elastic | randstad

SUCCESS STORY

Randstad Netherlands harnesses Elastic Security to protect tens of thousands of job candidates and customers from cyber attacks

Region
Netherlands

Industry
Professional Services

Solution
Elastic Security

Accelerates security alert resolution

Randstad Netherlands reduces mean time to resolution with Elastic.

Boosts security team productivity

With Elastic Security, Randstad Netherlands only requires two and half full-time employees for detections, engineering, and triaging of alerts.

Handles 73 million events per hour

Randstad Netherlands easily ingests massive volumes of data from dozens of security, cloud, and other applications within the business with Elastic.

Watch the video

|

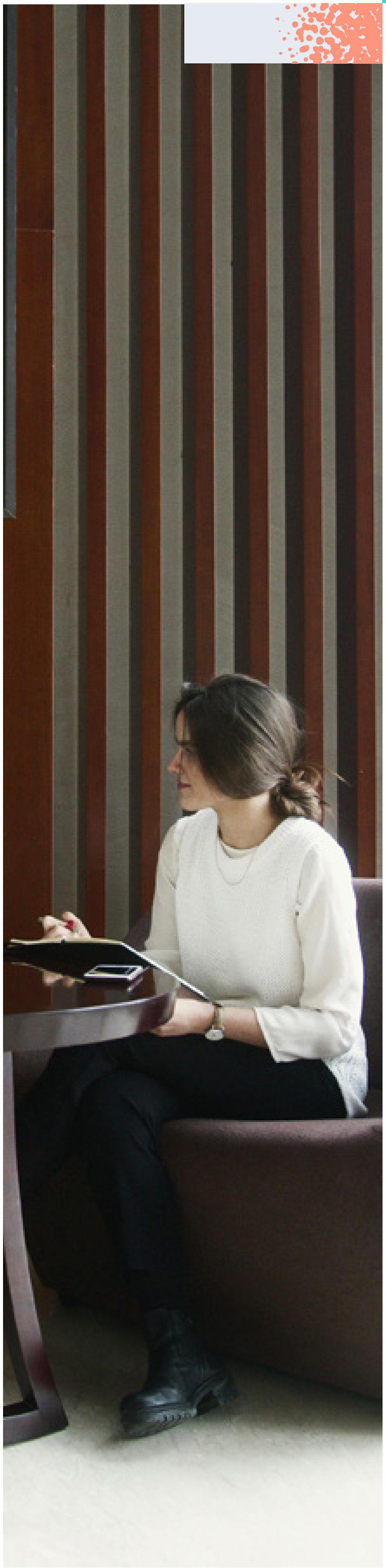
Leading Netherlands HR services provider deploys Elastic to protect its hybrid, multi-cloud environment against cyber-attacks

Founded more than 60 years ago in the Netherlands, Randstad has become one of the world's largest HR service providers, with more than 4,800 branches in 39 countries. In the Netherlands alone, the company places around 70,000 people a week at some of the biggest brands in the country, including Ahold, KPN, ABN-Amro, and KLM.

As a result, Randstad is responsible for the personal information of both clients and businesses, with millions of accounts that must be protected at all costs. The security team's first priority is defending against attacks that could impact the candidates who have placed their trust in Randstad's system. Cyber attacks that target individual weekly payments would be especially devastating. Stijn Holzhauer, Technical Lead Security Monitoring at Randstad Netherlands is responsible for the security operations center (SOC) of the Dutch business. "A successful attack on our systems could have a serious impact on the organizations who rely on us for temporary and permanent staff. Above all, it could prevent thousands of people from receiving their weekly salaries, seriously impacting their lives."

> With Elastic, we can detect threats in real time, with a single intuitive workflow. It makes our lives a great deal easier by saving time, increasing productivity, and boosting team morale.

Stijn Holzhauer
Technical Lead Security Monitoring,
Randstad Netherlands



Getting answers in seconds, not hours

When Holzhauer joined the business in 2017, Randstad Netherlands used Elastic for several years to monitor systems in its then-on-premise environment. “My predecessors originally deployed Elastic in 2015 to replace Splunk, another log management and observability platform that was becoming too expensive and lacked many of the features that the business required.”

After only a few months in the role, Holzhauer identified the potential to expand Elastic’s security capabilities and use it as the core technology for the business’s SOC. “We started off using Elastic Stack to automate tasks and maintain availability. We then deployed Elastic Security when it was launched in 2019 and have used it to strengthen our security posture ever since.”

As well as its advanced security capabilities, another reason for choosing Elastic is its scalability and observability features. “The ability to ingest any data source, quickly, is hugely valuable, especially from a security standpoint,” says Holzhauer. “It means we’re not constrained by the volume of data or the architecture of our multi-cloud, hybrid environment when defending our systems.”

> If you’re in a fast developing situation, you need to have answers as soon as possible. If we find out that there might have been an issue, getting to the bottom of it in seconds or minutes can be the difference between an incident and another Monday morning.

Stijn Holzhauer
Technical Lead Security Monitoring, Randstad Netherlands

Observability and integration

Holzhauer and his team use Elastic Observability to monitor custom build tooling including a simple security orchestration, automation, and response (SOAR) platform. Elastic Observability is also used on several applications to analyze access request logs for security, in addition to its use by development teams to analyze their applications. Machine learning in Elastic Observability is used to support anomaly detection in access logs and other user activity.

“By instrumenting our applications with Elastic APM, we get traces automatically and are able to detect URL issues,” says Holzhauer. These include parameters and directory brute force attacks as well as indicators of compromise such as the IP addresses involved and other technical details.

Elastic Observability also has an important role in Randstad’s evolving security posture. The business uses metrics such as context drivers to understand host performance when investigating. They have also deployed Elastic Observability to detect latency issues and outages, which can indicate DDoS attacks.

Randstad also benefits from Elastic’s integration with ServiceNow. Holzhauer says, “Once we finalize our investigation in Elastic, and if there is an issue, we push the relevant case to ServiceNow where an incident response process picks it up.”

As well as accelerating response times, Elastic Security enables Holzhauer and his team to be more proactive when identifying and preventing threats. “If we spot an issue, even if it isn’t my responsibility, I can address it based on data. I can contribute to our defenses by collaborating with the stakeholders.”

Boosting productivity and collaboration

Elastic also supports greater collaboration between Randstad teams. “We can ingest data from any source we have come across. For example, the APM and observability data for the development teams is utilized by security to do access monitoring and performance metrics are used for indications of business impact.”

Elastic also contributes to the productivity of Holzhauer’s team, which is comprised of two and a half full-time employees. “With Elastic, a small team can do detections, engineering, and all of the triaging of alerts at enterprise scale,” says Holzhauer. “Rather than spend a huge amount of time configuring Elastic features, most of what we need is already there. For example, we have deployed nearly 400 of Elastic’s out of the box detections along with 250 ‘custom’ detections.”

Kibana dashboards are another highlight. “With Kibana we get a single pane of glass for visualizing and analyzing security data from a multitude of sources. It means that we don’t have to switch between several platforms, which reduces or even mitigates platform fatigue for the team.”

In addition, the team has built a single Kibana Canvas slide which shows KPIs for the past month and is automatically sent to stakeholders as part of the reporting process.

Support on the cloud journey

Holzhauer highlights the support provided by the Elastic team, especially during Randstad’s migration to the cloud on AWS. “When we added a frozen storage tier, it had an unexpected impact on the performance of our searches. We raised the issue and our Elastic Customer Success Manager jumped into the challenge until we found a workaround. “

The Elastic community also plays a vital role in the partnership between Randstad Netherlands and Elastic. “The Elastic team is constantly publishing research and detection rules that enable us to stay ahead of malicious actors. There is also a highly engaged community on platforms such as GitHub and Slack contributing to rules development. It gives us confidence that we can continue to protect our business and keep up to date with evolving threat actors.”

In particular, Holzhauer is looking forward to deploying features like bidirectional integration between ServiceNow and the Elastic Agent to boost endpoint visibility to internal teams. He also sees value in the AI Assistant for Security, which provides teams with crucial alert context and in-depth security knowledge without having to invest in additional personnel.

In addition, the team has built a single Kibana Canvas slide which shows KPIs for the past month and is automatically sent to stakeholders as part of the reporting process.

Address complex threats with Elastic Security, built on the Elastic Search AI Platform, to streamline SecOps.

Learn more

|