Challenge
An energy giant needed better insight into their network, especially east-west (SMB)

Solution
Corelight provided a rich view of all kinds of traffic, enabling quick validation of alerts

Case Study

How Corelight cured an energy company's SOC of a serious SMB headache

Background

A Security Engineer at one of the world's largest energy companies found Corelight through his prior experience running Zeek, an open-source network security monitoring framework. The Security Engineer worked on an agile security engineering team within the organization's Security Operations Center (SOC) and managed network forensics across multiple regional offices.

Challenges

The company wanted a network traffic analysis (NTA) solution to provide real-time visibility into traffic spanning multiple offices. All traffic connected through a central location and averaged a few Gbps of throughput.

> ***"If I didn't have this data I wouldn't sleep well at night. I like to sleep well at night."***
>
> *-Security engineer*

They had had already installed next-generation firewall and IDS solutions, endpoint AV, and a SIEM to manage security alerts and responses. These technologies, however, did not give the Security Engineer and his SOC the deep network insight, and especially east-west visibility, that they needed to troubleshoot problems with their existing security solutions and quickly diagnose and respond to real security alerts.

Specifically:

- They often questioned the validity of alerts from their IDS and other sources, but didn't have data to disprove them. "While the IDS comes with its own connection log, I don't trust it. It's a poor man's connection log compared to Zeek's conn.log," the engineer said.

- Incident responders could not quickly answer key questions using existing logs. He noted his firewall connection logs were mediocre for protocol analysis and that NetFlow also failed them, citing its inability, for example, to identify that someone has started a new SSH daemon on a machine and is actively using it.

Solution

In selecting a vendor to help them address these challenges they established a number of solution requirements:

- Comprehensive network visibility: solution must provide actionable insight across all network protocols, with emphasis on protocols common in east-west traffic, like SMB traffic.
- Easy setup and operation: solution must offer easy, fast setup and require no ongoing maintenance.
- SIEM integration: solution must automatically export network visibility data to a SIEM solution.

The Security Engineer's familiarity with and trust in the power of the open-source Zeek framework made vendor selection simple given Corelight's unmatched Zeek expertise (Zeek's inventor and key-contributors founded Corelight).

"Before Zeek it was all speculation," he remarked. "I pride myself on being able to know my environment and it would eat at me if I couldn't."

Under the hood, Corelight's network traffic analysis capabilities come from a specialized Zeek engine, hardened and optimized for enterprise environments and supporting peak analysis throughput speeds that are up to 10x faster than what's achievable in open-source implementations of Zeek.

The company evaluated Corelight's AP 1000 Sensor, which can ingest traffic from an optical tap, SPAN port, or packet broker and can reliably scale its analysis to 10 Gbps of throughput. The Zeek logs it generates are neatly organized by protocol and comprise hundreds of data fields that comprehensively summarize each event on the network in specific actionable detail. Additionally, Corelight can export these logs to a range of storage and analytic tools, such as Amazon S3 or SIEM solutions like Splunk, Chronicle or Elastic.

> ***"If I didn't have this data I wouldn't sleep well at night. I like to sleep well at night."***
>
> *-Security Engineer*

Results

Setup and configuration

When asked to describe the difficulty of setting up the Corelight Sensor, the Security Engineer laughed.

"It was dead simple to set up. In fact, my SIEM support contact was genuinely surprised when Corelight's logs 'magically' flowed to their instance 'pre-cooked'. He thought it would require extra work to ingest, but the sensor comes pre-installed with the package to do that, right out of the box. It was flawless."

Following a test period, the SOC team determined that Corelight met and excelled in all solution requirements, and witnessed a dramatic example of the power of Corelight and Zeek during their technical evaluation period.

Corelight's SMB logs save the holiday

On the eve of the company's December holiday period, the Security Engineer's boss asked his team to undertake a critical investigation to understand if unauthorized internal sources had accessed a sensitive file on an SMB share.

When later asked to estimate how long it would have taken to resolve this issue without Corelight's SMB logs, the Security Engineer shuddered. "I don't even know that we would have been able to resolve it definitively. Which is scary, we probably would've had to forensically image the file server," he said. "There is no way to easily digest thousands of gigabytes of (read/write) access files from a host-based side."

> ***"These logs validate what's happening on your network vs. what you think may be happening."***
>
> *-Security engineer*

Instead, he searched Corelight's network logs in his SIEM for the file name and quickly located it and its unique Zeek file ID (which allows quick pivots to see where else that file has appeared, across all network protocols, regardless of the file name). The Corelight Sensor's rich SMB protocol log showed that an individual had, in fact, accessed the file in question.

The Security Engineer and his team discovered, documented, and shared this evidence with his boss in a matter of minutes and then left the office to join his family for the holiday, investigation completed.

Debugging an IDS

The data generated by the Corelight Sensor has also empowered their SOC to easily separate false positives from true positives in their alert stream by providing the context and evidence missing from these alerts.

"Whenever I need to debug something going wrong with Snort or my commercial IDS, I can identify what really happened using Corelight's Zeek logs," he said. "These logs validate what's happening on your network vs. what you think may be happening."

SMTP visibility & log enrichment

The Security Engineer also took advantage of the Zeek platform's extensibility, writing a custom script to automatically append the company's classifiers for sensitive emails and documents to Corelight's SMTP Zeek logs.

With enhanced email visibility, he created dashboards that monitor when confidential emails are sent to servers that do not allow STARTTLS. This allowed the SOC to significantly reduce unencrypted transmission of sensitive data.

IR ammunition and insurance

The Security Engineer also noted the data has given their incident response team faster routes to resolution since they can now cut to the truth with a few quick searches. He described how the logs, stored over time, represent an invaluable form of "insurance" in the inevitable event of an attack.

"If there's a major incident and I only have two days' worth of logs to give the incident response team it's going to be really tough to resolve. With Corelight, I can store months or years worth of rich network logs and that makes incident response much more powerful and efficient," he remarked.
"It's an incredible peace of mind to have these logs as insurance for this kind of situation. If I didn't have this data I wouldn't sleep well at night. I like to sleep well at night."

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