FINANCE

MATMUT

HOW LOGPOINT HELPED MATMUT IMPROVE EVENT VISIBILITY ACROSS THE ENTIRE IT ARCHITECTURE AND REDUCE INCIDENT RESPONSE TIME

BACKGROUND

French insurance company Groupe Matmut, originally established in Rouen in 1961 as Mutuelle des Travailleurs Mutualistes, is major player in the French insurance market. Initially focused on automotive insurance, the group today offers a broad range of products, including automobiles, motorcycles, boats, homes, third-party liability, family protection, health, legal protection and assistance. In addition, Matmut offers financial services and savings.

Still headquartered in Rouen today, Matmut currently insures over 3.8 million policyholders and manages nearly 7.2 million contracts. The company employs 6,200 people and generated a turnover of 2.1 billion Euros in 2017.

THE CHALLENGE

In 2017, the Matmut group wanted to acquire a log management solution that would deliver correlated views, facilitate incident searches, improve prevention and trigger threshold notifications. The scope was to improve event visibility across the entire IT architecture and reduce incident response time. The project was strategic for Matmut's IT division and prioritized in the company IT master plan.

“I wanted a flexible, fast-response and easy-to-use solution for all the teams, in particular, one that could easily be used to create dashboards and make data and subsets of data available on a selective basis. Cost- efficiency was also a prerequisite in the scoping of a solution”, says Cédric Chevrel, CISO at Matmut.

A SIEM solution would empower Matmut to reduce security risks, notably by achieving visibility of data and events such as suspicious extraction of data, statistics on use of Active Directory accounts (attempts, successes, failures, etc.) and the correlation of minor security events, that individually may pass unnoticed, but in combination triggers an alert.

FACTS	
Customer	Groupe Matmut
Industry	Financial services, Insurance
Location	Rouen, France
Objectives	Improve event visibility across the entire IT architecture and reduce incident response time
Results	• Visibility across the IT infrastructure and overview of the security posture • More resources for value-adding projects for the business

The aim was also to facilitate the correlation of events when handling load-balancing and inter-architecture communications across platforms.

THE SOLUTION

To implement the project, Groupe Matmut formed a project team including staff from different areas: system architecture, development, network, infrastructure, security and operations/production. It was important that the solution could be used both in security and operations. Although Information Systems security is the core task, analyzing log data can also reveal technical issues. The requirement for a central repository was essential, to provide a unified view of log data across all sources.

After several months of analysis and a successful Proof- of-Concept, the Logpoint solution was selected based on a number of winning criteria: The Logpoint solution is easy to install, configure and use.

It's NoSQL database is powerful and the system supports Intuitive queries, dashboards and reports. In addition, the Logpoint solution offers simple, transparent pricing, a great deal of flexibility, the capability to integrate all targeted data sources and it supports a wide range of uses. In the end, Logpoint was met by approval of the entire team.

"A Highly responsive support in deploying the solution plus total control over costs were decisive criteria in validating the Logpoint solution", says Cédric Chevrel. Deployment was completed in stages. For the Matmut CISO, the success of the project depended on getting the initial scope just right. This is why he decided to initially include just 20% of the entire Information System infrastructure by choosing representative elements of the architecture: Active Directory, business applications, websites, proxies, etc. and develop scenarios and use cases from there. The Logpoint solution was first used to collect logs and generate correlated views of the entire architecture to facilitate incident identification.

The scope was then expanded to include the security architecture elements like firewalls, antiviruses, reverse proxies, web proxies, etc. with a view to developing lead forensics.

"A highly responsive support in deploying the solution plus total control over costs were decisive criteria in validating the Logpoint solution. The savings generated by the Logpoint solution allowed us to upgrade the quality of service offered to our organization, which is an unexpected but much-welcomed benefit."

Cédric Chevrel
CISO

THE RESULTS

After one year in use, the Logpoint SIEM solution has reduced average incident resolution and forensic analysis time by 80-90% particularly when the architecture spans multiple servers. Forensic analysis by experts is easier, and the solution allows them to focus on factual analysis rather than tracing. Some log searches that previously could take hours to perform is now done in minutes.

New threat indicators were identified, most notably regarding user activity around directories and authentication systems. The Logpoint solution also provides visuals and metrics to Matmut subsidiaries in addition to the ability to produce entity-specific dashboards from the same log source. Finally, thanks to Logpoint, the Matmut security team were able to pick up threat indicators that were not detected by existing Web Application Firewalls. Several dozen requests on the same day from different IP addresses in a specific geographical area were flagged as potential threats. Analysis later revealed that the requests were in fact attempts to extract pricing information via several online quote requests.

“The savings generated by the Logpoint solution allowed us to upgrade the quality of service offered to our organization, which is an unexpected but much- welcomed benefit”, says Cédric Chevrel.

CONTACT LOGPOINT

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