LOGPOINT

PUBLIC ADMINISTRATION

LAPIT

HOW LOGPOINT IS HELPING LAPIT PROVIDE MANAGED SIEM SERVICES TO TO PUBLIC ORGANIZATIONS IN NORTHERN FINLAND

PUBLIC ADMINISTRATION

FACTS	
Customer	LapIT
Industry	Public Administration
Location	Northern Finland
Objectives	LapIT delivers a managed Logpoint SIEM service to public organizations in Northern Finland, providing information security visibility and incident management

LOGPOINT

- Provides situational awareness of cybersecurity in the infrastructure
- Efficiently handles logs from a multitude of sources and reduces time spent on incident investigation
- Supports compliance with GDPR and ISO27001 standards

LapIT delivers a managed Logpoint SIEM service to public organizations in Northern Finland, providing information security visibility and incident management

BACKGROUND

For more than 20 years, LapIT has provided Information Technology services to its customers in the Lapland region, in the Northernmost part of Finland. The customers are public organizations, including municipalities, regional government authorities, and hospitals, and as it happens, many of the customers are also among the owners of LapIT. LapIT is a not-for-profit company partly owned by 18 municipalities and is dedicated to providing efficient public information technology services in the vast, sparsely populated northern Finland.

Headquartered in Rovaniemi in the southern part of Lapland, LapIT serves its customers from 11 locations, from Taivalkoski in the south to Ivalo in the north. In total, 130 technology experts are providing a broad range of services, including infrastructure services, application and information systems services, consulting services, and end-user support. LapIT also provides datacenter and cloud services and generally serves as a digitalization partner for the public sector, deeply rooted in the northern communities.

THE CHALLENGE

LapIT supports more than 20.000 users in public organizations across Lapland, 9.000 workstations, and more than 1.300 different information systems, including databases, healthcare systems, pension records systems, and office applications, including mail servers. As the backbone provider of public IT services, the need for efficient cybersecurity and compliance solutions in LapIT became apparent in 2016-2017, with GDPR and ISO27001 compliance requirements being significant drivers.

At the same time, handling logs from a wide variety of systems was becoming increasingly difficult. LapIT had fragmented visibility of information security in the network and application landscape, and investigating security incidents efficiently was proving cumbersome and time-consuming. Risto Hoppula, the Security Manager at LapIT, set out to find a solution to provide situational overview, efficient collection, and management of logs, incident investigation, and support for compliance with regulations, standards, and audit requirements.

“We decided that the best way of managing these risks in a complex environment was to bring onboard a SIEM system to track all the activity that was going on across all different systems. Not only did we want a solution to manage logs from a security perspective and provide situational awareness, we also wanted a tool that could support the process to become GDRP and ISO27001 compliant and continuously document compliance”, says Risto Hoppula.

“Implementing Logpoint has not only increased situational awareness and cybersecurity in general. It has allowed us to respond faster and use less human resources on the cumbersome, repetitive work of manually collecting and analyzing data from different log sources in case of incidents. Those resources can then be deployed to improve service and security elsewhere.”

Risto Hoppula
Security Manager

THE SOLUTION

In response to the requirements, LapIT began discussions with the nationwide IT services provider Istekki, a non-profit company owned by public customers and established to provide efficient IT solutions for the public sector. Istekki is a major Logpoint partner in Finland and had already deployed the Logpoint SIEM solution across a number of local, regional and national public organizations in Finland. The SIEM project with Istekki was initiated at the end of 2017, enabling LapIT to launch the services to their customers in the beginning of 2018.

The Logpoint SIEM solution is hosted by Istekki, but offered by LapIT as a service to its customers in Lapland. It allows LapIT to ingest data from the infrastructure and numerous IT systems operated by customers, and then correlate data to find indicators of compromise and attack, or patterns of suspicious or threatening behavior. Logpoint's system is designed to be simple, flexible, and scalable, providing modular design, streamlined deployment, and integration tools that make it easy to implement.

"Using Logpoint fundamentally changes the way you work with log data in your infrastructure. Previously logs would only be checked in case of problems, and they would be difficult and time-consuming to access and analyze. With Logpoint, log data becomes a useful tool. It allows us to take control and get a meaningful, constant output that enables us to spot potential problems and react promptly. Before things turn into a real threat," says Hoppula.

THE RESULTS

Logpoint has provided LapIT the ability to deliver a highly valued, much-improved service to its customers and owners. The Logpoint SIEM solution is the primary tool for information security visibility, proactive threat monitoring, and incident investigation. Implementing the solution has been a driver for the definition of the processes for identifying and handling incidents. It has allowed LapIT to also focus on pre-emptive efforts, solving issues before they develop into an actual incident.

CONTACT LOGPOINT

If you have any questions or want to learn more about Logpoint and our modern SIEM solution visit www.logpoint.com

"Implementing Logpoint has not only increased situational awareness and cybersecurity in general. It has allowed us to respond faster and use less human resources on the cumbersome, repetitive work of manually collecting and analyzing data from different log sources in case of incidents. Those resources can then be deployed to improve service and security elsewhere", says Hoppula.

The Logpoint SIEM only requires one person for normal day-to-day operations and to handle any issues identified. However, across the LapIT organization, 8-10 staff has been trained to use the system, forming a security incident response team. As the extent of the SIEM service is growing, LapIT will be integrating more log sources and tune use cases to more specific purposes, and are also providing IT staff on customer premises their own system access to improve local information security visibility.