corelight

Service briefing datasheet

Corelight Resident Engineering

Service overview

The Corelight Resident Engineering service provides a dedicated, expert Resident Engineer to work alongside your team for a 3, 6, or 12-month engagement, supporting your network detection and response (NDR) solution achieves operational effectiveness and actionable security outcomes. This service focuses on architecture and design assistance, solution performance optimization, threat hunting support, detection analysis, and knowledge transfer to enable your team. By aligning with your operational and security goals, our Resident Engineer supports improvements in your NDR solution's reliability, visibility, and effectiveness in incident response, threat hunting, and SOC operations.

Deliverable description

- **Architecture and design documentation:** Formal design and architecture reviews, including high-level and low-level design documents tailored to your environment.
- **Solution performance reports:** Ongoing configuration, tuning, and visibility management reports to support optimal NDR performance and system health.
- **Scripting and advanced solutioning:** Development of Zeek® and other scripts focused on optimizing the performance of your Corelight solution. Scripts remain the property of Corelight.
- **Utilization and traffic consulting:** Optimizing monitoring strategies through analysis of what is monitored.
- **Data hygiene & log consulting:** Evaluation of data and log use for applied use cases.
- **Use case enablement:** Advisement on Corelight use and application based on customer mission objectives, to include solution configuration and calibration to meet identified use cases.
- **Threat hunting and detection analysis reports:** Actionable insights from Corelight data, including threat analysis, prioritized recommendations, and validated detections.
- **Key performance indicators (KPIs):** Customized KPIs for system health, network services, and security outcomes, developed in collaboration with your team.
- **Knowledge transfer materials:** Comprehensive documentation and training sessions to equip your staff with skills for system management, threat hunting, and advanced SOC workflows.
- **Staff augmentation:** Corelight expert operating as an extension of your existing staff.
- **Support liaison:** Liaison to Corelight teams to accelerate troubleshooting efforts and resolutions facilitated through Corelight support.

Engagement pre-requisites

- **System access:** Provide access to your Corelight NDR solution and relevant systems for configuration, tuning, and analysis.
- **Stakeholder engagement:** Ensure availability of customer's security and network team members to collaborate on design reviews, threat hunting, and knowledge transfer sessions.
- **Defined objectives:** Share operational and security goals to guide the Resident Engineer's efforts in aligning the NDR solution with your needs.

Service engagement process

- **Engagement kickoff:** Aligns the Resident Engineer with your team, establishes communication channels, and defines operational and security objectives for the engagement.
- **Architecture and design assistance**: Conducts formal reviews to develop and document high-level and low-level designs, ensuring the NDR solution aligns with your environment and goals.
- **Solution performance optimization:** Performs ongoing configuration, tuning, and visibility management to maintain efficient NDR performance, including developing KPIs for system health and network services.
- **Threat hunting and detection analysis:** Enables critical use cases (e.g., incident response, threat hunting, SOC operations) by analyzing Corelight data, providing actionable recommendations, and validating detections through iterative reviews.
- **Knowledge transfer:** Facilitates formal enablement sessions and provides documentation to equip your team with skills for system management, threat hunting, and advanced SOC workflows.
- **Support liaison and strategy advisement:** Acts as a liaison with Corelight support for enhanced troubleshooting and advises on security strategies and policies to strengthen SOC disciplines.
- **Ongoing reporting and review:** Delivers regular reports on performance, threat analysis, and resolutions, with periodic reviews to ensure alignment with your goals.

Terms and assumptions

- **Service scope:** Provides one designated Resident Engineer for a 3, 6, or 12-month term, focusing on architecture and design, solution optimization, threat hunting, detection analysis, and knowledge transfer.
- **Delivery:** Eligible for on-site or remote delivery; travel and expenses are not included.
- **Validity:** The service is valid for the term purchased.
- **Customer responsibilities:** Provide timely access to systems, personnel, and information to support the Resident Engineer's activities.
- **Limitations:** The service is non-exchangeable for training or other Corelight products.
- **Engagement flexibility:** The Resident Engineer adapts to your operational and security priorities, with scope adjustments requiring mutual agreement.

Deliverable description

- **Architecture and design documentation:** Formal design and architecture reviews, including high-level and low-level design documents tailored to your environment.
- **Solution performance reports:** Ongoing configuration, tuning, and visibility management reports to support optimal NDR performance and system health.
- **Scripting and advanced solutioning:** Development of Zeek and other scripts focused on optimizing the performance of your Corelight solution. Scripts remain the property of Corelight.
- **Utilization and traffic consulting:** Optimizing monitoring strategies through analysis of what is monitored.
- **Data hygiene & log consulting:** Evaluation of data and log use for applied use cases.
- **Use case enablement:** Advisement on Corelight use and application based on customer mission objectives, to include solution configuration and calibration to meet identified use cases.
- **Threat hunting and detection analysis reports:** Actionable insights from Corelight data, including threat analysis, prioritized recommendations, and validated detections.
- **Key performance indicators (KPIs):** Customized KPIs for system health, network services, and security outcomes, developed in collaboration with your team.
- **Knowledge transfer materials:** Comprehensive documentation and training sessions to equip your staff with skills for system management, threat hunting, and advanced SOC workflows.
- **Staff augmentation:** Corelight expert operating as an extension of your existing staff.
- **Support liaison:** Liaison to Corelight teams to accelerate troubleshooting efforts and resolutions facilitated through Corelight support.

https://corelight.com/contact

info@corelight.com | 888-547-9497