SOLUTION BRIEF

Stellar Cyber + Corelight

Together, we accelerate threat prevention, detection and response across the entire IT infrastructure

corelight

STELLAR CYBER®

Why We Work Better Together

- The foundation for the next generation security defense system for enterprises is built on the promise of consolidation, automation and simplification to enable them to radically reduce the risk of being compromised and dramatically improve both attack detection and response time.
- The joint solution through this partnership between Stellar Cyber and Corelight delivers a seamless integration between comprehensive network evidence collection from Corelight and AI-powered detection and automatic response technology from Stellar Cyber. Corelight transforms network and cloud activity into evidence that is fed to Stellar Cyber's Open XDR security operations platform for advanced analysis.
- As one of the native capabilities of Stellar Cyber's Open XDR platform, expansive security analysis with machine learning-driven detections correlates events from Corelight Sensors and many other data sources, including Threat Intelligence, to piece together complex attacks across the entire attack surface. Powerful, yet easy-to-build automatic response playbooks leverage high-fidelity detections, improving the SOC's efficacy and efficiencies.

Business Challenges

Today, cyber security experts have a wealth of products at their fingertips, but many of these products are siloed or disconnected from one another. This creates coverage gaps, making the investigation of each individual alert time-intensive, overloading already short-staffed security analysts, and prolonging the response time. Building 360-degree visibility across the network, endpoints, users, applications, and cloud is challenging with these silos and often means pulling together all the available tools or a large volume of data generated by each individual tool. This can be an extremely tedious manual task and is time-intensive for analysts. AI promises to improve the ability to piece together complex attacks and reduce alert fatigue, but there is more that can be done through integration and automation.

Solution at a Glance

Corelight provides comprehensive, correlated evidence that enables security analysts to unlock new analytics, investigate faster, hunt like an expert, and even disrupt future attacks.

Stellar Cyber's Open XDR is an open security operations platform for detection, investigation and automatic response by ingesting, normalizing, enriching, analyzing and correlating data from hundreds of tools, including Corelight's security solutions.

Open XDR's **AI-powered, high-fidelity detection and event correlation** reduces the alert noise so that security analysts can focus on more important tasks and not miss the attacks.

In addition, Open XDR has **many natively supported applications**, which complement the tools you already trust, removing product silos and filling the coverage gaps with your existing tools.

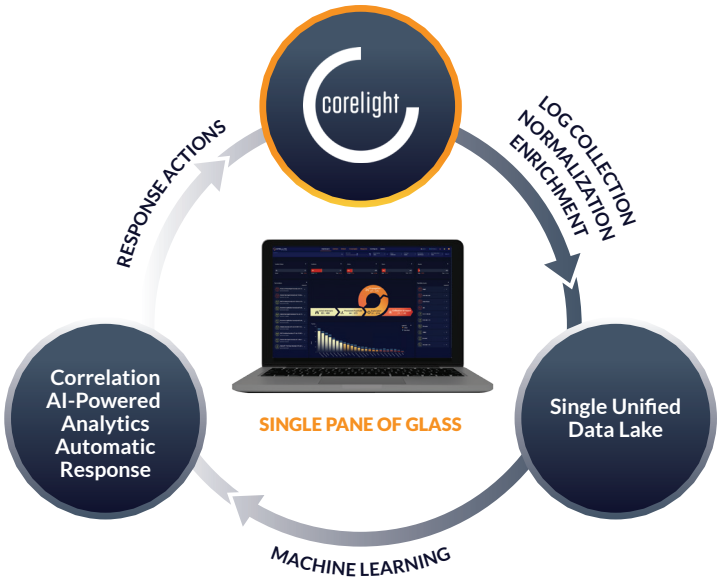
Another challenge is that firewalls, as a prevention technology, by nature are designed to block traffic, which can create a large amount of events that can lead to alert fatigue.

Moreover, this can lead security teams to fall behind or even to miss alerts as they don't have enough time to investigate them all fully. There are many tools out there that are great for detecting anomalous activity, but these tools often require additional monitoring and investigation with all the alerts they produce because anomalous activity is not always synonymous with malicious attacks.

A new approach to these problems is needed, and they can be solved with Corelight's network detection and response platform combined with Stellar Cyber's advanced detection with Machine Learning technology and automatic response through tight API integration. Together, we deliver an integrated advanced prevention, automated detection and response platform across the entire IT infrastructure.

Benefits

- Delivers 360-degree visibility and threat protection across networks, endpoint, users, applications and cloud.
- Enables analysts to quickly respond to high-fidelity detections across the entire kill chain improving both MTTD and MTTR.
- Radically improves security analysts' productivity and efficiency with dramatically reduced cost.



How It Works

Stellar Cyber's Open XDR security platform provides AI-powered detection, event correlation, threat investigation and automatic response capability, improving analyst productivity by piecing together attacks from across the entire IT infrastructure to reduce threat response time. Corelight transforms network and cloud activity into evidence so that data-first defenders can stay ahead of ever-changing attacks.

STELLAR CYBER®

Stellar Cyber's Open XDR platform delivers Everything Detection and Response by ingesting data from all tools, automatically correlating alerts into incidents across the entire attack surface, delivering fewer and higher-fidelity incidents, and responding to threats automatically through AI and machine learning. Our XDR Kill Chain™, fully compatible with the MITRE ATT&CK framework, is designed to characterize every aspect of modern attacks while remaining intuitive to understand. This reduces enterprise risk through early and precise identification and remediation of all attack activities while slashing costs, retaining investments in existing tools and accelerating analyst productivity. Typically, our platform delivers an 8X improvement in MTTD and a 20X improvement in MTTR.

For more information, visit stellarcyber.ai

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.

For more information: www.corelight.com