CIS Top 18 Controls

MAPPED TO VERVE SECURITY CENTER

VERVE

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
1	Inventory and Control of Hardware Assets							
1.1	Identify	Establish and Maintain Detailed Enterprise Asset Inventory	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, data asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	X	X	X	Yes	Verve provides a real time, comprehensive inventory of OS based assets, networking and communication gear as well as ICS specific equipment like controllers, relays, PLCs and others. Moreover, the Verve components also monitor the network for changes and can alert to new IP addresses if they appear on the network.
1.2	Respond	Address Unauthorized Assets	Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	X	X	X	Yes	Verve has a specific dashboard and alerting capability to bring new or unexpected assets to our clients attention as they are discovered.
1.3	Detect	Utilize an Active Directory Tool	Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.		X	X	Yes	Verve has a continuous ability to monitor for new threats rather than periodically. Any changes in results in an alert and a corresponding entry on our 'discovered assets' dashboard. This alert can also be sent via text or email or can be sent to ticketing systems as needed.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
1.4	Identify	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.		X	X	Yes	Verve uses ARP tables which is better than DHCP for OT as many OT asset IP addresses are manually assigned. By checking ARP tables which are required for transmitting we provide better coverage than DHCP integration.
1.5	Detect	Use a Passive Asset Discovery Tool	Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly or more frequently.			X	Yes	Verve has an automated alerting capability to constantly monitor for changes in the environment.
2	**Inventory and Control of Software Assets**							
2.1	Identify	Establish and Maintain a Software Inventory	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	X	X	X	Yes	Verve enumerates all software including version, install date, firmware, application software, etc.
2.2	Identify	Ensure Authorized Software is Currently Supported	Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	X	X	X	Yes	Verve tracks unsupported software and reviews that on a real-time basis.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
2.3	Respond	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	X	X	X	Yes	Verve enables users to identify unauthorized software AND remove that software.
2.4	Detect	Utilize Automated Software Inventory Tools	Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.		X	X	Yes	Verve is an automated inventory tool for all classes of OT assets (OS based, networking and embedded).
2.5	Protect	Allowlist Authorized Software	Use technical controls, such as application whitelisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		X	X	Yes	Verve enforces certain system settings such as software versions, users/permissions or even registry settings as needed.
2.6	Protect	Allowlist Authorized Libraries	Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.		X	X	Yes	Usually structural files and libraries are not 'restricted' in OT due to the nature of those systems but Verve is able to detect and track various library files and alert our clients as to their presence and/or use - such as our response to Log4J
2.7	Protect	Allowlist Authorized Scripts	Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			X	Yes	Verve locks down and/or alerts/ monitors for specific activities either through our agent on an endpoint (lockdown) or alerting through our host based intrusion detection and time series data collection.
3	**Data Protection**							
3.1	Identify	Establish and Maintain a Data Management Process	Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	X	X	X	Supports	Verve supports tracking of critical systems (including operational assets or informational) as well as various protections for those systems. Verve also has a robust encrypted communication method for its components and significant role based access control capabilities for managing access to the data we collect and generate.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
3.2	Identify	Establish and Maintain a Data Inventory	Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.	X	X	X	Supports	Verve supports tracking of critical systems (including operational assets or informational) as well as various protections for those systems. Verve also has a robust encrypted communication method for its components and significant role based access control capabilities for managing access to the data we collect and generate.
3.3	Protect	Configure Data Across Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	X	X	X	Supports	Verve has a very robust user and account tracking capability. We then share admin, dormant, expired or shared accounts through our reporting dashboard to help our clients assess and review access needs and practices.
3.4	Protect	Enforce Data Retention	Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.	X	X	X	Supports	Verve's reporting dashboard shows status of critical systems/shares and their backup and protection status as required.
3.5	Protect	Securely Dispose of Data	Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.	X	X	X	N/A	Data destruction is a process - Verve is a management platform or software.
3.6	Protect	Encrypt Data on End-User Devices	Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	X	X	X	N/A	Endpoint encryption and data encryption not typically used in OT environments.
3.7	Protect	Establish and Maintain a Data Classification Scheme	Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.		X	X	N/A	Data labeling is a process and not typically part of an end point management software platform.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
3.8	Identify	Document Data Flows	Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.		X	X	N/A	Data labeling is a process and not typically part of an end point management software platform for OT assets.
3.9	Protect	Encrypt Data on Removable Media	Encrypt data on removable data.		X	X	N/A	Verve is not a removable media management tool.
3.10	Protect	Encrypt Sensitive Data in Transit	Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		X	X	Yes	All of Verve's component communications are encrypted as long as it is supported by both devices in the communication path. Our agent to the database is encrypted, our protocol outreach (ADI) is encrypted and our storage of data and credentials is encrypted.
3.11	Protect	Encrypt Sensitive Data at Rest	Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		X	X	Supports	For Verve collected data and infrastructure, yes.
3.12	Protect	Segment Data Processing and Storage Based on Sensitivity	Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.		X	X	N/A	Verve monitors access between higher and lower security segments to ensure data is not accessed from an insecure network to a more secure one.
3.13	Protect	Deploy a Data Loss Prevention Solution	Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			X	Supports	Verve provides endpoint criticality (to operations) and status of endpoint backup, configuration and risk scores in support of DLP efforts.
3.14	Detect	Log Sensitive Data Access	Log sensitive data access, including modification and disposal.			X	Yes	Verve logs various access and failed attempts at access in support of this initiative.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
4	Secure Configuration of Enterprise Assets and Software							
4.1	Protect	Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	X	X	X	Yes	Verve immediately reports on how endpoints (OS based and a growing list of Networking gear) are configured relative to best practice security hardening guidelines.
4.2	Protect	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	X	X	X	Yes	Verve immediately reports on how endpoints (OS based and a growing list of Networking gear) are configured relative to best practice security hardening guidelines.
4.3	Protect	Configure Automatic Session Locking on Enterprise Assets	Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	X	X	X	Yes	Verve can be used to tune OS based devices right down to group policy and registry level settings, no OT assets ever have lockout policies applied.
4.4	Protect	Implement and Manage a Firewall on Servers	Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	X	X	X	Supports	Verve shows and reports on status of host-based firewall status as required.
4.5	Protect	Implement and Manage a Firewall on End-User Devices	Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	X	X	X	N/A	Default deny is never typically deployed in OT. However, Verve tracks many networks running configurations and alerts to the use of specific ports/services and/or alert to communications that are not authorized between various subnets/ systems as needed. Verve can also monitor and ensure device-level firewalls are enabled on devices.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
4.6	Protect	Securely Manage Enterprise Assets and Software	Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	X	X	X	Yes	Verve reports on how endpoints (OS based and a growing list of Networking gear) are managed relative to best practice security hardening guidelines we can help our clients to automate the implementation and enforcement of those standards if required.
4.7	Protect	Manage Default Accounts on Enterprise Assets and Software	Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	X	X	X	Yes	Verve has a very robust user and account tracking capability. We share admin, dormant, expired or shared accounts through our reporting dashboard to assess and review access needs and practices. We also rename, disable or otherwise to manage those accounts as well.
4.8	Protect	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		X	X	Yes	Verve's agent allows for very granular management and control of OS based assets. Either with end user support directly at the console (recommended for OT) or automatically for low impact/high risk settings like disabling the guest account.
4.9	Protect	Configure Trusted DNS Servers on Enterprise Assets	Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.		X	X	No	Verve does not configure DNS servers.
4.10	Respond	Enforce Automatic Device Lockout on Portable End-User Devices	Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.		X	X	Yes	Verve does this in an OT safe manner. Our agent enforces whatever policy an organization wants to implement, but it is highly rare to see automated response mechanisms in OT. This is why we report on system configurations as well as monitor and alert for thresholds like described here, but we typically stop short of automated response in those situations.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
4.11	Protect	Enforce Remote Wipe Capability on Portable End-User Devices	Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.		X	X	N/A	This is not a function OT environments typically require.
4.12	Protect	Separate Enterprise Workspaces on Mobile End-User Devices	Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.			X	N/A	This is not a function OT environments typically require.
5	Account Management							
5.1	Identify	Establish and Maintain an Inventory of Accounts	Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	X	X	X	Yes	Verve has a very robust user and account tracking capability. We share admin, dormant, expired or shared accounts through our reporting dashboard to assess and review access needs and practices. We also rename, disable or otherwise help to manage those accounts as well
5.2	Protect	Use Unique Passwords	Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	X	X	X	Yes	Verve tracks password complexity and identifies dormant accounts, share logins etc.
5.3	Respond	Disable Dormant Accounts	Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	X	X	X	Yes	This can be done automatically but rarely is within OT. We bring these accounts to our clients' attention and use our tech to disable/delete, but these are usually done in conjunction with operational staff at the specific asset under controlled circumstances.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
5.4	Protect	Restrict Administrator Privileges to Dedicated Administrator Accounts	Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	X	X	X	Yes	Verve supports this type of analysis and alerting but does not usually enforce or automate any specific actions due to an abundance of concern for OT safety.
5.5	Identify	Establish and Maintain an Inventory of Service Accounts	Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.		X	X	Yes	Verve lists all manner of accounts (not just AD created ones - we extend to local/workgroup account management well).
5.6	Protect	Centralize Account Management	Centralize account management through a directory or identity service.		X	X	N/A	We enumerate and help manage accounts including environments where a directory or identity service is not available.
6	**Access Control Management**							
6.1	Protect	Establish an Access Granting Process	Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	X	X	X	Supports	Verve supports, through its detailed system and operational data, the assets that require specific user/role access and which do not. We report on access per system as needed to define and administer policies such as this.
6.2	Protect	Establish an Access Revoking Process	Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	X	X	X	Supports	Verve supports, through its detailed system and operational data, the assets that require specific user/role access and which do not. We report on access per system as needed to define and administer policies such as this.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
6.3	Protect	Require MFA for Externally-Exposed Applications	Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.	X	X	X	Supports	Verve focuses on assets internal to the operational environment. External access is outside of our scope. Verve can track use of remote access by user and system and add system level logging to monitor what remote users are doing to a specific asset.
6.4	Protect	Require MFA for Remote Network Access	Require MFA for remote network access.	X	X	X	N/A	This is a policy, not a function of software.
6.5	Protect	Require MFA for Administrative Access	Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	X	X	X	N/A	This is a policy, not a function of software.
6.6	Identify	Establish and Maintain an Inventory of Authentication and Authorization Systems	Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.		X	X	N/A	This is a policy, not a function of software.
6.7	Protect	Centralize Access Control	Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		X	X	N/A	This is a policy, not a function of software.
6.8	Protect	Define and Maintain Role-Based Access Control	Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			X	Supports	This is more of a policy than a control but Verve can outline which accounts are present on which assets and show inherited permissions. This type of data helps clients to achieve this control by providing detailed data.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
7	**Continuous Vulnerability Management**							
7.1	Protect	Establish and Maintain a Vulnerability Management Process	Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	X	X	X	Supports	This is a policy but the policy can be developed and managed through Verve data and management capabilities.
7.2	Respond	Establish and Maintain a Remediation Process	Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.	X	X	X	Supports	This is a policy but the policy can be developed and managed through Verve data and management capabilities.
7.3	Protect	Perform Automated Operating System Patch Management	Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	X	X	X	Yes	Verve provides automated patching, but in OT, it is usually more gradual and hands-on which Verve is purpose built for. With our platform our clients pre-load OS patches, test at their leisure and update as required. We provide the ability to deploy compensating controls to a system when a patch is not yet tested. A control such as disabling remote desktop access or the guest account if the BlueKeep patch can't be deployed.
7.4	Protect	Perform Automated Application Patch Management	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	X	X	X	Yes	Verve deploys the same type of automated or staged deployment for application updates as for OS based patching as needed.
7.5	Identify	Perform Automated Vulnerability Scans of Internal Enterprise Assets	Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		X	X	Yes	Verve is an improvement on this requirement. We do not scan assets so are safer for OT plus we regularly map vulnerabilities to our asset database. This means Verve clients get a one-to-one mapping of all vulnerabilities in OT (including embedded devices) as frequently as the risk data updates as opposed to large time gaps between scans that most vulnerability scanning tools are subject to.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
7.6	Identify	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.		X	X	N/A	OT does not (should not) have externally exposed assets. However if a client does have such assets, Verve provides the same real-time scanning of vulnerabilities all other assets benefit from.
7.7	Respond	Remediate Detected Vulnerabilities	Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.		X	X	Yes	Verve provides OS or application patching. With our platform clients pre-load updates, test at their leisure and update as required. We provide the ability to deploy compensating controls to a system when a patch is not yet tested. A control such as disabling remote desktop access or the guest account if the BlueKeep patch can't be deployed.
8	**Audit Log Management**							
8.1	Protect	Establish and Maintain an Audit Log Management Process	Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	X	X	X	Supports	This is a process, not a software feature, but Verve lists which systems are capable of (or not) providing logs to Verve or a corporate system. We also alert when those logs fail to be received and/or if those logs indicate compromise.
8.2	Detect	Collect Audit Logs	Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	X	X	X	Yes	Verve tracks which systems send logs and which are technically incapable of doing so for future project/upgrade opportunities.
8.3	Protect	Ensure Adequate Audit Log Storage	Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	X	X	X	Supports	This is more of a procedure, but Verve monitors system health including network card use, hard drive storage space/health in support of this requirement.
8.4	Protect	Standardize Time Synchronization	Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		X	X	N/A	This is a service Verve can provide but is not part of our software capabilities.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
8.5	Detect	Collect Detailed Audit Logs	Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		X	X	Yes	Verve has a robust host-based intrusion detection capability which includes transactional data about the activity and deep asset data itself to provide OT context to the assets in scope.
8.6	Detect	Collect DNS Query Audit Logs	Collect DNS query audit logs on enterprise assets, where appropriate and supported.		X	X	No	Verve does not do this but integrates with network monitoring tools that do.
8.7	Detect	Collect URL Request Audit Logs	Collect URL request audit logs on enterprise assets, where appropriate and supported.		X	X	No	Verve does not do this.
8.8	Detect	Collect Command-Line Audit Logs	Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.		X	X	Yes	Verve collects command line audit logs.
8.9	Detect	Centralize Audit Logs	Centralize, to the extent possible, audit log collection and retention across enterprise assets.		X	X	Yes	The host-based data we collect (syslog, netflow, system health, event logs, etc.) is streamed to a central storage and analysis location.
8.10	Protect	Retain Audit Logs	Retain audit logs across enterprise assets for a minimum of 90 days.		X	X	Yes	This is supported.
8.11	Detect	Conduct Audit Log Reviews	Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		X	X	Yes	Verve has nearly 300 anomaly detection and SIEM based threshold alerts it monitors in real-time from the data it gets.
8.12	Detect	Collect Server Provider Logs	Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events.			X	Yes	Because Verve collects event logs from the hosts themselves we are able to collect all of these types of alerts as well as many others.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
9	Email and Web Browser Protections							
9.1	Protect	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	X	X	X	Yes	Verve lists and alerts to what browser is in place and being used on specific systems. While we enforce this standard in OT, we stop short of enforcement as some legacy software applications may require a browser that is not an enterprise standard but is critical to safe operations.
9.2	Protect	Use DNS Filtering Services	Use DNS filtering services on all enterprise assets to block access to known malicious domains.	X	X	X	Supports	Typically OT assets do not connect directly to the internet so this is not usually in scope however Verve alerts on communications between assets to/from specific subnets to provide an alerting method for detecting if this activity were to take place.
9.3	Protect	Maintain and Enforce Network-Based URL Filters	Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		X	X	N/A	OT assets do not connect to websites directly.
9.4	Protect	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		X	X	Yes	Verve enumerates and enforces this policy if needed but is usually done under specific circumstances for specific systems only.
9.5	Protect	Implement DMARC	To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.		X	X	N/A	Email is not a tool in use in OT.
9.6	Protect	Block Unnecessary File Types	Block unnecessary file types attempting to enter the enterprise's email gateway.		X	X	Supports	OT actions are usually not automated but rather informed/alerted on to be as 'OT safe' as possible.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
9.7	Protect	Deploy and Maintain Email Server Anti-Malware Protections	Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.			X	N/A	Email is not a tool in use in OT.
10	**Malware Defenses**							
10.1	Protect	Deploy and Maintain Anti-Malware Software	Deploy and maintain anti-malware software on all enterprise assets.	X	X	X	Supports	Verve is not an Anti-malware tool itself but integrates with multiple software offerings. This is particularly valuable to OT practitioners to look at all status regardless of the vendor/software type. In OT multiple software for multiple vendors are typical and an aggregated view is very useful in these situations.
10.2	Protect	Configure Automatic Anti-Malware Signature Updates	Configure automatic updates for anti-malware signature files on all enterprise assets.	X	X	X	Supports	Verve is not an Anti-malware tool itself but integrates with multiple software offerings. This is particularly valuable to OT practitioners to look at all status regardless of the vendor/software type. In OT multiple software for multiple vendors are typical and an aggregated view is very useful in these situations.
10.3	Protect	Disable Autorun and Autoplay for Removable Media	Disable autorun and autoplay auto-execute functionality for removable media.	X	X	X	Supports	Verve supports tracking of whitelisting tools and their status. Verve establishes and/or enforces registry level settings on endpoints like disabling auto-run or other settings as well (like disable USB ports entirely).
10.4	Detect	Configure Automatic Anti-Malware Scanning of Removable Media	Configure anti-malware software to automatically scan removable media.		X	X	No	This is a function of AV software itself and is outside the function/capabilities of Verve.
10.5	Protect	Enable Anti-Exploitation Features	Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		X	X	N/A	Not typically supported in OT environments or assets.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
10.6	Protect	Centrally Manage Anti-Malware Software	Centrally manage anti-malware software.		X	X	N/A	This is not related to Verve functionality but as illustrated above, Verve can aggregate multiple Anti-malware versions/databases into a single risk view
10.7	Detect	Use Behavior-Based Anti-Malware Software	Use behavior-based anti-malware software.		X	X	N/A	This is a policy/feature choice for specific anti-malware software.
11	Data Recovery							
11.1	Recover	Establish and Maintain a Data Recovery Process	Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	X	X	X	Supports	This is a policy but Verve data is instrumental in helping clients decide asset and data criticality so fundamentally informs the creation and adherence to policies such as this.
11.2	Recover	Perform Automated Backups	Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.	X	X	X	Yes	Verve provides tracking of all OS device backups to ensure that backups are run regularly and complete. Verve provides backups for congifurations of network devices and critical OT devices such as protective relays.
11.3	Protect	Protect Recovery Data	Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	X	X	X	N/A	This is a policy/procedure requirement of a backup program in general.
11.4	Recover	Establish and Maintain an Isolated Instance of Recovery Data	Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services.	X	X	X	Supports	As outlined above, Verve directs OT teams to when and where backups should run relative to asset criticality and risk indicators.
11.5	Recover	Test Data Recovery	Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.		X	X	N/A	This is a policy/procedure requirement of a backup program in general.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
12	Network Infrastructure Management							
12.1	Protect	Ensure Network Infrastructure is Up-to-Date	Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.	X	X	X	Supports	Verve enumerates all networking gear including hardware, software, firmware, etc. in support of this type of requirement.
12.2	Protect	Establish and Maintain a Secure Network Architecture	Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		X	X	Supports	Verves data collection and presentation allow our clients to design and enforce network topology and segmentation needs. Verve enables alerts on changes to network protections or where communications breach intended network segmentation.
12.3	Protect	Securely Manage Network Infrastructure	Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.		X	X	Supports	Verve's connectivity to specific networking gear shows current status, running config and hardening parameters to ensure the infrastructure is indeed secure. We incorporate syslog and netflow data to provide detection and alerting capabilities as well.
12.4	Identify	Establish and Maintain Architecture Diagram(s)	Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.		X	X	Yes	Vere's network mapping/topology capabilities shows current connections and interconnections and also drills into specific networking devices and down into endpoint data across multiple security indicators.
12.5	Protect	Centralize Network Authentication, Authorization, and Auditing (AAA)	Centralize network AAA.		X	X	Supports	Verve's data on applications, local users, data flows, etc. help to both design and enforce access requirements.
12.6	Protect	Use of Secure Network Management and Communication Protocols	Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).		X	X	Supports	By tracking ports/services in use on various devices the Verve platform shapes specific protocol and services usage as required.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
12.7	Protect	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure	Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.		X	X	Supports	Verve provides a compelling mix of functionality to audit, monitor, and manage remote access to systems. Without any additional tooling, Verve audits user accounts and their access on a system. Verve also monitors process creation, logins, and remote access offering a log of what a user does when they are on a system down to the CPU and memory usage during their session. These logs go through our detection and machine learning engines to detect malicious behavior like network traversal, credential dumping, etc. during their session. Verve also works with logs from Microsoft Remote Desktop Gateway which allows centralized control of remote desktop access while still benefitting from Verve's detections and anomaly monitoring. Other tools Verve customers use to control remote access include the Web VPN capability from Fortigate and Cisco.
12.8	Protect	Establish and Maintain Dedicated Computing Resources for All Administrative Work	Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.			X	Supports	Verve tracks account use on specific assets to define and enforce this requirement.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
13	Network Monitoring and Defense							
13.1	Detect	Centralize Security Event Alerting	Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.		X	X	Yes	Verve extends logging deep into OT environments then brings them back to a central Verve component where over 265 Alerts/Thresholds are then used to filter and analyze the collected data.
13.2	Detect	Deploy a Host-Based Intrusion Detection Solution	Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.		X	X	Yes	Verve is a host-based intrusion detection system. We collect syslog, netflow, system health, event logs and incorporate AV/Whitelisting alerts and even process event data to be filtered through our 265 SIEM/Threshold and Machine Learning/Anomaly Detection algorithms. We provide alerts along with rich endpoint data.
13.3	Detect	Deploy a Network intrusion Detection Solution	Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.		X	X	Supports	Verve ingests NIDS alerts and feeds to further augment our SIEM/ML capabilities. Network-based alerts are ingested by Verve and related host data is added to the overall analysis capabilities.
13.4	Protect	Perform Traffic Filtering Between Network Segmentations	Perform traffic filtering between network segments, where appropriate.		X	X	Supports	Most OT environments never filter or block but rather monitor and tune manually. Verve monitors through a number of methods (netflow, port/service listings, etc.) which are populated on dashboards or sent via webhook/email to various ticketing systems as needed.
13.5	Protect	Manage Access Control for Remote Assets	Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.		X	X	Yes	In the regulated environment of NERC CIP these are transient cyber assets and are common in OT when a technician brings a laptop to a specific operating environment and/or subnet. Verve uses its agent to track their location and ensure the asset itself is up-to-date on security indicators from vulns to patching to system hardening as required by corporate standards.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
13.6	Detect	Collect Network Traffic Flow Logs	Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.		X	X	Supports	Verve collects and analyzes syslog and netflow data as part of our SIEM/ Machine Learning capabilities.
13.7	Protect	Deploy a Host-Based Intrusion Prevention Solution	Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.			X	Yes	Verve is a host-based intrusion detection system. We collect syslog, netflow, system health, event logs and incorporate AV/Whitelisting alerts and process event data to be filtered through our 265 SIEM/Threshold and Machine Learning/Anomaly Detection algorithms. We provide alerts along with rich end point data.
13.8	Protect	Deploy a Network Intrusion Prevention Solution	Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.			X	Supports	Verve integrates with NIDS solutions and adds our rich and diverse host-based data to any of their alerts to provide greater context.
13.9	Protect	Deploy Port-Level Access Control	Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.			X	Supports	Verve monitors ports to ensure controls are enabled.
13.10	Protect	Perform Application Layer Filtering	Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.			X	Supports	Verve monitors for application firewalls or gateways that have been deployed.
13.11	Detect	Tune Security Event Alerting Thresholds	Tune security event alerting thresholds monthly, or more frequently.			X	Yes	Verve has a host of security and threat update capabilities and always sends new algorithms and updates to clients as they emerge.
14	**Security Awareness and Skills Training**							
14.1	Protect	Establish and Maintain a Security Awareness Program	Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.	X	X	X	Supports	Verve data and monitoring is instrumental in providing detailed tracking of various security behaviors which are used for training purposes.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
14.2	Protect	Train Workforce Members to Recognize Social Engineering Attacks	Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.	X	X	X	N/A	This is a process not a software function or feature.
14.3	Protect	Train Workforce Members on Authentication Best Practices	Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.	X	X	X	Supports	Verve data and monitoring is instrumental in providing detailed tracking of various security behaviors which are used for training purposes. In this case, the use of complex passwords, identifying shared logins and minimizing administrative accounts are all part of our capabilities.
14.4	Protect	Train Workforce Members on Data Handling Best Practices	Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.	X	X	X	N/A	This is a process not a software function or feature.
14.5	Protect	Train Workforce Members on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.	X	X	X	Supports	Verve supports alerting and reporting on USB use and/or transient cyber assets in and out of sensitive environments.
14.6	Protect	Train Workforce Members on Recognizing and Reporting Security Incidents	Train workforce members to be able to recognize a potential incident and be able to report such an incident.	X	X	X	Yes	Verve alerting and monitoring is well tuned to bring events to the attention of interested users. We provide context of the alert and are building 'playlists' to accompany events that explain how to react to specific events.
14.7	Protect	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.	X	X	X	Yes	Verve shows any number of security and software/configuration violations in its dynamic dashboard.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
14.8	Protect	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.	X	X	X	N/A	This is a process not a software function or feature.
14.9	Protect	Conduct Role-Specific Security Awareness and Skills Training	Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, OWASP® Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles.		X	X	N/A	This is a process not a software function or feature.
15	Service Provider Management							
15.1	Identify	Establish and Maintain an Inventory of Service Providers	Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.	X	X	X	N/A	This is a process not a software function or feature.
15.2	Identify	Establish and Maintain a Service Provider Management Policy	Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.		X	X	N/A	This is a process not a software function or feature.
15.3	Identify	Classify Service Providers	Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		X	X	N/A	This is a process not a software function or feature.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
15.4	Protect	Ensure Service Provider Contracts Include Security Requirements	Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.		X	X	N/A	This is a process not a software function or feature.
15.5	Identify	Assess Service Providers	Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.			X	N/A	This is a process not a software function or feature.
15.6	Detect	Monitor Service Providers	Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.			X	N/A	This is a process not a software function or feature.
15.7	Identify	Securely Decommission Service Providers	Securely decommission service providers. Example considerations include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.			X	N/A	This is a process not a software function or feature.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
16	Application Software Security							
16.1	Protect	Establish and Maintain a Secure Application Development Process	Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.		X	X	N/A	This is a process for software development which is not a part of OT environments or practices.
16.2	Protect	Establish and Maintain a Process to Accept and Address Software Vulnerabilities	Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.		X	X	N/A	This is a process for software development which is not a part of OT environments or practices.
16.3	Protect	Perform Root Cause Analysis on Security Vulnerabilities	Perform root cause analysis on security vulnerabilities. When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that create vulnerabilities in code, and allows development teams to move beyond just fixing individual vulnerabilities as they arise.		X	X	N/A	This is a process for software development which is not a part of OT environments or practices.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
16.4	Protect	Establish and Manage an Inventory of Third-Party Software Components	Establish and manage an updated inventory of third-party components used in development, often referred to as a "bill of materials," as well as components slated for future use. This inventory is to include any risks that each third-party component could pose. Evaluate the list at least monthly to identify any changes or updates to these components, and validate that the component is still supported.		X	X	N/A	This is a process not a software function or feature.
16.5	Protect	Use Up-to-Date and Trusted Third-Party Software Components	Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.		X	X	N/A	This is a process not a software function or feature.
16.6	Protect	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities	Establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed. This process includes setting a minimum level of security acceptability for releasing code or applications. Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first. Review and update the system and process annually.		X	X	N/A	This is a process not a software function or feature.
16.7	Protect	Use Standard Hardening Configuration Templates for Application Infrastructure	Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.		X	X	N/A	This is a process not a software function or feature.
16.8	Protect	Separate Production and Non-Production Systems	Maintain separate environments for production and non-production systems.		X	X	N/A	This is a process not a software function or feature.
16.9	Protect	Train Developers in Application Security Concepts and Secure Coding	Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training can include general security principles and application security standard practices. Conduct training at least annually and design in a way to promote security within the development team, and build a culture of security among the developers.		X	X	N/A	This is a process not a software function or feature.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
16.10	Protect	Apply Secure Design Principles in Application Architectures	Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.		X	X	N/A	This is a process not a software function or feature.
16.11	Protect	Leverage Vetted Modules or Services for Application Security Components	Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.		X	X	N/A	This is a process not a software function or feature.
16.12	Protect	Implement Code-Level Security Checks	Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.			X	N/A	This is a process not a software function or feature.
16.13	Protect	Conduct Application Penetration Testing	Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.			X	N/A	This is a process not a software function or feature.
16.14	Protect	Conduct Threat Modeling	Conduct threat modeling. Threat modeling is the process of identifying and addressing application security design flaws within a design, before code is created. It is conducted through specially trained individuals who evaluate the application design and gauge security risks for each entry point and access level. The goal is to map out the application, architecture, and infrastructure in a structured way to understand its weaknesses.			X	N/A	This is a process not a software function or feature.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
17	**Incident Response Management**							
17.1	Respond	Designate Personnel to Manage Incident Handling	Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	X	X	X	N/A	This is a process for software development which is not a part of OT environments or practices.
17.2	Respond	Establish and Maintain Contact Information for Reporting Security Incidents	Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.	X	X	X	Supports	Verve records/reports on asset criticality and contact information for specific users. This aids in the development and execution of incident response activities.
17.3	Respond	Establish and Maintain an Enterprise Process for Reporting Incidents	Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	X	X	X	Supports	Verve's data and alerts can be automatically sent to ticketing or CMDB databases to initiate a formal response process.
17.4	Respond	Establish and Maintain an Incident Response Process	Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		X	X	N/A	This is a process not a software function or feature.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
17.5	Respond	Assign Key Roles and Responsibilities	Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		X	X	N/A	This is a process not a software function or feature.
17.6	Respond	Define Mechanisms for Communicating During Incident Response	Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		X	X	N/A	This is a process not a software function or feature.
17.7	Recover	Conduct Routine Incident Response Exercises	Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision making, and workflows. Conduct testing on an annual basis, at a minimum.		X	X	Supports	Verve data is instrumental in designing and tuning an incident response program as well as identifying when key components of a plan or environment are at risk (like failed backups, misconfigured devices, systems offline, etc.)
17.8	Recover	Conduct Post-Incident Reviews	Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.		X	X	N/A	This is a process not a software function or feature.
17.9	Recover	Establish and Maintain Security Incident Thresholds	Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard.			X	N/A	This is a process not a software function or feature.
18	**Penetration Testing**							
18.1	Identify	Establish and Maintain a Penetration Testing Program	Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.		X	X	Supports	Active penetration tests are often risky for OT environments. Verve's comprehensive data allows users to conduct multiple simulated penetrations to determine possible threat vectors not protected.

CIS Control	Security Function	Title	Description	IG1	IG2	IG3	Verve Solution	Comments
18.2	Identify	Perform Periodic External Penetration Tests	Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.		X	X	Supports	Active penetration tests are often risky for OT environments. Verve's comprehensive data allows users to conduct multiple simulated penetrations to determine possible threat vectors not protected.
18.3	Protect	Remediate Penetration Test Findings	Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.		X	X	Yes	Verve is very adept at helping to prioritize and remediate security risks based on its contextual endpoint and transactional data. Pen test findings can be remediated and additional alerts/monitoring components can be added post test via Verve and reported on regularly.
18.4	Protect	Validate Security Measures	Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing.			X	Yes	As part of our continual tuning and evolution of alerting and events this is a natural output for Verve intrusion detection capabilities.
18.5	Identify	Perform Periodic Internal Penetration Tests	Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.			X	Supports	Not typically recommended for OT but Verve alerting and monitoring capabilities detects Pen testing activities.