elastic

SUCCESS STORY

World leader in energy and construction maximises the value and protection of its data with Elastic Observability and Security

Leading global company in energy and construction strengthens its global data infrastructure and enhances its defense against cybersecurity risks with Elastic.

Region
France

Industry
Energy and Utilities

Solution
Elastic Observability, Elastic Security for SIEM, APM, Training and Consulting

Protecting a global corporation
Implementing Elastic cybersecurity best practices improves visibility and reduces risk.

Modern data platform creates exponential value
Issues are rapidly detected and resolved for over 1,900 companies within the group.

Flexibility that unlocks limitless possibilities
Elastic's powerful analytics and visualization capabilities significantly reduce time to market.

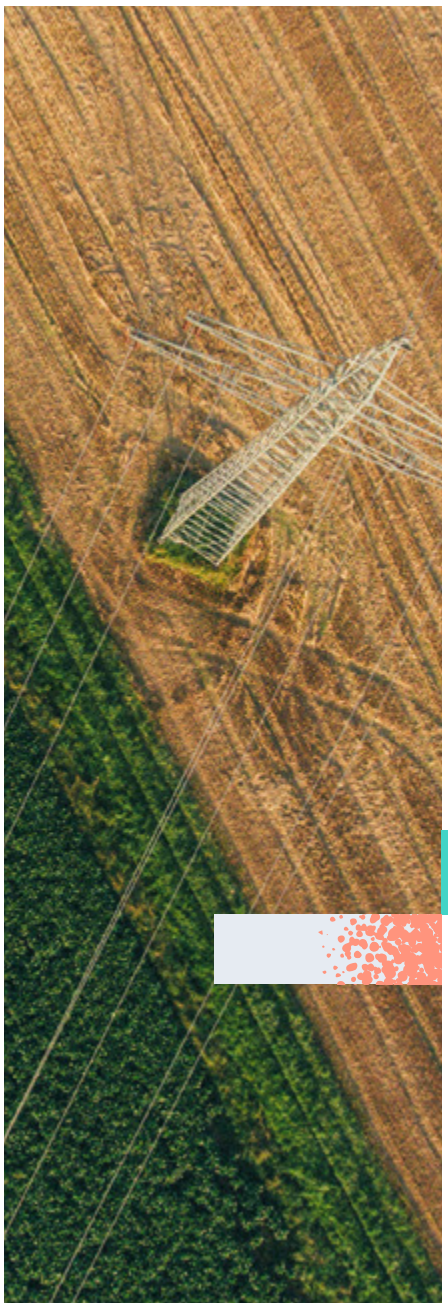
As a subsidiary of a larger European conglomerate with global reach, this large energy company specializes in transport and energy infrastructure equipment, energy assistance and consultancy for industry, sustainability and energy performance for buildings, and supporting companies in their digital transformation process. Its operations span 97,000 employees with presence in more than 120 countries.

Over 800 people work for the Deputy Head of Systems and Networks in the global IT department, managing the group's IT, communication, and management tools, infrastructure, networks and systems, including security and security service edge (SSE) tools.

The company operates internationally, which presents challenges: "The importance of internal support, available 24 hours a day, requires developing the skills and capacity to intervene in the central information service," says the Deputy Head of Systems and Networks, with specific focus on its energy subsidiary.

The 1,900 entities comprising the company are joined by new companies every year — each with its own systems and IT culture. "In this context, it's a question of limiting risks," the Deputy Head of Systems and Networks says.

Since 2015, a dedicated team has enabled the business to continuously improve its cybersecurity. A careful approach has reduced risk, but a lack of visibility across logs and the difficulty of correlating them limited progress. The company has a decentralized model which also complicated the implementation of a unified information system aimed at applying the same network and security standards to all of its group companies.



> The primary challenge lies in data quality, and quality data is key to ensuring security for all the Group's employees. Without trustworthy data, effectively identifying and responding to attacks becomes difficult.

Deputy Head of Systems and Networks
Top European Energy & Construction Company

Unifying the whole organization with a flexible solution

“Splunk met our early needs, but it lacked the necessary flexibility. The product could not handle our scaling, and as our data grew, costs increased significantly,” says the Deputy Head of Systems and Networks.

To improve visibility and keep up with data growth, the team experimented with the open-source version of Elastic on a single server for a few hundred MB of logs per day. The Deputy Head of Systems and Networks emphasizes this preference: “It’s all in the name!” he declares. “Splunk is just not as elastic as Elastic.”

This large European energy company chose Elastic Security to defend against cyberattacks with the powerful security information and event management (SIEM) solution, and Elastic Observability as a reliable and scalable reference solution for operations-focused visibility and analysis.

Elastic quickly became popular with other teams, who saw its flexible dashboards and visualizations, easier integrations, and superior power. More employees wanted access to the platform and were also interested in improving cash flow through pay-as-you-go billing.

It’s all in the name! Splunk is just not as elastic as Elastic.

Deputy Head of Systems and Networks
Top European Energy & Construction Company

 |

elastic

With Elastic, we could quickly identify several anomalies and inappropriate settings. A problem that had persisted for three years was fixed in as little as a week.

Deputy Head of Systems and Networks
Top European Energy & Construction Company

The power of Elastic to efficiently harness data at massive scale

Elastic has helped the business implement cybersecurity best practices and standards. While the energy side of the company is particularly vigilant about its central information system, monitoring specific business applications can be handed over to group subsidiaries.

For optimal speed and effectiveness at a company this large and distributed, security practitioners from central and local offices alike need access to the same SecOps tools. Before Elastic, manual correlation required involving everyone at every stage of the data journey.

The environment is changing rapidly, with technological advances and security needs evolving hand in hand. Elastic's speed has been key, enabling the team to retrieve information far faster than before. The Deputy Head of Systems and Networks explains, "When you need to search over a long period of time, you need to find the relevant data from billions of log entries." With Elastic, they can also create dashboards for uses that were not possible with other solutions.

Elastic Observability is used to make the most of the more than one terabyte of logs collected on a daily basis. Real-time monitoring with Elastic helps stop potential threats while powerful analytics capabilities turn data into actionable insights.

This large energy company focuses on sustainable relationships in infrastructure, industry, building solutions and ICT.

elastic

The versatility to do more

In the IT environment, applications are supported by an ecosystem of services, networks, and security technologies. “Our resource planning system is the heart of the business,” explains the Deputy Head of Systems and Networks, “but we must not forget everything around it: one deficient tool inevitably affects the system.”

The company operates a mix of cloud and on-premises systems. Here too, the flexibility of Elastic works wonders. Technologies developed for the cloud are also efficiently used on-premise. Thanks to Elastic integrations, the teams save a lot of time analyzing logs and can focus on more value-added tasks. The ability to retrieve logs quickly and easily has been instrumental in improving the company’s security posture.

Administrators can easily collect and process data with prebuilt integrations, saving time for higher-leverage tasks. The ability to quickly retrieve these logs accelerates mean time-to-respond for SecOps and IT teams alike.

For developers, Elastic has become part of everyday life. “With Elastic, the only limit is our imagination,” says the Deputy Head of Systems and Networks, underlining the many ways in which this company relies on Elastic.

“Elastic has provided us with the flexibility to seamlessly integrate, visualize, and, most importantly, correlate data, enabling us to swiftly extract information from billions of log entries in mere seconds. With Elastic, locating a needle in a haystack becomes effortlessly achievable.”

Deputy Head of Systems and Networks
Top European Energy & Construction Company

 |

elastic

Succeeding in a complex environment

Elastic has proven invaluable in enhancing security and improving uptime, says the Deputy Head of Systems and Networks. Elastic Security equips the company to detect suspicious activities quickly, reducing the likelihood and severity of security incidents. Further, it streamlines the incident response process by providing immediate, centralized access to previously lost or siloed data.

Elastic Observability helps the IT department operate more efficiently. For example, the company's Wi-Fi had been experiencing performance problems that had affected internal customers. By ingesting data from a few Wi-Fi hotspots, his team was able to fix a longstanding problem.

The sky's the limit

In the near term, this energy company will strategically expand its use of Elastic to meet key business needs. These efforts include tackling new security challenges, exploring migration to Elastic APM (Application Performance Monitoring), and investing in Elastic training and certification.

Already, team members are actively engaging in Elastic training and certification programs, by enrolling in courses such as Data Analysis with Kibana, exploring a wide range of on-demand training modules, and developing expertise in Observability and Elastic Security.

Selecting Elastic has yielded remarkable results, thanks in part to the unwavering support provided by the Elastic team and their shared vision for a bright future.

