elastic | Doctolib

SUCCESS STORY

# Doctolib establishes a powerful in-house security operations center with Elastic Security, reducing false positives by 50% and scaling to manage 12 times more data

**Region**
France

**Industry**
Software & Technology

**Solution**
Elastic Security, Elastic Observability, Kibana

**Building an in-house SOC results in 50% fewer false positives and faster threat response**

Doctolib brought its SOC in-house with Elastic Security to take advantage of advanced alerts, reducing false positives by 50% and significantly improving threat response times.

**Doctolib scales data retention 12x while cutting costs by 75%**

By moving from OpenSearch to Elastic, Doctolib extended data retention from one month to one year, managing 12 times more data while paying four times less in total costs.

**Reduced incident response time and analyst administration**

Elastic's machine learning and automated alerting capabilities allowed Doctolib to reduce the mean time to detect, investigate, and resolve incidents, while improving overall analyst efficiency.

# Elastic empowers Doctolib to optimize security operations and save on costs without sacrificing scale

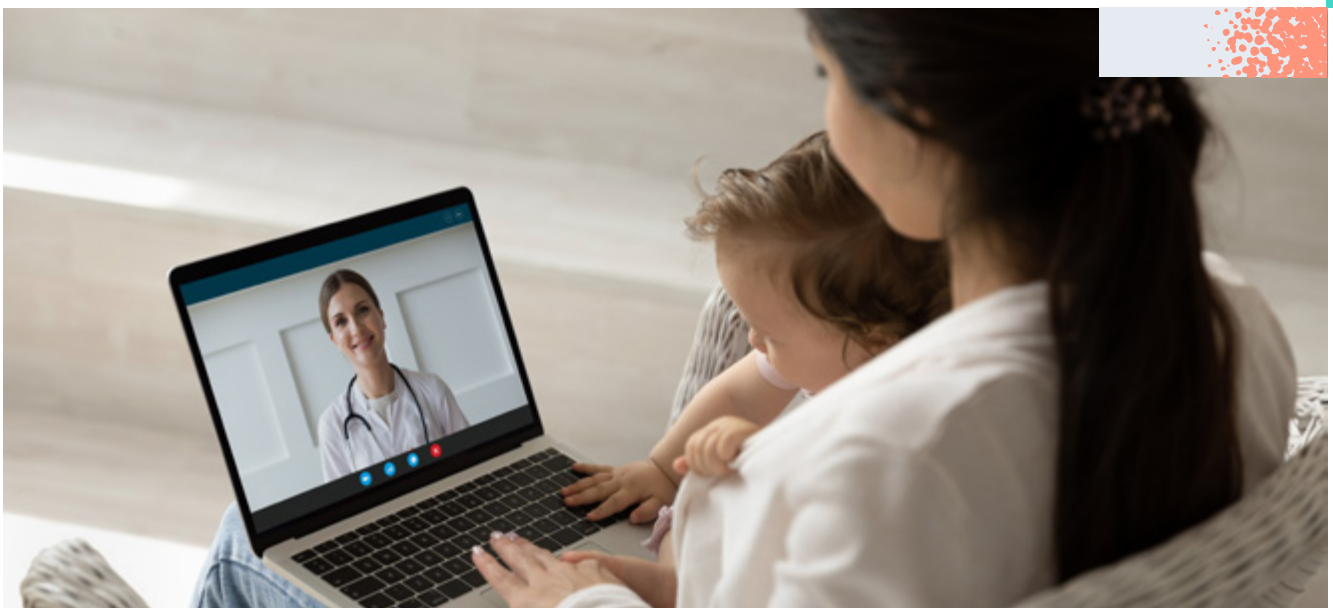
Doctolib, the leading e-health platform in Europe, connects over 90 million patients with 400,000 healthcare professionals across France, Germany, Italy, and the Netherlands. As the platform grew, it faced challenges securing large amounts of sensitive data, complying with strict healthcare regulations, and maintaining an optimal experience for millions of users. Adding to these problems was an outsourced security operations center that had frequent false positives, slow response times, and high costs.

The platform's rapid expansion, particularly during high-pressure times like the COVID-19 pandemic, highlighted the need for a more resilient and scalable security solution. Doctolib needed a way to bring its SOC in-house, reduce false positives, and improve threat detection and response — all while handling an ever-increasing volume of data.

Facing these critical challenges, Doctolib turned to Elastic Security. The mission: build a robust SOC that can meet today's demands and scale for tomorrow.

> Elastic didn't just enhance our security, it gave us the tools to scale efficiently and maintain high standards.

**Jordan Langue**
Security Platform Team, Doctolib



# Empowered cybersecurity: building an in-house SOC

Facing increasing threats and the limitations of an outsourced SOC, Doctolib recognized the need for greater control over its security operations. “Elastic was the key to bringing our SOC in-house,” says Othmane El Massari, Platform Security Engineer, Doctolib. Previously, Doctolib relied on an outsourced SOC based on OpenSearch, which led to challenges like frequent false positives and slower response times.

With Elastic’s SIEM, the company was able to internalize these operations, giving it the autonomy to manage its security with more precision and speed. After internalizing their SOC, Doctolib has similar alerting rules but more relevant alerts, which has directly reduced false positives. “By using Elastic, we cut false positives by 50%, so our team could focus on real threats,” added Tanguy Segarra, Blue Team Tech Lead, Doctolib.

# Unifying security operations with a comprehensive SIEM solution

Elastic Security became the heart of Doctolib’s InfoSec strategy. By centralizing logging, monitoring, and alerting across multiple data sources — including Google Drive, Jira, and internal applications — and migrating over from OpenSearch, Doctolib unified its security operations into a single, cohesive platform. “Transitioning to an internal SOC with Elastic has given us unprecedented control over our security operations,” reflects Segarra. The integration was smooth and the results were immediate — fewer false positives and faster, more effective responses to potential threats.

# Expanding observability to support development teams

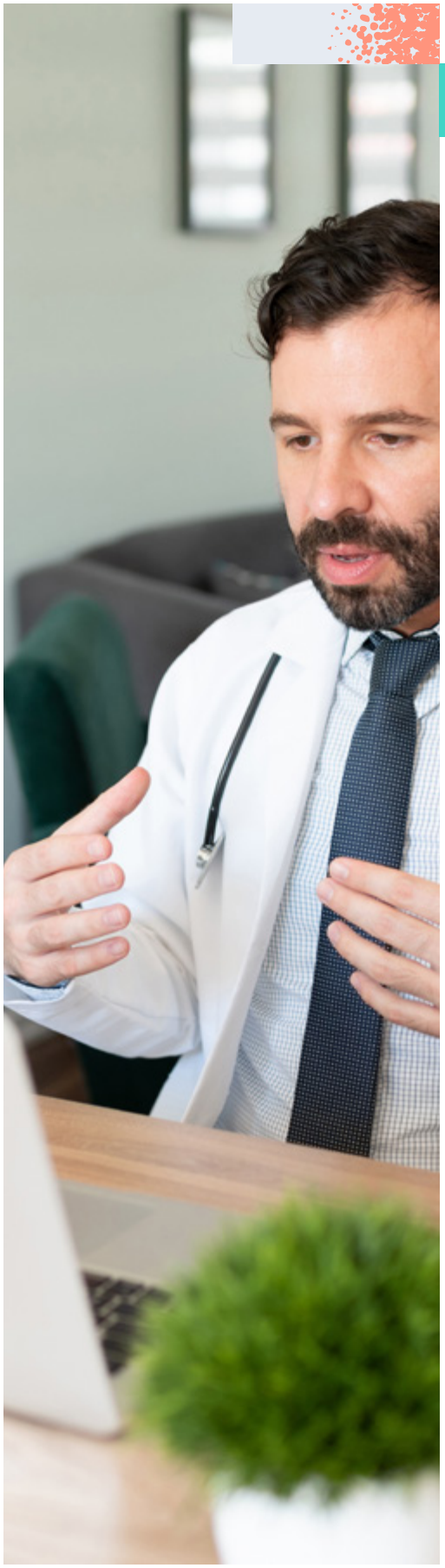
Beyond the security team, Elastic has also transformed the work of Doctolib’s developers. “Today, Elastic is widely used across nearly all tech teams at Doctolib,” says Segarra. “Developers now have access to the application logs they work on, which wasn’t possible with our previous solution. This transparency has greatly facilitated the work for many teams, especially when debugging.” With Elastic’s versatility, Doctolib can work more efficiently and effectively across multiple departments.

## Scaling data retention while cutting costs

As Doctolib grew, so did its data retention needs. Previously, with OpenSearch, Doctolib was unable to scale its data retention cost-effectively, keeping only one month's worth of data. Elastic's scalable architecture allowed Doctolib to extend its data retention period from one month to one year, all while managing 12 times more data.

With 2TB of logs per day and a need for better data retention, Doctolib invested in Elastic to scale its operations. While their total costs have doubled, they can now handle 12 times more data than before. This means the cost per terabyte has dropped by about 83%, making it much more efficient and cost-effective than if they had used OpenSearch for the same solution. "We've achieved significant improvements in our data retention strategy, extending from one month to one year without breaking the bank," explains Langue.



## Improving incident management and analyst performance

With its automated alerting and machine learning capabilities, Elastic improved Doctolib's security analysts' performance. "Elastic has made our analysts more productive by cutting down on routine tasks and false positives, so they can spend more time investigating real threats instead of looking for them," says Langue.

Using Elastic, the team focused less on mean time to detect (MTTD) due to automated alerting and a 50% reduction in false positives. This meant the team could focus on high-priority issues: reducing the mean time to investigate (MTTI), and resolve (MTTR) security incidents. With this increase in productivity, Doctolib's security posture has been strengthened, and threats can be managed more proactively.

## Easy integration and ongoing support from Elastic

Deploying Elastic's solutions within Doctolib's AWS cloud environment was a smooth process, thanks to Elastic's dedicated support team. From initial setup to ongoing management, Elastic's professional services team provided the guidance and expertise to ensure a smooth transition from OpenSearch.

"Elastic's support team helped us see the potential of Elastic's solutions in our context," says El Massari. "They customized the solution to fit our needs and ensured the transition went smoothly." After the successful integration, Doctolib was able to focus on what matters most: providing high-quality healthcare services.

## Future AI capabilities for next-level security

Doctolib's partnership with Elastic played a key role in bringing its SOC in-house, cutting false positives by 50%, extending data retention to one year, and improving analyst efficiency — all while reducing costs. As Doctolib continues to grow as a major digital health platform in Europe, Elastic remains a key ally in its commitment to top-tier security.

Looking ahead, Doctolib plans to deepen its use of Elastic's machine learning and AI tools to improve threat detection and strengthen its security measures. "Elastic's machine learning is already helping us catch issues we might have missed before," says El Massari. "We're planning to take this even further, using AI to identify and stop threats before they become problems."

> Elastic gave us the visibility we needed to respond to incidents and upgrade our security posture quickly, so that we could stay on top of healthcare tech.

**Othmane El Massari**
Platform Security Engineer, Doctolib

See for yourself how your business can benefit from Elastic in the Cloud, with a free 14 day trial.

Get started

elastic