight Foundational Training

Service overview

Corelight's Foundational Training is a three-day, instructor-led, lab-enabled foundational course designed to empower up to 20 participants with the skills to effectively operate and leverage Corelight's Network Detection and Response (NDR) solution. This comprehensive training covers Corelight Sensor administration, log analysis, incident response, and threat hunting, with hands-on labs to reinforce practical application. Delivered virtually or on-site, the course equips your team with the knowledge to maximize the value of Corelight's platform and accelerate user adoption.

Deliverable description

- **Training materials:** Comprehensive slide decks, lab guides, and reference resources covering Corelight Sensor administration, Zeek® logs, Suricata, YARA, and threat hunting techniques.
- **Hands-on lab exercises:** Two Capture the Flag (CTF) lab sessions to practice real-world scenarios, including log analysis, incident response, and threat hunting.
- **Course completion certificate:** Issued to participants upon successful completion of the three-day training.
- **Knowledge transfer summary:** A wrap-up document summarizing key concepts, lab outcomes, and additional resources for continued learning.

Engagement prerequisites

- **Participant readiness:** Attendees should have basic familiarity with network security concepts; no prior Corelight experience is required.
- **Technical requirements (virtual delivery):** Participants must have 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 format (virtual or on-site), ensuring alignment with your needs.
- **Day 1:** Corelight sensor administration & fundamentals:
  - Introduces Network Traffic Analysis (NTA), NDR, Zeek, and Corelight's value proposition.
  - Covers sensor deployment (hardware, virtual, cloud), diagnostic shell, monitoring, Corelight Fleet installation, Suricata, Zeek levels, and sensor health operations.
- **Day 2:** Deep dive into logs & hands-on labs:
  - Explores Zeek logs in-depth, as well as Corelight Collections and Packages, including encrypted traffic, command-and-control (C2), entity collection, core collection, and ICS/OT collection.
  - Conducts Capture the Flag (CTF) Lab – Round 1 for practical application of log analysis skills.
- **Day 3:** Incident response, threat hunting & advanced labs:
  - Focuses on using Corelight data for incident response and threat hunting.
  - Introduces YARA and Zeek scripting for advanced analysis.
  - Conducts Capture the Flag (CTF) Lab – Round 2 to apply incident response and threat hunting techniques.
  - Concludes with a course wrap-up, participant feedback, and resource sharing.
- **Course wrap-up:** Reviews key takeaways, collects participant feedback, and provides resources for ongoing learning.

Terms and assumptions

- **Service scope:** Includes a three-day, instructor-led foundational training for up to 20 participants, delivered as a dedicated offering, with hands-on labs 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-refundable and non-transferable for other Corelight services or products.

https://corelight.com/contact

info@corelight.com | 888-547-9497