Deloitte.

Microsoft Defender for IoT monitoring at Global Industrial Company

Deloitte implemented OT / IoT device inventory, automated discovery, registration and monitoring with Microsoft Defender for IoT, and recommended standardised cybersecurity processes at an industrial company facing limited asset visibility and weak cybersecurity controls. This strengthened asset security, improved global oversight, and established a resilient operational technology environment that reduces the risk of cyberattacks and production disruptions.

The Challenges

The client had limited overview onsite of existing assets, with no standardised processes in place.

Sites did not adhere to cybersecurity standards, exposing the client network and production processes to potential cyberattacks.

This lack of visibility and control over assets increased the risk of vulnerabilities and compromised the integrity of the operational technology environment, potentially leading to significant disruptions and security breaches.

The Solution

Deloitte recommended multiple controls, including network segregation where required and defined remediation actions.

Deloitte established monitoring with the client's selected technology platform, Microsoft Defender for IoT, and recommended extending the coverage of existing monitoring tools.

In addition, we paved the way for future standard processes by recommending cybersecurity standards.

By creating unprecedented visibility and understanding of the sites, we enabled quicker response times to vulnerabilities and incidents. This enhances detection and ensures continuous protection of the OT environment, enabling proactive management of cybersecurity threats.

The Impact

Previously exposed assets and networks are now more secure.

The global inventory facilitates better management and oversight of assets, representing an initial step towards a standardised and secure OT environment on a global scale.

Enhanced visibility and control over assets has improved the cybersecurity posture, reducing the risk of cyberattacks and ensuring the resilience of production processes.

This initiative lays the foundation for a robust and secure operational technology framework across all sites.

For more information, please contact:

Guy-Florian Seka
gfseka@deloitte.ch

Klaus Julisch
kjulisch@deloitte.ch