

# 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 traffic analysis (NTA) solutions. 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.

### 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.

## Executive Summary

### Company

- EF Education First

### About

- A global education services company with over 40,000 employees.

### Solution Requirements

- Visibility across all network protocol types
- No interference with end user network experience
- Does not generate alert noise
- SIEM integration
- Minimal TCO

### Results

- Met all solution requirements
- Reduced average incident response time from around 3 hours to under 10 minutes (95% reduction)
- Enabled resolution of previously unresolvable security incidents due to insufficient information
- Unlocked new operational capacity to threat hunt with Corelight's network logs, supplemented with 3rd party threat intelligence

### Key Quote

"With Corelight, the ability to track lateral movement in your network skyrockets."

- Ken Hanson, Sr. Security Engineer



- Hanson’s team could not easily judge the relevance of vendor security alerts and pinpoint the corresponding network flows for deeper investigation.

The 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 NTA 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 Sensor’s 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 was the easiest product to use. Setting up their appliance took me only 15 minutes, fully integrated, and I had already filtered out the logs I didn’t want,” he added.

“Corelight was the easiest product to use. Setting up their appliance took me only 15 minutes, fully integrated, and I had already filtered out the logs I didn't want.”

- Ken Hanson, Sr. Security Engineer

The Corelight Sensor operates out-of-band and is built on Bro, the powerful and widely-used open source framework for network monitoring and analysis.

The sensor can ingest traffic from an optical tap, SPAN port, or packet broker and can reliably scale its analysis to 10 Gbps of throughput. The sensor outputs 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, ArcSight or QRadar.

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.

Table 1: Customer Results with Corelight

Before	With Corelight
3 hour average incident response time.	<10 minute average incident response time.
Network logs scattered across multiple servers & 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.

“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.”

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 your ability to track lateral movement in your network skyrockets."

The **Corelight Sensor** can be used to help investigate and help prevent a wide range of attacks, including:

- Phishing and mail-based incidents
- Malware infection
- Ransomware
- Denial of service
- Data exfiltration
- Abuse
- Port scanning
- Advanced persistent threat (APT)
- Insider threat
- Unauthorized access
- Misconfiguration

## Corelight Sensor

Transform network traffic into high-fidelity data for your security teams. Designed by the creators of open source Bro, the Corelight Sensor is a turn-key solution tuned for performance at enterprise scale. Configure in minutes, and gain exceptional visibility into your network activity.

**Evaluate a unit for 30 days. Call us.**

✉ [info@corelight.com](mailto:info@corelight.com)

☎ **510-281-0760**

🌐 [corelight.com](https://corelight.com)



[bro.org](https://bro.org)

