corelight

Challenge
A major manufacturer was unable to use Zeek for network visibility at scale

Solution
Corelight delivered a robust, high bandwidth solution with minimal packet loss

Integrations
SIEM Splunk, *Analytics* RITA

Case Study

Major manufacturer

Background

A security administrator at a Fortune 250 company and one of the world's largest commercial steel producers, had been running Zeek, the open source network security monitoring platform for about two years before migrating to Corelight. The security administrator reports that Zeek was primarily being used for load balancing support but there was concern that it was not capable of capturing all of the network data.

Challenges

The SOC team, located in North America, is responsible for securing the network perimeter as well as responding to incident escalations. The team works with a third party SOC which is charged with identifying and triaging security events.

> ***"...it provides us insights into what is going on in the network."***
>
> *-Security Administrator*

The SOC had deployed a wide range of solutions including next generation firewalls and anti-virus and email filters, a SIEM as well as log aggregation tools, including RITA (Real Intelligence Threat Analytics), an open source network traffic analysis platform that ingests Zeek logs to adversarial activity like DNS tunnelling and beaconing.

As the team began to migrate their Internet connection from 1GB to 10GB concern grew about their ability to scale open-source Zeek to those throughput speeds. The team needed a Zeek-based solution capable of handling the additional traffic with easy deployment and minimal operational costs.

"When we were moving to 10GB on our firewall we were going to need the ability to capture more data and rather than making sure we were tweaking open-source Zeek, it was easier to purchase the Corelight Sensor, which we found to be pretty much plug-and-play," said the security administrator.

Solution

The team selected the Corelight AP 1000 Sensor and deployed it at the egress point to capture all traffic that is going out or coming in the network from the Internet/DMZ, exporting the logs to their instances of RITA and Splunk.

The team found that not only was Corelight simple and quick to deploy in the current network setup, it also provided access to the DNS logs, something that the security administrator shared was previously being done through Microsoft Active Directory but that only provided the queries and not the answers, making it a challenge to connect events with DNS responses.

Another benefit of Corelight is the ability to see SSL connections, something that Zeek was also handling and is important for analyzing whether or not there are beacons on the network, but by using only Zeek, the team was not sure if they were getting complete visibility into the traffic as there was some packet loss though the team was not entirely certain that Zeek was dropping packets.

Results

"Corelight does everything that we anticipated that it would do. It is very easy to use and it provides us insights into what is going on in the network," said the security administrator. "Firewall logs can only go so far and may only provide information at the end of an event. The Corelight Sensor gives us information on active sessions and allows us to see what has been open for long periods of time, giving us time to remediate before a serious incident occurs."

Solution requirements

- Traffic analysis via Zeek Network Security Monitor
- Deep visibility into traffic leaving the network
- Supports 10+ Gbps throughput
- Supports log export to RITA
- Easy sensor setup & minimal maintenance requirements
- Broader support for DNS logging

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