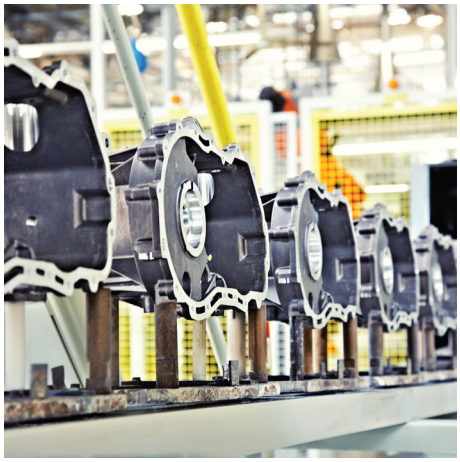
NetIQ

Customer Success Story

Sentinel

# Leading Automotive Technology Supplier

The company wanted to centralise and improve its operational and security monitoring capabilities as it was struggling to react effectively to external or internal threats to its IT systems. By implementing NetIQ® Sentinel™, the company has taken advantage of cutting-edge Security Information and Event Management (SIEM) technology to analyse and correlate events worldwide to boost IT security.



## Overview

This global company specialises in innovative design, R&D and manufacturing and is a leading supplier to the automotive industry. With annual revenues of billions of euros and over 70,000 employees, it was imperative that the company find a way of maintaining high levels of IT security to protect its information assets.

## Challenge

As the company expanded worldwide, IT staff found monitoring the operational and security infrastructure across the entire enterprise increasingly difficult. The company wanted to centralise and automate the monitoring and management processes to better detect and mitigate potential security risks and reduce manual workload.

The company decided to implement a Security Information and Event Management (SIEM) solution to boost its IT security with better visibility of possible threats.

**"Thanks to the flexibility and extensibility of Sentinel, we quickly and easily integrated our various systems to take full advantage of all information available in our IT service management systems."**

**SPOKESPERSON**

Leading Automotive Technology Supplier

## Solution

After evaluating offerings from a range of vendors, the company chose to implement Sentinel to overcome its monitoring challenges and tighten IT security.

The company successfully deployed Sentinel and now runs a large, distributed system with a total of 25 Collector Managers located around the world. These managers gather log files from over 4,500 Linux, UNIX and Windows servers, 40 security systems and 55,000 endpoints across the global enterprise. In this tiered high-performance architecture, each Collector Manager sends data to one of eight Sentinel servers on one of three different continents.

The distributed Sentinel solution is fully integrated with the company's operations management. Monitoring systems feed log data into Sentinel, and Sentinel analyses all log data and automatically creates tickets in the connected incident management system as needed. This enables the company to centrally monitor all events throughout its entire IT infrastructure to improve its security defences and the visibility of threats.

NetIQ Consulting drafted and implemented the Sentinel solution and integrated the existing IT infrastructure and services including the configuration management system, IP address management (which provides data about the network topology), location of systems and the global directory service.

## At a Glance

**Industry**

Automotive

**Location**

Undisclosed

**Challenge**

The company needed to implement a Security Information and Event Management (SIEM) solution to boost its IT security.

**Solution**

Use Sentinel to centrally monitor all events throughout the entire IT infrastructure to improve security defences and the visibility of threats.

**Results**

+ Gained a comprehensive view of its global IT infrastructure
+ Provided the ability for IT staff to focus on threats and work more efficiently
+ Introduced automated processes, which speeds up administration and frees IT staff to dedicate more time to non-routine tasks

**“With Sentinel, we can identify issues and generate incident tickets with useful contextual information to reduce security risks and improve service quality.”**

**SPOKESPERSON**
Leading Automotive Technology Supplier

www.netiq.com

“The collaboration with NetIQ Consulting was seamless. The NetIQ team was very competent and the support throughout the project was great,” said a company spokesperson.

The solution also uses public reputation data and blacklists to generate risk intelligence. Adjustments can be made easily, giving the company more control of its security system and incident management.

## Results

The solution plays a vital role in helping the company effectively meet its large-scale security and threat monitoring challenges.

As a result of integrating its IT service management, operational and security monitoring systems, the company has gained a comprehensive view of its global IT infrastructure. The solution provides real-time visibility into activity, centralising and simplifying monitoring tasks. Previously, manually identifying and locating security risks across such a vast network was a time- and labour-intensive process. By processing event logs and generating tickets automatically, IT staff can focus on actual threats and work much more efficiently. Sentinel helps facilitate the detection of internal and external security threats, enabling IT staff to respond to any potential attacks much more rapidly. Automation speeds up administration and frees IT staff to dedicate more time to non-routine tasks.

The company is confident that Sentinel will enable it to deal with any future security threats because its IT infrastructure is well-prepared and its information assets well-protected.

The company spokesperson concluded, “Thanks to the flexibility and extensibility of Sentinel, we quickly and easily integrated our various systems to take full advantage of all information available in our IT service management systems. This means we can identify issues and generate incident tickets with useful contextual information to reduce security risks and improve service quality.”


**Denmark**
+45 45 16 00 20

**France**
+33 1 55 70 30 13

**Germany**
+49 89 42094 0

**Italy**
+39 02 366 349 00

**Netherlands**
+31 172 50 55 55

**Poland**
+48 22 537 5000

**Portugal**
+55 11 3627-0900

**Spain**
+34 91 640 25 25

**Sweden**
+46 8 752 25 00

**NetIQ**
**Worldwide Headquarters**
Houston, Texas
713 548 1700
888 323 6768

**www.netiq.com**