Challenge
A major law firm didn't have the visibility they needed to hunt threats effectively

Solution
Corelight provided rich, structured, interlinked evidence for hunting at scale

Case Study

Global law firm unlocks new threat hunting capabilities with a Corelight sensor and Zeek Logs

Background

A major international law firm with hundreds of employees and dozens of satellite offices wanted to expand its threat hunting capabilities through analysis techniques that required deeper network visibility.

An information security engineer with the firm discovered Corelight when researching commercial solutions for the open-source Zeek Network Security Monitor.

Challenges

The law firm wanted a threat hunting solution based on network traffic analysis to provide real-time, comprehensive insight into traffic spanning multiple data centers and satellite offices around the world that collectively saw throughput speeds of up to 6 Gbps.

> ***"I don't want to spend time maintaining open source Zeek infrastructure: I just want the data. Corelight takes care of it for us and has given us more bandwidth to threat hunt."***
>
> *-Information Security Engineer*

The security team had already deployed firewalls on the perimeter and internally, as well as a host-based IDS, endpoint AV, and a log management system, but lacked the network visibility needed to effectively hunt for threats.

"Threat hunting and general east-west visibility was the most important challenge for us to address. Once that initial machine is compromised and lateral movement starts we had no way to effectively track it before Corelight," remarked the firm's information security engineer.

He determined that the open-source Zeek Network Security Monitor was the best traffic analysis framework for achieving their security and visibility goals and noted that they initially tried installing and running their own open-source Zeek server, but could not scale it to their environment.

“We knew we wanted to use Zeek so we first set up a Security Onion server, but when you’re doing 6 Gbps of network throughput it doesn’t scale and it constantly broke down,” he said. “We discovered Corelight in our research for a commercial Zeek solution.”

Solution

Beyond delivering real-time data for threat hunting via the Zeek framework, the law firm also had these solution requirements:

- **Scalability:** solution must reliably scale its traffic analysis to 6 Gbps of throughput.
- **Minimal TCO:** the solution must be quick and easy to setup and require minimal ongoing maintenance by the Customer.

> ***“I plugged it in, gave it an internal IP address, whitelisted the Corelight IP address on the firewall, and had it up and running in minutes.”***
>
> *-Information security engineer*

The Information Security Engineer and his team investigated a range of products and concluded that Corelight’s AP 1000 Sensor met all their requirements and excelled compared to the other vendors they evaluated.

“We looked at several other products that include Zeek inside, but also deliver alerts and analytics, but there was too much noise and no easy way to access the raw data to create our own queries,” he said. “Corelight made it easy to get the data and we also liked the fact that you can live stream the Zeek logs from their sensor.”

Asked how easy or difficult he found the installation and configuration of the sensor he stated: “It wasn’t difficult at all. I plugged it in, gave it an internal IP address, whitelisted the Corelight IP address on the firewall, and had it up and running in minutes.”

Corelight’s sensors operate out-of-band and were developed by key contributors to the open-source Zeek project. 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 per sensor.

The sensor outputs Zeek logs that summarize all network traffic by protocol-specific tables that comprise hundreds of data fields and describe each event in specific, actionable detail. Organizations can flexibly export logs to storage and analytic tools of their choice, such as Amazon S3 or SIEM solutions like Splunk, Elastic Stack, Spark or Chronicle.

Results

Pleased with the reliability and performance of Corelight's AP 1000 Sensor, the security team used the Zeek logs to build a workflow for threat hunting by feeding them into the open-source Real Intelligence Threat Analysis (RITA) tool.

"We use RITA to analyze our Zeek logs to look for beacons and also apply some of our own analyses like DNS lookups and certificate inspection," he said. "RITA sends us a daily report and after reviewing the report we'll often go back to the raw Zeek logs to get answers to follow up questions in our investigation."

The new threat hunting capabilities afforded by the Corelight and RITA integration has allowed the firm's security team to develop a more scalable, proactive approach to defending against advanced attacks.

"Instead of constantly chasing IOCs we can focus instead on threat hunting and identifying the common denominator for all breaches: beaconing out to attacker-controlled machines," he said. "If a malicious payload gets dropped it will eventually need to beacon out, so I'm not worried about the latest and greatest threat. We might not catch them on Day 0, but we'll catch them on Day 1."

Moreover, the information security engineer and his team now have more time to spend on threat hunting since they don't have to manage an open-source Zeek implementation.

"I don't want to spend time maintaining open-source Zeek infrastructure: I just want the data. Corelight takes care of it and has given us more bandwidth to threat hunt," he said.

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