

Case Study:

Top University Builds Custom Detection Scripts Using Corelight's Bro 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 Bro 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 Bro 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 Bro logs, their network visibility largely came from an open-source Argus implementation that generated large text netflow records.

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.

The Solution

Beyond comprehensive network visibility, fast log search, and support for enrichment and custom scripting, the university had these additional requirements: (see next page ->)

Executive Summary

Company

- A top research university

About

- Multiple campus networks with aggregate total utilization reaching 35 Gbps

Solution Requirements

- Deep network protocol visibility
- Fast log search
- Log enrichment and custom scripting support
- Minimal overhead costs
- Elasticsearch integration
- Splunk integration

Results

- Met all solution requirements
- Fast network log searches
- Expanded custom detection scripting capabilities

Key Quote

"The best feature of Bro is that it is extensible and that is what makes it powerful."

- Information Security Specialist

Case Study: Building Custom Detection Scripts



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

"We did look at doing an open-source Bro 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," he said. "So we went with Corelight's off-the-shelf offering instead and we appreciate the ease of management their sensors provide."

Compared to open-source Bro, the Corelight Sensor offers 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 Bro's inventor and its key open-source developers.

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

Fast Query Ability

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

Regarding the role that Bro 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 Bro 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 Bro," he said - citing, as an example, the superiority of Bro's DHCP logs compared to server logs since Bro 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:

"Bro understands a lot of protocols and if we need it to analyze a new protocol we can simply add that with Bro scripts. We plan to add TLS client fingerprinting and Stratum (cryptocurrency) protocol detection, for example," he said. "The best feature of Bro is that it is extensible and that is what makes it powerful."

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

☎ **510-281-0760**

🌐 corelight.com

👁 bro.org