The bridge to possible

Cisco Utilities Thought Leadership

Defending the power grid from cyber security threats

The bridge to possible

Benefits

A well thought-out, implemented, and operationally-effective security posture requires a partnership between IT and OT and starts at the foundation – the network.

Improve industrial cybersecurity and compliance for the network by:

- Asset inventory and discovery
- Secure access at the edge
- Security incident containment
- Threat detection and mitigation
- Malware protection
- Secure data transport

Securing the smart grid

The current shift to more connected and data-driven grid operations is driving improvements in system reliability, efficiency, and safety. However, this modernization and the digitization that it enables increases the attack surface through which threat agents can target utility infrastructure. Further, utilities and energy organizations are part of the critical infrastructure of any nation, which makes them a high-profile target for cyberterrorists and hackers alike. Utilities are additionally under constant scrutiny from regulators to comply with security standards. To be ahead of cyberattackers and respond to evolving threats, utilities must do more than simply comply with regulations.

The foundation to a reliable digital grid is a properly architected secure OT network that embeds defense in depth across the entire OT domain. What follows is a review of many of the basic constructs that are desired in building a reliable and secure OT digital foundation. The detailed grid security design guide can be found here: Grid Security Design Guide - Cisco.

Network segmentation

Industrial security best practices suggest migrating networks toward architectures compliant with IEC62443 zones and conduits. Utilities need to place assets that do not need to communicate to each other into isolated network segments to help prevent an attack from spreading through the industrial infrastructure. With most breaches beginning in the IT domain, particular emphasis on segmenting the IT and OT domains is required. Operational traffic flows have legitimate reasons to cross these segmentation boundaries, so a vital component of securing grid operations are thoughtful rules on when these boundaries can be crossed, which are often deployed in firewalls or routing rules.

Authentication, authorization, and accounting

Access control within the utility environment requires identification and authentication. The identity of users (humans, software processes, devices) requesting access must be verified before activating communication. The aim is to prevent illegitimate (unauthenticated) access of selected devices or data in the OT domain. It is important to define what devices are connected to a network, at what location, and who, if anyone, is operating that device. Scalable rules and mechanisms that allow only known users and devices

A well-architected and comprehensive security solution can provide a secure, compliant, and operationally efficient OT network. A single system is easier to maintain, more reliable and trusted, with fewer integration costs and ongoing operational costs.

to connect to a substation bus or distribution automation gateways are mandatory. Once an entity is authenticated, it is required that the OT security scheme control and limit access to only the authorized resources while also maintaining logs of device, application, and user OT transactions and events.

Operational visibility and insights

Deploying firewalls to build a demilitarized zone (DMZ) between industrial networks and the IT domain is a foundational first step in securing grid operations. As utility organizations connect more devices, enable more remote access, and build new applications, the airgap created by firewalls erodes and falls short of being sufficient. Subsequently, securing an industrial IoT network requires in-depth visibility. Utilities need to understand what devices are on the network, how they are communicating, and where those communications are going. Visibility functions can also provide detailed asset information that can be leveraged to identify power system device vulnerabilities and aid in grid asset inventory. As in the IT domain, Cisco has embedded the ability of the network to be the visibility sensor: An Edge Architecture Approach to Securing Industrial IoT Networks - Cisco.

Threat detection and mitigation

Visibility is the foundation of what enables a truly effective threat detection strategy. The goal of threat detection is to recognize the presence of abnormal traffic, applications, or users as soon as possible post threat initialization with the objective of protecting critical assets against cyberattacks and insider threats. Threat analytics within the OT environment require utility-specific protocol support, and unlike in IT, human-initiated containment is currently preferred over automated threat containment due to the strict uptime requirements of grid operations. Accelerating threat hunting and incident management by aggregating and correlating intelligence and data across your infrastructure can be achieved via Cisco SecureX™: Cisco SecureX Threat Response - Security That Works Together - Cisco.

Incident response

Given that grid operators are critical national infrastructure, it is a recommended best practice for utilities to have both proactive and reactive incident response coverage. With the global security talent shortage, combined with an increase in incidents, these additional services deliver the visibility and threat intelligence that utilities need to help prepare, respond, and recover from a breach by bringing the operational rigor and advanced tooling required by energy providers: Cisco Security Services for Incident Response and Retainer At-a-Glance - Cisco.

Takes partners

While cyber risks will continue to pose challenges, utilities are well positioned to manage cyber risks in partnership with industry peers, regulators, and security solution providers like Cisco.

More information

Visit these resources to learn more about:

- Utilities and grid security
- Cisco Industrial Threat Defense
- Cisco Industrial Security
- Cisco Secure portfolio

CXX-XXXXXX-00 03/22