corelight

Service briefing datasheet

Corelight Investigator Quickstart service

Service overview

The Corelight Investigator Quickstart service accelerates your detection and response capabilities by delivering a tailored onboarding experience for the Investigator solution. This service combines foundational training, expert-led configuration, and in-depth detection analysis to align the Investigator platform with your specific security requirements and Corelight's recommended practices. Our goal is to equip your team to confidently leverage Investigator for rapid threat detection and long-term operational success.

Deliverable description

- **Configured Investigator platform:** Fully operational setup of Investigator components, customized to your environment and integrated with one (1) SIEM, based on best practices.
- **Alert reductions (2):** Tuning of Investigator alerting thresholds with a focus on identifying meaningful detections within the monitored environment.
- **Detection reports (2):** Comprehensive reports detailing detected vulnerabilities, alerts, affected entities, and suggested remediation actions.
- **Executive summary report:** Summarizes findings, recommendations, and outcomes from detection review sessions for leadership visibility.
- **As-built documentation:** Detailed documentation of the solution's high-level and low-level design and final Investigator configuration for ongoing reference and management.
- **Knowledge transfer:** Insights and guidance provided through detection tuning and consultation sessions to support team readiness.

Engagement pre-requisites

- **Recommended training:** Customers are encouraged to complete the included one-day virtual training prior to configuration activities to build a foundational understanding of Investigator capabilities.
- **System access:** Provide access to relevant systems and data for configuration and integration purposes.
- **Stakeholder availability:** Ensure key customer SOC personnel are available for training, detection review, and consultation sessions to maximize engagement outcomes.

Service engagement process

- **Engagement kickoff:** Aligns Corelight and customer teams, establishes a communication plan, sets the engagement timeline, and identifies unique requirements.
- **One-day virtual training:** Interactive, foundational training for up to 20 participants, led by Corelight experts to build proficiency in Investigator's capabilities.
- **Platform configuration:** Configures the Investigator platform based on your requirements and Corelight's practices, aiming to align integration with the monitored environment.
- **Detection analysis and reporting (two iterations):** Conducts two in-depth reviews of the Investigator instance to optimize configurations, enhance threat visibility, and validate detections. Resulting in two (2) detection reports.
- **Detection consultation review sessions (two sessions):** Facilitates discussions to support implementation of Corelight's recommendations and address technical questions. Investigator tuning is performed after each session to iteratively calibrate Investigator based on customer feedback.
- **Operational transfer:** Provides as-built documentation, an executive summary report, and a formal knowledge transfer to ensure your team is equipped to manage Investigator effectively.

Terms and assumptions

- **Service scope:** Includes deployment advisement, configuration of all Investigator components, two detection reports, and four hours of project management.
- **Training:** One-day virtual training for up to 20 participants is included but not exchangeable for other Corelight products or services.
- **Validity:** The service is valid for one year from the date of purchase.
- **Delivery:** Eligible for on-site delivery; travel and expenses are not included.
- **Customer responsibilities:** Provide timely access to systems, personnel, and information required for successful engagement execution. Delays may result in rescheduling or scope adjustment.
- **Critical detections:** Corelight's team is available for swift response and assistance if critical detections require immediate attention during the engagement.
- **Limitations:** The service is non-exchangeable for training or other Corelight products.

https://corelight.com/contact

info@corelight.com | 888-547-9497