CASE STUDY

IT firm deploys Corelight to gain east-west visibility and accelerate incident response

BACKGROUND

Ednon, headquartered in Spain, is an information technology and cybersecurity services provider with over 150 customers worldwide. Ednon's Security Operations Center / Security Incident Response Team (SOC-CSIRT) delivers a wide range of services to clients, including vulnerability management, detection and threat hunting, and incident response.

Ednon's Cybersecurity Business Unit Director, Antonio Gómez-Iglesias Rubio, wanted a cybersecurity solution that could deliver continuous, comprehensive and actionable visibility across their customers' networks, especially for east-west traffic, to address threats like command and control (C2) servers and data exfiltration. Gómez-Iglesias Rubio knew that telemetry from a network detection and response (NDR) solution, aggregated and analyzed in their SIEM in conjunction with telemetry from their existing EDR tool, could close critical visibility gaps and unlock faster and more effective threat detection and response for their clients.

CHALLENGES
Ransomware, lateral movement, network & EDR visibility gaps

SOLUTION
Corelight Open NDR Platform

RESULTS
Expanded visibility & detection capabilities at earliest attack stages

CHALLENGES

As a global services provider, Ednon's SOC-CSIRT monitors and defends a highly distributed series of networks across clients locations, many of which have high traffic volumes and continual east-west connectivity between servers and data centers.

Ednon's team had previously deployed firewall and IPS tools in these environments, but found that they left detection gaps around east-west connectivity and could not deliver the depth of visibility required to quickly and consistently validate alerts and respond to threats, slowing down their response times to certain incidents.

> ***"Network detection and response (NDR) are essential to identify attack patterns and malicious behaviors that could go unnoticed with other solutions, providing an additional layer of defense against sophisticated threats."***
>
> Antonio Gómez-Iglesias Rubio, Ednon Cybersecurity Business Unit Director

SOLUTION

To close these visibility gaps and expand detection coverage, the Ednon team required an NDR platform that excelled at monitoring east-west flows, could reliably scale to large traffic volumes, and that seamlessly integrated with their existing SIEM.

The team evaluated various commercial NDR vendors and chose Corelight's Open NDR Platform based on its ability to satisfy these requirements and due to its threat detection strength and ease of integration, among other competitive differentiators they surfaced during their product evaluation.

"The need to improve visibility and responsiveness led us to seek an NDR solution," said Gómez-Iglesias Rubio. "We made our selection based on Corelight's reputation for its network-centric approach, scalability, and its flexibility of distributed architecture for our clients."

Gómez-Iglesias Rubio and the Ednon team also appreciated that Corelight is National Information Assurance Plan Common Criteria (NIAP CC) certified, making its NDR platform suitable for deployment in public organizations so they could deploy Corelight in different government networks across their customer base.

RESULTS

Ednon successfully deployed Corelight and integrated it with their SIEM, allowing the team to continuously monitor and analyze network traffic across their customer sites, detect suspicious and malicious behaviors, and boost their organizational capacity to support clients with prevention, defense, analysis, investigation, recovery, and response. Key use cases for Ednon's SOC-CSIRT enabled by Corelight include:

- Deep inspection of data transferred through key protocols such as SMB, SMTP, DNS, and FTP, as well as visibility around encrypted protocols like RDP, SSH, and SSL
- Detection of inappropriate/anomalous usage and identification of unauthorized/abusive activities to minimize the number of false positives
- Verification of unidentified attack patterns and unexpected behavior of network clients
- Providing corrective recommendations and improvement plans to help prevent significant security incidents and enhance overall security posture.

"We have experienced significant improvements in network visibility, more comprehensive detection coverage, and faster incident response. These improvements have effectively reduced our operational costs and strengthened our security posture by integrating Corelight with the rest of our security stack."

Antonio Gómez-Iglesias Rubio, Ednon Cybersecurity Business Unit Director

"Corelight stands out for its ability to provide a holistic view of the network and detect sophisticated threats that could go unnoticed by other tools," said Gómez-Iglesias Rubio. "Corelight has proven to be a valuable addition to our cybersecurity toolset, enhancing our ability to face evolving threats and mitigate risks."

Request a demo of the Open NDR Platform at **https://corelight.com/contact**

corelight

Corelight provides security teams with network evidence so they can protect the world's most critical organizations and companies. 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.

info@corelight.com | 888-547-9497