# Cyber Security Requirements in OT & IoT Environments

| Criteria | | Benefits |
|---|---|---|
| **Asset inventory and visibility of the entire OT infrastructure** | | |
| | Detection of all assets (IT-, IoT- and OT-based devices) in the OT network without affecting operation | → Technology and process consolidation<br>→ Joint monitoring<br>→ Elimination of departmental silos<br>→ Increase responsibility and minimise costs<br>→ Merging IT and OT<br>→ Optimised asset management<br>**Nozomi users recognise the customer benefit within minutes of minutes after implementation.** The rapid asset detection and network visualisation increase the awareness of security operations teams. |
| | Comprehensive support of IT, IoT and OT protocols | |
| | Interactive automatically created asset inventory with assets, communication relations and protocols | |
| | Identification of new devices (device type, firmware version, etc.) | |
| | Monitoring of all remote control accesses | |
| | Optional: active query options without effects on the operation, for Windows, Unix hosts or network devices | |
| **Protection of IoT/OT configurations** | | |
| | Identification of changes to Programmable Logic Controllers (PLC) or Human Machine Interfaces - PLC programme Code, firmware, configuration changes | → Complete log of ICS activities |
| | Monitoring and analysis for IoT and OT<br>Process variables | |
| **Vulnerability analysis and risk management** | | |
| | Identification of specific IT, IoT and OT vulnerabilities | → Enhanced insights for risk management without having to build up additional resources<br>→ Workflow for the **rapid detection of anomalies** for the existing Security Operations Team<br>→ The integrated Cyber Threat Detection combines behavioural anomaly detection, signature-based threat detection and asset intelligence for comprehensive risk monitoring |
| | Detection of anomalies and manipulation in network traffic | |
| **Advanced Cyber Threat Detection - threat detection incl. alerting** | | |
| | Use of the continuously updated safety databases | → Rapid detection of cyber-attacks and proactive mitigation<br>→ Increases robustness against cyber attacks<br>→ Active block function in combination with a firewall system<br>→ **Instant protection against ransomware** |
| | Proactive vulnerability and risk detection and identification of MITRE Attack vectors | |
| | Real-time alerts on suspicious activities and threats in OT networks (e.g., malware detection) | |



Blechturmgasse 11 | A-1050 Wien | Phone: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com

| | | |
|---|---|---|
| **Audit and compliance** | | |
| | Non-modifiable audit logs | → Compliance with national and operational requirements for cyber security |
| | Fully comprehensive time machine (snapshot-function) incl. version comparison check | |
| | Support for the implementation of international standards such as EC 62443, CIS Critical Security Controls, ISO 2700 series incl. 27001, MITRE ICS Attack Framework | |
| | Monitoring via surveillance of zones and conduits according to IEC 62443 | |
| | Supporting the implementation of the NIS(2) Regulation | |
| **Integration into the enterprise architecture and support of security operations teams** | | |
| | Instant integration with leading security partners, Active Directory, SIEM, Syslog, REST API, Data Exports | → Actionable alerts, dashboards and reports that accelerate security response and significantly improve OT and IoT risk management |
| | Customisable analyses and reports | → **Seamless integration with SOC/IT tools** and workflows, including automated **response to block attacks** when integrated with compatible firewalls and endpoint security products |
| | Scalable solution models for on-premises requirements | → **Global scalability** to protect thousands of locations |
| | Scalable solution models for SaaS requirements | → Deployment flexibility with physical, virtual container and portable on-premises appliances, as well as SaaS-powered and cloud deployments |

Your advantages with **Nozomi Networks MSSP and Platinum Partner IKARUS Security Software:**

Our interdisciplinary team of experts with IT, OT and IoT security expertise enables easy commissioning and results within minutes. We provide knowledge transfer and customised support to help you build your IT/IoT/OT security operations team.

https://www.IKARUSsecurity.com/en/industrial-cyber-security



Blechturmgasse 11 | A-1050 Wien | Phone: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com