tenable OT Security

USE CASE

SECURING YOUR SMART GRID

TOP TRENDS

- Rapid adoption of IIoT and convergence of IT and OT
- Large distributed and more interconnected networks
- Introduction of renewable and intermittent energy sources
- Migration to universal TCP/IP based standards such as IEC 61850 & IEC 104

KEY CHALLENGES

- Distributed substations require visibility and context to properly secure service
- Time and mission critical resource where resiliency is essential for reliable and constant delivery
- The vast area that grid and power networks cover, along with the various communication protocols, creates a large attack surface for both

BACKGROUND

Power grids are evolving. The rise of the Smart Grid, the introduction of renewable resources and the evolution of a variety of storage options require grids to be more flexible than ever before. Balancing supply and demand when incorporating new sources of intermittent energy, such as wind and solar power, means the grid must respond and adapt in real-time. That is not an easy task.

To face these challenges, grids are becoming increasingly more intelligent, interconnected and digitized. As a result, network visibility, security and control must be achieved from the grid level all the way to the bay level and individual intelligent electronic device (IED). Improving smart grid inter-connectivity, leveraging modern TCP/IP based standards such as IEC- 61850 and IEC-60870-5-104, and employing new techniques of data acquisition are becoming the de facto industry standard.

An interconnected network, while creating great efficiencies, also yields a much wider attack surface with the capacity to easily move from one provider to the next. Therefore, grid based industrial cyber threats have become core risks to safety, reliability and business continuity.

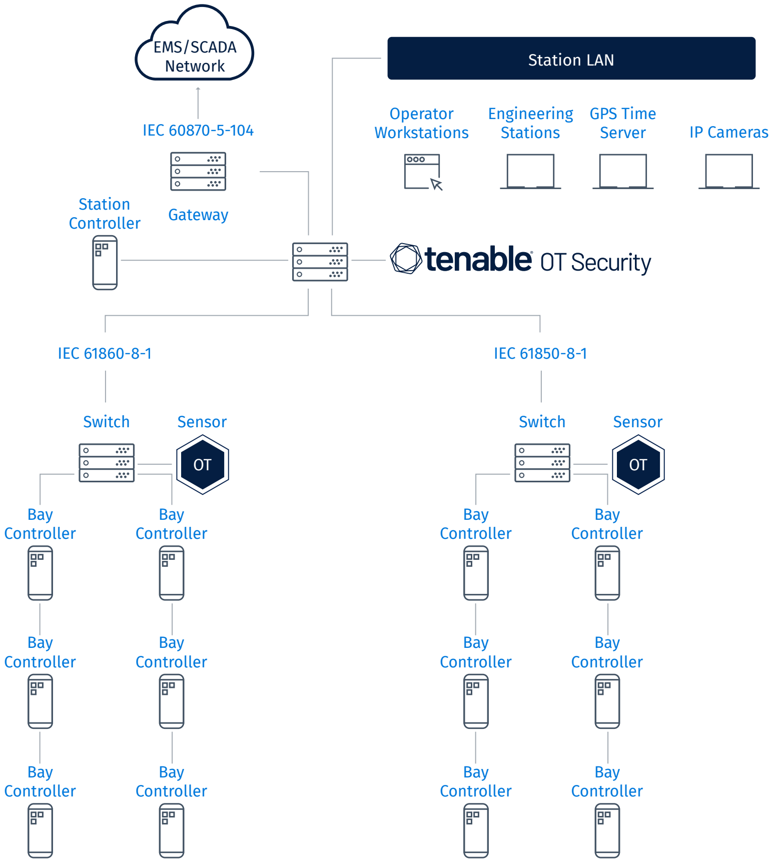
ANATOMY OF A CYBER ATTACK IN SMART GRID

- Initial infiltration to the power grid network
- Establishing a beachhead in one of the assets in the network
- Initiating reconnaissance activity to map out the targets and vulnerable devices
- Propagating to other assets to reach the areas of interest
- The "last mile" of the attack disrupts grid operations

Recent Events

- **May 2023:** Newly-discovered CosmicEnergy malware is an example of malware that could disrupt power generation and do physical damage. (Source)
- **April 2022:** Industroyer2 was discovered targeting regional high-voltage electrical substations in Ukraine less than two months after Russia attacked Ukraine. (Source)
- **Mid 2020:** China-linked group RedEcho used the AXIOMATICASYMPTOTE infrastructure to carry out its intrusions targeting a large swathe of India's power sector during border tension. (Source)

STANDARD SCADA DEPLOYMENT



Common Standards for Grid Operations

IEC 61850 Communication networks and systems for power utility automation

EC 61970 Energy management system application program interface including the common information model

IEC 61968 System interfaces for distribution management

IEC 61400-25 Communications for monitoring and control of wind power plants

EC 62325 Framework for energy market communication

IEC 62351 Standard for the data transfer security

IEC 62056 Data exchange for meter reading, tariff and load control

EC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC 61131 Programmable controllers

EC 61334 Distribution automation using distribution line carrier systems

ISO/IEC 14543 Home Electronic System (HES) architecture

IEC 61499 Distributed control and automation

IEEE 1547 IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces

NO VISIBILITY OR CONTEXT

In grid environments the "last mile" action can involve sending legitimate protocol commands to controllers, relays and IEDs. These commands can be in documented protocols such as IEC-61850, IEC-60870-5 and DNP3 or in proprietary vendor protocols. Disruption can have dire consequences on safety and grid stability.

These types of events should be accounted for in full. Attacks, however, should be identified long before the last mile stage. Traffic should be monitored everywhere including at the substation bus itself. Events should be clearly understood and should incorporate enough context to discern if the events are malicious in nature or part of regular operation. The solution should be adaptable to the specific needs of each power grid to minimize false-positives and keep network managers focused on regular operations.

To identify events at any stage of the attack, multiple detection engines are essential.

1. DPI engines for both documented and proprietary protocols to identify "last mile" and reconnaissance events.
2. General traffic mapping and traffic visualization need to identify an alert on communication attempts from external sources.
3. An anomaly detection mechanism should be used to pinpoint traffic patterns that are outside of the regular network operation.
4. Signature based detection should be leveraged to identify known threats which are used by attackers for establishing beachheads or propagating through the network.

PHYSICAL TAMPERING

Unlike traditional IT networks or manufacturing plants that are usually located in a single large building, power networks are physically distributed across a large area. An effective OT security solution must periodically query individual devices at all locations to identify if any changes have been performed. It is necessary to query all IEDs in the network as they control regular grid operations. It is also important to query servers, workstations, networking equipment, gateways, and OT devices that are critical to the regular network operations.

Tenable.ot leverages patented active querying technologies and is also the first to specifically build active querying engines for power networks. The technology employs active querying for both documented and undocumented protocols to achieve maximum situational awareness and provides coverage of all devices in the distributed power grid network.

MANAGE ALL ASSETS

Power networks tend to have large infrastructures. Many different devices are spread across a vast area and sometimes across several networks. Networks generally have multi-generations of devices in addition to a variety of makes and models. A solution should be able to combine several discovery methods to create an updated asset inventory of the entire distributed environment.

Asset tracking is required to keep the inventory updated and to be alerted for any unaccounted changes. This provides the required visibility to all types of devices that are found in power networks such as IEDs, EMS servers, GPS time servers, protection devices, etc. It should scale for large networks with many heterogeneous devices. What's more, it should account for dormant devices that are not communicating regularly over the network.

Organizations that implement hybrid asset tracking can passively extract details that are picked up over the wire from the SPAN port or from sensors and will identify all assets along with specific details on each of them. Tenable.ot combines passive technology with patented active device querying technology to account for all devices including "dormant" devices that are not communicating regularly.

About Tenable

Tenable® is the Exposure Management company. Approximately 43,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies.

Learn more at www.tenable.com.

PROACTIVE VULNERABILITY MANAGEMENT

Power networks tend to contain a mix of older devices which are randomly upgraded or replaced. With various patch levels across each device type, maintaining an up to-date patch management program can be difficult. If this is performed manually, the potential exists for misses and mistakes not to mention the dedication of massive amounts of time and effort. That said, maintaining deep awareness of state and characteristics of every device is necessary. This includes accurate matching between the specific condition of the devices and the available knowledge base on vulnerabilities to eliminate false positives. Because of the dynamic nature of grid environments, this body of knowledge should be updated regularly and kept in sync with newly discovered vulnerabilities. After building an accurate asset inventory, and by leveraging both active and passive detection mechanisms, Tenable.ot extracts detail on devices (e.g. model, firmware, patch levels, installed software, serial number). This delivers the patch management and security required to keep all devices up-to-date and fully operational.

SUMMARY

Cybersecurity is now widely recognized as a core risk to power networks. To mitigate that risk, it is essential to maintain full visibility into all operational assets including IEDs, RTUs PLCs, breakers, meters, drivers and other devices.

Tenable.ot uses both passive detection in documented and undocumented protocols as well as its patented active querying technology, to detect any threat to grid environments. In addition, Tenable.ot has developed a comprehensive policies mechanism that allows network management to create rules that are adapted to the routine of each individual network. The use of both types of security methods, combined with Tenable.ot's flexible deployment options will ensure smart grids operate safely and with reduced risk.

TENABLE OT SECURITY

Tenable OT Security brings visibility, security, and control to industrial environments, critical infrastructure, building management systems, and more, helping organizations maintain productivity, meet compliance requirements, and stay safe from cyber attacks. Using a patented hybrid discovery approach to safely gain visibility into devices and cyber-physical systems without causing disruption, Tenable OT Security delivers a thorough asset inventory along with deep situational awareness across all global sites, all in a single interface. From vulnerability management and threat detection, to configuration control and reporting, Tenable OT Security lets organizations prioritize action and enables their IT and OT security teams to work better together.