infopulse
Part of Tietoevry Create

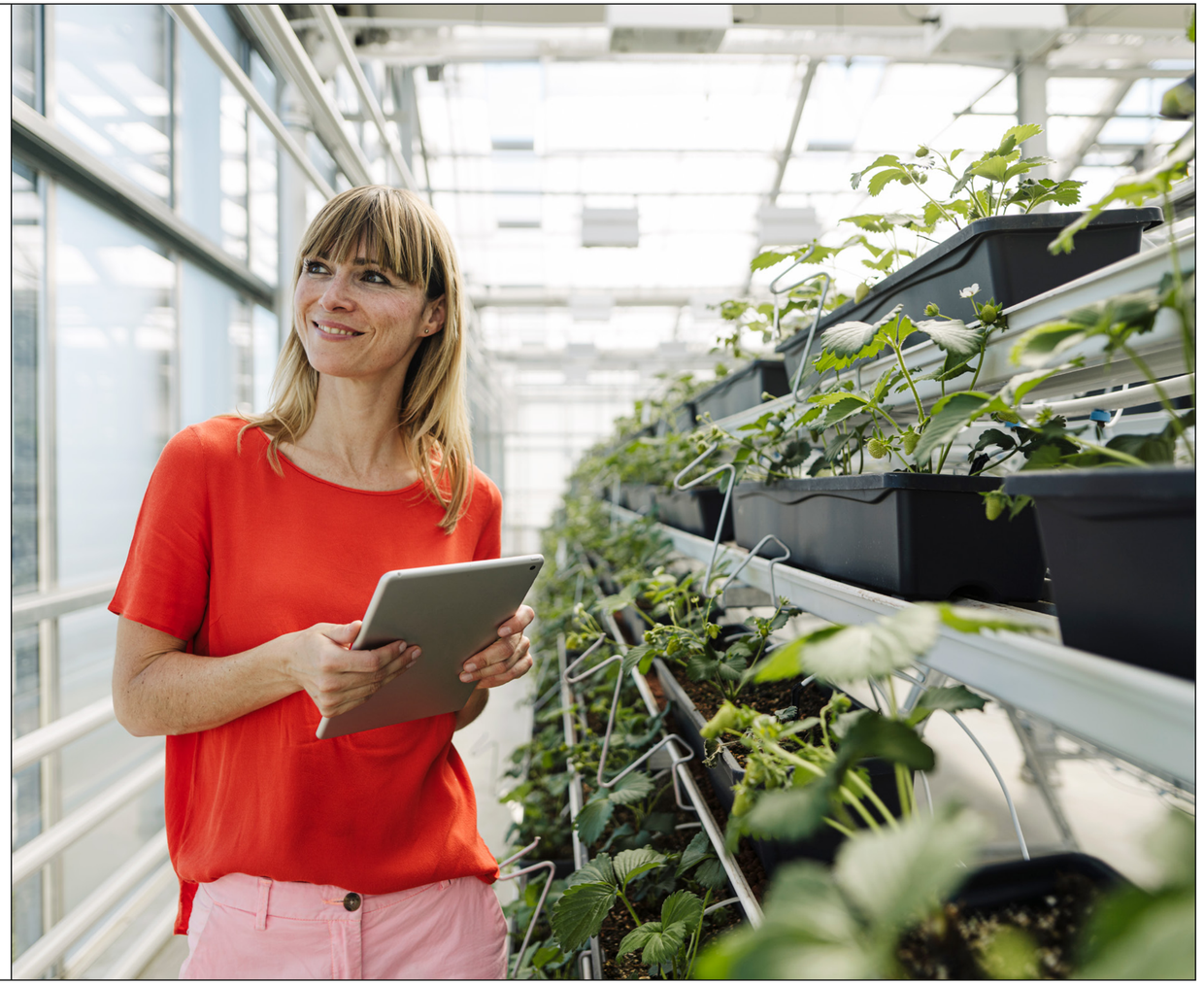
GOODVALLEY
Since 1994

Proactive Security with a SOC and Cloud SIEM for Goodvalley_

A SOC to Proactively Secure Hybrid Infrastructure of
a Multi-National Agri-Food Producer

Industry: **Agriculture & Food** **Location:** **Denmark, Poland, Ukraine**

Employees: **1,700+**



Client Background

Website:
https: www.goodvalley.com

Goodvalley is an international agrifood producer committed to responsible farming practices and delivering high-quality pork products. The company's approach entails complete quality control over the production process from field-to-fork. Goodvalley's production network includes a total of 37 farms in Poland and Ukraine, 33,500 hectares of arable land and 9 biogas plants closing the production cycle, and contributing to the reduction of emissions and impact on the climate. Goodvalley's business is highly reliant on IT systems to run and control operations; thus, stability and security are crucial for preventing business interruptions and financial risks.

Executive Summary_

Goals

Deploy a SOC with an efficient SIEM system to monitor data security threats within the entire IT infrastructure. Develop and maintain an efficient cyber security strategy and deliver multi-level support for security monitoring and incident management.

Solution

Infopulse security engineers built a managed SOC based on Microsoft Sentinel and ensured dedicated security maintenance, covering the client's entire IT infrastructure across multiple locations including the cloud.

Benefits

Enhanced cyber security, proactive security risk management, comprehensive protection of the entire IT infrastructure, including cloud resources, automation of processing recurring issues, reduced costs for security operations, and continuous improvement of security systems to stay ahead of evolving threats.

Services delivered

Cybersecurity, Security Operations Center (SOC), SIEM & SOAR, Security Assessment, Microsoft Sentinel

Business Challenge_

Goodvalley started exploring options for SOC adoption back in 2021. By late 2023, Goodvalley sought to find a reliable security provider who would help them achieve the following:

- Implement SOC with SIEM solution to cover the entire hybrid IT infrastructure
- Enable efficient cyber security monitoring
- Automate security incident processing
- Ensure dedicated data security support and maintenance

The following aspects were of greater importance for the company:

- Suitability of the proposed technologies and toolset
- Overall project cost
- Our abilities for strategic approach and proactive position in implementing security enhancements.

Goodvalley selected Infopulse as a trusted security partner with industry-specific experience and a deep understanding of the company's infrastructure specifics. We suggested a solution based on Microsoft Defender that met the unique client's needs, perfectly fitting their current security ecosystem.

Solution & Business Value_

Infopulse implemented a powerful managed SOC solution based on Microsoft Sentinel, connecting IT the infrastructure components of Goodvalley to SIEM for continuous security monitoring.

Along with multi-layered security maintenance and support, our client could benefit from:

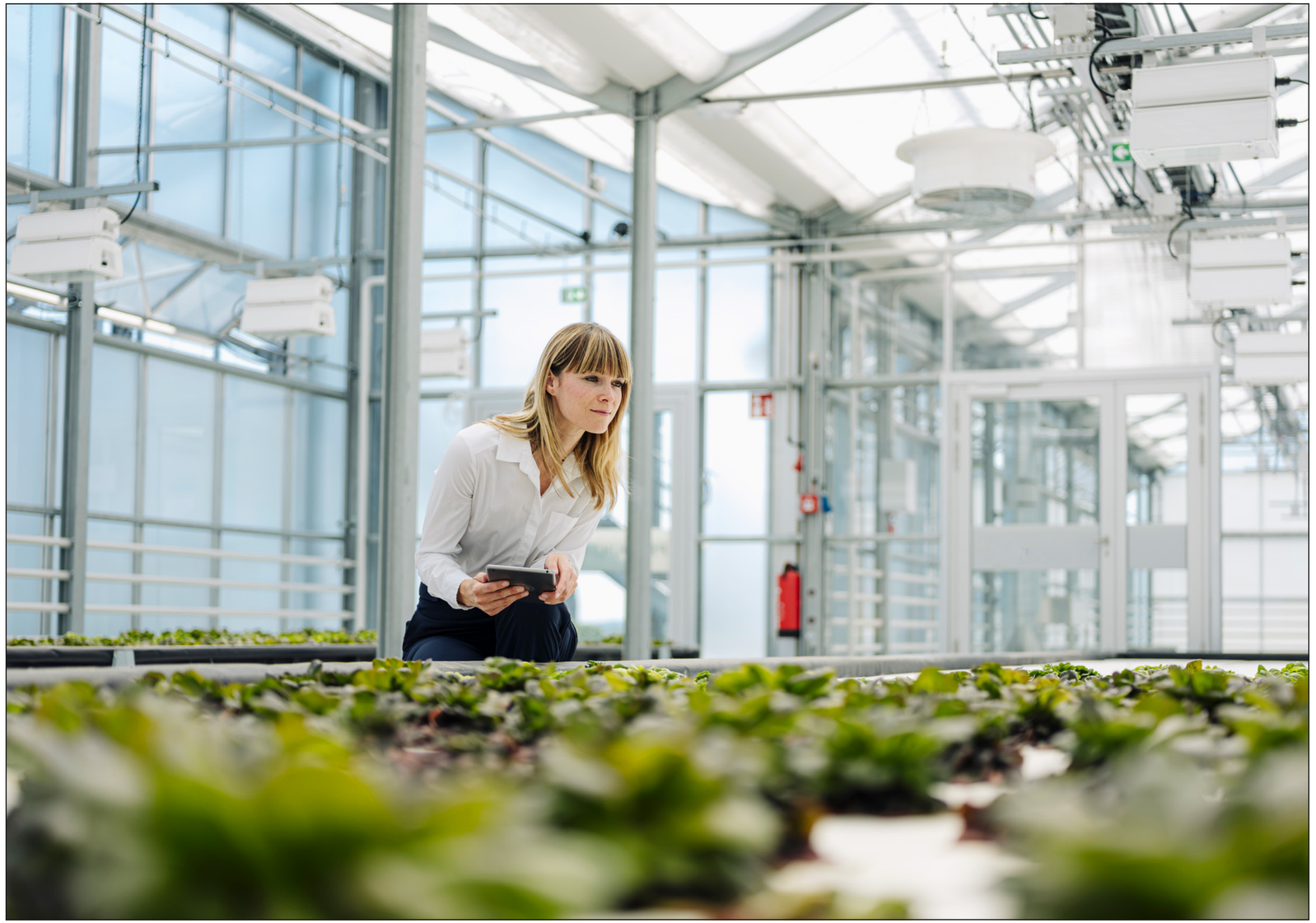
- Significantly enhanced risk management and cybersecurity stability
- Continuous strategic enhancements for the company's cybersecurity posture
- Proactive approach to cyber security incident processing
- Reduced costs for IT infrastructure and security operations

The joint effort of Infopulse security engineers and Goodvalley's IT department helped the agrifood enterprise achieve a stabley high level of cybersecurity efficiency and avoid critical security incidents.

Technical Details

Upon conducting an in-depth research of the client's needs, Infopulse suggested deploying **Microsoft Sentinel** – a strategic choice, as Goodvalley's IT infrastructure mainly relies on the Microsoft ecosystem.

We initiated a pilot project to demonstrate the capabilities of Microsoft Sentinel so that the client could see all the advantages of the proposed solution in action. For the pilot project, our partner Microsoft provided all the necessary licenses for free, so that Goodvalley could verify the viability of the solution without any expenses.



After the successful pilot, we implemented the full-scale project, with its scope comprising the following:

1. **Conducted SIEM system integration** by connecting all on-premises and cloud resources. Based on the results of the pilot project, we calculated the required budget and proposed specific network optimizations to offer competitive pricing.
2. We **deployed Microsoft Sentinel solution and enabled cloud services**, such as Azure, Microsoft 365, various SaaS tools, etc. Next, we connected the Cortex XDR and Fortinet firewalls, as well as the rest of the infrastructure to SOC.
3. **Set up analytical rules** to detect security incidents and enable suitable processing mechanisms. It allowed to filter real incidents from all the received system alerts and mitigate them correctly, ensuring efficient SOC performance.
4. SIEM monitoring revealed improper network settings; thus, we provided **recommendations for network optimization** that allowed Goodvalley to decrease infrastructure workloads and, therefore, save resources and costs.
5. **Reduced excessive data logs.** To reduce data volumes with no practical value for security, we filtered unnecessary data and aggregated data from all analyzed sources. This allowed us to significantly decrease the amount of data stored in the cloud without affecting its informative value.

The initial setup and deployment of the SOC took appr. 3 months. During this phase, we started implementing security and IT infrastructure improvements as soon as we received the first monitoring logs. We proactively identified and addressed potential weaknesses and ensured a seamless transition from the previous solution with zero interruptions.

After the initial implementation phase, our dedicated SOC team started providing comprehensive “Security-as-a-Service” multi-layer maintenance and support:

- **Layer 0** includes automatic incident processing to mitigate recurrent low-impact security use cases.
- **Layer 1:** Initial alert analysis performed by previously created playbooks. The service is delivered by a team of security specialists located in Ukraine and the EU.
- **Layer 2 / 3:** Processing non-typical and complex incidents. It is performed by two dedicated specialists. After processing each such incident, they create instructions for L1 specialists to process similar alerts in the future if such alerts appear.
- **Forensic scan:** A detailed investigation and documentation of complicated incidents with the highest level of potential impact. Fortunately, the client had no such security incidents during our collaboration.

We also integrated the SOC alert system with the client’s internal ticketing system, giving their IT specialists full visibility and ease in managing security tasks.

The project is ongoing, with weekly meetings to update Goodvalley on SOC performance, suggest improvements, and discuss all other data security aspects.

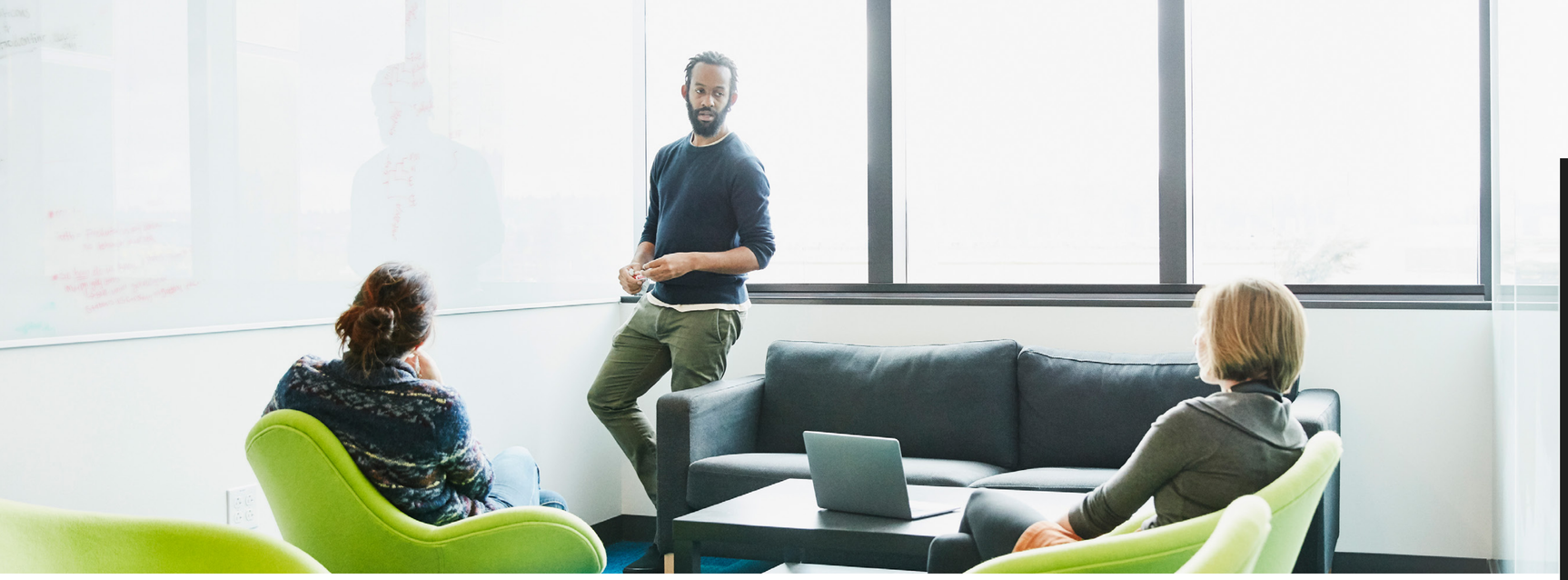
Technologies & Tools_

Microsoft Azure

Microsoft Sentinel

Cortex XDR

Fortinet Firewall



About Infopulse

Infopulse, part of the leading Nordic digital services company Tietoevry Create, is an international vendor of services in the areas of cybersecurity, IT infrastructure protection, SIEM/SOAR, and SOC solution deployment. Our services cover all the cybersecurity needs of modern businesses, considering industry-specific requirements to gain operational resilience and robust protection against cyber threats. Infopulse is trusted by many established brands, such as Corteva Agriscience, Delta Wilmar, EarthDaily Agro, Goodvalley, Kernel, MHP, RAGT Semences Ukraine, Zeppelin, BICS, Bosch, LMT, Microsoft, Metinvest, Offshore Norge, OLX, SAP, 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