Challenge
Need for actionable data on the network for quick queries during incident investigations

Solution
Corelight sensors have enabled faster incident response & better data for threat hunting

Integrations
Elastic Stack; Apache Kafka; IDS: Suricata and Wazuh

Case Study

TietoEVRY achieves faster incident response, better network analysis

Background

TietoEVRY, headquartered in Finland, is a leading global digital services and software company. With 24,000 experts deployed around the world, the company serves thousands of enterprise and public sector customers in more than 90 countries.

The SOC/CSIRT operations team, responsible for security monitoring/detection and incident response, works alongside a network operations team collaborating on architecture and network design decisions. The team had been using open source Zeek network security monitor for nearly a decade so when they began the search for a commercial solution, transitioning to Corelight was an easy choice.

Challenges

As an IT infrastructure and service provider, the TietoEVRY team faces many network security threats due to the diversity of their customer base, so it's critical that they secure their core infrastructure. Integral to that goal is the ability to easily access comprehensive and actionable data for incident investigations. The team considered next generation firewalls for visibility, but found the limited network data they captured could not satisfy this use case.

> ***"We don't think there is another network telemetry tool that can beat Zeek logs."***
>
> *-Markus Fors, lead security engineer*

Solution

Ultimately the team deployed a mix of Corelight AP 1001 and AP 3000 sensors across five datacenters and three different geographical locations and are currently looking to expand this even further including public cloud deployments. The team found the Corelight sensors relatively simple to deploy, needing only to rebuild data flows and work processes that operated slightly different from those running on their open source Zeek deployments.

At the core, the team runs Zeek logs generated by Corelight through Apache Kafka that let different tools like Elastic Stack and customer dedicated SIEMs consume data related to different network segments.

The team continues to rely on Zeek logs as the primary source of data that analysts pivot to first when investigating an alert, removing the need for netflow. The team also pivots to PCAP from Zeek log review in cases where they need specific payload information not captured by Zeek.

Results

Today their network sees roughly 30Gbps of throughput pushed through to all Corelight sensors, with the greatest volume comprised of north-south traffic.

Since deploying, TietoEVRY has seen an acceleration in average incident response times, better data for threat hunting, and better data for network diagnostics and truth.