infopulse
Part of TietoEVRY Group

MAJOR AGRICULTURAL COMPANY

CASE STUDY

Assessing Azure Sentinel Capabilities for a Major Agricultural Company

Leveraging cybersecurity automation to test the cloud-native security system

Client: European leader in agriculture | **Industry:** Agriculture | **Employees:** 14,000+ employees | **Location:** Ukraine

CLIENT BACKGROUND

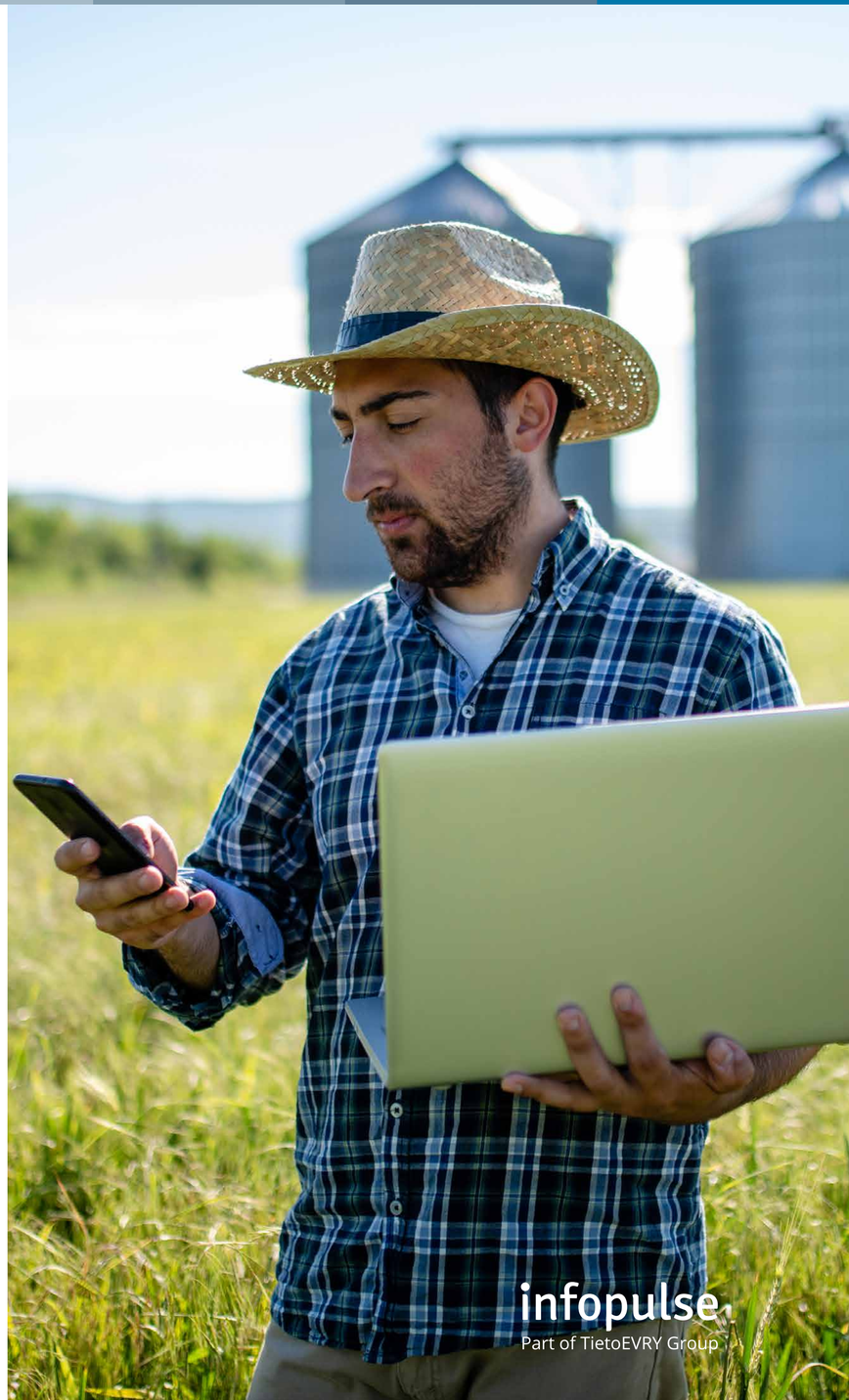
Our client is one of the leaders in the European agricultural sector. They have a diverse network of fields, processing, and storage premises that enable the continuous supply of high-quality produce to 80 countries worldwide.

BUSINESS CHALLENGE

As part of the global digitization strategy, our client aimed to enhance the already existing cybersecurity landscape. The company was looking for a service provider to assist with the deployment of a SIEM/SOAR system based on Azure Sentinel and to leverage the business value of the solution.

To demonstrate the performance potential of Azure Sentinel to our client, it was necessary to:

- Assess the capabilities of Azure Sentinel as a holistic SIEM/SOAR system
- Reconfigure the current Azure 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 Azure Sentinel integration with an ITSM system, business applications, etc.



SOLUTION

After assessing the existing IT perimeter, our experts developed the high-level architecture and implementation strategy of the solution. To validate the Azure Sentinel capabilities, Infopulse created and executed four SIEM/SOAR test cases:

1 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.

2 IDENTIFYING CORPORATE DATA LEAKAGE VIA EMAILS:

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

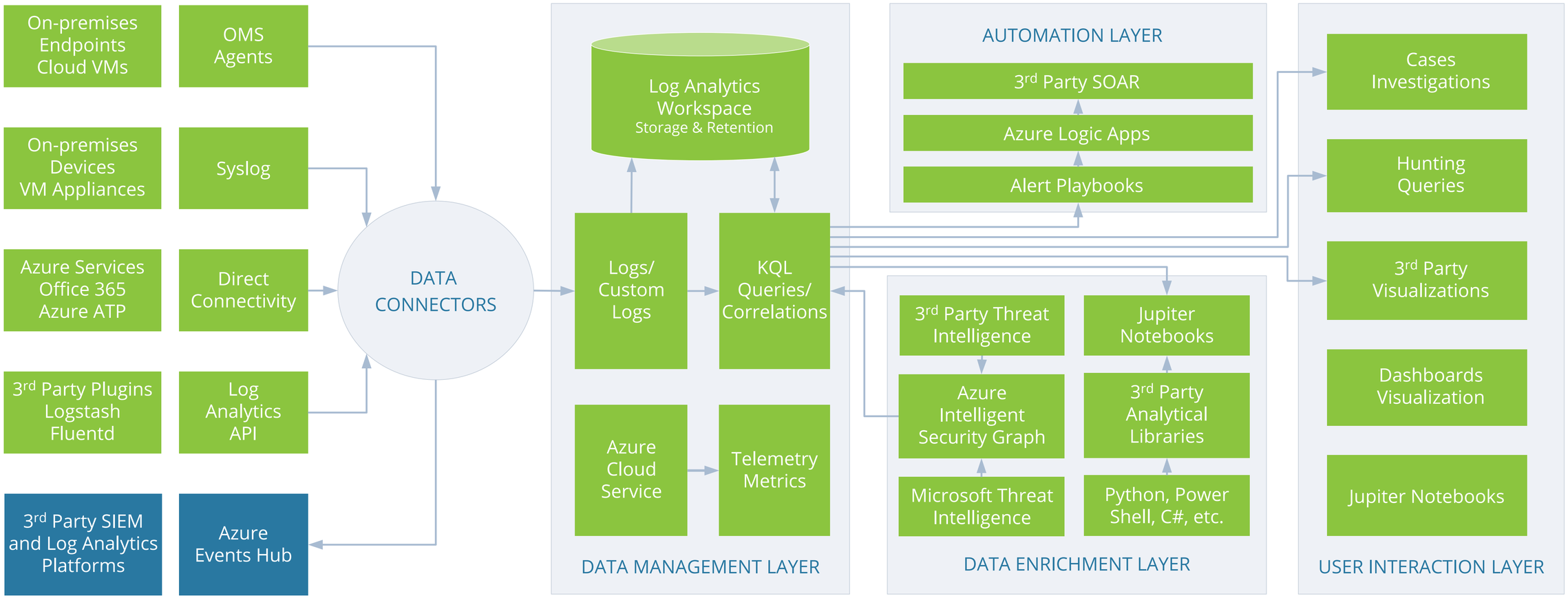
3 REJECTING POTENTIALLY HARMFUL FILES WHEN THEY ARE UPLOADED TO THE CORPORATE CLOUD STORAGE:

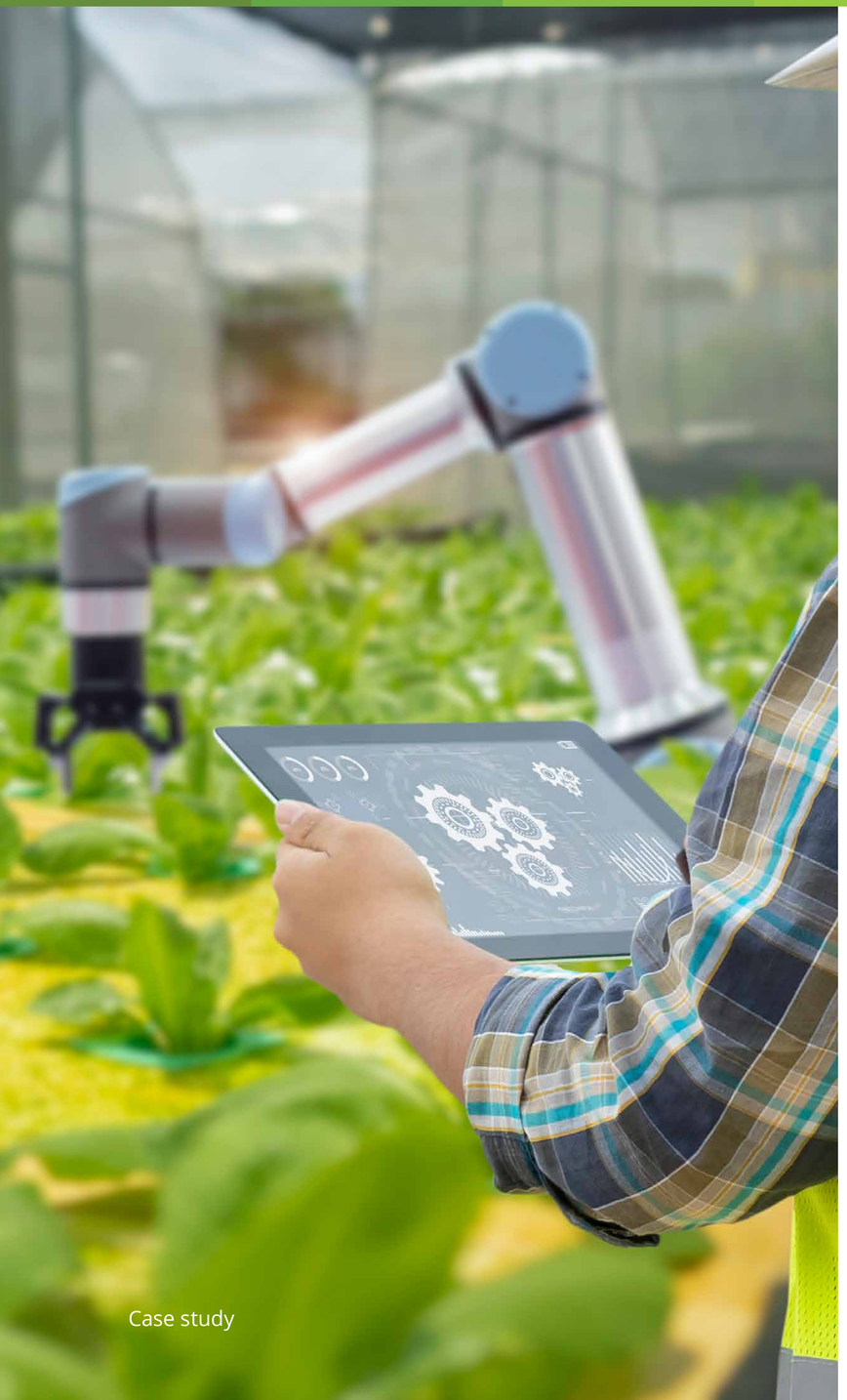
- Configured an analytical rule to detect the uploading of potentially harmful executable files to common folders in SharePoint and OneDrive.
- Developed an algorithm for scenario testing.
- Confirmed successful rule execution with a simulated cyber threat.

4 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.

SIEM/SOAR AZURE SENTINEL FOR A MAJOR AGRICULTURAL COMPANY - ARCHITECTURE





Case study

TECHNOLOGIES:

Azure Sentinel | Power BI | Logic Apps | Microsoft Teams | Microsoft Defender 365 | Office 365 Management Activity API

BUSINESS VALUE

Test scenarios demonstrated the advantages and capabilities of Azure Sentinel as a cloud-native (SaaS) security system with a process automation functionality. Upon their successful execution, Infopulse provided our client with extensive recommendations on the further development of the cybersecurity system based on Azure Sentinel according to the current and future business demands.

VALIDATING AZURE SENTINEL CAPABILITIES PROVIDED OUR CLIENT WITH THE FOLLOWING TANGIBLE BENEFITS:

- Automated cybersecurity rules for the selected test cases that allow minimizing the human factor.
- Successful integration of Azure Sentinel with Exchange, SharePoint, Teams, and other solutions such as Microsoft Threat Protection and firewalls.
- Automated report generation via Azure Sentinel and Power BI.
- The roadmap for the further implementation of Azure Sentinel with extended integration into the company's IT infrastructure.
- Estimated the reduced license costs for Azure Sentinel as a single SIEM & SOAR system.
- A series of Q&A and learning sessions for the company's security experts.

Satisfied with the results of the test cases, the Infopulse client now plans on the further implementation of Azure 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 2,000 professionals and is represented in 7 countries across Europe and North and Latin America. Infopulse is trusted by many established brands, such as BICS, Bosch, British American Tobacco, Citrix, Credit Agricole, ING Bank, Gorenje, METRO Cash & Carry, Microsoft, Mondelēz, OTP Bank, Raiffeisen Bank Aval, SAP, UkrSibbank BNP Paribas Group, VEON, Vodafone, and others.

For more information, please visit

www.infopulse.com

CONTACT US

UA: +38 (044) 585-25-00
US: +1 (888) 339-75-56
FR: +33 (172) 77-04-80
BG: +359 (876) 92-30-90
DE: +49 (3222) 109-52-35
UK: +44 (8455) 280-080
PL: +48 (663) 248-737
BR: +55 (21) 99298-3389

info@infopulse.com

FOLLOW US