infopulse
Part of Tietoevry Create

Case for **Gold Mining Company**

Unmatched SAP Security with Microsoft Sentinel for Gold Mining Company

Safeguarding Business-critical Application Data with Microsoft Sentinel & Custom Security Rules

Industry: Manufacturing **Location: Central Asia**

Employees: 9,000+

Client Background

Our client is one of the largest gold mining and production companies in Central Asia. Owning a vast portfolio of assets that spans multiple large-scale gold deposits across the region, the company produces millions of tons of gold ore annually. As an industry leader, the client covers the entire mine-to-market value chain – from geological exploration to mining, processing, and distribution of precious metals, along with the design and construction of gold production facilities.

Executive Summary_

Goals

Select and implement a SIEM solution that would minimize the risks of insider threats and ensure comprehensive security monitoring of the corporate SAP ERP system, while also meeting the cost-efficiency requirements.

Solution

Infopulse seamlessly integrated Microsoft Sentinel into the client's hybrid infrastructure, implemented 80+ custom security monitoring rules, and provided consultations on establishing an efficient incident management process that would allow reacting to alerts in near real-time.

Benefits

The capabilities of Microsoft Sentinel coupled with tailored security rules allowed the company to enable the utmost protection of their SAP environments, rapidly detect potential threats, and significantly reduce TCO costs, all while optimizing the work of the internal security team.

Services delivered

Cybersecurity & Security Assessment services, Microsoft Sentinel implementation, SIEM/SOAR Deployment.

Business Challenge_

Our client operates a complex hybrid infrastructure that includes both cloud-based and on-premises IT systems. Recognizing the growing security risks due to the global proliferation of cyber threats, they aimed to protect business-critical IT assets across all estates.

The collaboration of Infopulse and the gold mining company began with multiple joint projects that involved an implementation of Microsoft Sentinel for the company's backup cloud infrastructure as well as a disaster recovery solution for their on-premises SAP system.

Once the pilot projects were complete, the company continued to assess its security posture and realized that their SAP system, which stores large volumes of sensitive corporate data, was lacking efficient security monitoring capabilities.

This fundamental weakness could lead to data leaks caused by unauthorized access or other insider threats resulting in significant financial losses and reputational damage. Furthermore, the company could have faced downtimes and financial disruptions, as the SAP system is also used to process invoices and other transactions.

Thus, the key challenges for the client were to:

- Establish efficient security monitoring and rapid incident response that would ensure all-around data protection for the corporate SAP ERP.
- Find a solution that would suit the client's requirements in terms of its capabilities and cost ratio.
- Integrate the solution with the existing SIEM system – IBM QRadar.

To help the client select a solution that would effectively address their challenges, **Infopulse implemented another pilot project** that was focused on connecting the initially deployed Microsoft Sentinel solution to the on-premises SAP system and implementing 7 test scenarios for monitoring the SAP environment.

Being satisfied with the results of the pilot project, the client decided to proceed with **a full-scale implementation of Microsoft Sentinel for SAP.**

Solution & Business Value_

After seamlessly **integrating Microsoft Sentinel into the client's complex hybrid infrastructure,** Infopulse developed, tested, and deployed **80+ custom security monitoring rules** to ensure unmatched data protection for the client's SAP ERP.

As a result, the gold mining company received a full range of benefits:

- **Reinforced security posture** – the robust security monitoring powered by Microsoft Sentinel helps the gold mining company safeguard their SAP landscape, minimizing the risks of costly data breaches.
- **Rapid threat detection** – the near real-time incident management system empowered our client with rapid detection of illegitimate operations and suspicious user behavior.
- **Reduced TCO** – in addition to having all the required monitoring capabilities, Microsoft Sentinel turned out to be a perfect choice cost-wise and is simpler to deploy, configure, and fine-tune in comparison to alternative SIEM tools.
- **Cost optimization** – by implementing cloud-based Sentinel, the company could optimize costs for purchasing, setting up, and supporting additional on-premises infrastructure.
- **Flawless system interoperability** – by integrating Microsoft Sentinel with the client's on-premises SAP system and the backup cloud-based ERP, Infopulse ensured a smooth flow of security logs across all estates, thus helping the client avoid duplicated efforts and extra costs.
- **Streamlined security operations** – some security rules were adjusted to exclude the "alert fatigue" for the client's security operators. Moreover, Infopulse provided in-depth guides on incident analysis and response for the company.

Technical Details

At the beginning of the project, the key task for Infopulse was to ensure seamless interoperability and data exchange between Microsoft Sentinel and the client's cloud-based and on-premises IT infrastructure. Our team used Microsoft's proprietary data connectors for SAP applications to integrate Microsoft Sentinel with the client's backup ERP system that resides in the cloud (Microsoft Azure).

The integration of Microsoft Sentinel with the client's SAP ERP was performed via the following approach. Our team configured and deployed a log forwarder – a Linux-based virtual machine that collects the logs from the Cloud and on-premises SAP environment and transfers them to Microsoft Sentinel for further processing.

To connect the company's on-premises SIEM system IBM QRadar with Microsoft Sentinel, Log Analytics workspace in Microsoft Azure and Cloud REST API connector were used, being officially supported both by Microsoft and IBM platforms.

Consequently, Infopulse proceeded with the development of **80+ security event monitoring rules** that fall into one of **three categories:**

- Custom security monitoring rules tailored to the client's requirements
- Built-in Microsoft Sentinel rules for monitoring SAP environments
- A set of rules that was based on SAP Enterprise Threat Detection

The implementation of the security rules was highly dependent on the deployed SAP modules and the specifics of the client's operations. Infopulse worked in close cooperation with the client's security team, as well as employees from various departments to outline normal and abnormal user behavior across finance and accounting, HR, supply chain management, and other processes. To maintain business continuity for the company, our team did not establish any restrictions – the entire analysis was carried out in the form of a seamless process discovery.

The security rules were designed to **combat both intentional and negligent insider threats.** Some of the examples include – the detection of unauthorized access attempts, illegitimate operations, or configuration changes in the SAP environment, as well as suspicious user activities, such as direct connection to the database, transferring large volumes of corporate data to a USB flash drive, etc.

Ultimately, the security monitoring rules developed by Infopulse served as a foundation for enabling **near-real-time incident management,** which includes the following stages:

- A security event occurs in the SAP system and generates logs that are transferred to Sentinel
- Microsoft Sentinel analyzes the logs to identify illegitimate actions/abnormalities and triggers an alert
- The security operator analyzes the alert and responds according to the internal security policies

Infopulse thoroughly reviewed and tested each of the 80+ security rules. Upon confirming that the rule was feasible and worked as expected, our team continued to improve it. Certain rules had to be optimized, as they generated too many incidents, which could potentially hamper the work of the security operators. Therefore, to minimize the "alert fatigue" for the client's security team, some of the **rules were implemented in the form of dashboards,** regularly checked by the operators.

Lastly, to further facilitate the work of the client's security team, we developed **numerous playbooks with detailed instructions** on how to analyze and respond to specific security alerts.

Microsoft Sentinel

Microsoft Azure

SAP

IBM QRadar

About Infopulse

Infopulse, part of Tietoevry Create, delivers the broadest range of tailored cybersecurity services, including SIEM/SOAR Deployment, Cloud Security, Security Assessment, SOC, IT infrastructure protection, DevSecOps, and more.

With 18+ years of experience in Microsoft technologies and SAP solutions, Infopulse offers a holistic portfolio of Microsoft and SAP-focused consulting, development, and managed services. Our expertise is supported by long-term partnerships with Microsoft and SAP and is recognized through Azure Expert MSP Status and numerous Microsoft Solutions Partner Designations.

Infopulse is trusted by many established brands, such as Bosch, Zeppelin, Metinvest, SAG, IPCO, Petruzalek Ukraine, Offshore Norge, Credit Agricole, Delta Wilmar, ING Bank, Microsoft, SAP, OLX, OTP Bank, Santander, UKRSIBBANK BNP Paribas Group, VEON, Vodafone, and others.

For more information, please visit www.infopulse.com

Contact us

PL	+48 (221) 032-442
DE	+49 (69) 505-060-4719
US	+1 (888) 339-75-56
UA	+38 (044) 585-25-00
BG	+359 (876) 92-30-90
NL	+31 (70) 89-10-8534
BR	+55 (21) 99298-3389

✉ info@infopulse.com