splunk> a CISCO company

CASE STUDY

La Poste Stamps Out False Alerts by 10x, Protecting the Data of 1.3M Customers

Key Challenges

High data volumes either caused latency or crashes on the systems that La Poste's cybersecurity team used, slowing investigations and endangering the security of customers' information.

Key Results

After adopting [Splunk Enterprise Security](), La Poste's security team can better detect and mitigate threats, reducing false positives by tenfold and resolving alerts faster.

LA POSTE

Industry: Public Sector

Solutions: Security

Products: [Splunk Enterprise Security]()

La Poste is the largest mail delivery provider in France.

Whenever you place an online order, open a new credit card, or send a letter to your grandma, you're relying on the postal service to deliver your purchase on time, make sure your credit card arrives securely, and whisk your letter straight into grandma's hands. 1.3 million customers across 63 countries entrust La Poste each day with not only their letters and parcels, but also their data — such as personal addresses and contact information. And so, on top of reliable delivery services, La Poste must also protect the data of its customers.

This responsibility falls primarily to its 80-strong cybersecurity department, Service de Lutte Contre la Cybercriminalité (SLCC). It's no small task. La Poste, like many organizations, is up against a treacherous threat landscape rife with increasingly sophisticated attacks and geopolitical incidents. High-profile events such as the 2024 Paris Olympic Games mean bolstering the group's defenses has never been more vital.

Outcomes

- 80% of alerts now take under 13 minutes to process
- False positive alerts reduced by 10x
- Up to 20 terabytes of data are processed each day

La Poste's cybersecurity team adopted Splunk Enterprise Security as its SIEM in 2015. Because of its complex environment, La Poste needed a solution that had the capacity to handle immense quantities of data and diverse systems, and also capabilities for its teams to conduct investigations and thwart threats. "Our mission is to protect the group against threats and threat actors," says Olivier Cassignac, Responsable Détection des Incidents de Sécurité (Head of Security Incident Detection) at La Poste. "These attacks come in all shapes and sizes, and protecting the group means protecting its infrastructure, employees, and customers."

Powering high-speed investigations

The SLCC's main objective is to identify anomalies as early as possible so first-level analysts can process and notify relevant branches. However, high data volumes led to system crashes and delayed investigations. La Poste typically processes more than 20 terabytes of data each day, with the SLCC alone managing an average of five terabytes per day. Prior to implementing

Splunk, even with a far smaller volume of data, searching for specific events would take hours or simply crash the system.

After adopting Splunk Enterprise Security, the SLCC can now analyze vast volumes of data from previous weeks or months in a matter of seconds, saving critical time and resources to provide a robust foundation for the group's cybersecurity infrastructure. "During investigations, search tool performance is paramount as data volumes are huge. Splunk is a great asset because data is queried at high speed, giving analysts more time to make sense of it and move forward with the investigation," says Olivier.

Streamlining alerts

The SLCC is inundated with thousands of alerts each year, and it needed a solution to filter, categorize, and prioritize each potential threat. Splunk's Risk-Based Alerting (RBA) solution fit all these needs, and also cut the average time of alert processing to just 13 minutes. (From the time it takes the SLCC to receive the alert to the time it forwards it to the next relevant branch).

How did La Poste achieve this? The SLCC used Splunk Enterprise Security's capabilities and customized it according to its needs, tailoring every alert dashboard, function, rule, and search. ES's risk-based alerting capabilities also assign risk scores to events and issue an alert if the risk score reaches a certain threshold. This means the SLCC can now comprehensively detect potential threats and suspicious activity. The team has also seen a tenfold reduction in the rate of false positives, which empowers analysts to focus on real, urgent threats and work more efficiently.

> "The level of customization within Splunk is critical. There are no limits to the tool. There are plenty of solutions on the market, but to my knowledge, none of them offer such a high level of customization. You can really tailor every dashboard, function, rule, and search to your needs."
>
> **Olivier Cassignac,** Responsable Détection des Incidents de Sécurité (Head of Security Incident Detection) at La Poste

Facing new threats together

In the ever-evolving risk landscape, Splunk Enterprise Security's threat intelligence management feature has been a valuable tool in La Poste's arsenal. When the SLCC team detects a novel threat, the threat intelligence management feature analyzes it and converts it into a technical metric. This metric is then used to enhance the alerts, so the new threat can be identified and classified going forward. Importantly, it also conducts retroactive detection, combing back through events to see if the newly detected threat had occurred before.

It takes a village to stave off threats and secure an organization, and La Poste is no exception. Its cybersecurity organization of 200 includes the SLCC and various SOC members among its branches. Adopting Splunk means that all the teams can consolidate insights and use a common tool with tailored interfaces, depending on whatever use cases were needed — advanced analysis, KPI monitoring, manual searches, you name it. Splunk has let the cybersecurity teams not only conduct faster, more thorough investigations, but also better collaborate with other teams.

Download Splunk for free or get started with the free cloud trial. Whether cloud, on-premises or for large or small teams, Splunk has a deployment model that will fit your needs.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com