

NERC CIP STANDARDS

MAPPED TO VERVE INDUSTRIAL PROTECTION



NERC CIP Mapping to Verve Industrial Protection

Standard Section		Requirement	Verve Capability	Method
CIP-002 - 5- BES Cyber System Identification and Categorization	R1.1-1.3	BES Cyber System Identification [High, Medium and Low]	Automatic connectivity and profiling of all assets and ability to monitor for new assets	Technology
	R2.1-2.2	Scheduled Review and Approval	Integration with 3rd-party workflow and documentation tools allow for real-time input of asset list to approval process	Technology & Services
CIP-003 - 8 - Security Management Controls	R1	Cyber Security Policy [High and Medium]	Long history in the development, deployment and enforcement of NERC CIP policies	Services Experience
	R2	Cyber Security Policy [Low]	Monitor LEAP boundaries, detect changes, collect and present related logs and verify network controls	Technology & Services
	R3	Identification of Senior Manager	Long history in the development, deployment and enforcement of NERC CIP policies	Services Experience
	R4	Delegation of Authority	Long history in the development, deployment and enforcement of NERC CIP policies	Services Experience
CIP-004 - 6 - Training & Personnel Security	R1	Awareness Program	Dashboard and alerting functions add to awareness content and sharing	Technology & Services
	R2	Training Program	Endpoint data, risk/patch aging and reporting/tracking all lead to training program content	Technology & Services
	R3	Personnel Risk Assessment Program	Long history in the development, deployment, and enforcement of NERC CIP policies	Services Experience
	R4	Access Management Program	Certify and enforce users in electronic access and verify transient cyber asset access for physical policy adherence	Technology & Services
	R5	Access Revocation Program	Certify, enforce and add/remove users automatically if needed	Technology & Services

Standard Section

Requirement

Verve Capability

Method

Standard Section	Requirement	Verve Capability	Method	
CIP-005 - 5 - Electronic Security Perimeter	R1.1	All Cyber Assets within a Defined ESP	Full asset and connectivity review allows for strict tracking and awareness of assets within the defined ESP - verify presence or lack of communication outside the ESP	Technology
	R1.2	All External Routable Connectivity through EAP	Verify presence or lack of communication outside the ESP	Technology
	R1.3	In/Outbound Access Permissions	List firewall configuration and alert to changes in support of compliance proof	Technology & Services
	R1.4	Dial Up Connectivity	Not currently supported	
	R2	Interactive Remote Access Management	Verve monitors activities on remote access devices to ensure security	
CIP-006 - 6 - Physical Security of BES Systems	R1	Physical Security Plan	Monitors and managed physical security system health	Technology
	R2	Visitor Control Program	Log retention and detection of new assets or IPs when vendors/visitors connect - transient Cyber Asset Tracking	Technology
	R3	Maintenance & Testing Program	Long history in the development, deployment and enforcement of NERC CIP policies	Services Experience
CIP-007- 6 - Systems Security Management	R1.1-1.2	Ports & Services	Verve provides for near real-time port/services listing along with the ability to disable/enforce removal of unwanted ports/services. Time series data alerts on changes to those settings	Technology
	R2.1-2.4	Security Patch Management	Patching tracking available on all assets, all OS, all embedded devices and types. Patch application available for all OS updates, software updates [3rd party] and software installation/removal from central console reporting	Technology & Services

Standard Section	Requirement	Verve Capability	Method	
CIP-007 - 6 - Systems Security Management (cont.)	R3.1-3.3	Malicious Code Prevention	Integration with whitelisting tools allows for granular lockdown of endpoints - Manage and monitor antivirus tools, process signature updates and alert on changes/events	Technology
	R4.1-4.4	Security Event Monitoring	Verve's time series data collects syslog, Windows log, Windows beats, Netflow and DCS alarms to provide the most comprehensive OS SIEM available	Technology
	R5.1-5.7	System Access Controls	Verve enumerates user accounts, system hardening parameters like password length, complexity, lockout duration, failed attempt limits and to alert or enforce any requirements	Technology
CIP-008 - 5 - Incident Reporting & Response Planning	R1.1-1.4	Cyber Incident Response Plan	Strong correlation between multiple contexts (asset level and other tools) significantly aid in the detection, response and resolution of any incident - cyber or otherwise, which Verve provides in near real-time across all OT assets	Technology & Services
	R2.1-2.3	Cyber Security Incident Response Plan Implementation & Testing	Detect and react to incidents in real-time and record action/changes through Verve to prove testing requirements and speed recovery	Technology & Services
	R3.1-3.2	Cyber Security Incident Response Plan Review, Update, Communication	Evidence tracking and event history aid in analysis of events post-incident	Technology & Services

Standard Section	Requirement	Verve Capability	Method	
CIP-009 - 6 - Recovery Plans for BES Cyber Systems	R1.1-1.5	Recovery Plan Specifications	Baselines coupled with other asset info such as a last backup status and location, whitelisting profile, patching levels, users, etc. are all tracked and managed by our platform, as well as transactional data (logs), significantly speeding the time and increasing the accuracy/effectiveness of recover plans - including embedded OT systems	Technology & Services
	R2.1-2.3	Recovery Plan Implementation & Testing	Whether live or in testing mode, our solution speeds in recovery/restoration of all assets from relays and PLCs to HMIs, engineering stations and networking gear	Technology & Services
	R3.1-3.2	Recovery Plan Review, Update & Communication	Evidence tracking and event history aid in analysis of events post-incident	Technology & Services
CIP-010 - 2 - Configurations Change Management & Vulnerability Assessments	R1.1-1.5	Configuration Change Management	Provide a robust and detailed asset inventory including ports, services, software, users, etc. Track and report on least privilege system hardening practices for both OS-based and networking assets	Technology & Services
	R2	Configuration Monitoring	Alert system setting changes to initiate change management or workflow activities	Technology & Services
	R3.1-3.4	Vulnerability Assessments	Verve provides comprehensive vulnerability assessment on a regular basis. No need to run scans to capture vulnerabilities. Verve's software and patch inventory automatically identifies vulnerabilities in real-time as new vulnerabilities are published.	Technology & Services

Standard Section		Requirement	Verve Capability	Method
CIP-010 - 2 - Configurations Change Management & Vulnerability Assessments (cont.)	R4	TCA & Removable Media	Verve monitors for TCA access and ensure compliance on all TCA devices. In addition, Verve integrates with leading application whitelisting software such as Carbon Black/Bit9 to confirm compliance with USB lockdown and alerts on deviations from compliance.	Technology
CIP-011 - 2 - Information Protection	R1.1-1.2	Information Protection	Reporting console tightly integrated with active directory and database controls to manage user access to information very granularly. Additional ability to watermark or identify reporting pages/ screens as confidential.	Technology & Services
	R2.1-2.2	BES Cyber Asset Reuse & Disposal	Track and manage retired assets and support the process of system disposal.	Technology & Services

To learn more, visit www.verveindustrial.com or contact us at info@verveindustrial.com