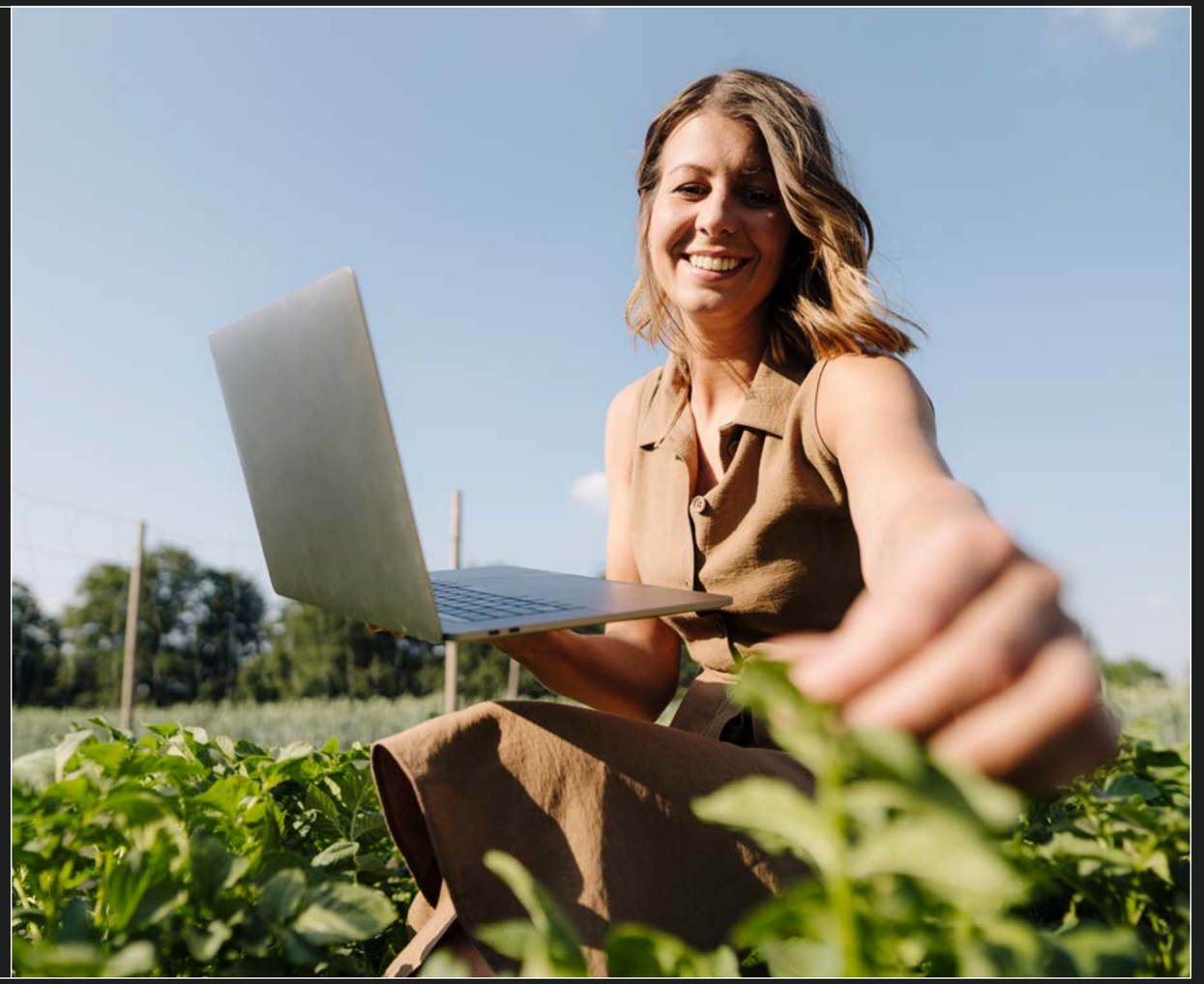
infopulse

Fallbeispiel für **ein Landwirtschaftliches Unternehmen**

Bewertung der Microsoft Sentinel Fähigkeiten für ein großes landwirtschaftliches Unternehmen_

Nutzung der Cybersecurity-Automatisierung zum Testen des Cloud-nativen Sicherheitssystems

Branche: **Landwirtschaft** **Ort:** **Ukraine** **Mitarbeiter:** **14,000+**



Über den Kunden

Unser Kunde ist eines der führenden Unternehmen im europäischen Agrarsektor. Sie verfügen über ein weit verzweigtes Netz von Anbauflächen, Verarbeitungs- und Lagerstätten, welches die kontinuierliche Lieferung von Qualitätsprodukten in 80 Länder weltweit ermöglicht.

Anforderung

Als Teil der globalen Digitalisierungsstrategie wollte unser Kunde die bereits bestehende Cybersicherheitslandschaft verbessern. Der Kunde suchte einen Dienstleister, der ihn bei der Einführung eines SIEM/SOAR-Systems auf der Basis von Microsoft Sentinel unterstützt und den geschäftlichen Nutzen der Lösung ausschöpft. Um unserem Kunden das Leistungspotenzial von Microsoft Sentinel zu demonstrieren, war es notwendig:

- die Fähigkeiten von Microsoft Sentinel als ganzheitliches SIEM/SOAR-System zu bewerten
- das aktuelle Microsoft Sentinel-Setup mit maximaler Effizienz zu rekonfigurieren
- Routineprozesse, wie z. B. die Meldung und Untersuchung von Vorfällen, mit Hilfe des auf maschinellem Lernen basierenden Modells zu automatisieren
- Signale von mehreren Unternehmenssystemen unter einer einzigen Konsole zu zentralisieren
- die Integration von Microsoft Sentinel mit einem ITSM-System, Geschäftsanwendungen usw. sicherzustellen

Lösung

Nach der Bewertung der bestehenden IT-Umgebung entwickelten unsere Experten die High-Level-Architektur und die Implementierungsstrategie der Lösung. Zur Validierung der Microsoft Sentinel-Funktionen entwarf Infopulse vier SIEM/SOAR-Testfälle und führte sie aus:

Erkennung potenzieller Bedrohungen bei der Verwendung von Microsoft Teams:

- Die Experten von Infopulse konfigurierten eine Reihe von Analyseregeln, um verdächtige Aktivitäten innerhalb der App zu überwachen, z. B. das Hinzufügen von externen Benutzern aus anomalen Organisationen zu einem Team oder das Löschen mehrerer Teams durch einen einzelnen Benutzer.
- Sie richten eine umfangreiche Datenanalyse und Protokollerfassung über Logic Apps und Office 365 Management Activity API ein.
- Und nutzten interaktive Diagramme, um die Interaktion von Microsoft Teams-Benutzern mit externen Benutzern zu visualisieren.

Identifizierung von Datenlecks in Unternehmen via E-Mails:

- Sie richteten eine automatische Regel für Microsoft Sentinel ein, um Benutzer zu erkennen, die mehrere E-Mails an dieselbe externe SMTP-Adresse weiterleiten.
- Und entwickelten einen Algorithmus für Szenariotests.

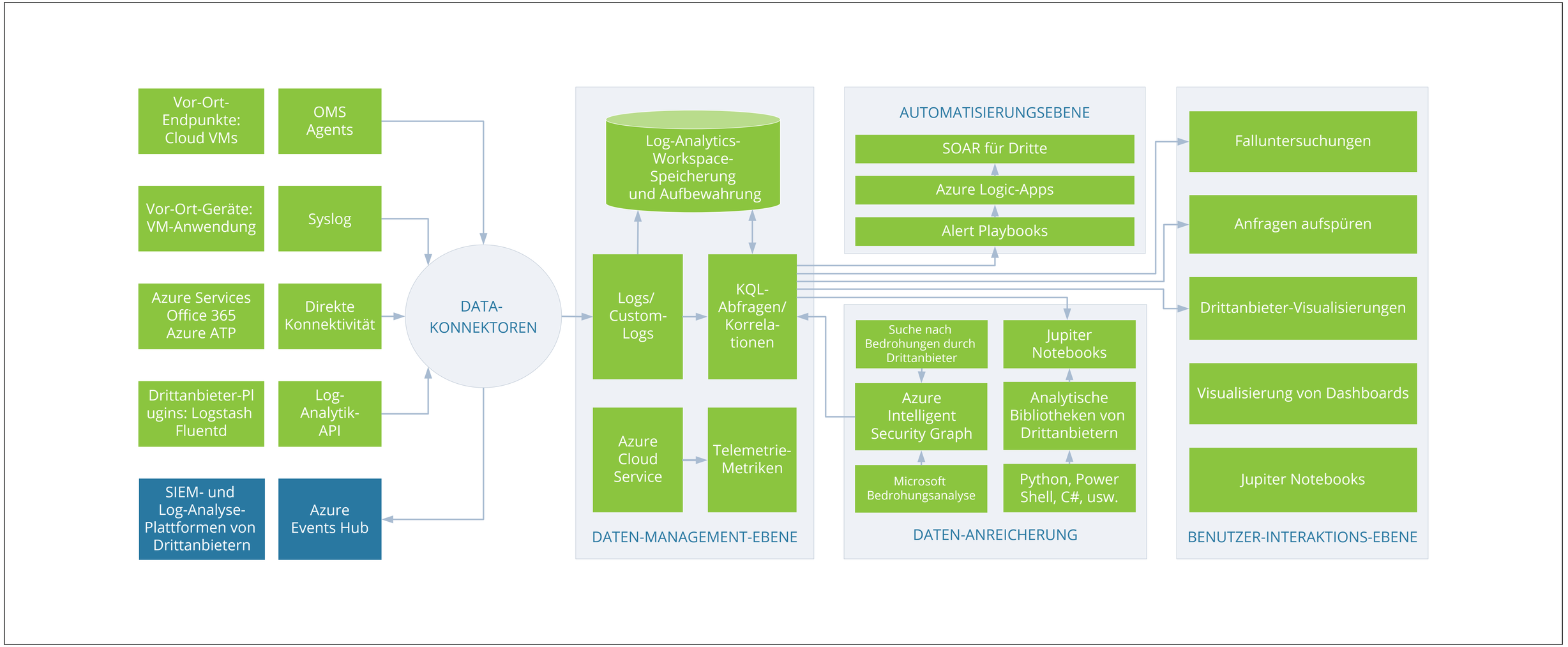
Ablehnung potenziell schädlicher Dateien, wenn sie in den Cloud-Speicher des Unternehmens hochgeladen werden:

- Sie konfigurierten eine Analyseregel, um das Hochladen potenziell schädlicher ausführbarer Dateien in gemeinsame Ordner in SharePoint und OneDrive zu erkennen.
- Und entwickelten einen Algorithmus für Szenariotests.
- Sie bestätigten die erfolgreiche Ausführung einer Regel mit einer simulierten Cyber-Bedrohung.

Identifizierung potenziell gefährdeter Konten:

- Sie richteten eine Analyseregel ein, um Fälle erfolgreicher Anmeldungen von IP-Adressen zu identifizieren, die versuchten, gesperrte oder deaktivierte Benutzerkonten auszunutzen.
- Und verifizierten Ereigniswarnungen gemäß der konfigurierten Regel mit einem Testszenario.

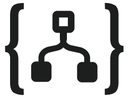
SIEM/SOAR Microsoft Sentinel für ein großes Landwirtschaftsunternehmen — Architektur



Technologien

Microsoft Sentinel

Power BI



Logic Apps

Microsoft Teams

Microsoft Defender 365

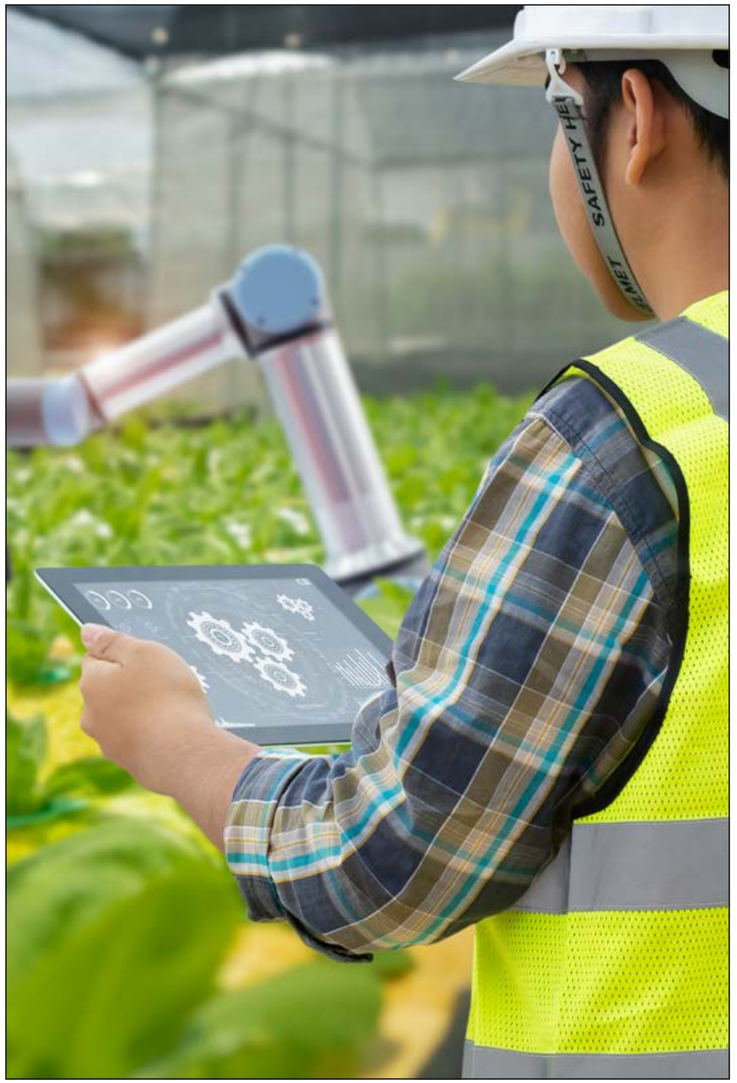
Office 365 Management Activity API

Ergebnis

Die Testszenarien demonstrierten die Vorteile und Fähigkeiten von Microsoft Sentinel als Cloud-natives (SaaS) Sicherheitssystem mit einer Prozessautomatisierungsfunktion. Nach der erfolgreichen Durchführung gab Infopulse unserem Kunden umfangreiche Empfehlungen zur Weiterentwicklung des auf Microsoft Sentinel basierenden Cybersecurity-Systems entsprechend den aktuellen und zukünftigen Geschäftsanforderungen.

Die Validierung der Microsoft Sentinel-Funktionen brachte unserem Kunden die folgenden greifbaren Vorteile:

- Automatisierte Cybersicherheitsregeln für die ausgewählten Testfälle, die es ermöglichen, den Faktor Mensch zu minimieren.
- Erfolgreiche Integration von Microsoft Sentinel mit Exchange, SharePoint, Teams und anderen Lösungen wie Microsoft Threat Protection und Firewalls.
- Automatisierte Berichterstellung über Microsoft Sentinel und Power BI.
- Die Roadmap für die weitere Implementierung von Microsoft Sentinel mit erweiterter Integration in die IT-Infrastruktur des Unternehmens.
- Schätzung der reduzierten Lizenzkosten für Microsoft Sentinel als einzelnes SIEM- und SOAR-System.
- Eine Reihe von Q&A- und Lernsitzungen für die Sicherheitsexperten des Unternehmens.
- Zufrieden mit den Ergebnissen der Testfälle, plant der Infopulse-Kunde nun die weitere Implementierung von Microsoft Sentinel.



Über Infopulse

Infopulse, Teil des führenden nordischen digitalen Dienstleistungs- unternehmens TietoEVRY, ist ein internationaler Anbieter von Dienstleistungen in den Bereichen Software-F&E, Anwendungsmanagement, Cloud- und IT-Betrieb sowie Cybersicherheit für KMUs und Fortune 100 Unternehmen auf der ganzen Welt.

Das 1991 gegründete Unternehmen verfügt über ein Team von über 2.000 Fachleuten und ist weltweit in 7 Ländern vertreten.

Infopulse ist ein von der IAOP® anerkanntes Global Outsourcing 100® — Unternehmen und genießt das Vertrauen vieler etablierter Marken wie BICS, Bosch, Credit Agricole, FNT, ING Bank, Gorenje, METRO Cash & Carry, Microsoft, OTP Bank, Raiffeisen Bank Aval, UkrSibbank BNP Paribas Group, VEON, Vodafone, Zeppelin Group und vieler anderer. Für weitere Informationen, besuchen Sie bitte www.infopulse.com/de

Kontaktieren Sie Uns:

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