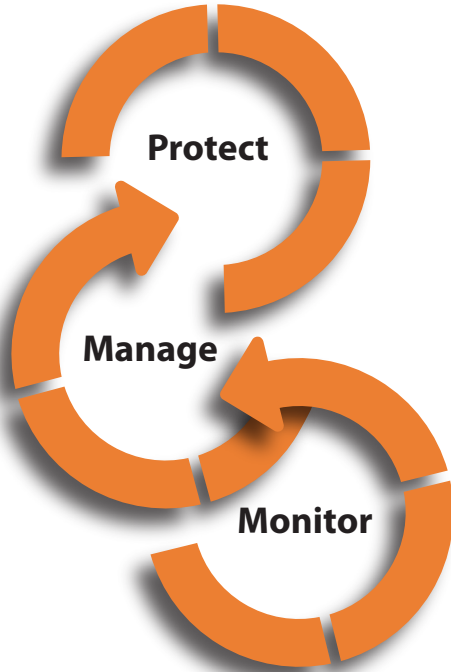


Security and Compliance Challenges Threaten Operational Excellence at Power Generation Facilities

Monitor, Manage and Protect Solutions for Power Generation Facilities



NERC CIP: A Major Burden for Power Generators

Achieving and then maintaining compliance with NERC CIP standards is not a simple task. CIP-002 through CIP-009 cover all aspects of critical infrastructure protection. For example, CIP-005 R3 calls for automated access monitoring, CIP-007 R1 requires port and systems management and CIP-007 R3 mandates patch management programs and malware prevention tools. In addition to implementation, power generation facilities must also prove that these protection measures are indeed in place and functioning as prescribed by NERC CIP.

Today's power generation facilities face unprecedented challenges. The automation systems that underlie their production infrastructure – including distribution control, balance of plant, continuous emissions monitoring and turbine control systems, among others – are increasingly on the defensive. According to the SANS Institute, increasingly sophisticated, persistent and financially motivated hackers have extorted, “hundreds of millions of dollars... and possibly more.” Without question, denial of service attacks and hostile infiltrations are increasing in frequency.

Due to the need for real-time business intelligence, the boundaries between power generation facilities' corporate IT and automation environments are eroding. While the diminished network separation helps meet business needs, it becomes a significant cause for concern from an operations perspective since control systems are often designed with the hopes of air-gaps for security. The truth, according to NSS Labs, is that “very few (control systems) are properly air-gapped.” This growth in connectivity increases health and safety concerns, as well as the likelihood of significant performance degradation, and the reputational and financial consequences associated with an incident.

Given the stakes, regulators have enacted requirements such as the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) which mandate that critical infrastructure owners implement and periodically verify specific security protections. This regulation-driven approach to securing automation systems is neither capricious nor temporary. Critical infrastructure owners should expect increased oversight in the future.

These challenges require organizations to balance requirements on three different fronts: operations, security and compliance. It is important to recognize that each area cannot be approached in isolation as addressing one area alone may create risks for another.

The Solution

Thanks to its exclusive focus on automation systems that support critical infrastructure, Industrial Defender understands the importance of a unified strategy to drive operational excellence. Power generation facilities must enhance an automation system's performance and reliability, defend against emerging security threats, and sustain compliance with operational requirements and NERC-CIP while efficiently and effectively managing their automation systems.

Industrial Defender enables this approach with a set of purpose-built, integrated solutions. The Monitor, Manage and Protect solutions are powered by automation system agents specifically designed for power generator's critical automation systems from vendors including ABB, Emerson, GE, Honeywell, Invensys, Siemens, Yokogawa and others. The automation system agents collect application specific log files and unify operations, security and compliance across multiplatform environments.

These solutions allow power generators to monitor security and health activities in real-time; to manage critical activities such as configurations, patches, policies, and security events; and to protect against threats to vital automation systems. The result is enhanced operational excellence, and sustained security and compliance.

The Industrial Defender Difference

Unlike the security and compliance technologies typically deployed in the corporate IT environment, Industrial Defender technologies that underlie the Monitor, Manage and Protect solutions are specifically built to work with critical automation systems including legacy systems & protocols. Thanks to this developmental focus, the solutions have minimal impact on systems availability and performance, support live installations without operational disruption, and add value in hours or days, rather than weeks or months.

Supplemental Defense-In-Depth Security Technologies

To supplement the capabilities included in the Monitor, Manage & Protect solutions, Industrial Defender offers additional technologies that enable organizations to gain real-time visibility into network activity through a network intrusion detection system (NIDS), to enforce a hardened electronic security perimeter via unified threat management (UTM) technology, and to implement secure authentication and access controls at remote sites. These technologies help organizations address additional NERC CIP requirements.

To Learn More

To learn more about Industrial Defender's Monitor, Manage, and Protect solutions as well as supplemental Defense-In-Depth security products, please contact Sales@IndustrialDefender.com.

Industrial Defender

16 Chestnut Street, Suite 300

Foxborough, MA, USA, 02035

T: +1-508-718-6700

F: +1-508-718-6701

E: Sales@industrialdefender.com

W: www.IndustrialDefender.com

Monitor

Monitoring is the first step in building a unified security and compliance management strategy that supports operational requirements. The centralized collection, correlation and archiving of events enables critical infrastructure owners to quickly identify and respond to operational threats jeopardizing their automation systems. In this sense, monitoring is the backbone of a sustainable security and compliance capability and, therefore, a major focus of NERC CIP-005.

Industrial Defender's Monitor solution is powered by security event management (SEM) technology. Available as an on-site deployment or a managed service, this solution provides real-time security and health activity monitoring across automation systems, networks and applications. This technology allows system administrators, control engineers and operators to quickly discover and mitigate events impacting security, compliance and operational efficiency and to meet NERC CIP's monitoring requirements.

Manage

Manage builds upon the monitoring of critical events across automation systems, networks and applications. Centralizing and automating the maintenance and management of configurations, systems status, policy modifications and patching can significantly enhance operational efficiency. This type of management is also explicitly required by NERC CIP-007. These capabilities ease analytical processes and reporting obligations which greatly reduces the burden of demonstrating compliance with NERC CIP, other regulations, and internal operational mandates.

With the data captured by the Monitor solution, Industrial Defender's Manage solution enables customers to manage critical activity across automation infrastructure. As prescribed by NERC CIP, the solution's compliance management technology consolidates and analyzes asset inventories, event logs, system configurations, software patch status and user accounts. It also archives log and configuration files for automation control applications, operating systems, firewalls, network devices and end-point industrial devices. This data is then automatically transformed into actionable information that is available for daily operations support, system assessments and formal NERC CIP audits.

Protect

With Monitor and Manage in place, power generators can further extend these capabilities and ensure that control systems are protected against unauthorized applications and memory exploits by including a host intrusion prevention system.

The host intrusion prevention system (HIPS) delivered by Industrial Defender defeats malware that would compromise control system availability, performance, security and compliance. This integration improves overall security situational awareness, addresses NERC CIP's malware prevention requirements and includes the ability to correlate and associate events and responses in different areas of the automation systems environment.

Capability Highlights: Monitor, Manage and Protect Solutions for Power Generation

Capabilities

- Identify security events
- Understand health & performance
- Uncover performance degradation
- Maintain central config policy
- Centrally track changes, patches, configs
- Analyze & report across environment
- Enforce host-level application policies
- Prevent rogue applications/malware

Add-On Capabilities

- Real-time visibility into network activity
- Enforce hardened electronic security perimeter
- Enact secure access and authentication for remote site locations

