infopulse

Case for **a European leader in agriculture**

Consulting a Major Agricultural Company on Microsoft Sentinel Capabilities to Secure IT Infrastructure_

Leveraging cybersecurity automation to test the cloud-native security system

Industry: Agriculture **Location:** Ukraine **Employees:** 14,000+

Client Background

Our client is one of the leaders in the European agricultural sector. They have a diverse network of fields, processing, and storage premises that enable the continuous supply of high-quality produce to 80 countries worldwide.

Business Challenge

Our client aimed to enhance their cybersecurity landscape. The company was already using a legacy security solution to monitor own security perimeter. However, due to infrastructure changes and migration to the cloud, this legacy solution could not provide the relevant level of defense. Thus, the company was looking for a service provider to assist with the deployment of a modern **SIEM (Security information and event management) & SOAR (Security Orchestration, Automation, and Response)** system.

Upon considering the ups and downs of various security platforms, Infopulse offered to implement such a system on basis of **Microsoft Sentinel** (formerly Azure Sentinel) based on our client requirements and business needs. As an official long-term Microsoft partner with Azure Expert MSP status, multiple specializations, and dedicated expertise in cybersecurity solutions, Infopulse had the exact practical experience required by our client to implement such a project. Besides, Infopulse has previously implemented Microsoft Sentinel as an important part of Infopulse's own defense perimeter after conducting extensive testing and considering all its benefits.

To demonstrate the Security monitoring and detection capabilities of Microsoft Sentinel to our client, it was necessary to:

- Assess the capabilities of Microsoft Sentinel as a holistic SIEM/SOAR system
- Reconfigure the current Microsoft Sentinel setup with maximum efficiency
- Automate routine processes, such as incident reporting and investigation, utilizing the model powered by machine learning
- Centralize signals from multiple enterprise systems under a single console
- Ensure Microsoft Sentinel integration with an ITSM (IT Service Management) system, business applications, etc.

Solution

After assessing the existing IT perimeter, Infopulse experts conducted a preliminary analysis and proposed the architecture of the new modern SIEM/SOAR solution. Upon confirming our proposition with the client, we developed the high-level architecture and implementation strategy of the solution.

To validate the Microsoft Sentinel capabilities, Infopulse created and executed four SIEM/SOAR test cases:

1. **Identifying potentially compromised accounts:**

- Set up an analytical rule to identify cases of successful logins from IP addresses that tried to exploit blocked or disabled user accounts.
- Verified incident alerts according to the configured rule with a test scenario.

2. **Identifying corporate data leakage via emails:**

- Set up an automated rule for Microsoft Sentinel to detect users forwarding multiple emails to the same external SMTP address.
- Developed an algorithm for scenario testing.

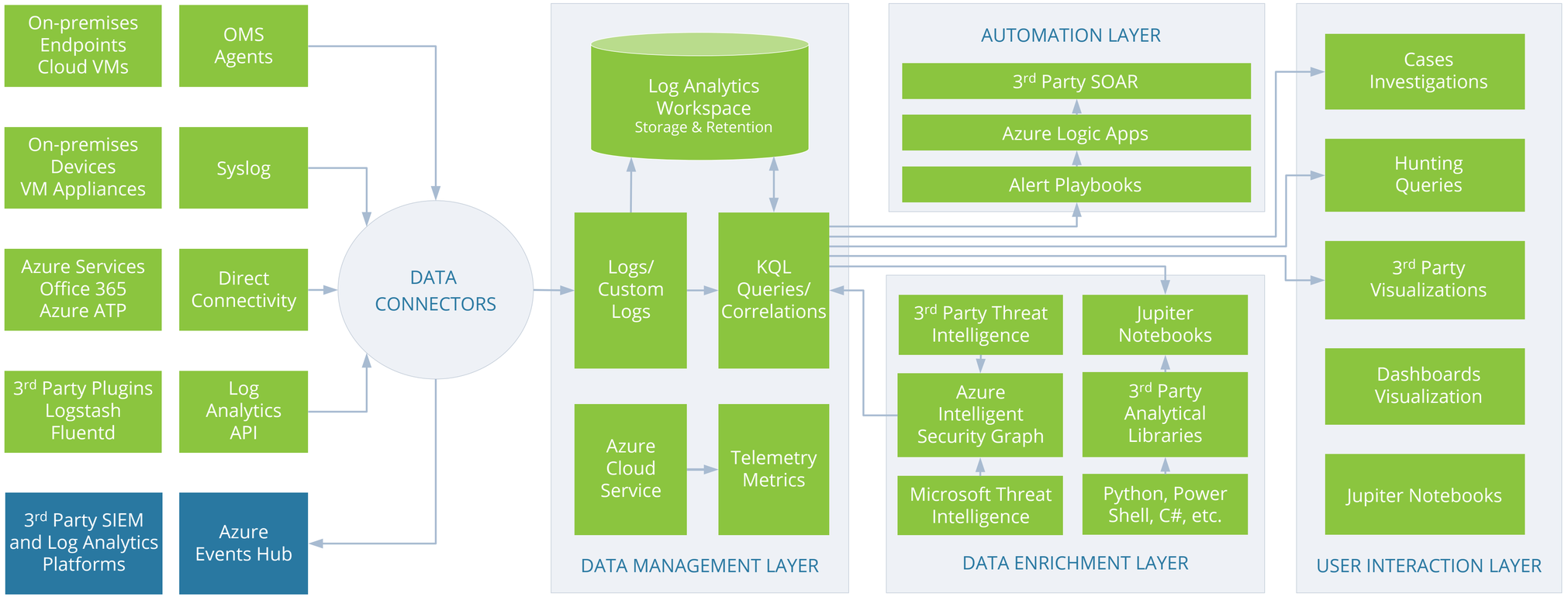
3. **Detecting potential threats while using Microsoft Teams:**

- Infopulse experts configured a set of analytical rules to monitor suspicious activity within the app, such as adding external users from anomalous organizations to a team or deleting multiple teams by a single user.
- Set up extensive data parsing and log collection via Logic Apps and Office 365 Management Activity API.
- Utilized interactive charts to visualize Microsoft Teams users' interaction with external users.

4. **Rejecting potentially harmful files when they are uploaded to the corporate cloud storage:**

- Configured an analytical rule to detect the uploading of potentially harmful executable files to common folders in SharePoint and OneDrive.
- Developed an algorithm for scenario testing.
- Confirmed successful rule execution with a simulated cyber threat.

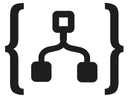
SIEM/SOAR Microsoft Sentinel for a Major Agricultural Company — architecture



Technologies

Microsoft Sentinel

Power BI



Logic Apps

Microsoft Teams

Microsoft Defender 365

Office 365 Management Activity API

Business Value

Since Microsoft Sentinel was working in parallel with the existing system, we could show its drastic advantages over the legacy solution used by the client. Test scenarios performed by Infopulse demonstrated the advantages and capabilities of Sentinel as a cloud-native (SaaS) security system with process automation functionality. Upon successful execution of the test scenarios, Infopulse security professionals provided our client with extensive recommendations on the further development of the cybersecurity system based on Microsoft Sentinel according to the current and future business demands.

Infopulse validated Microsoft Sentinel capabilities for our client with the following tangible benefits:

- Automated cybersecurity rules for selected test cases, minimizing the human factor and resulting in a faster and higher quality of IT security operations.
- Seamless integration of Microsoft Sentinel with Exchange, SharePoint, Teams, and other solutions, such as Microsoft Threat Protection and firewalls, ensuring better integrity and reducing IT security risks.
- Automated report generation via Microsoft Sentinel and Power BI provides better visibility into IT security operations and faster decision-making for potential critical incidents.
- A roadmap for further implementation of Microsoft Sentinel with extended integration into the company's IT infrastructure to reduce IT security risks and strengthen customer trust.
- Reduced licensing costs for Microsoft Sentinel as a single SIEM & SOAR system, improving overall financial footprint.
- A series of Q&A and learning sessions for the company's security experts, building a foundation for dedicated IT security staff readiness.

Satisfied with the results of the test cases performed by Infopulse and the numerous benefits brought by Microsoft Sentinel in comparison to their legacy system, the client of Infopulse now plans on the further implementation of Microsoft Sentinel.

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.

A long-term Microsoft partner with Azure Expert MSP status and reliable provider of cybersecurity services & solutions, Infopulse is trusted by many established brands, such as Allianz Bank, BICS, Bosch, British American Tobacco, Credit Agricole, Delta Wilmar, ING Bank, Microsoft, Offshore Norge, OLX, OTP Bank, Santander, SAP, UkrSibbank BNP Paribas Group, Vodafone, Zeppelin, 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

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