infopulse

Case for **Industrial Solutions Manufacturer**

A SOC with a Cloud SIEM/SOAR System Enhanced Security Posture for a Swiss Manufacturer_

24/7 Monitoring and Incident Response
with Azure Sentinel for a Leading Manufacturer

Industry: **Manufacturing** Location: **Switzerland** Employees: **3,500+**

Client Background

Our client is one of the world leaders in providing cutting-edge solutions for industrial products. With a presence in over 30 countries, our client supports its customers from a broad range of industries with tailored, customized, and extensive expertise.

Business Challenge

The client approached Infopulse with a request to synchronize and centralize its security initiatives. Establishing a Security Operations Center (SOC) was a primary objective and the best way to unify professional service, industry experts, and solid security management in one solution.

Since our client operates numerous branches that have different standards and processes, they stumbled upon the challenge of synchronizing cybersecurity standards/policies and gaining more visibility into security processes. After considering carefully the client's needs, we advised Azure Sentinel by Microsoft as the most relevant security platform in terms of its commercial and technical efficacy. It was a perfect fit because our client already had a Microsoft ecosystem that allowed for easier built-in integrations and reduced overhead costs.

Solution

In the course of 6 months, the Infopulse team implemented Azure Sentinel as a SIEM/SOAR platform to facilitate the client's security operations.

During the onboarding stage, we conducted an in-depth security pre-assessment of the client's infrastructure, business process, and users' workflow to build a tailored SOC implementation roadmap.

Elements of SOC

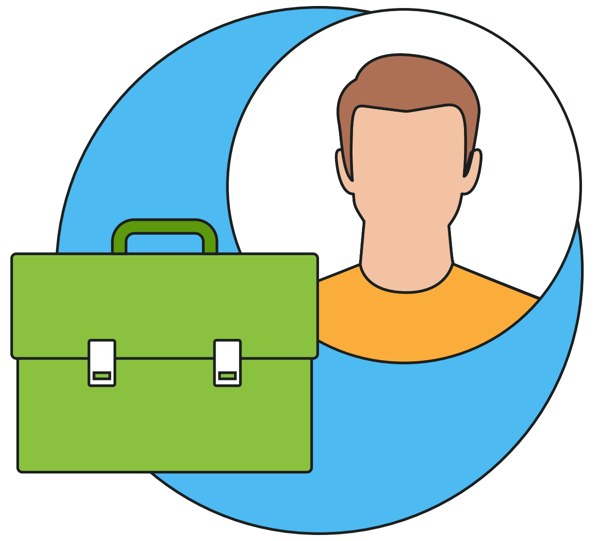
Before proceeding with the establishment of SOC, we defined and approved its key aspects with the client:

1. A powerful technical platform:

We chose Azure Sentinel as a SIEM/SOAR solution to ensure a high level of resilience of business-critical systems.

2. Scope of service:

We defined relevant use cases that had to be covered by the SOC service by identifying the core aspects of the client’s infrastructure.



3. Assembling a team:

Under a shared responsibility model, we offered a team of industry experts with the fitting skillset for incident analysis, management, and recommendations.

The scope of establishing SOC included the following activities:

- Deployed a cloud-based Azure Sentinel solution to the company's Azure environment
- Built a team of security experts to cover L1/L2 support
- Enabled a step-by-step onboarding to connect different regions to the platform, aligned with the internal reorganization project
- Configured log collection from cloud-based and on-premises systems, such as domain controllers, firewalls, and antiviruses; developed custom connectors
- Set up processes to enable continuous monitoring, rapid incident response, and escalation to the in-house team
- Developed a number of custom use cases in addition to built-in ones to cover specific threats relevant to the customer environment
- Initiated the development of a unified dashboard for real-time security monitoring
- Helped the client adopt the EDR system for better endpoint visibility and faster threat mitigation
- Automated the incident response process to reduce the alarm management pressure on the security team

Technologies

- **Azure Sentinel**
- **Azure Logic Apps**
- **Custom Log Parsing Scripts**
- **Jira**
- **Azure Arc**
- **O365 Identity Protection**
- **Commercial threat intelligence feeds**
- **FortiEDR and others**

Business Value

Through the comprehensive security audit and SOC establishment, the client has gained visibility into its security posture and is now able to streamline its security strategy. The project brought the value of:

- A newly introduced proactive approach to cybersecurity
- Significantly reduced risk of data breaches and cyberattacks
- 500+ security incidents are detected and resolved on a monthly basis
- Mature security level regarding security operations
- Enabled 24/7 monitoring + vulnerability scanning across the client's branches in Central Europe, Asia, and North and South America
- Provided extensive recommendations that allowed fine-tuning internal security policies and strengthening the protection of the company's workloads

Since February 2021, Infopulse has continued to provide the SOC service and currently has the role of a trusted security advisor to the client.

Contact us

PL	+48 (221) 032-442
DE	+49 (69) 505-060-4719
US	+1 (888) 339-75-56
UK	+44 (8455) 280-080
UA	+38 (044) 585-25-00
BG	+359 (876) 92-30-90
BR	+55 (21) 99298-3389

✉ info@infopulse.com

About Infopulse

Infopulse, part of the leading Nordic digital services company Tietoevry, is an international vendor of services in the areas of Software R&D, Application Management, Cloud & IT Operations, and Cybersecurity to SMEs and Fortune 100 companies across the globe. Founded in 1991, the company has a team of over 2,300 professionals and is represented in 7 countries across Europe and the Americas.

Infopulse is trusted by many established brands, such as BICS, Bosch, British American Tobacco, Credit Agricole, Delta Wilmar, ING Bank, Microsoft, Offshore Norge, OLX Group, OTP Bank, SAP, UkrSibbank BNP Paribas Group, Vodafone, Zeppelin Group, and others.

For more information, please visit **www.infopulse.com**