PACKETSLED

FLUKE CASE STUDY

MAY, 2018

FLUKE CASE STUDY

SUMMARY

The World Leader in Compact, Professional Electronic Test Tools Turned to PacketSled For Automated Network Security and Visibility.

FLUKE CORPORATION

From industrial electronic installation, maintenance and service, to precision measurement and quality control, Fluke tools help keep business and industry around the globe up and running. Fluke has achieved the number one or number two position in every market in which it competes. The Fluke brand has a reputation for portability, ruggedness, safety, ease of use and rigid standards of quality.

Manufacturing centers are located in the USA, the UK, Asia and The Netherlands. Fluke's sale and service companies are located in Europe, North America, South America, Asia and Australia. Fluke continues to grow by expanding applications for its tools and by acquiring companies and complementary product lines.

COMPLIANCE REGULATIONS

Adhere to all compliance regulations, including but not limited to, SOX, PCI, GDPR, DFARS, ITAR, Chinese and Russian data privacy laws.

THE CHALLENGE

With a global network of 40 locations in 20 countries and over nine thousand employees utilizing their network, Fluke needed a large-scale network visibility and threat detection solution to monitor world-wide network traffic. This included virtual sensor deployment and the ability to secure and consolidate all ingress/egress points into a single security "hub." Fluke continues to grow by expanding applications for its tools and by acquiring companies / complementary products and thus, needed a threat detection and network visibility platform that was scalable and could integrate seamlessly with Fluke's existing cloud-based threat intelligence and SIEM technologies.

Fluke specifically required a robust Bro-based solution that allowed for the management of sensors in both deployment arenas (on premise or cloud), as well as the ability to manage sensors centrally; a feature PacketSled calls *Dynamic Sensor Management*. Some of their initial requirements when evaluating solutions included:

Fluke's Goals / Requirement	Solved by PS
The ability to continuously monitor, investigate, and react to global security events in real-time.	Yes
Flexibility of deployment - having the ability to migrate between cloud or on premise.	Yes
Have a system that can Integrate with both Threatstream and Splunk in the cloud.	Yes
Capability to get visibility into custom-built applications and customized product stacks	Yes

Identify advanced malware, phishing and network attacks in multiple geographic locations.	Yes
Combine full packet capture with threat intelligence across diverse environments without a substantial investment in new infrastructure or a large learning curve.	Yes
Manage sensors and their risk profiles centrally and in real-time.	Yes

PACKETSLED'S SOLUTION

When Fluke evaluated PacketSled, they realized the potential in the platform's ability to leverage data for not just security metrics, but also for network baselining, user-agent types, client distributions and others. They also liked how PacketSled was quick to implement feature requests and integrations and could be deployed on premise or in the cloud, based on the need of each Fluke location. But most importantly, Fluke's security team would be empowered with real-time threat identification and greater network visibility across the expanse of their global operation. Other gained benefits include:

- ✓ Uncovering hidden attack signals that were not previously visible.
- ✓ Improved network context to the threat hunting and anomaly detection processes.
- ✓ Utilization of built-in interactive visualizations and custom detections that provide meaningful situational awareness during IR.
- ✓ PacketSled is also used by Fluke for Merger and Acquisition risk assessment.
- ✓ Improved security monitoring on internal segments.
- ✓ Quickly retrieve historical network data during incident response exercises.
- ✓ Automatically check traffic against built in, open source and custom detection signatures.
- ✓ The ability to add custom detections.
- ✓ The ability to leverage the data for not just security metrics, but network baselining, user-agent types and client distributions.
- ✓ The product is Bro-based and is quick to implement detections for new threats or attack vectors globally.
- ✓ Full network telemetry byproduct, which enabled usability outside of the security team.

> *"Fluke is accountable to several compliance frameworks and risk associated with our business model. PacketSled provides us a hybrid of deployment solutions and assessment capabilities for a small team to centralize, visualize, detect, report and manage risk. We use PacketSled's full telemetry to evaluate risk either in responding to incidents or as part of our acquisition risk assessment strategy."*
>
> *Brandon Glaze – Information Security Officer*

ABOUT PACKETSLED

PacketSled automates incident response by fusing business context, AI, entity enrichment and detection with network visibility. Used for real-time analysis and response, PacketSled's platform leverages continuous stream monitoring and retrospection to provide network forensics and security analytics. Used by breach response teams worldwide, security analysts and SOC teams can integrate

PacketSled's deep network context into their playbooks, SIEMs, or utilize PacketSled on a standalone basis to dramatically reduce investigation time, cost and expertise required to respond to persistent threats, malware, insider attacks and nation state espionage efforts. The company has been named an innovator in leading publications and by security analysts, including SC Magazine, earning a perfect score in the online fraud group test. PacketSled has offices in San Diego, CA and in Seattle, WA. For more information, visit https://packetsled.com/.

ABOUT FLUKE

Founded in 1948, Fluke Corporation is the world leader in compact, professional electronic test tools and software for measuring and condition monitoring. Fluke customers are technicians, engineers, electricians, maintenance managers, and meteorologists who install, troubleshoot, and maintain industrial, electrical, and electronic equipment and calibration processes. For more information, visit http://www.fluke.com/.