HOW TREND MICRO PORTABLE SECURITY™ 3 STREAMLINES NERC CIP COMPLIANCE

HOW TREND MICRO PORTABLE SECURITY™ 3 STREAMLINES NERC CIP COMPLIANCE

The North American Electric Reliability Corporation **(NERC)** Critical Infrastructure Protection **(CIP)** is a set of regulatory standards which specifies the security requirements for the cyber systems critical to the operation of bulk electric systems **(BES)**. These standards include requirements outlining the minimum controls and policies that must be implemented by electric utilities in order to ensure the safety and reliability of electric system operations and protect infrastructure in North America.

Trend Micro Portable Security™ 3 provides effective malware scanning and removal to standalone computers and air-gapped systems. It facilitates utility companies to ensure the bulk electric system (BES) is secure and reliable. It is a portable tool that plugs into the USB port of any Windows or Linux cyber assets to detect and eliminate malware without installing software. The collected asset information generates an inventory list, helping to improve OT visibility and eliminate shadow OT. Its companion Management Program can deploy scanning configuration settings to multiple scanning tools, either remotely or physically. It also compiles and integrates scan logs and asset information from multiple scanning tools in multiple locations, providing a holistic view of all endpoints. Some of the world's largest and most complex energy utilities depend on TMPS3 to streamline their cyber security management for their control centers and substations.

Trend Micro Portable Security™ 3 SUPPORTS NERC CIP COMPLIANCE FOR THE FOLLOWING STANDARDS:

- **CIP-002: Generates detailed inventories for all scanned cyber assets.**
- **CIP-003: Facilitates implementation & documentation of security policies.**
- **CIP-007: Mitigates detected malicious threats for Windows and Linux.**
- **CIP-008: Streamlines IR processes and integrates with SIEM.**
- **CIP-010: Simplifies the cyber security management of transient cyber assets.**

The following table lists some of the key requirements of **NERC CIP** and explains how **Trend Micro Portable Security™ 3 (TMPS3)** can help your organization implement those requirements to achieve compliance with NERC. This mapping could be used as a reference guide to help you implement policies and procedures tailored to your organization's unique situation and needs.

▲ Trend Micro Portable Security™ 3
Installation-free endpoint security inspection

CIP-002: BES CYBER SYSTEM CATEGORIZATION

To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

NERC CIP Requirement	How TMPS3 Helps
R1.1 Identify each of the high impact BES Cyber Systems R1.2 Identify each of the medium impact BES Cyber Systems R1.3 Identify each asset that contains a low impact BES Cyber System	• Trend Micro Portable Security™ 3 (TMPS3) generates detailed information of all scanned assets while scanning. This asset information includes comprehensive details of each asset, including IP address, MAC address, host name, OS version, patch list, installed application list, and so on. • The collected asset information can be exported to the CSV format through the centralized Management Program as an asset inventory, or sent to an SIEM or Rsyslog server for further asset management such as maintaining a BES asset inventory or identifying impact levels, known vulnerabilities, and cyber risks.

CIP-003 SECURITY MANAGEMENT CONTROLS

To specify consistent and sustainable security management controls that establish responsibility and accountability in order to protect BES Cyber Systems against compromises that could lead to misoperation or instability in the Bulk Electric System (BES).

NERC CIP Requirement	How TMPS3 Helps
R2 Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1. • Requirement R2, Attachment 1, Section 5.1 -Transient Cyber Asset(s) Managed by the Responsible Entity. • Requirement R2, Attachment 1, Section 5.2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.	• Implement TMPS3 in the cyber security plan to achieve the objective of mitigating the risk of malicious code being introduced. • Generate an inventory for all scanned assets including Transient Cyber Assets such as laptops, desktops, and diagnostic test equipment that may interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code to BES Cyber Assets. • Document and address the risks posed by malicious code with on-demand scanning when connecting Transient Cyber Assets that are listed in the CIP-003-8 Requirement R2, Attachment 1, Section 5. • Flexibly manage cyber security to Transient Cyber Assets or standalone devices that do not regularly connect to receive scheduled updates.

CIP-007: SYSTEMS SECURITY MANAGEMENT

To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromises that could lead to misoperation or instability in the BES.

NERC CIP Requirement	How TMPS3 Helps
R2.1 A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. R2.2 At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1. R2.3 For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan.	TMPS3 collects asset information, including an installed patch list and an application list, while scanning. The advantage of portability solves the problem of identifying the inventory of standalone Cyber Assets where no asset management system can probe. The patch list collected by the TMPS3 Scanning Tool can be exported to CSV files or transferred to an SIEM (such as QRadar or Splunk) or Rsyslog server for further investigation and asset management.
R3.1 Deploy method(s) to deter, detect, or prevent malicious code. R3.2 Mitigate the threat of detected malicious code. R3.3 For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	TMPS3 is a purpose-built tool to detect, remove, and quarantine malware for Cyber Assets. It's able to scan Windows and Linux systems, including legacy OSes such as Windows 7, XP, or 2000. • Scan and quarantine malware such as viruses, worms, ransomware, trojans, rootkits, packers, and so on. • Detect known notorious ICS/OT malware such as TRITON, Black Energy, Industroyer, NotPetya, WannaCry, and EKANS. • Multiple scan options such as prompting user confirmation, creating logs while taking no action, or taking a set recommended action • Simplify the processes of detection, removal, and quarantine • Quarantined files can be restored to the original system • No impact to BES Cyber Systems • New patterns released regularly. Easily keep pattern files up-to-date

R4.1 Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1.Detected successful login attempts; 4.1.2.Detected failed access attempts and failed login attempts; 4.1.3.Detected malicious code.	• Each scan will be logged to support Security Event Monitoring • Detailed scan information will be logged for every detected malicious file.
R4.3 Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances. R4.4 Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Scan logs can be retained for 90 days or more at your discretion. You can access aggregated scan logs on the Management Program to get a summary of scan reports for all scanned assets by all Scanning Tools. Scan logs can be also exported to CSV files or transferred to an SIEM (such as QRadar or Splunk) or Rsyslog server for further investigation and asset management.

CIP-008: INCIDENT REPORTING AND RESPONSE PLANNING

To mitigate risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

NERC CIP Requirement	How TMPS3 Helps
R2.2 Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	TMPS3 can be used as a forensics tool. Its threat detection and quarantine functionalities help you to identify, analyze and initiate response to a cyber security incident. This allows you to build your incident response processes and strategy. The detailed scan logs and reports allow you to understand the target, nature, and potential impact of a threat.
R2.3 Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system.	You can retain scan logs in the Scanning Tools or transfer the scan logs to the Management Program for a company-wide or factory-wide view. Scan logs can also be exported to CSV files and then stored as evidence for nonrepudiation purposes or transferred to an SIEM (such as QRadar or Splunk) or Rsyslog server.

CIP-010: CONFIGURATION CHANGE MANAGEMENT AND VULNERABILITY ASSESSMENTS

To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromises that could lead to misoperation or instability in the Bulk Electric System (BES).

NERC CIP Requirement	How TMPS3 Helps
R.1 Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	TMPS3 generates an inventory of all scanned assets, which includes information such as host name, domain names, IP address, MAC address, OS version, hardware info, network info, application software, application software versions, and security patches applied on the asset. All of the asset info in the TMPS3 Management Program provides the ability to create a new baseline to accommodate changes in application software and patches installed. Asset info can also be exported to CSV files as a baseline for further change management.
R1.2 Authorize and document changes that deviate from the existing baseline configuration. R1.3 For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	Each scan by TMPS3 Scanning Tools collects the latest inventory of scanned assets. The latest asset info can be manually compared with the baseline to keep baseline documentation up to date.
R.4 Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1.	Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems such as diagnostic test equipment or equipment used for BES Cyber System maintenance. TMPS3 streamlines the process of implementing plans for Transient Cyber Assets and Removable Media in CIP-010-3 - Attachment 1 and Attachment 2. With the installation-free TMPS3, you can easily plug the Scanning Tool into Transient Cyber Assets to achieve the objective of mitigating the introduction of malicious code. No software installation is required. Meanwhile, it simplifies the processes of managing signature or pattern updates for Transient Cyber Assets and Removable Media. Scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.

Conclusion

Several of the world's most sizable electric utilities have already discovered that **Trend Micro Portable Security™ 3 (TMPS3)** provides reliable threat detection across air-gapped and standalone assets, freeing up working hours for other important tasks and making the necessities of safety and security more manageable. The cyber defense, record-keeping, and incident response procedures necessary to stay in line with the NERC CIP, while numerous, can be made a much more convenient part of workplace routines with the appropriate solution. **Trend Micro Portable Security™ 3 (TMPS3)** makes it possible to complete these tasks while neatly organizing crucial records in a single location via Management Program.

Trend Micro Portable Security™ 3

Seamless and installation free

Portable Security 3 comes on an enhanced USB flash drive designed for the most convenient use possible with no installation needed to perform antivirus scans. This installation-free architecture gives you a very low operational footprint, has no impact on manufacturing, and can be used without voiding your ICS warranty.

Easily detect and stop malware

Use the tool at your checkpoint to prepare partners, vendors, or consultants coming on-site with a quick pre-scan. Before guests connect their potentially infected laptops or USBs to your ICS network or assets, you can easily plug in Portable Security 3 and follow the intuitive on-screen instructions to seamlessly scan and secure devices. The built-in LED lights indicate whether malware has been detected or eliminated and if further investigation is required.

Comprehensive visibility for regulatory and operational efficiency

While performing antivirus scans on target devices, Portable Security 3 also compiles and integrates scan logs and asset information from multiple scanning tools, improving OT visibility and eliminating the shadow OT. Its companion management program provides a holistic view of all endpoints to create an audit trail and ensure data integrity. This allows you to keep up with industry regulations much more easily.

For more information about Portable Security 3, please visit:
TXOne Network Product Introduction: https://www.txone-networks.com/en-global/products/index/tmps3
Product Demo video: https://www.youtube.com/watch?v=GO22TLYHiSI

About TXOne Networks

TXOne Networks, a subsidiary company of Trend Micro, offers cybersecurity solutions tailored to the protection of industrial control systems, ensuring reliability and safety from cyberattacks. At TXOne Networks, we work together with both leading manufacturers and critical infrastructure operators to create practical, actionable approaches to cyber defense. Our solutions eliminate the security weaknesses prevalent in industrial environments, create visibility, and minimize time spent on maintenance. TXOne Networks' mission is to provide practical cybersecurity solutions to safeguard and accelerate the progress of automation and data exchange in the industrial world.

Visit https://www.txone-networks.com for more information.

www.txone-networks.com
support@txone-networks.com