NIST CSF STANDARDS

MAPPED TO VERVE INDUSTRIAL PROTECTION

VERVE
A ROCKWELL AUTOMATION COMPANY

Function ID	Category	Description	Verve Solution	Comments
IDENTIFY			Y = yes, N = no , S = platform supports the practice, P = procedural requirements	
ID.AM	Asset Management	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	Y	Verve's endpoint asset management solution collects 1,000+ pieces of information beyond network devices for 360-degree IT and OT asset visibility. Prioritizing risk remediation is key to the management of the asset inventory.
ID.BE	Business Environment	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cyber security roles, responsibilities, and risk management decisions.	S	The inventory is the base but the context of the asset helps organizations to better scope roles, responsibilities and activities of the most appropriate (ie, IT or OT) personnel.
ID.GV	Governance	The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cyber security risk.	S	Verve's real time view into actual system and risk configuration, activities and trends support and prove adherence or direct activities as required. Verve is a real time view into current risk and status of OT assets.
ID.RA	Risk Assessment	The organization understands the cyber security risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Y	Verve's 360-degree asset analysis aggregates a full view of the environment into a single database to understand the vulnerability landscape and prioritize remediation actions.
ID.RM	Risk Management Strategy	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Y	Verve's approach provides a quantifiable reduction in risk using proprietary risk scoring and remediation planning.
ID.SC	Supply Chain Risk Management	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	S	As noted above, Verve provides real time data coupled with OT asset context to allow for owner/operators to make informed, contextual decisions about risk and assets.

Function ID	Category	Description	Verve Solution	Comments
PROTECT			Y = yes, N = no , S = platform supports the practice, P = procedural requirements	
PR.AC	Identity Management & Access Control	Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	Y	Verve enumerates users, shared accounts, admin accounts, password expiry and tracks access to specific systems or actions on those systems as needed.
PR.AT	Awareness & Training	The organization's personnel and partners are provided cyber security awareness education and are trained to perform their cyber security-related duties and responsibilities consistent with related policies, procedures, and agreements.	S	Verve data informs existing programs. For example, Verve displays non-patched assets with vendor approved status to show when patching cycles are lagging. Similarly, Verve enumerates user/access permissions. Clients often find this data invaluable in performing annual access reviews.
PR.DS	Data Security	Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	S	Data handling is not currently a part of the Verve platform. However, Verve provides very granular control of access to risk and asset data which extends corporate information handling to the area of OT cyber security as provided by Verve.
PR.IP	Information Protection Processes & Procedures	Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	S	As noted above, Verve is very useful in determining the adherence (or not) to corporate standards of risk, behavior and maintenance tasks.
PR.MA	Maintenance	Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	N	Verve is not a maintenance platform, but identifies end-of-life assets as needed.
PR.PT	Protective Technology	Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Y	Verve is exactly this type of security tool, providing. OT Systems Management across a wide range of security practice from inventory to vulnerabilities, patching, software and user management, as well as system configuration (hardening) and monitoring and detection (Host Based Intrusion Detection).

Function ID	Category	Description	Verve Solution	Comments
DETECT			Y = yes, N = no , S = platform supports the practice, P = procedural requirements	
DE.AE	Anomalies & Events	Anomalous activity is detected and the potential impact of events is understood.	Y	The Verve Security Center detects anomalous patterns in behavior that indicate potential threats in the environment.
DE.CM	Security Continuous Monitoring	The information system and assets are monitored to identify cyber security events and verify the effectiveness of protective measures.	Y	Verve ships with hundreds of alerting and detection thresholds. We are continually evolving the capabilities of this function as real world risk evolves, thus providing clients with valuable monitoring capabiIities in line with emerging threats.
DE.DP	Detection Processes	Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Y	OT/ICS-specific signals create alerts which can be sent to critical parties for vulnerability management, risk and compliance processes.

Function ID	Category	Description	Verve Solution	Comments
RESPOND			Y = yes, N = no , S = platform supports the practice, P = procedural requirements	
RS.RP	Response Planning	Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	S	Verve's SIEM allows for rapid response as soon as alerts are identified in a way that is controlled by OT engineers to ensure quick but reliable event response.
RS.CO	Communications	Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	S	Verve identifies in scope assets - this, coupled with a 360-degree view of an asset allows users to identify an asset, its owner, manufacturer and a host of other indicators that speed in the triage but also streamline the communication process during and after an incident.
RS.AN	Analysis	Analysis is conducted to ensure effective response and support recovery activities.	Y	Verve's integrated visibility to current and past alarms allow for root cause analysis and incident handling.
RS.MI	Mitigation	Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Y	Verve is a real time view into risk as well as a mechanism to reactively (or proactively) take action on assets to reduce risk and/or mitigate impact. Verve is the only tool on the market that combines detection with remediation in the same platform.
RS.IM	Improvements	Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Y	Verve's technology-enabled vulnerability assessment identifies potential gaps and provides an accurate view of the potential risks in each environment. This coupled with our HIDS and the analysis/ data from those events are key contributors to learning from an event.

Function ID	Category	Description	Verve Solution	Comments
RECOVER			Y = yes, N = no , S = platform supports the practice, P = procedural requirements	
RC.RP	Recovery Planning	Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cyber security incidents.	S	Verve helps clients design and monitor backup/recovery mechanisms. From identifying high impact (high priority) assets to monitoring third party tools for backup success/fail, we provide significant insight into the creation and execution of a robust backup/recovery program.
RC.IM	Improvements	Recovery planning and processes are improved by incorporating lessons learned into future activities.	Y	Verve's tracking and monitoring capabilities help our clients learn with real data and context to continually improve their program and the actions it requires.
RC.CO	Communications	Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	S	Verve's status tracking before, during and after an event provide detailed insight into system status, health, configuration, etc.