SmartIS
PAMETNI INFORMACIJSKI SISTEMI

www.smartis.si
info@smartis.si

IoT and Operational Technology (OT) Assets discovery and visibility

Azure Defender for IoT help businesses auto-discover Internet of Things and operational technology (OT) assets, identify critical vulnerabilities, and detect anomalous activity with behavioral analytics and machine learning.

Why do we need OT Cybersecurity?

For many years, industrial systems (OT) had no connection to the outside world that why they did not deal with the same kinds of vulnerabilities. Today, IT/OT convergence is a cornerstone and an enabler for Industry 4.0. and IoT. Due to the standardisation of communication protocols and growing interconnectivity have drastically increased the cyber-attacks on OT system over the years.

Why customers choose SmartIS?

- Experienced Cyber Security Team
- References in OT Security
- Experience in IoT software development projects
- Stream computing and Big Data expertize

SOLUTION

Azure Defender for IoT incorporates agentless technology from Microsoft's acquisition of CyberX, an IoT/OT security firm it bought in June 2020 as part of a broader strategy to expand the scope of its Azure IoT cloud-based security monitoring to include industrial network devices.

Visibility Continuous and real-time

- all installed OT assets and there mapping
- displays device details
- visual representation attack vector chains

Zero (0) impact on production

- zero impact due to its passive Network Traffic Analysis (NTA) approach.
- uses agent-less technology
- non-invasive technology

Heterogeneous and vendor-agnostic

- IoT and OT vendor-agnostic architecture supports all industrial automation protocols and equipment
- integrating with existing SOC workflows and security tools

> CyberX solution gave us centralized view of OT risk with real-time protection.
>
> Alenka Kolar, CIO, Elektro Ljubljana