FINANCE

SCILDON

HOW LOGPOINT IS HELPING SCILDON IMPROVE CYBERSECURITY WHILE SAVING ADMINISTRATORS' RESOURCES

BACKGROUND

Scildon is a Dutch Life- and Pension Insurance company, based in Hilversum in the Netherlands. Originally founded in 1984 as Legal & General Nederland, the company was renamed Scildon in 2017 when it was acquired by the UK-based Chesnara-group, that owns life and pension companies in the UK, Sweden, and the Netherlands.

Scildon is an award-winning provider of risk and investment-linked products in the Dutch market, sold through independent financial advisers to high net worth customers. The company also offers a group pension platform focusing on SME's. The company manages EUR 2 bn of funds on behalf of 278.000 customers in the Netherlands.

The Scildon IT department supports approx. 175 users in a network with upwards of 150 serves and network devices. Also, the infrastructure includes more than 400 assets such as computers, printers, and other end-user devices.

THE CHALLENGE

In 2015 Scildon wanted to gain more insight into the log sources within the company IT infrastructure, to be able to mitigate the risks they saw in their daily business. In a complex IT environment, manually accessing and analyzing log files was becoming increasingly ineffective, resource consuming and cumbersome.

"In addition to being labor-intensive, manually scanning generic log files also meant that analysis was inherently retrospective. Effectively we would be reviewing the previous day, which is far from optimal from a security perspective," says Alastair Kirkman, Security Manager at Scildon. "Also we wanted to extend access to log files to our application support team in a controlled fashion, making sure that information was shared on a need-to- know basis," he says.

Following a comprehensive review of SIEM solutions in the market, Kirkman and his team shortlisted three vendors. Logpoint was proposed by iSOC24, a Logpoint certified Gold partner since 2013, specializing in cybersecurity in the Benelux-region. Following a Proof- of-Concept, Logpoint was selected as the platform of choice.

SCILDON
LIFE | PENSION

FACTS	
Customer	Scildon
Industry	Financial services, Life and Pension
Location	Hilversum, the Netherlands
Objectives	Increasing cybersecurity and reducing administrators workload
Results	• Provides flexible and efficient security analytics • Mitigates risk in a complex IT environment • Saves 75% on IT administrators' resources • Is a dedicated SIEM provider

THE SOLUTION

A key factor in the selection of Logpoint as a SIEM provider for Scildon, was the flexibility and the unique taxonomy of the platform, that allows for the ingestion of log files from multiple sources across the IT infrastructure, including network hardware, servers, databases, and standard applications as well as in-house custom built applications. Data across the various sources are then normalized into a common format, enabling search queries across the entire infrastructure.

“Working with Logpoint is very easy. You import your data. Apply analytics and adjust the rules. Logpoint is a very dynamic platform, change is easy, and the user interface has a great look and feel. Our standard log sources were included based on out-of-the-box integrations, whereas we did integration of in- house developed applications ourselves,” says Kirkman.

In addition, Logpoint’s predictable licensing model was a key factor in the selection. Cost is based on the number of devices (nodes) sending logs, not on the volume of data (GB) or events per second:

“The license model enabled us to maintain an accurate budget for our SIEM solution. Any concerns about data limits disappeared, allowing us to scale for future needs in a predictable manner”, says Kirkman.

While technology matters a lot, an important factor in choosing Logpoint as the SIEM vendor for Scildon, was focus: “Logpoint is SIEM. Logpoint is a SIEM business. Other vendors provide a bit of everything, but somewhere along the way they lose focus. We appreciate the vision that Logpoint has for the development of its SIEM solution, and with every update, we experience improvements in features, functionality, and speed”, says Kirkman.

“Previously we would take turns spending hours analyzing the logs of the previous day. It was a dreadful and time- consuming task, often including conversion of data to other formats and split-screen work for manual correlation between log sources. Today everything is nicely served up, and if anything is missing, I’ll just take 15 min to create a dashboard that will tell me what I need. A 50% reduction was the target, but in reality, it’s more like 75%.”

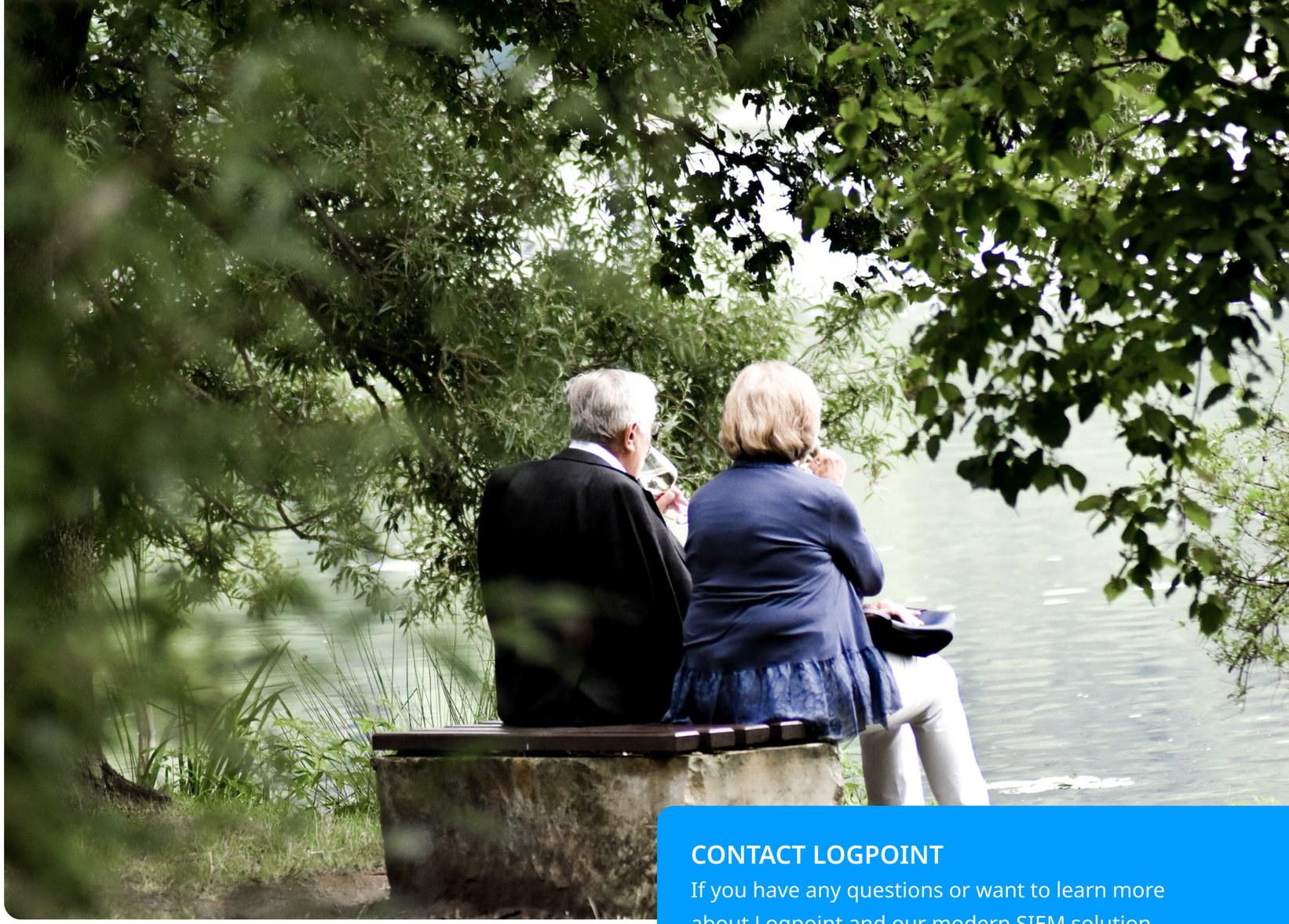
Alastair Kirkman
Security Manager

THE RESULTS

In the business case prepared by Kirkman and his team, prior to the selection of the SIEM solution for Scildon, a reduction of 50% on the resources spent manually analyzing logs was a key target. With Logpoint, this goal was successfully surpassed:

“Previously we would take turns spending hours analyzing the logs of the previous day. It was a dreadful and time-consuming task, often including conversion of data to other formats and split-screen work for manual correlation between log sources. Today everything is nicely served up, and if anything is missing, I’ll just take 15 min to create a dashboard that will tell me what I need. A 50% reduction was the target, but in reality, it’s more like 75%”, says Kirkman.

The Logpoint SIEM solution allows the Scildon team to continually fine-tune the installation making false positives a rare occasion Manual analysis has been drastically reduced and the bottom line is that the target of the business case has been fulfilled. However, there is another and perhaps more important bottom line:
“Logpoint actually does it better. Being in control of our security has improved, which is crucial in this day and age. That’s the real bottom line”, says Kirkman.



CONTACT LOGPOINT

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