Security for the Utility Grid

Global utilities are designing and building resilience in their modern grid deployments. Cisco enables new business models to enhance grid security postures without compromising reliability or network response time.

300%
Surge of cyberattacks on industrial devices in 2019[1]

41%
Of ICS computers attacked at least once in 1H2019[2]

$3.5 Billion
Lost to cyber-scams and ransomware in 2019[3]

Distributed Energy Resources

Transmission Substation Automation

Secondary Substation Automation

Advanced Metering Infrastructure

Common Roadblocks and Solutions

⚠ **Inability to see all of my devices on the ICS network**
✓ Utilize Cisco Cyber Vision to identify assets, vulnerabilities, communication patterns, and detect process anomalies

⚠ **Cyber/OT-security and regulatory compliance**
✓ Deploy an end-to-end/port-to-port OT and cybersecurity approach through the entire grid

⚠ **Perimeter security and application control not implemented Behaviors and threats not visible**
✓ Employ Cisco Secure Firewall ISA3000 to build a perimeter defense to detect and protect against intrusions and malicious or unintended commands

⚠ **On-premises and remote user access and activities are unmanaged**
✓ Automate and enforce access control with Cisco ISE to provide identity services by user, device, and location

⚠ **Delayed fault location, isolation, and service restoration**
✓ Improve responsiveness with a singular network distribution grid to drive reliability and compliance

⚠ **Time lapse between breach detection and threat mitigation**
✓ Monitor real-time network flow, detect traffic anomalies, and predict malware propagation with Cisco Secure Network Analytics (Stealthwatch)

⚠ **Build grid resilience and efficiency**
✓ Deploy IEC 61850 over WAN network, segmentation of SCADA teleprotection, voice and video surveillance

Cisco Grid Security Solutions will:

1. Build an inventory of devices and applications operating in your grid network
2. Enable visibility into industrial control systems (ICS) to develop baselines for devices, applications, and traffic profiles
3. Secure touchpoints where people and their devices securely interact with the industrial control systems (ICS)
4. Prepare for the inevitable shift of operational technology (OT) components moving to the cloud
5. Deploy tools that enable and inform rapid incident response
6. Align with industry security compliance standards such as NERC|CIP, and EU NIS

For more information

Contact your Cisco representative or learn more online at:

cisco.com/go/gridmodernization

Get Your IT/OT Security Profile:

cisco.com/go/itotsecurityprofile

Sources: 1. https://blog.f-secure.com/attack-landscape-h1-2019-iot-smb-traffic-abound/
2. https://ics-cert.kaspersky.com/reports/2019/09/30/threat-landscape-for-industrial-automation-systems-h1-2019/#_Toc19618313
3. https://pdf.ic3.gov/2019_IC3Report.pdf

Cisco IoT

Cisco-IoT-UtilityNetworkGridSecurity-09022021