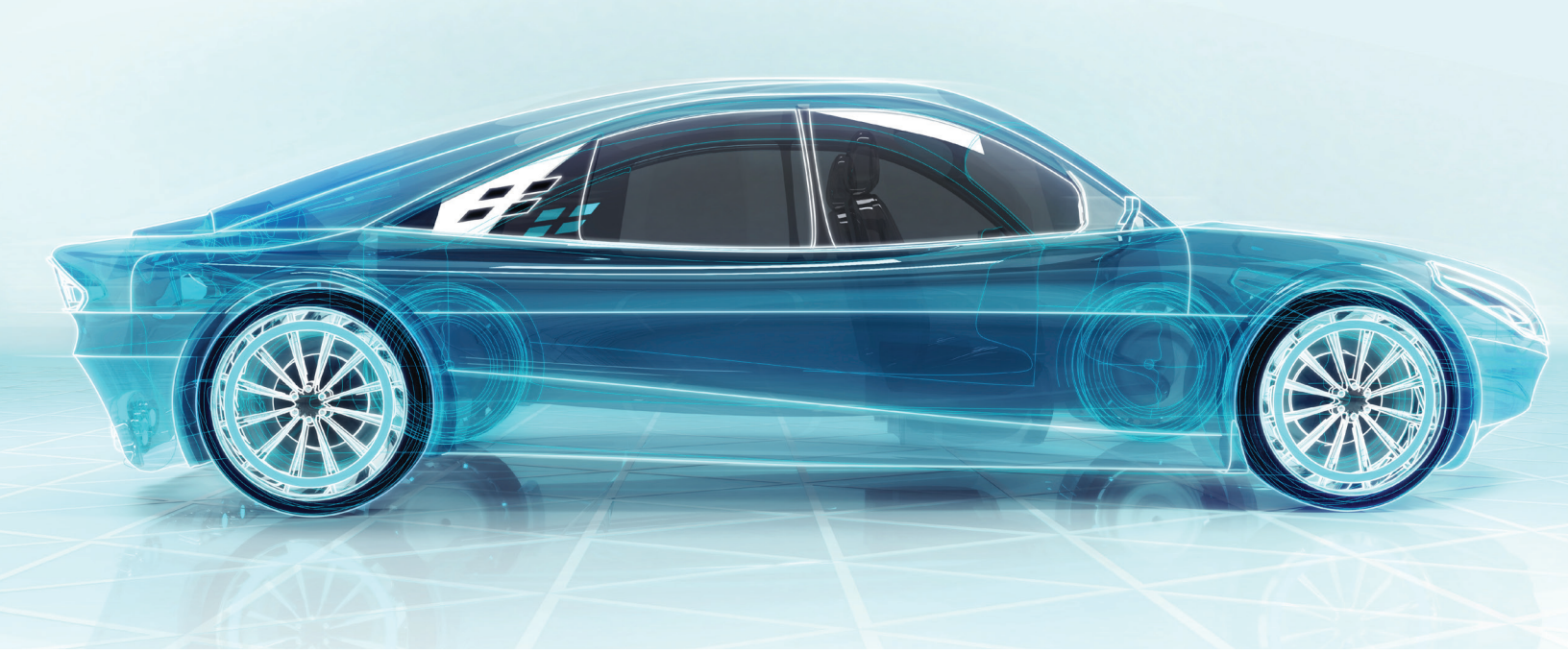


FORVIA faurecia

CASE STUDY

Forvia Faurecia puts security automation in the driving seat with Palo Alto Networks

As the automotive industry increasingly embraces automation, so Forvia Faurecia is embracing automation in its Security Operations Centre (SOC). By standardising on Palo Alto Networks Cortex XSOAR, this global automotive supplier is unifying case management, collaboration, and threat intelligence across more than 70,000 endpoints. The innovative platform manages alerts across all sources, helps increase SOC productivity by 70%, and in certain cases reduces alert volume by 99%.

paloalto® NETWORKS

IN BRIEF

Customer
Forvia Faurecia

Organisation Size
257 industrial sites across 39 countries; 111,000 employees

Industry
Manufacturing

Featured Products and Services
Automotive products and services

Location
Paris, France

Challenges

Security Operations Centre (SOC) lacked the resources and scalable processes to keep pace with an overwhelming volume of alerts from SIEM and EDR. Analysts wasted time pivoting across consoles for data collection, determining false positives, and performing repetitive, manual tasks throughout the incident lifecycle.

Requirements

- Collect inputs from almost any source.
- Define incident response procedures using digital workflow.
- Free resources to focus on more strategic SOC tasks.

Solution

Palo Alto Networks Cortex® XSOAR

CHALLENGES

Top 10 global automotive supplier

One in three automobiles feature Forvia Faurecia components. The US$16 billion organisation is a top 10 global automotive supplier, inspiring mobility through four business groups: Seating, Interiors, Mobility, and Electronics. Headquartered in France, Forvia Faurecia operates 257 industrial sites across 39 countries and has 111,000 employees.

Autonomous driving, electrification, connectivity, and other trends are upending more than a century of tradition in the automotive sector. Forvia Faurecia is responding to this seismic change by deploying next-generation technologies at scale. This demands a modern, resilient cybersecurity strategy to steer digital transformation, ensure uptime, and reduce risk.

The challenge for the six people in Forvia Faurecia's SOC was to manage the mass of cybersecurity alerts across approximately 70,000 endpoints and servers starting with the alerts prompted by the organisation's managed extended detection and response (EDR) platform.

Olivier Daloy, Group Chief Information Security Officer (CISO) at Forvia Faurecia, explains: "Our bias is to concentrate on alerts collected at the endpoint rather than on the infrastructure, because this is where the applications and data reside. If ransomware or malware is detected on a machine, for example, we need to isolate that machine very quickly with EDR."

EDR is only one layer of Forvia Faurecia's defensive curtain. The organisation also relied on a security information and event management (SIEM) platform to automate everyday log management processes in the SOC and recognize potential threats before they could disrupt business operations. Olivier again: "Of course, we don't neglect the logs that come from our security infrastructure. We use the logs to understand how and where an attack happened."

The overwhelming monitoring challenge didn't stop there. The SOC team was also scrutinising alerts for potentially malicious events in multicloud environments. Plus there were the alerts submitted by end users through the IT service management (ITSM) system.

When Matthieu Favris joined Forvia Faurecia as an Incident Response Manager in the SOC, he saw the problem first-hand. "When I arrived, the SOC team was crumbling under the load of alerts. They had a really difficult time distinguishing the non-priority alerts from the real emergencies. This in turn placed the business at risk."

It was time for action.

> Our bias is to concentrate on alerts collected at the endpoint rather than on the infrastructure, because this is where the applications and data reside. If ransomware or malware is detected on a machine, for example, we need to isolate that machine very quickly with EDR.
>
> **–Olivier Daloy, Group Chief Information Security Officer, Forvia Faurecia**

REQUIREMENTS

Automate operations with SOAR

Faced with this situation, Forvia Faurecia decided to deploy a security orchestration, automation, and response (SOAR) platform to improve the agility of security operations. The platform was required to:

- Collect inputs from almost any source, including the SIEM, and EDR.
- Capture threat intelligence and apply it to all relevant cybersecurity solutions.
- Define incident analysis and response procedures using digital workflow.
- Free SOC resources to focus on more strategic and value-added cybersecurity tasks.

SOLUTION

Best-in-class security made easy

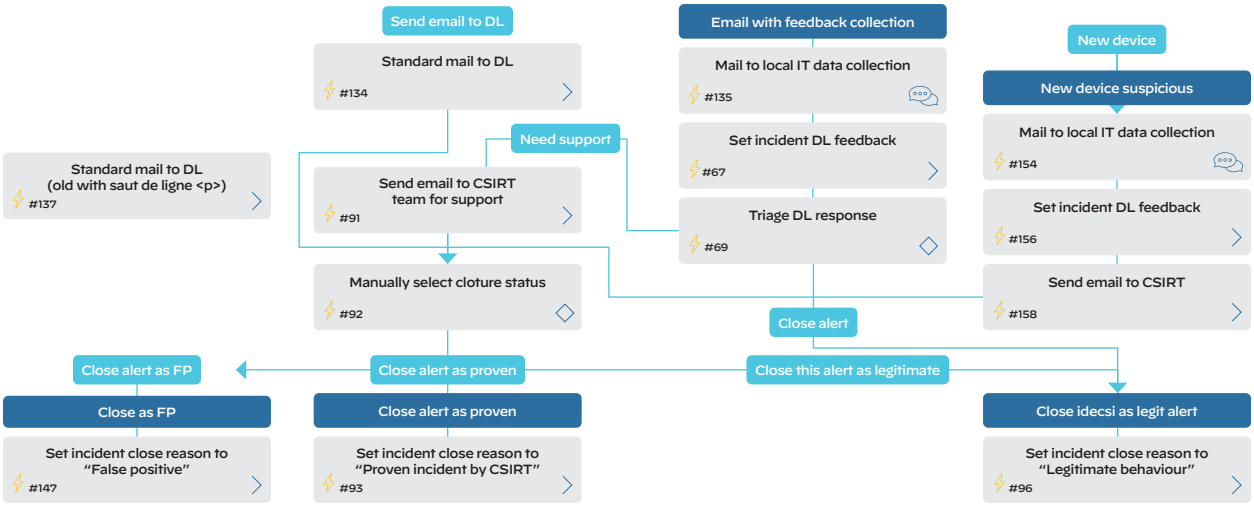
Palo Alto Networks Cortex® XSOAR ingests alerts across sources and executes automated workflows/playbooks to speed up incident response. "Our SIEM is not dead, but XSOAR has taken its place," says Matthieu.

Playbooks are at the heart of the Cortex XSOAR system. They enable Matthieu and his team to automate security processes such as handling investigations, processing SIEM alerts, and managing tickets.

He explains: "Our playbooks are fully automated. Most are hybrid, comprising an automatic and a manual component. For example, a playbook will automatically send an email to local IT teams, who confirm whether an alert is legitimate or not. Analysts only act if a malicious activity is confirmed."

In addition, XSOAR enables the team to answer internal audit requests related to their procedures and processes by simply providing a copy of the relevant playbooks. Not only does XSOAR enable the team to provide an answer, but the answer is trusted and accurate to what is being executed on the ground.

This modern orchestration platform also leverages threat intelligence data to automatically verify a resource's IP and domain. Similarly, XSOAR will include a database of the hostname nomenclature and directory information to help the SOC team make an accurate assessment of severity and impact.



> Cortex XSOAR is the most complete SOAR solution we evaluated. It connects seamlessly with our cybersecurity operations environment, including threat intelligence, the EDR, and an external sandbox. We can develop playbooks remarkably easily, and incident management is now centralised. I've also worked with Palo Alto Networks in the past, so I knew I could trust their people and technologies.

–Matthieu Favris, Incident Response Manager, Forvia Faurecia

BENEFITS

Faster response and increased productivity

Forvia Faurecia is standardising and automating security processes for faster response and increased productivity with Palo Alto Networks Cortex XSOAR, which:

- **Drives increase in SOC productivity:** Process automation, playbooks, real-time collaboration, and seamless API-based connectivity to other systems are at the heart of a huge productivity increase. According to Matthieu, "Cortex XSOAR has increased Forvia Faurecia's SOC productivity by 70%." As Matthieu further explains: "The recent release of a new internal solution generated nearly 20,000 alerts, but fewer than 200 alerts were handled manually. Everything else was done automatically. This represents a 99% reduction in manual workload and achieved an immediate return on our XSOAR investment."
- **Enables intelligent response:** Machine learning capabilities drive intelligent security management, accelerate playbook development, and enable leaner, more efficient security operations. "The Cortex XSOAR War Room is great," says Matthieu. "We can run real-time security actions through the command-line interface (CLI) without switching consoles, for example; or chat with other people for joint investigations. All of this boosts the speed of investigation. We can isolate a machine in one click."
- **Creates unified response:** Cortex XSOAR accelerates Forvia Faurecia's incident response by unifying alerts, incidents, and indicators from any source on a single platform for faster search, query, and investigation. "We can enrich an investigation with a mass of external data. And the insights are all there within the single pane of glass. We don't waste time searching for the data," says Matthieu. "We can also easily search for previous incidents and see if it's the same incident reoccurring."

> The role of our company is to manufacture car seats and dashboards, not to create correlation rules for a SIEM. Palo Alto Networks Cortex XSOAR gives Forvia Faurecia the automation and intelligence to automate security operations, freeing our limited SOC resources to make decisions that matter, rather than drown in reactive, piecemeal responses.
>
> **–Olivier Daloy, Group Chief Information Security Officer, Forvia Faurecia**

For more information about the Palo Alto Networks security platform, visit the Cortex XDR and Cortex XSOAR webpages.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com