The Road to Industrial IoT Security

Industrial networks have become a target for hackers. Ensure the continuity, resilience, and safety of your operations by following this road towards an efficient Industrial IoT Security journey.

Identify your industrial assets
- Know what’s connected to your industrial network
- Understand what IoT assets are communicating with
- Identify asset vulnerabilities and their exposure to cyber risks

Segment your control network
- Group assets into logical zones per ISA/SP844/REICHMANN
- Define security policies between zones
- Leverage network switches to enforce zones and conduct

Enforce security policies
- Clean malware and malicious traffic
- Block attempts to scan and modify industrial assets
- Control communications on your industrial network

Extend IT security to OT
- Detect abnormal behaviors from industrial assets
- Share OT data with IT security tools
- Run converged OT/IT threat investigations

The Cisco Route to Industrial IoT Security

1. Build your industrial DMZ with Cisco Secure Firewalls
2. Block malware and intrusions with Cisco IDS/IPS powered by Cisco Talos
3. Inventory assets and assess your security posture with Cisco Cyber Vision
4. Enforce micro-segmentation with Cisco ISE
5. Control remote access with Cisco AnyConnect and Secure Mobility Access
6. Detect anomalous activities with Cisco Cyber Vision and Secure Analytics
7. Investigate and remediate threats with Cisco SecureX

Start your journey to industrial IoT security with Cisco
From OT visibility to network segmentation and all the way to a converged IT/OT security strategy, Cisco has a range of solutions to help you secure your operations and mitigate risks. Learn more in our free e-book.

Learn more in our free e-book

© 2023 Cisco and/or its affiliates. All rights reserved. C14-259138-00, Rev. 1 04/2023. Cisco, the Cisco logo, and Cisco Secure are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries.