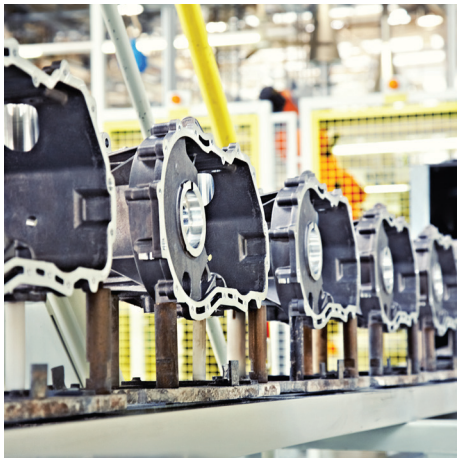
NetIQ

**Anwenderbericht**

Sentinel

# Führender Zulieferer von Automobiltechnologie

Das Unternehmen hatte Schwierigkeiten, die Sicherheit der IT-Systeme zu gewährleisten. Aus diesem Grund hat es die operative und sicherheitstechnische Überwachung zentralisiert, um so effektiv auf externe oder interne Bedrohungen für seine IT-Systeme zu reagieren. Mit der Implementierung von NetIQ Sentinel entschied sich das Unternehmen für eine intelligente SIEM-Technologie, die die einfache Analyse und Korrelation von Ereignissen weltweit analysiert und so die IT-Sicherheit verbessert.



## Überblick

Dieses globale Unternehmen ist ein führender Automobilzulieferer und auf innovatives Design, Forschung und Entwicklung sowie Fertigung spezialisiert. Bei einem Jahresumsatz von mehreren Milliarden Euro und über 70.000 Mitarbeitern war es für das Unternehmen wichtig, die IT-Sicherheit zu erhöhen und wichtige Informationen zu schützen.

## Herausforderung

Mit der weltweiten Expansion fiel es IT-Mitarbeitern zunehmend schwerer, die operative Struktur sowie die Sicherheitsinfrastruktur des gesamten Unternehmens zu überwachen. Ziel war daher die Zentralisierung und Automatisierung von Überwachungs- und Verwaltungsprozessen, um potentielle Sicherheitsrisiken besser zu identifizieren sowie manuelle Workloads zu reduzieren.

Das Unternehmen entschied sich für die Implementierung einer SIEM-Lösung (Security Information and Event Management), um die IT-Sicherheit zu erhöhen, indem Bedrohungen besser identifiziert werden können.

**„Dank der Flexibilität und der Erweiterbarkeit von Sentinel haben wir unsere verschiedenen Systeme schnell und einfach integriert, um alle Informationen optimal zu nutzen, die in unseren IT-Servicemanagementsystemen verfügbar sind.“**

**SPRECHER**

Führender Zulieferer von Automobiltechnologie

## Lösung

Nach der Auswertung zahlreicher Angebote von verschiedenen Anbietern entschied sich das Unternehmen für die Implementierung von Sentinel, um Überwachung und Sicherheit der IT-Systeme zu verbessern.

Nach der erfolgreichen Implementierung von Sentinel hat das Unternehmen nun ein großes, verteiltes System mit insgesamt 25 Collector-Managern weltweit im Einsatz. Diese Manager erfassen die Protokolldateien von über 4.500 Linux-, UNIX- und Windows-Servern, 40 Sicherheitssystemen und 55.000 Endpoints aus dem gesamten Unternehmen. Innerhalb dieser mehrstufigen Hochleistungsarchitektur sendet jeder Collector Manager Daten an einen der acht Sentinel-Server auf einem von drei Kontinenten.

Die verteilte Sentinel-Lösung ist vollständig in das operative Management des Unternehmens integriert. Überwachungssysteme leiten Protokolldaten an Sentinel weiter, Sentinel analysiert diese und erstellt bei Bedarf automatisch Tickets über das verbundene Incident-Managementsystem. Dies ermöglicht die zentralisierte Überwachung aller Vorfälle über die gesamte IT-Infrastruktur hinweg, um so deren Sicherheitsfunktionen und die Sichtbarkeit von Bedrohungen zu verbessern.

NetIQ Consulting hat die Sentinel-Lösung aufgesetzt, implementiert und in die bestehende IT-Infrastruktur sowie Services integriert, einschließlich des Konfigurations- und IP-Adressenmanagementsystems (das Daten zur Netzwerktopologie liefert), der Systemstandorte und des globalen Verzeichnisdienstes. „Die Zusammenarbeit mit NetIQ Consulting verlief reibungslos. Das

## Auf einen Blick

**Branche**

Automobile

**Standort**

Unbekannt

**Herausforderung**

Das Unternehmen musste eine SIEM-Lösung (Security Information and Event Management) implementieren, um die IT-Sicherheit zu erhöhen.

**Lösung**

Nutzung von Sentinel zur zentralisierten Überwachung aller Vorfälle über die gesamte IT-Infrastruktur hinweg, um so deren Sicherheitsfunktionen und die Sichtbarkeit von Bedrohungen zu verbessern.

**Ergebnisse**

+ Umfassender Überblick über die globale IT-Infrastruktur des Unternehmens
+ IT-Mitarbeiter können sich auf Bedrohungen konzentrieren und effizienter arbeiten
+ Einführung automatisierter Prozesse, welche die Verwaltung beschleunigen und IT-Mitarbeitern mehr Zeit für Aufgaben geben, die nicht routinemäßig durchgeführt werden müssen

**„Wir können mit Sentinel Probleme identifizieren und Incident-Tickets generieren, die hilfreiche Informationen enthalten, um IT-Sicherheitsrisiken zu reduzieren und die Servicequalität zu verbessern.“**

**SPRECHER**
Führender Zulieferer von Automobiltechnologie

**www.netiq.com**

NetIQ Team war äußerst kompetent und hat uns während des gesamten Projekts großartig unterstützt“, erklärte ein Sprecher des Unternehmens.

Die Lösung nutzt außerdem öffentliche Reputationsdaten und Blacklists zur Erstellung von Risikoanalysen. Durch die Möglichkeit zur einfachen Anpassung erhält das Unternehmen mehr Kontrolle über Sicherheitssysteme und Incident-Management.

## Ergebnisse

Die Lösung spielt für das Unternehmen eine wesentliche Rolle bei der Überwachung von Sicherheitsrisiken und potentiellen Bedrohungen.

Dank der Integration von IT-Servicemanagement- sowie operativen und Sicherheitsüberwachungssystemen erhält das Unternehmen einen umfassenden Überblick über seine globale IT-Infrastruktur. Die Lösung liefert einen Echtzeitüberblick über Aktivitäten und zentralisiert und erleichtert so die Aufgabenüberwachung. Bisher war die manuelle Identifizierung und Lokalisierung von Sicherheitsrisiken in einem so großen Netzwerk ein zeit- und arbeitsaufwendiger Prozess. Dank der automatisierten Verarbeitung von Ereignisprotokollen und der automatischen Ticketerstellung können IT-Mitarbeiter sich nun auf tatsächliche Bedrohungen konzentrieren und effizienter arbeiten. Sentinel hilft bei der Erkennung von internen und externen Sicherheitsbedrohungen und ermöglicht es IT-Mitarbeitern, schneller auf potentielle Angriffe zu reagieren. Durch die Automatisierung werden die Verwaltungsprozesse erheblich beschleunigt und IT-Mitarbeitern bleibt mehr Zeit für Aufgaben, die nicht routinemäßig durchgeführt werden müssen.

Das Unternehmen ist zuversichtlich, dass zukünftige Sicherheitsbedrohungen mithilfe von Sentinel abgewehrt werden können, da es nun über eine gut vorbereitete IT-Infrastruktur verfügt und wichtige Informationen geschützt sind.

Der Sprecher des Unternehmens kommentiert dies wie folgt: „Dank der Flexibilität und der Erweiterbarkeit von Sentinel haben wir unsere verschiedenen Systeme schnell und einfach integriert, um alle Informationen optimal zu nutzen, die in unseren IT-Servicemanagementsystemen verfügbar sind. „Wir können Probleme identifizieren und Incident-Tickets generieren, die hilfreiche Informationen enthalten, um IT-Sicherheitsrisiken zu reduzieren und die Servicequalität zu verbessern.“

**NetIQ**
**Deutschland**
Fraunhoferstr. 7
85737 Ismaning
Tel: +49 (0)89 420940
Email: infoDE@netiq.com

**Schweiz**
Flughafenstrasse 90
P.O. Box 253 8058 Zürich
Tel: +41 (0)43 456 2400
Email: infoCH@netiq.com

info@netiq.com
www.netiq.com/communities
www.netiq.com

**Die vollständige Liste unserer Niederlassungen** in Nordamerika, Europa, Nahost, Afrika, Lateinamerika sowie im asiatisch-pazifischen Raum finden Sie unter: www.netiq.com/contacts

**www.netiq.com**