Challenge
A research university using Netflow needed better data to write custom scripts

Solution
Corelight delivered unmatched, rich data along with outstanding flexibility

Integrations
SIEM Elasticsearch + Splunk

Case Study

Top university builds custom detection scripts using Corelight's Zeek logs

Background
A top research university wanted a network traffic analysis solution that could overcome usability challenges posed by netflow records so that they could better analyze and protect their networks.

The university selected the Zeek network analysis framework to reach this goal, and after considering an open-source implementation they chose instead to buy several Corelight AP 1000 Sensors given their ease-of-management compared to open-source Zeek implementations.

An information security specialist spoke to us about what led the university to seek such a solution, and explained why his team ultimately selected Corelight.

Challenges
The university's network footprint spanned multiple campuses, with average utilization exceeding 35 Gbps. Before Corelight and Zeek logs, their network visibility largely came from an open-source Argus implementation that generated large text netflow records.

> ***"We went with Corelight's off-the-shelf offering instead and we appreciate the ease of management their sensors provide."***
>
> *-Information security specialist*

The university wanted a network traffic analysis solution that could generate logs that were protocol comprehensive, fast to search and extensible, capable of supporting log enrichment and scripting for custom monitoring and detection.

The challenge, in short, was that while the security team wanted to create more custom detection scripts, their netflow records and existing server and firewall logs did not provide rich enough network protocol data to support the development of such scripts.

Solution

Beyond comprehensive network visibility, fast log search, and support for enrichment and custom scripting, the university had these additional requirements:

- **Minimal operational costs:** solution must offer easy, fast setup and require minimal ongoing maintenance
- **Elasticsearch & Splunk integration:** solution must be able to export network logs to Elasticsearch and sensor performance metrics to Splunk

The team determined that Zeek network protocol analysis logs offered the rich detail and extensibility they needed, but the cost of building and running their own open-source Zeek sensors would divert resources from other engineering efforts, making Corelight the logical choice.

“We did look at doing an open-source Zeek implementation using clusters of virtual sensors and customized drivers, but the decision came down to staffing constraints. With finite staff, we had to make choices about where to put custom effort.”

Compared to open-source Zeek, Corelight Sensors offer a number of advantages, including performance that’s 2-3x what’s achievable in open-source implementations as well as additional enterprise features such as streamlined export to Elasticsearch and Splunk, custom filters to tune log volumes, and enterprise support from Zeek’s inventor and its key open-source developers.

> ***“The best feature of Zeek is that it is extensible and that is what makes it powerful.”***
>
> *-Information security specialist*

The university purchased several Corelight AP 1000 Sensors, which can ingest traffic from an optical tap, span port, or packet broker. Each sensor can analyze 10 Gbps of production traffic and allows customers to easily export the logs to storage and analytic tools of their choice.

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."

Fast query ability

“We wanted an indexed solution with a good API in place where we could do rapid queries,” he said. “With Zeek logs in Elasticsearch I find it easy to perform the searches that I need to generate actionable detections.”

Regarding the role that Zeek logs now play in his network visibility strategy, he added, “While we have server logs and firewall logs, our primary source of network visibility comes from Corelight’s Zeek logs in our Elasticsearch instance.”

Enrichment & custom detection scripts

The information security specialist and his team now enrich these network logs with intelligence and routinely write custom detection scripts around behaviors like known C2 server communications or anomalies such as large numbers of SSH connections, port scanning, and sketchy TLS certificates.

“Providing rich data is the whole point of why we’re using Zeek,” he said, citing the superiority of Zeek’s DHCP logs compared to server logs, since Zeek captures connection detail that can reveal unauthorized DHCP servers in an environment. Lastly, he noted the flexibility his team now enjoys in their network analysis capabilities: “Zeek understands a lot of protocols and if we need it to analyze a new protocol we can simply add that with Zeek scripts. We plan to add TLS client fingerprinting and Stratum (cryptocurrency) protocol detection, for example.”

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