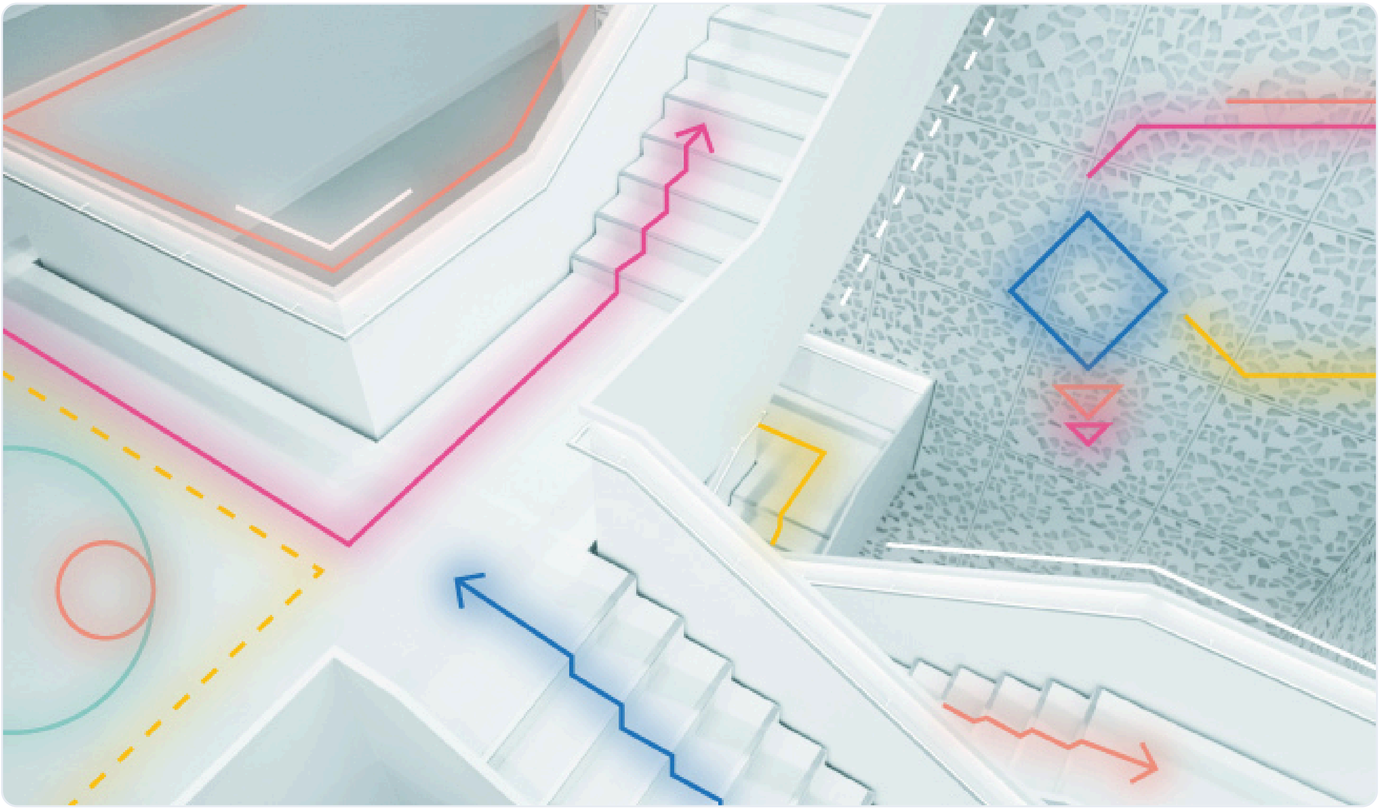
Building a next-gen SOC at Pinewood, a leading MSSP, underpinned by Elastic SIEM

By **Sebastiaan Kors**

06 June 2024

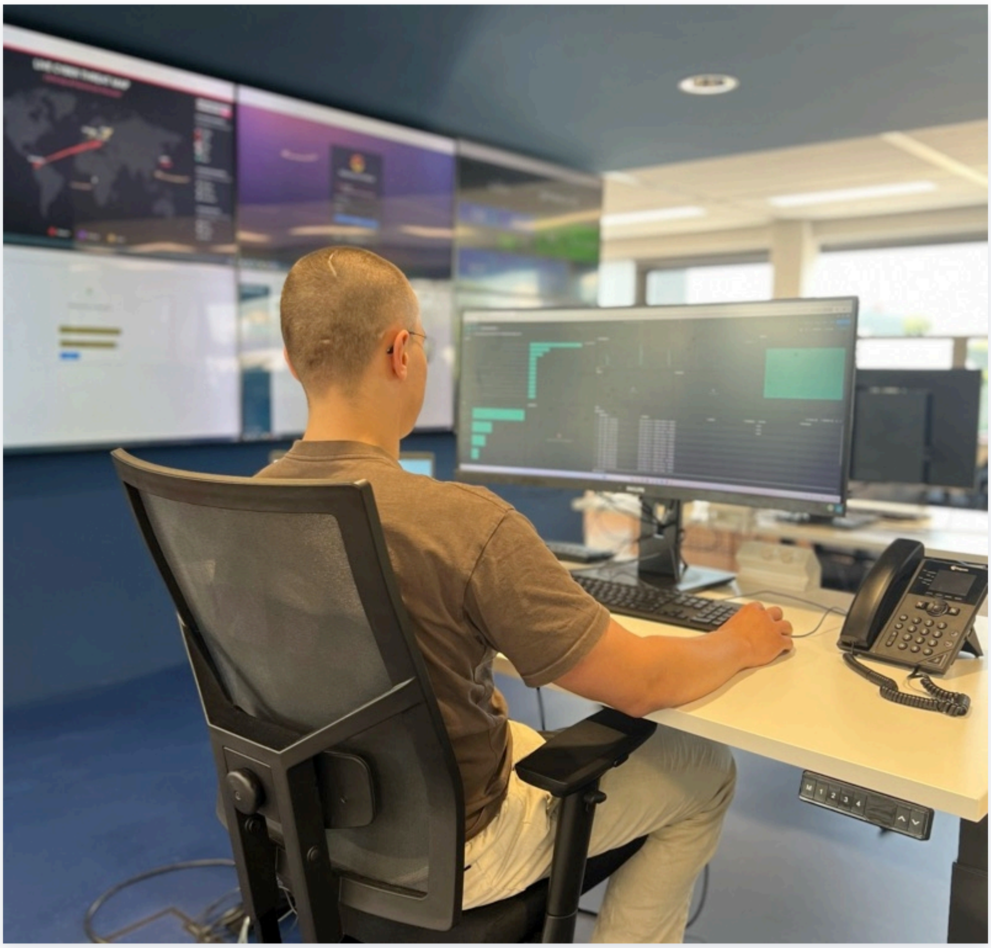


Cybersecurity is a critical and challenging domain that requires constant vigilance, innovation, and adaptation. As cyber threats evolve and become more sophisticated, so do the tools and techniques to defend against them. One of the most effective ways to achieve comprehensive and proactive security is to implement a security information and event management (SIEM) platform that can collect, analyze, and correlate data from various sources to provide actionable insights and alerts.

In this blog post, I will share how Pinewood — a leading cybersecurity company that provides managed security services, consulting, and training — successfully implemented Elastic SIEM to enhance our customers' security posture and visibility. From my experience as CEO of Pinewood, I will also highlight some of the key benefits and features of Elastic Security that make it a powerful and flexible solution for any managed security service provider (MSSP) that wants to improve its security operations.

The challenge

Pinewood is an MSSP that serves clients across various industries — such as finance, healthcare, retail, and government. The company offers a range of services, such as threat detection and response, vulnerability management, penetration testing, incident response, and security consultancy. We also operate a 24/7 security operations center (SOC) that monitors and responds to security incidents for our clients.



As an MSSP, Pinewood faces a high volume and variety of cyber threats from different customers on a daily basis. It's essential that our clients' applications, networks, and systems are secure and resilient — as well as our own. We also need to fulfill various functionalities like scalability, multi-tenancy, enhanced reporting, reduced false-positives, and an easy to use platform that empowers our security analysts to search quickly through tons of data.

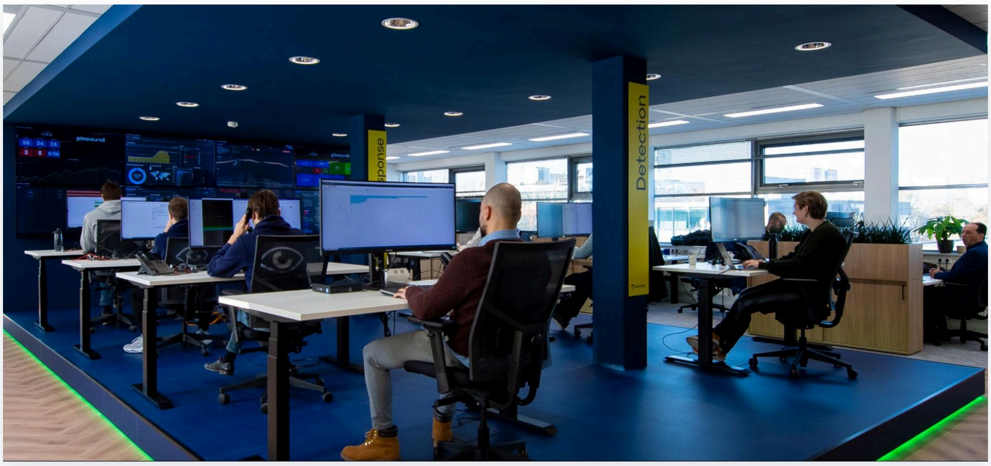
In the past, Pinewood relied on a legacy SIEM platform that was inflexible and outdated. The legacy SIEM platform had several limitations, such as:

- Platform instability that required a lot of hardware and maintenance
- A rigid and proprietary data schema that made it difficult to ingest and normalize data from different sources and formats
- A limited and outdated user interface that made it hard to visualize and explore data, create dashboards and reports, or customize alerts and workflows
- Poor scalability and performance issues that affected the reliability and timeliness of data analysis and alerting
- Limited integration and extensibility options that hindered the ability to leverage other tools and technologies, such as threat intelligence, threat hunting, orchestration, and automation

These limitations made it challenging to achieve comprehensive and proactive security monitoring. We needed a new SIEM that could overcome these challenges.

The solution

From the long list of SIEM functionalities required, we shortlisted three strong contenders. Due to the speed of search as well as the reporting and dashboard capabilities, Elastic immediately gained a preference with our analysts. Another appealing element of Elastic's solution was the support of the local Dutch Elastic team. For a business like Pinewood, choosing a new SIEM vendor is a critical and strategic choice and having a dedicated team partner from the onset made a huge difference.



Elastic Security provided the following benefits and features that addressed our needs and challenges:

- Cost-effective and scalable licensing with no usage restrictions that can run on any infrastructure, whether on-premises, in the cloud, or hybrid

- Very easy to implement and connect data-sources, with simplistic onboarding and customer migration that can be handled in a few weeks — our entire custom based migrated within nine months!
- Flexible and open, supporting the ingestion and normalization of data from any source and format — Beats, Logstash, and Elastic Agents support all of Pinewood's customers, regardless of their resources
- User-friendly and powerful, offering different customers their own modern and intuitive user interface — additionally, Kibana supports data visualization and exploration, dashboarding and reporting, and alerting and workflow customization
- Simplistic data analysis, especially from Elastic Security's distributed and resilient architecture that supports real-time and historical search and analytics with features like data streams, rollups, and frozen indices
- Seamless integration across tools and technologies such as threat intelligence, orchestration, and automation is supported with features like Elastic Agent and Fleet

By implementing Elastic Security, Pinewood was able to achieve a much more comprehensive and proactive security monitoring platform and improve our security operations and outcomes. Some of the results and benefits we achieved with Elastic Security are:

- **Increased coverage of data types by 20%** — ingested and normalized data from various sources and formats such as network, endpoint, cloud, application, and threat intelligence
- **Improved data quality by 60%** — enriched and analyzed data using custom rules, queries, and aggregations while applying consistent data fields and formats using Elastic Common Schema (ECS)
- **Enhanced data visibility by 30%** — leveraged interactive and customizable dashboards, maps, charts, and tables, alongside easy reporting and alerts
- **Accelerated data search and results by 400%** — detected and responded to security incidents much faster

The outcome: flexibility, visibility, and security

Elastic Security provides Pinewood with a powerful and flexible platform to improve our security posture and visibility across our entire base of SOC clients. With Elastic, we overcame the limitations of our legacy SIEM and made significant improvements to data coverage, quality, visibility, and response. Our security analyst teams are now empowered to achieve comprehensive and streamlined searches for the security posture of their clients.

Bonus feature:
For those customers who run Elastic SIEM but don't have the manpower or skills running a 24/7 operation themselves, we now offer a unique shared platform. Choosing Elastic also gives us the possibility to onboard existing Elastic customers very easily and have a platform that allows shared management and SOC capabilities.

Check out Pinewood's solutions, and keep an eye out for our upcoming hackathon event to showcase the team's skills and the Elastic solution.

Sebastiaan Kors

CEO, Pinewood

Sebastiaan Kors is the CEO of Pinewood, a leading cybersecurity firm in the Netherlands and part of the Interstellar group. Sebastiaan has worked in the field of cybersecurity for over 20 years.

pinewood

THE **INTERSTELLAR** COLLECTION

The release and timing of any features or functionality described in this post remain at Elastic's sole discretion. Any features or functionality not currently available may not be delivered on time or at all.

SHARE

Table of contents

Sign up for Elastic Cloud free trial

Spin up a fully loaded deployment on the cloud provider you choose. As the company behind **Elasticsearch**, we bring our features and support to your Elastic clusters in the cloud.

Start free trial

FOLLOW US

ABOUT US

About Elastic

Our story

Leadership

DE&I

Blog

Newsroom

JOIN US

Careers

Career portal

PARTNERS

Find a partner

Partner login

Request access

Become a partner

TRUST & SECURITY

Trust center

EthicsPoint portal

ECCN report

Ethics email

INVESTOR RELATIONS

Investor resources

Governance

Financials

Stock

EXCELLENCE AWARDS

Previous winners

ElasticON Tour

Become a sponsor

All events