Challenge
A services company couldn't respond to incidents due to broken or missing data

Solution
Corelight delivered rich, pivotable evidence that lead to massive improvements

Case Study

Security team sees 95% reduction in incident response time with Corelight's network visibility

Background
Founded in 1965, Education First is a privately held education services company operating over 500 offices and schools worldwide, and staffed by more than 40,000 employees. The company has three global business divisions focused on language and schools, educational travel, and cultural exchange programs.

Ken Hanson, Sr. Security Engineer at Education First, discovered Corelight when researching network security monitoring (NSM). Hanson runs an agile security team at Education First, and is responsible for the security program of nine business sites spanning the Americas and the European Union.

> ***"With Corelight, the ability to track lateral movement in your network skyrockets."***
>
> *-Ken Hanson, Sr. security engineer*

Challenges
Education First needed a network visibility and monitoring solution to provide real-time, detailed insight into network traffic spanning multiple business sites that each averaged approximately 1 Gbps of throughput.

The company had already implemented next-generation firewalls, an AV solution, and a SIEM solution to coordinate security alerts and responses. These tools, however, could not give Hanson and his team the deep network visibility they needed to efficiently and effectively respond to security incidents and hunt for threats in their network. Specifically:

- It took hours, on average, to gather and correlate network data for incident response with logs scattered across many servers and business units.
- Incident responders could not answer certain critical questions because available server logs or records (e.g., NetFlow) gave only partial insights.
- Hanson's team could not easily judge the relevance of vendor security alerts and pinpoint the corresponding network flows for deeper investigation.

Solution

Education First sought a vendor to help address these network visibility challenges, and presented a number of solution requirements:

- Comprehensive visibility: Solution must provide actionable insight across all network protocol types
- Negligible TCO: Solution must offer easy, fast setup and requires no ongoing maintenance
- No user pain: Solution must not generate security noise nor interfere with user network experiences
- SIEM integration: Solution must automatically export network visibility data to a SIEM solution

Hanson and his team evaluated a range of NSM products and determined that Corelight not only met all solution requirements, but clearly excelled amongst competitive vendors when it came to the depth of network information provided and the product ease-of-use.

On the richness of the Corelight Sensors' network logs, Hanson remarked, "The insight we can get from these logs is actually amazing," citing the visibility he now has around internal apps running in his environment and his ability to pivot quickly through the logs and evaluate security alerts from his firewall or AV solution.

Corelight Sensors operate out-of-band and are built on Zeek, the powerful and widely-used open source framework for network monitoring and analysis.

Corelight Sensors can ingest traffic from an optical tap, SPAN port, or packet broker and can reliably scale analysis to 25 Gbps+ of throughput. The Sensors output logs describing all network traffic, organized by protocol and comprising hundreds of data fields that comprehensively summarize each event in specific, actionable detail. Organizations can export these logs to a range of storage and analytic tools, such as Amazon S3 or SIEM solutions like Splunk, Chronicle, or Elastic.

Results

Hanson and his team saw immediate benefits from deploying Corelight, including substantially reduced incident response time and an enhanced ability to perform threat hunting.

"Now when we get an alert from our AV vendor, we routinely use Corelight logs to rapidly investigate the issue by pivoting from IP address, to device, to user, to source in a matter of minutes," said Hanson. "Before Corelight that task was very inefficient and in some cases impossible because of a lack of available information."

Without Corelight	With Corelight
3 hour average incident response time.	<10 minute average incident response time.
Network logs scattered across multiple servers and business units.	Network logs available from a single, central source of truth.
Inability to answer critical network questions because of incomplete information.	Definitive ability to answer critical network questions with granular precision.
Difficulty evaluating and investigating security alerts.	Can easily investigate security alerts to identify true/false positives and locate related PCAP files.
Limited bandwidth to threat hunt given inefficiencies of incident response process.	Unlocked team bandwidth to threat hunt using rich Corelight logs and 3rd party threat intelligence.

The deep network visibility afforded by Corelight also gave Hanson's team unexpected advantages, including expanded compliance monitoring capabilities across their network and the ability to definitively resolve conflicts that sometimes arose between vendor security alerts and end users.

With respect to threat hunting, Hanson's team not only unlocked operational capacity previously devoted to incident response, but also supplemented Corelight's DNS logs with third party threat intelligence to proactively flag potential indicators of compromise for an attack in progress. The comprehensiveness and granular event detail of Corelight's logs have empowered his team to more capably track actors and incidents across Education First's networks.

"I haven't seen a more comprehensive tool for tracking lateral movement," Hanson offered. "With Corelight the ability to track lateral movement in your network skyrockets."

corelight

Defenders have always sought the high ground in order to see farther and turn back attacks. Corelight delivers a commanding view of your network so you can outsmart and outlast adversaries. We capture, interpret, and connect the data that means everything to defenders.

info@corelight.com | 888-547-9497