ResearchSOC

researchsoc.iu.edu
rsoc@iu.edu

Mapping ResearchSOC Services to CIS Top 20

OVERVIEW OF CONTENTS

1. **Service Centric (All Groups) - v8 Controls**

   The new set of 18 CIS Control Groups and Sub-Controls broken down using the key to the right. New controls for v8 are highlighted and a field is included to map the v8 sub-controls to the v7.1 version.

   ResearchSOC enables our clients to jump start their security program by providing or supporting adoption of nearly all Implementation Group 1 controls at the end of initial onboarding. ResearchSOC basic and premium services further allow clients to implement the majority of Implementation Group 2 controls, while the proposed SIMSCI project aims to provide advanced red-teaming capabilities for organizations focused on meeting regulatory or compliance requirements in Implementation Group 3.

2. **Service Centric (All Groups) - v7.1 Controls**

   All CIS Top 20 Control Groups and Sub-Controls broken down using the key to the right. Implementing a baseline control set is a key pillar of implementing a comprehensive security program. ResearchSOC enables our clients to jump start their security program by providing or supporting adoption of nearly all Implementation Group 1 controls at the end of initial onboarding. ResearchSOC basic and premium services further allow clients to implement the majority of Implementation Group 2 controls, while the proposed SIMSCI project aims to provide advanced red-teaming capabilities for organizations focused on meeting regulatory or compliance requirements in Implementation Group 3.

3. **Implementations Group 1**

   This group contains accessible and high value controls representing a set of core defenses that organizations of all resource levels and risk exposure should focus on. Group 1 controls provide effective security value and provide the basis for more sophisticated controls and response.

4. **Implementations Group 2**

   This group contains controls which build upon the IG1 control sets for organizations with more resources and higher risk exposure. These controls enable an organization with dedicated security resources to respond to more complex and specific threats in a proactive manner.

5. **Implementations Group 3**

   This group contains advanced controls which allow organizations with expert security resources to proactively defend against high complexity attacks against specific resources and to protect sensitive data that is subject to regulatory or compliance oversight.

Service Centric (All Groups) - v8 Controls

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3	Covered by RSOC Services?	Relevant Service	Status of Implementation	v7.1 CIS Safeguard
1				**Inventory and Control of Enterprise Assets+E2:E218**	**Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.**							
1	1.1	Devices	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, enterprise 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	ResearchSOC Enables	VIS/OmniSOC/VST	ResearchSOC onboarding will encourage clients to build or update inventory, and provide some information on doing so. Clients may opt to recieve informational reports from ResearchSOC in order to support this process. Virtual Cybersecurity Service at the Virtual Security Team level can provide this	1.4 Maintain Detailed Asset Inventory, 1.5 Maintain Asset Inventory Information, 15.1 Maintain an Inventory of Authorized Wireless Access Points, 9.1 Associate Active Ports, Services, and Protocols to Asset Inventory
1	1.2	Devices	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	ResearchSOC supports	PL/VST	If this is logged on the client's network hardware and provided in feeds to ResearchSOC, it can be provided back as part of a regular (human- or machine-readable) report to the client for maintenance of their inventory.	1.6 Address Unauthorized Assets
1	1.3	Devices	Detect	Utilize an Active Discovery 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	ResearchSOC Supports	VIS/VST	VST can run VIS internal scans in addition to the external scans normally provided by VIS to add another data gathering mechanism.	1.1 Utilize an Active Discovery Tool
1	1.4	Devices	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	ResearchSOC Enables	PL/VST	If this is logged on the client's network hardware and provided in feeds to ResearchSOC, it can be provided back as part of a regular (human- or machine-readable) report to the client for maintenance of their inventory.	1.3 Use DHCP Logging to Update Asset Inventory
1	1.5	Devices	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	ResearchSOC Enables	OmniSOC	Logs from DNS servers and ARP tables from network devices can be analyzed to passively identify assets, producing a regular (human- or machine-readable) report to the client for maintenance of their inventory.	1.2 Use a Passive Asset Discovery Tool, 15.2 Detect Wireless Access Points Connected to the Wired Network
2				**Inventory and Control of Software Assets**	**Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.**							
2	2.1	Applications	Protect	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	ResearchSOC Supports	VST	VST will help client inventory software and draft policies to manage software inventory in the future	2.1 Maintain Inventory of Authorized Software, 2.4 Track Software Inventory Information
2	2.2	Applications	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	ResearchSOC Supports	VST	VST will help client enforce authorized software policies through risk assessment and automated processes.	2.2 Ensure Software is Supported by Vendor
2	2.3	Applications	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	2.6 Address Unapproved Software, 13.4 Only Allow Access to Authorized Cloud Storage or Email Providers

COLOR KEY

⬜ **New CIS Sub-Control**
Sub-control introduced with version 8 of the CIS Controls.

🟩 **ResearchSOC Provides**
ResearchSOC and their partners provide provide tools and services that meet this control with no burden on the client.

🟨 **ResearchSOC Enables**
ResearchSOC collects and/or provides information allowing the client to implement a control to meet the requirement (e.g. OmniSOC collects DNS query logs that can be used to build a passive device inventory).

🟦 **ResearchSOC Supports**
ResearchSOC will advise, coach, and/or train the client to implement and enforce controls.

⬛ **Not Currently Offered**
Controls which are not currently addressed by ResearchSOC in any form.

🟩 **VST (service add-on)**
ResearchSOC Virtual Security Team (VST) members act as an outsourced security team and can consult on, revise, create and enforce policies and procedures to help clients to meet policy or oversight based controls.

🟩 **SIMSCI**
Security Intrusion Modeling for Scientific CyberInfrastructure (SIMSCI) is a proposed red-team service operated by ResearchSOC. SIMSCI will allow organizations to comprehensively test

Service Centric (All Groups) - v8 Controls

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3	Covered by RSOC Services?	Relevant Service	Status of Implementation	v7.1 CIS Safeguard
2	2.4	Applications	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	Not Currently Offered			2.3 Utilize Software Inventory Tools
2	2.5	Applications	Protect	Allowlist Authorized Software	Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		x	x	ResearchSOC Supports	VST	VST will work with client to draft and implement appropriate allowlists to enforce policy	2.7 Utilize Application Whitelisting
2	2.6	Applications	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	ResearchSOC Supports	VST	VST will work with client to draft and implement appropriate allowlists to enforce policy	2.8 Implement Application Whitelisting of Libraries
2	2.7	Applications	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	ResearchSOC Supports	VST	VST will work with client to draft and implement appropriate allowlists to enforce policy	2.9 Implement Application Whitelisting of Scripts, 4.7 Limit Access to Scripting Tools, 7.3 Limit Use of Scripting Languages in Web Browsers and Email Clients
3				**Data Protection**	**Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.**							
3	3.1	Data	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	ResearchSOC Supports	VST	The VST will advise client on drafting data and enforce management policies and processes	New
3	3.2	Data	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	13.1 Maintain an Inventory of Sensitive Information
3	3.3	Data	Protect	Configure Data Access 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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	14.6 Protect Information Through Access Control Lists
3	3.4	Data	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	ResearchSOC Supports	VST	The VST will advise client on drafting data and enforce management policies and processes	New
3	3.5	Data	Identify	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	New, 13.2 Remove Sensitive Data or Systems Not Regularly Accessed by Organization
3	3.6	Devices	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	13.6 Encrypt Mobile Device Data
3	3.7	Data	Identify	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	ResearchSOC Supports	VST	The VST will advise client on drafting data and enforce management policies and processes	New
3	3.8	Data	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	ResearchSOC Supports	VST	The VST will advise client on collecting and documenting data management processes	New
3	3.9	Data	Protect	Encrypt Data on Removable Media	Encrypt data on removable media.		x	x	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	13.7 Manage USB Devices, 13.9 Encrypt Data on USB Storage Devices
3	3.1	Data	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	14.4 Encrypt All Sensitive Information in Transit, 16.5 Encrypt Transmittal of Username and Authentication Credentials, 15.7 Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data

Service Centric (All Groups) - v8 Controls

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3	Covered by RSOC Services?	Relevant Service	Status of Implementation	v7.1 CIS Safeguard
3	3.11	Data	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	14.8 Encrypt Sensitive Information at Rest, 16.4 Encrypt or Hash All Authentication Credentials
3	3.12	Network	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	2.10 Physically or Logically Segregate High Risk Applications, 14.1 Segment the Network Based on Sensitivity
3	3.13	Data	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	Not Currently Offered			14.5 Utilize an Active Discovery Tool to Identify Sensitive Data, 14.7 Enforce Access Control to Data Through Automated Tools, 13.3 Monitor and Block Unauthorized Network Traffic
3	3.14	Data	Detect	Log Sensitive Data Access	Log sensitive data access, including modification and disposal.			x	ResearchSOC Enables	OmniSOC	OmniSOC logs can capture and analyze this data if desired.	14.9 Enforce Detail Logging for Access or Changes to Sensitive Data
4				**Secure Configuration of Enterprise Assets and Software**	**Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).**							
4	4.1	Applications	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	5.1 Establish Secure Configurations, 5.4 Deploy System Configuration Management Tool, 14.3 Disable workstation-to-workstation communication
4	4.2	Network	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	11.1 Maintain Standard Security Configurations for Network Devices, 11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes
4	4.3	Users	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	16.11 Lock Workstation Sessions After Inactivity
4	4.4	Devices	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	9.2 Ensure Only Approved Ports, Protocols, and Services Are Running, 9.4 Apply Host-Based Firewalls or Port-Filtering, 12.4 Deny Communication Over Unauthorized Ports, 11.2 Document Traffic Configuration Rules
4	4.5	Devices	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	9.2 Ensure Only Approved Ports, Protocols, and Services Are Running, 9.4 Apply Host-Based Firewalls or Port-Filtering, 12.4 Deny Communication Over Unauthorized Ports, 11.2 Document Traffic Configuration Rules
4	4.6	Network	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	ResearchSOC Supports	VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	New
4	4.7	Users	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	4.2 Change Default Passwords

Service Centric (All Groups) - v8 Controls

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3	Covered by RSOC Services?	Relevant Service	Status of Implementation	v7.1 CIS Safeguard
4	4.8	Devices	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	New, 9.2 Ensure Only Approved Ports, Protocols, and Services Are Running, 15.6 Disable Peer-to-Peer Wireless Network Capabilities on Wireless Clients, 15.9 Disable Wireless Peripheral Access of Devices, 15.4 Disable Wireless Access on Devices if Not Required
4	4.9	Devices	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	Not Currently Offered			New
4	4.1	Devices	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	New
4	4.11	Devices	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	New
4	4.12	Devices	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	New
5				**Account Management**	**The processes and tools used to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.**							
5	5.1	Users	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	ResearchSOC Supports	VST	VST will advise client and facilitate establishing and maintaining documentation to meet this control	4.1 Maintain Inventory of Administrative Accounts, 16.6 Maintain an Inventory of Accounts
5	5.2	Users	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	4.4 Use Unique Passwords
5	5.3	Users	Respond	Disable Dormant Accounts	Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	x	x	x	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	16.8 Disable Any Unassociated Accounts, 16.9 Disable Dormant Accounts, 16.10 Ensure All Accounts Have An Expiration Date
5	5.4	Users	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	4.3 Ensure the Use of Dedicated Administrative Accounts
5	5.5	Users	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	ResearchSOC Supports	VST	VST will advise client and facilitate establishing and maintaining documentation to meet this control	New, 3.3 Protect Dedicated Assessment Accounts, 20.8 Control and Monitor Accounts Associated With Penetration Testing
5	5.6	Users	Protect	Centralize Account Management	Centralize account management through a directory or identity service.		x	x	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	16.2 Configure Centralized Point of Authentication
6				**Access Control Management**	**The processes and tools used to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.**							
6	6.1	Users	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	New

Service Centric (All Groups) - v8 Controls

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3	Covered by RSOC Services?	Relevant Service	Status of Implementation	v7.1 CIS Safeguard
6	6.2	Users	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	16.7 Establish Process for Revoking Access
6	6.3	Users	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	New, 16.3 Require Multi-Factor Authentication
6	6.4	Users	Protect	Require MFA for Remote Network Access	Require MFA for remote network access.	x	x	x	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	12.11 Require All Remote Logins to Use Multi-Factor Authentication
6	6.5	Users	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	4.5 Use Multi-Factor Authentication for All Administrative Access
6	6.6	Users	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	16.1 Maintain an Inventory of Authentication Systems
6	6.7	Users	Protect	Centralize Access Control	Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		x	x	Not Currently Offered			New
6	6.8	Data	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	Not Currently Offered			New
7				**Continuous Vulnerability Management**	**Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.**							
7	7.1	Applications	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	New
7	7.2	Applications	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	ResearchSOC Provides	VST/VIS	Project Liaisons advise clients on mitigation of found vulnerabilities and can assist with the creation of a risk registry. VST can perform risk assessment and provide registry	New, 3.7 Utilize a Risk-Rating Process, 3.6 Compare Back-to-Back Vulnerability Scans
7	7.3	Applications	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	ResearchSOC Enables	VST	VST will advise client on setting up automated patch management and enforcing compliance	3.4 Deploy Automated Operating System Patch Management Tools
7	7.4	Applications	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	ResearchSOC Enables	VST	VST will advise client on setting up automated patch management and enforcing compliance	3.5 Deploy Automated Software Patch Management Tools, 11.4 Install the Latest Stable Version of Any Security-Related Updates on All Network Devices
7	7.5	Applications	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	ResearchSOC Provides	VST/VIS	VIS scanning fulfills this control when done with firewall rules in place. VST can perform this task.	3.1 Run Automated Vulnerability Scanning Tools, 3.2 Perform Authenticated Vulnerability Scanning, 9.3 Perform Regular Automated Port Scans, 12.2 Scan for Unauthorized Connections Across Trusted Network Boundaries
7	7.6	Applications	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	ResearchSOC Provides	VST/VIS	VIS scanning fulfills this control when done with firewall rules in place. VST can perform this task.	3.1 Run Automated Vulnerability Scanning Tools, 9.3 Perform Regular Automated Port Scans, 12.2 Scan for Unauthorized Connections Across Trusted Network Boundaries
7	7.7	Applications	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	ResearchSOC Supports	PL/VST	PL will advise client on remediated detected vulnerabilites. VST will take active role in facilitating remediation with client.	New

Service Centric (All Groups) - v8 Controls

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3	Covered by RSOC Services?	Relevant Service	Status of Implementation	v7.1 CIS Safeguard
8				**Audit Log Management**	**Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.**							
8	8.1	Network	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	ResearchSOC Provides	OmniSOC/PL	PL and OmniSOC will work with client during onboarding to ensure that all relevant logs are being captured for collection	New
8	8.2	Network	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	ResearchSOC Provides	OmniSOC	Should be actively tracked during the onboarding process so that clients are capturing logs from all identified assets and shipping to Kafka cluster.	6.2 Activate Audit Logging, 8.6 Centralize Anti-Malware Logging
8	8.3	Network	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	ResearchSOC Provides	OmniSOC	OmniSOC sizes the onsite appliance appropriately and maintains records of gathered logs for an extended period.	6.4 Ensure Adequate Storage for Logs
8	8.4	Network	Protect	Standardize Time Synchronization	Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		x	x	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	6.1 Utilize Three Synchronized Time Sources
8	8.5	Network	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	ResearchSOC Enables	OmniSOC	Ensure that security audit is being captured by Kafka and ingested to OmniSOC during the onboarding process.	6.3 Enable Detailed Logging, 4.8 Log and Alert on Changes to Administrative Group Membership, 4.9 Log and Alert on Unsuccessful Administrative Account Login, 16.12 Monitor Attempts to Access Deactivated Accounts
8	8.6	Network	Detect	Collect DNS Query Audit Logs	Collect DNS query audit logs on enterprise assets, where appropriate and supported.		x	x	ResearchSOC Provides	OmniSOC/PL	PL and OmniSOC will ensure adequate data is captured during onboarding	8.7 Enable DNS Query Logging
8	8.7	Network	Detect	Collect URL Request Audit Logs	Collect URL request audit logs on enterprise assets, where appropriate and supported.		x	x	ResearchSOC Provides	OmniSOC	OmniSOC can monitor web requests for malicious sites, but I'm not sure if that's something that is actively monitored/tracked.	7.6 Log All URL Requests
8	8.8	Devices	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	ResearchSOC Provides	OmniSOC	Via elastic endpoint logging (planned)	8.8 Enable Command-Line Audit Logging
8	8.9	Network	Detect	Centralize Audit Logs	Centralize, to the extent possible, audit log collection and retention across enterprise assets.		x	x	ResearchSOC Provides	OmniSOC	OmniSOC monitoring fulfills this requirement.	6.5 Central Log Management
8	8.1	Network	Protect	Retain Audit Logs	Retain audit logs across enterprise assets for a minimum of 90 days.		x	x	ResearchSOC Provides	OmniSOC	OmniSOC monitoring fulfills this requirement.	New
8	8.11	Network	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	ResearchSOC Provides	OmniSOC	OmniSOC provides 24/7/365 eyes on glass monitoring	6.7 Regularly Review Logs
8	8.12	Data	Detect	Collect Service 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	ResearchSOC Enables	OmniSOC	If desired OmniSOC and PL will need to work with client and SP to ensure logs are captured during onboarding	New
9				**Email and Web Browser Protections**	**Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.**							
9	9.1	Applications	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	7.1 Ensure Use of Only Fully Supported Browsers and Email Clients
9	9.2	Network	Protect	Use DNS Filtering Services	Use DNS filtering services on all enterprise assets to block access to known malicious domains.	x	x	x	ResearchSOC Provides	STINGAR	STINGAR active blocking can block known bad IPs in real time using a client's IDS system or optional Black Hole Routing protocol with BGP router.	7.7 Use of DNS Filtering Services, 12.3 Deny Communications With Known Malicious IP Addresses
9	9.3	Network	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	Not Currently Offered			7.4 Maintain and Enforce Network-Based URL Filters, 7.5 Subscribe to URL Categorization Service, 13.4 Only Allow Access to Authorized Cloud Storage or Email Providers

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3	Covered by RSOC Services?	Relevant Service	Status of Implementation	v7.1 CIS Safeguard
9	9.4	Applications	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	7.2 Disable Unnecessary or Unauthorized Browser or Email Client Plugins
9	9.5	Network	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	ResearchSOC Supports	PL/VST	VST will work with system administrators to secure email services with client	7.8 Implement DMARC and Enable Receiver-Side Verification
9	9.6	Network	Protect	Block Unnecessary File Types	Block unnecessary file types attempting to enter the enterprise's email gateway.		x	x	Not Currently Offered			7.9 Block Unnecessary File Types
9	9.7	Network	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	Not Currently Offered			New, 7.10 Sandbox All Email Attachments
10				**Malware Defenses**	**Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.**							
10	10.1	Devices	Protect	Deploy and Maintain Anti-Malware Software	Deploy and maintain anti-malware software on all enterprise assets.	x	x	x	Not Currently Offered			New
10	10.2	Devices	Protect	Configure Automatic Anti-Malware Signature Updates	Configure automatic updates for anti-malware signature files on all enterprise assets.	x	x	x	ResearchSOC Supports	PL/VST	PL will assess client compliance with this control during onboarding and encourage them to adopt appropriate tools	8.2 Ensure Anti-Malware Software and Signatures Are Updated
10	10.3	Devices	Protect	Disable Autorun and Autoplay for Removable Media	Disable autorun and autoplay auto-execute functionality for removable media.	x	x	x	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	8.5 Configure Devices to Not Auto-Run Content
10	10.4	Devices	Detect	Configure Automatic Anti-Malware Scanning of Removable Media	Configure anti-malware software to automatically scan removable media.		x	x	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	8.4 Configure Anti-Malware Scanning of Removable Media
10	10.5	Devices	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies
10	10.6	Devices	Protect	Centrally Manage Anti-Malware Software	Centrally manage anti-malware software.		x	x	Not Currently Offered			8.1 Utilize Centrally Managed Anti-Malware Software
10	10.7	Devices	Detect	Use Behavior-Based Anti-Malware Software	Use behavior-based anti-malware software.		x	x	Not Currently Offered			New
11				**Data Recovery**	**improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.**							
11	11.1	Data	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	New
11	11.2	Data	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	Not Currently Offered			10.1 Ensure Regular Automated Backups, 10.2 Perform Complete System Backups
11	11.3	Data	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	Not Currently Offered			10.4 Protect Backups
11	11.4	Data	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	Not Currently Offered			10.5 Ensure All Backups Have at Least One Offline Backup Destination
11	11.5	Data	Recover	Test Data Recovery	Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.		x	x	Not Currently Offered			10.3 Test Data on Backup Media
12				**Network Infrastructure Management**	**Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.**							
12	12.1	Network	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	11.4 Install the Latest Stable Version of Any Security-Related Updates on All Network Devices

Service Centric (All Groups) - v8 Controls

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3	Covered by RSOC Services?	Relevant Service	Status of Implementation	v7.1 CIS Safeguard
12	12.2	Network	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	New, 15.10 Create Separate Wireless Network for Personal and Untrusted Devices
12	12.3	Network	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
12	12.4	Network	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	ResearchSOC Supports	OmniSOC	OmniSOC will establish this information during onboarding	12.1 Maintain an Inventory of Network Boundaries
12	12.5	Network	Protect	Centralize Network Authentication, Authorization, and Auditing (AAA)	Centralize network AAA.		x	x	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	New
12	12.6	Network	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	New, 15.8 Use Wireless Authentication Protocols That Require Mutual, Multi-Factor Authentication
12	12.7	Devices	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	New
12	12.8	Devices	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	4.6 Use Dedicated Workstations For All Administrative Tasks, 11.6 Use Dedicated Workstations for All Network Administrative Tasks, 11.7 Manage Network Infrastructure Through a Dedicated Network
13				**Network Monitoring and Defense**	**Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.**							
13	13.1	Network	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	ResearchSOC Provides	OmniSOC	OmniSOC monitoring fulfills this requirement.	6.6 Deploy SIEM or Log Analytic Tools
13	13.2	Devices	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	ResearchSOC Provides	OmniSOC	Elastic endpoint monitoring (planned)	New
13	13.3	Network	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	ResearchSOC Supports	PL/VST	Clients should have an IDS already implemented before undergonig RSOC onboarding. RSOC PL and VST will help client configure and integrate IDS with RSOC services.	12.6 Deploy Network-Based IDS Sensors
13	13.4	Network	Protect	Perform Traffic Filtering Between Network Segments	Perform traffic filtering between network segments, where appropriate.		x	x	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	14.2 Enable Firewall Filtering Between VLANs
13	13.5	Devices	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	Not Currently Offered			12.12 Manage All Devices Remotely Logging Into Internal Network, 12.2 Scan for Unauthorized Connections Across Trusted Network Boundaries
13	13.6	Network	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	ResearchSOC Provides	OmniSOC	Netflow, Zeek or Suricata data collected by OmniSOC meet this control	12.8 Deploy NetFlow Collection on Networking Boundary Devices
13	13.7	Devices	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	Not Currently Offered			New
13	13.8	Network	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	Not Currently Offered			12.7 Deploy Network-Based Intrusion Prevention Systems, 15.3 Use a Wireless Intrusion Detection System
13	13.9	Devices	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	Not Currently Offered			1.7 Deploy Port Level Access Control, 1.8 Utilize Client Certificates to Authenticate Hardware Assets
13	13.1	Network	Protect	Perform Application Layer Filtering	Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.			x	Not Currently Offered			9.5 Implement Application Firewalls, 12.9 Deploy Application Layer Filtering Proxy Server, 18.10 Deploy Web Application Firewalls

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3	Covered by RSOC Services?	Relevant Service	Status of Implementation	v7.1 CIS Safeguard
13	13.11	Network	Detect	Tune Security Event Alerting Thresholds	Tune security event alerting thresholds monthly, or more frequently.			x	ResearchSOC Provides	OmniSOC	OmniSOC support team is constantly refining and tuning the SIEM.	6.8 Regularly Tune SIEM
14				**Security Awareness and Skills Training**	**Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.**							
14	14.1	N/A	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	ResearchSOC Provides	VST	RSOC provides webinars regularly, and can perform specific training and security exercises at clients to address specific controls and issues.	17.3 Implement a Security Awareness Program, 17.4 Update Awareness Content Frequently
14	14.2	N/A	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	ResearchSOC Provides	VST	The virtual security team will work to assess and improve client personnel preparedness and awareness	17.6 Train Workforce on Identifying Social Engineering Attacks
14	14.3	N/A	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	ResearchSOC Provides	VST	The virtual security team will work to assess and improve client personnel preparedness and awareness	17.5 Train Workforce on Secure Authentication
14	14.4	N/A	Protect	Train Workforce 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	ResearchSOC Provides	VST	The virtual security team will work to assess and improve client personnel preparedness and awareness	17.7 Train Workforce on Sensitive Data Handling
14	14.5	N/A	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	ResearchSOC Provides	VST	The virtual security team will work to assess and improve client personnel preparedness and awareness	17.8 Train Workforce on Causes of Unintentional Data Exposure
14	14.6	N/A	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	ResearchSOC Provides	VST	The virtual security team will work to assess and improve client personnel preparedness and awareness	17.9 Train Workforce Members on Identifying and Reporting Incidents
14	14.7	N/A	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	ResearchSOC Provides	VST	The virtual security team will work to assess and improve client personnel preparedness and awareness	New
14	14.8	N/A	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	ResearchSOC Provides	VST	The virtual security team will work to assess and improve client personnel preparedness and awareness	New
14	14.9	N/A	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	ResearchSOC Provides	VST	RSOC provides webinars regularly, and can perform specific training and security exercises at clients to address specific controls and issues.	17.2 Deliver Training to Fill the Skills Gap
15				**Service Provider Management**	**Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.**							
15	15.1	N/A	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	New
15	15.2	N/A	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	New

Service Centric (All Groups) - v8 Controls

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3	Covered by RSOC Services?	Relevant Service	Status of Implementation	v7.1 CIS Safeguard
15	15.3	N/A	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	New
15	15.4	N/A	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	Not Currently Offered			New
15	15.5	N/A	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	ResearchSOC Supports	VST	VST will assess service providers and provide recommendations as desired	New
15	15.6	Data	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	ResearchSOC Supports	VST	VST can perform regular review of service providers compliance with implemented policy	New
15	15.7	Data	Protect	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	Not Currently Offered			New
16				**Application Software Security**	**Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.**							
16	16.1	Applications	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	Not Currently Offered			18.1 Establish Secure Coding Practices
16	16.2	Applications	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	Not Currently Offered			18.8 Establish a Process to Accept and Address Reports of Software Vulnerabilities
16	16.3	Applications	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	ResearchSOC Supports	VST	VST will work with client to conduct and document RCA	New
16	16.4	Applications	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	New, 18.3 Verify That Acquired Software Is Still Supported

Service Centric (All Groups) - v8 Controls

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3	Covered by RSOC Services?	Relevant Service	Status of Implementation	v7.1 CIS Safeguard
16	16.5	Applications	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	18.4 Only Use Up-to-Date and Trusted Third-Party Components
16	16.6	Applications	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	ResearchSOC Supports	PL/VST	Project Liaisons advise clients on mitigation of found vulnerabilities and can assist with the creation of a risk registry. VST can perform risk assessment and provide registry	New, 3.7 Utilize a Risk-Rating Process
16	16.7	Applications	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	Not Currently Offered			18.11 Use Standard Hardening Configuration Templates for Databases
16	16.8	Applications	Protect	Separate Production and Non-Production Systems	Maintain separate environments for production and non-production systems.		x	x	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	18.9 Separate Production and Non-Production Systems
16	16.9	Applications	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	18.6 Ensure Software Development Personnel Are Trained in Secure Coding
16	16.1	Applications	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	Not Currently Offered			New, 18.2 Ensure That Explicit Error Checking Is Performed for All In-House Developed Software
16	16.11	Applications	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	ResearchSOC Supports	VST	VST will advise client on drafting and enforcing policy to meet this control and can vet modules on request	New, 18.5 Use only Standardized and Extensively Reviewed Encryption Algorithms
16	16.12	Applications	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	Not Currently Offered			New, 18.7 Apply Static and Dynamic Code Analysis Tools
16	16.13	Applications	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	Not Currently Offered		Possible future service	New
16	16.14	Applications	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	Not Currently Offered		Possible future service	New

Service Centric (All Groups) - v8 Controls

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3	Covered by RSOC Services?	Relevant Service	Status of Implementation	v7.1 CIS Safeguard
17				**Incident Response Management**	**Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.**							
17	17.1	N/A	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	19.3 Designate Management Personnel to Support Incident Handling
17	17.2	N/A	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	19.5 Maintain Contact Information For Reporting Security Incidents
17	17.3	N/A	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	19.4 Devise Organization-wide Standards For Reporting Incidents, 19.6 Publish Information Regarding Reporting Computer Anomalies and Incidents
17	17.4	N/A	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	ResearchSOC Provides	VST	The VST will work with client to draft and implement an IRP	19.1 Document Incident Response Procedures
17	17.5	N/A	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	19.2 Assign Job Titles and Duties for Incident Response
17	17.6	N/A	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	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy	New
17	17.7	N/A	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	ResearchSOC Provides	PL/VST	ResearchSOC PL and VST will provide regular incident response training and exercises for clients	19.7 Conduct Periodic Incident Scenario Sessions for Personnel
17	17.8	N/A	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	ResearchSOC Provides	PL/VST		New
17	17.9	N/A	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	ResearchSOC Provides	VST		19.8 Create Incident Scoring and Prioritization Schema
18				**Penetration Testing**	**Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.**							

Service Centric (All Groups) - v8 Controls

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3	Covered by RSOC Services?	Relevant Service	Status of Implementation	v7.1 CIS Safeguard
18	18.1	N/A	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	Not Currently Offered		Possible future offering	20.1 Establish a Penetration Testing Program
18	18.2	Network	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	Not Currently Offered		Possible future offering	20.2 Conduct Regular External and Internal Penetration Tests, 20.3 Perform Periodic Red Team Exercises, 20.4 Include Tests for Presence of Unprotected System Information and Artifacts
18	18.3	Network	Protect	Remediate Penetration Test Findings	Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.		x	x	Not Currently Offered		Possible future offering	New, 3.7 Utilize a Risk-Rating Process
18	18.4	Network	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	Not Currently Offered		Possible future offering	New
18	18.5	N/A	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	Not Currently Offered		Possible future offering	20.2 Conduct Regular External and Internal Penetration Tests, 20.3 Perform Periodic Red Team Exercises

Service Centric (All Groups) - v7.1 Controls

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
Basic	**2**	**1**	**Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.**			*See the following descriptions at the 1.X level.*
	2	1.1	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.	ResearchSOC Supports	VIS / VST	VST can run VIS internal scans in addition to the external scans normally provided by VIS to add another data gathering mechanism.
	3	1.2	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.	ResearchSOC Enables	OmniSOC	Logs from DNS servers and ARP tables from network devices can be analyzed to passively identify assets, producing a regular (human- or machine-readable) report to the client for maintenance of their inventory.
	2	1.3	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.	ResearchSOC Enables	OmniSOC	If this is logged on the client's network hardware and provided in feeds to ResearchSOC, it can be provided back as part of a regular (human- or machine-readable) report to the client for maintenance of their inventory.
	1	1.4	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.	ResearchSOC Enables	VIS/OmniSOC / VST	ResearchSOC onboarding will encourage clients to build or update inventory, and provide some information on doing so. Clients may opt to recieve informational reports from ResearchSOC in order to support this process. Virtual Cybersecurity Service at the Virtual Security Team level can provide this
	2	1.5	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.	Not Currently Offered		Possible future VST function at mature clients
	1	1.6	Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	1.7	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.	Not Currently Offered		
	3	1.8	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.	Not Currently Offered		
Basic		**2**	**Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.**			*See the following descriptions at the 2.X level.*
	1	2.1	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.	ResearchSOC Supports	VST	
	1	2.2	Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.	ResearchSOC Supports	VST	
	2	2.3	Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.	Not Currently Offered		
	2	2.4	The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.	Not Currently Offered		

COLOR KEY

■ **ResearchSOC Provides**
ResearchSOC and their partners provide provide tools and services that meet this control with no burden on the client.

■ **ResearchSOC Enables**
ResearchSOC collects and/or provides information allowing the client to implement a control to meet the requirement (e.g. OmniSOC collects DNS query logs that can be used to build a passive device inventory).

■ **ResearchSOC Supports**
ResearchSOC will advise, coach, and/or train the client to implement and enforce controls.

■ **Not Currently Offered**
Controls which are not currently addressed by ResearchSOC in any form.

■ **VST (service add-on)**
ResearchSOC Virtual Security Team (VST) members act as an outsourced security team and can consult on, revise, create and enforce policies and procedures to help clients to meet policy or oversight based controls.

■ **SIMSCI**
Security Intrusion Modeling for Scientific CyberInfrastructure (SIMSCI) is a proposed red-team service operated by ResearchSOC. SIMSCI will allow organizations to comprehensively test all aspects of their security posture in real world conditions, through advanced penetration testing and threat intelligence modeling.

Service Centric (All Groups) - v7.1 Controls

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
	3	2.5	The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.	Not Currently Offered		
	1	2.6	Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	ResearchSOC Supports	VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	2.7	Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.	Not Currently Offered		
	3	2.8	The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc) are allowed to load into a system process.	Not Currently Offered		
	3	2.9	The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1,,*.py, macros, etc) are allowed to run on a system.	Not Currently Offered		
	3	2.10	Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incur higher risk for the organization.	Not Currently Offered		
Basic		**3**	**Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.**			*See the following descriptions at the 3.X level.*
	2	3.1	Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.	ResearchSOC Provides	VIS/VST	VIS scanning partially fulfills this control when done with firewall rules in place. VST can perform this task.
	2	3.2	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.	ResearchSOC Provides	VST	VIS is currently set up to do remote scanning only. VST can perform internal scanning for clients
	2	3.3	Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.	ResearchSOC Supports	VST	VST can assist client with drafting and enforcing relevant policy
	1	3.4	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	ResearchSOC Provides	VST	Patch management
	1	3.5	Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	ResearchSOC Provides	VST	Patch management
	2	3.6	Regularly compare the results from back-to-back vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.	ResearchSOC Provides	VST	Project Liaisons perform this task when reveiwing VIS scans and preparing client results.
	2	3.7	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.	ResearchSOC Provides	VST	Project Liaisons advise clients on mitigation of found vulnerabilities and can assist with the creation of a risk registry. VST can perform risk assessment and provide registry
Basic		**4**	**The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.**			*See the following descriptions at the 4.X level.*
	2	4.1	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.	Not Currently Offered		Consider as possible VST function for the future in more mature clients
	1	4.2	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy

Service Centric (All Groups) - v7.1 Controls

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
	1	4.3	Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	4.4	Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	4.5	Use multi-factor authentication and encrypted channels for all administrative account access.	Not Currently Offered		
	1	4.6	Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	4.7	Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	4.8	Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.	ResearchSOC Enables	OmniSOC	Ensure that security audit is being captured by Kafka and ingested to OmniSOC during the onboarding process.
	2	4.9	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.	ResearchSOC Enables	OmniSOC	Ensure that security audit is being captured by Kafka and ingested to OmniSOC during the onboarding process.
Basic		**5**	**Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.**			*See the following descriptions at the 5.X level.*
	1	5.1	Maintain documented, standard security configuration standards for all authorized operating systems and software.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	5.2	Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	5.3	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	5.4	Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.	Not Currently Offered		
	2	5.5	Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.	Not Currently Offered		
Basic		**6**	**Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.**			*See the following descriptions at the 6.X level.*
	2	6.1	Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy

Service Centric (All Groups) - v7.1 Controls

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
	1	6.2	Ensure that local logging has been enabled on all systems and networking devices.	ResearchSOC Provides	OmniSOC	Should be actively tracked during the onboarding process so that clients are capturing logs from all identified assets and shipping to Kafka cluster.
	2	6.3	Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.	ResearchSOC Provides	OmniSOC	Ensure logging levels are accurate with client and OmniSOC during the onboarding process.
	2	6.4	Ensure that all systems that store logs have adequate storage space for the logs generated.	ResearchSOC Provides	OmniSOC	OmniSOC sizes the onsite appliance appropriately and maintains records of gathered logs for an extended period.
	2	6.5	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.	ResearchSOC Provides	OmniSOC	OmniSOC monitoring fulfills this requirement.
	2	6.6	Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.	ResearchSOC Provides	OmniSOC	OmniSOC monitoring fulfills this requirement.
	2	6.7	On a regular basis, review logs to identify anomalies or abnormal events.	ResearchSOC Provides	OmniSOC	OmniSOC provides 24/7/365 eyes on glass monitoring
	3	6.8	On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.	ResearchSOC Provides	OmniSOC	OmniSOC engineers tune and revisit site baselines on a regular basis.
Foundational		**7**	**Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.**			*See the following descriptions at the 7.X level.*
	1	7.1	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	7.2	Uninstall or disable any unauthorized browser or email client plugins or add-on applications.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	7.3	Ensure that only authorized scripting languages are able to run in all web browsers and email clients.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	7.4	Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.	Not Currently Offered		
	2	7.5	Subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.	Not Currently Offered		
	2	7.6	Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.	ResearchSOC Provides	OmniSOC	OmniSOC can monitor web requests for malicious sites, but I'm not sure if that's something that is actively monitored/tracked.
	1	7.7	Use DNS filtering services to help block access to known malicious domains.	ResearchSOC Provides	STINGAR	STINGAR active blocking can block known bad IPs in real time using a client's IDS system or optional Black Hole Routing protocol with BGP router.
	2	7.8	To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail(DKIM) standards.	ResearchSOC Supports	VST	VST will work with system administrators to secure email services with client
	2	7.9	Block all e-mail attachments entering the organization's e-mail gateway if the file types are unnecessary for the organization's business.	Not Currently Offered		
	3	7.10	Use sandboxing to analyze and block inbound email attachments with malicious behavior.	Not Currently Offered		

Service Centric (All Groups) - v7.1 Controls

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
Foundational		**8**	**Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.**			*See the following descriptions at the 8.X level.*
	2	8.1	Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.	Not Currently Offered		PL will assess client compliance with this control during onboardin and encourage them to adopt appropriate tools
	1	8.2	Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	Not Currently Offered		PL will assess client compliance with this control during onboardin and encourage them to adopt appropriate tools
	2	8.3	Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	1	8.4	Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	1	8.5	Configure devices to not auto-run content from removable media.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	8.6	Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.	ResearchSOC Provides	OmniSOC	Configure monitoring of anti-malware during onboarding and capture logs for OmniSOC
	2	8.7	Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.	ResearchSOC Provides	OmniSOC	PL and OmniSOC will ensure adequate data is captured during onboarding
	2	8.8	Enable command-line audit logging for command shells, such as Microsoft Powershell and Bash.	ResearchSOC Provides	OmniSOC	Possible future implementation vis elastic endpoint monitoring
Foundational		**9**	**Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.**			*See the following descriptions at the 9.X level.*
	2	9.1	Associate active ports, services and protocols to the hardware assets in the asset inventory.	ResearchSOC Provides	VST	
	2	9.2	Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	9.3	Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.	ResearchSOC Enables	VIS	VIS scans all ports on connected IPs, clients will need to implement their own monitoring/alerting
	1	9.4	Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	9.5	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.	Not Currently Offered		
Foundational		**10**	**The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.**			*See the following descriptions at the 10.X level.*
	1	10.1	Ensure that all system data is automatically backed up on regular basis.	Not Currently Offered		All Group 10 controls not offered at this time, PL should asses client's ability to enforce these controls operationally during onboarding and encourage them to implement group 1 and 2 controls where possible
	1	10.2	Ensure that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.	Not Currently Offered		
	2	10.3	Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.	Not Currently Offered		

Service Centric (All Groups) - v7.1 Controls

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
	1	10.4	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.	Not Currently Offered		
	1	10.5	Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.	Not Currently Offered		
Foundational		**11**	**Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.**			*See the following descriptions at the 11.X level.*
	2	11.1	Maintain standard, documented security configuration standards for all authorized network devices.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	11.2	All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual’s name responsible for that business need, and an expected duration of the need.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	11.3	Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	1	11.4	Install the latest stable version of any security-related updates on all network devices.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	11.5	Manage all network devices using multi-factor authentication and encrypted sessions.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	11.6	Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	11.7	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
Foundational		**12**	**Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.**			*See the following descriptions at the 12.X level.*
	1	12.1	Maintain an up-to-date inventory of all of the organization's network boundaries.	ResearchSOC Supports	OmniSOC	OmniSOC onboarding process.
	2	12.2	Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.	ResearchSOC Provides	SIMSCI	This is dependent on the successful funding of the SIMSCI proposal, otherwise can be consdidere as "ResearchSOC Enables" and provided by the VST team.
	2	12.3	Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries,.	ResearchSOC Provides	STINGAR	Active blocking and policy enforcement
	1	12.4	Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	12.5	Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.	ResearchSOC Provides	OmniSOC	OmniSOC network monitoring fulfills this control.

Service Centric (All Groups) - v7.1 Controls

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
	2	12.6	Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	12.7	Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	12.8	Enable the collection of NetFlow and logging data on all network boundary devices.	ResearchSOC Provides	OmniSOC	OmniSOC considers netflow data superflous if adequate monitoring is in place via Zeek/Corelight
	3	12.9	Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	12.10	Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.	Not Currently Offered		
	2	12.11	Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	12.12	Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.	Not Currently Offered		
Foundational		**13**	**The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.**			*See the following descriptions at the 13.X level.*
	1	13.1	Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	1	13.2	Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	13.3	Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.	Not Currently Offered		
	2	13.4	Only allow access to authorized cloud storage or email providers.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	13.5	Monitor all traffic leaving the organization and detect any unauthorized use of encryption.	ResearchSOC Provides	OmniSOC	OmniSOC can detect unauthorized encryption if configured to do so.
	1	13.6	Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	13.7	If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	13.8	Configure systems not to write data to external removable media, if there is no business need for supporting such devices.	Not Currently Offered		
	3	13.9	If USB storage devices are required, all data stored on such devices must be encrypted while at rest.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy

Service Centric (All Groups) - v7.1 Controls

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
Foundational		**14**	**The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.**			*See the following descriptions at the 14.X level.*
	2	14.1	Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	14.2	Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	14.3	Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	14.4	Encrypt all sensitive information in transit.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	14.5	Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider and update the organization's sensitive information inventory.	Not Currently Offered		
	1	14.6	Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	14.7	Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.	Not Currently Offered		
	2	14.8	Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.	Not Currently Offered		
	2	14.9	Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).	ResearchSOC Enables	OmniSOC	OmniSOC logs can capture and analyze this data if desired.
Foundational		**15**	**The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANs), access points, and wireless client systems.**			*See the following descriptions at the 15.X level.*
	2	15.1	Maintain an inventory of authorized wireless access points connected to the wired network.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	15.2	Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.	Not Currently Offered		
	2	15.3	Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network.	Not Currently Offered		
	3	15.4	Disable wireless access on devices that do not have a business purpose for wireless access.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	15.5	Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
	3	15.6	Disable peer-to-peer (adhoc) wireless network capabilities on wireless clients.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	1	15.7	Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	15.8	Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), that requires mutual, multi-factor authentication.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	15.9	Disable wireless peripheral access of devices (such as Bluetooth and NFC), unless such access is required for a business purpose.	Not Currently Offered		
	1	15.10	Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
Foundational		**16**	**Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.**			*See the following descriptions at the 16.X level.*
	2	16.1	Maintain an inventory of each of the organization's authentication systems, including those located onsite or at a remote service provider.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	16.2	Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	16.3	Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	16.4	Encrypt or hash with a salt all authentication credentials when stored.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	16.5	Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.	ResearchSOC Enables	OmniSOC/VST	OmniSOC monitoring can detect unencrypted credentials and alert client.
	2	16.6	Maintain an inventory of all accounts organized by authentication system.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	16.7	Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	1	16.8	Disable any account that cannot be associated with a business process or business owner.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	1	16.9	Automatically disable dormant accounts after a set period of inactivity.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	16.10	Ensure that all accounts have an expiration date that is monitored and enforced.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	1	16.11	Automatically lock workstation sessions after a standard period of inactivity.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	16.12	Monitor attempts to access deactivated accounts through audit logging.	ResearchSOC Provides	OmniSOC/Assessment	OmniSOC audit logs enabled during onboarding process.
	3	16.13	Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.	Not Currently Offered		
Organizational	**2**	**17**	**For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.**			*See the following descriptions at the 17.X level.*

Service Centric (All Groups) - v7.1 Controls

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
	2	17.1	Perform a skills gap analysis to understand the skills and behaviors workforce members are not adhering to, using this information to build a baseline education roadmap.	ResearchSOC Provides	VST	The virtual security team will work to assess and improve client personnel preparedness and awareness
	2	17.2	Deliver training to address the skills gap identified to positively impact workforce members' security behavior.	ResearchSOC Provides	VST	RSOC provides webinars regularly, and can perform specific training and security exercises at clients to address specific controls and issues.
	1	17.3	Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.	ResearchSOC Provides	VST	RSOC provides webinars regularly, and can perform specific training and security exercises at clients to address specific controls and issues.
	2	17.4	Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards and business requirements.	ResearchSOC Provides	VST	The virtual security team will work to assess and improve client personnel preparedness and awareness
	1	17.5	Train workforce members on the importance of enabling and utilizing secure authentication.	ResearchSOC Provides	VST	The virtual security team will work to assess and improve client personnel preparedness and awareness
	1	17.6	Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams and impersonation calls.	ResearchSOC Provides	VST	The virtual security team will work to assess and improve client personnel preparedness and awareness
	1	17.7	Train workforce on how to identify and properly store, transfer, archive and destroy sensitive information.	ResearchSOC Provides	VST	The virtual security team will work to assess and improve client personnel preparedness and awareness
	1	17.8	Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.	ResearchSOC Provides	VST	The virtual security team will work to assess and improve client personnel preparedness and awareness
	1	17.9	Train employees to be able to identify the most common indicators of an incident and be able to report such an incident.	ResearchSOC Provides	VST	The virtual security team will work to assess and improve client personnel preparedness and awareness
Organizational		**18**	**Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.**			*See the following descriptions at the 18.X level.*
	2	18.1	Establish secure coding practices appropriate to the programming language and development environment being used.	Not Currently Offered		Direct clients to Trusted CI or partners such as SWAMP
	2	18.2	For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.	Not Currently Offered		Direct clients to Trusted CI or partners such as SWAMP
	2	18.3	Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	18.4	Only use up-to-date and trusted third-party components for the software developed by the organization.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	18.5	Use only standardized and extensively reviewed encryption algorithms.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	18.6	Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	18.7	Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.	Not Currently Offered		Direct clients to Trusted CI or partners such as SWAMP
	2	18.8	Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group.	Not Currently Offered		Direct clients to Trusted CI or partners such as SWAMP

Service Centric (All Groups) - v7.1 Controls

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
	2	18.9	Maintain separate environments for production and nonproduction systems. Developers should not have unmonitored access to production environments.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	18.10	Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.	Not Currently Offered		
	2	18.11	For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.	Not Currently Offered		
Organizational		**19**	**Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.**			*See the following descriptions at the 19.X level.*
	1	19.1	Ensure that there are written incident response plans that defines roles of personnel as well as phases of incident handling/management.	ResearchSOC Provides	VST	VST. Optional
	2	19.2	Assign job titles and duties for handling computer and network incidents to specific individuals and ensure tracking and documentation throughout the incident through resolution.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	1	19.3	Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	19.4	Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	1	19.5	Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and ISAC partners.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	1	19.6	Publish information for all workforce members, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	19.7	Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real world threats. Exercises should test communication channels, decision making, and incident responders technical capabilities using tools and data available to them.	ResearchSOC Provides	VST	PL and VST will perform exercises with varying frequency and complexity depending on terms of service
	3	19.8	Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures.	ResearchSOC Provides	VST	PL and VST will perform exercises with varying frequency and complexity depending on terms of service

Service Centric (All Groups) - v7.1 Controls

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
Organizational		**20**	**Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.**			*See the following descriptions at the 20.X level.*
	2	20.1	Establish a program for penetration tests that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks.	ResearchSOC Provides	SIMSCI	
	2	20.2	Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.	ResearchSOC Provides	SIMSCI	
	3	20.3	Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.	ResearchSOC Provides	SIMSCI	
	2	20.4	Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation.	ResearchSOC Provides	SIMSCI	
	2	20.5	Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.	Not Currently Offered		
	2	20.6	Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.	ResearchSOC Provides	SIMSCI	VST. Optional
	3	20.7	Wherever possible, ensure that Red Teams results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.	ResearchSOC Provides	SIMSCI	VST. Optional
	2	20.8	Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy

Implementation Group 1

ResearchSOC

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
	1	1.4	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.	ResearchSOC Enables	VIS/OmniSOC / VST	ResearchSOC onboarding will encourage clients to build or update inventory, and provide some information on doing so. Clients may opt to recieve informational reports from ResearchSOC in order to support this process. Virtual Cybersecurity Service at the Virtual Security Team level can provide this
	2	1.5	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.	Not Currently Offered		Possible future VST function at mature clients
	1	1.6	Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.	ResearchSOC supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	1.7	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.	Not Currently Offered		
	3	1.8	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.	Not Currently Offered		
Basic		**2**	**Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.**			*See the following descriptions at the 2.X level.*
	1	2.1	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.	ResearchSOC Supports	VST	
	1	2.2	Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.	ResearchSOC Supports	VST	
	2	2.3	Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.	Not Currently Offered		
	2	2.4	The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.	Not Currently Offered		
	3	2.5	The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.	Not Currently Offered		
	1	2.6	Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	ResearchSOC Supports	VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	2.7	Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.	Not Currently Offered		
	3	2.8	The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc) are allowed to load into a system process.	Not Currently Offered		
	3	2.9	The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc) are allowed to run on a system.	Not Currently Offered		
	3	2.10	Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incur higher risk for the organization.	Not Currently Offered		

COLOR KEY

🟩 **ResearchSOC Provides**
ResearchSOC and their partners provide provide tools and services that meet this control with no burden on the client.

🟩 **ResearchSOC Enables**
ResearchSOC collects and/or provides information allowing the client to implement a control to meet the requirement (e.g. OmniSOC collects DNS query logs that can be used to build a passive device inventory).

🟦 **ResearchSOC Supports**
ResearchSOC will advise, coach, and/or train the client to implement and enforce controls.

⬛ **Not Currently Offered**
Controls which are not currently addressed by ResearchSOC in any form.

🟩 **VST (service add-on)**
ResearchSOC Virtual Security Team (VST) members act as an outsourced security team and can consult on, revise, create and enforce policies and procedures to help clients to meet policy or oversight based controls.

🟩 **SIMSCI**
Security Intrusion Modeling for Scientific CyberInfrastructure (SIMSCI) is a proposed red-team service operated by ResearchSOC. SIMSCI will allow organizations to comprehensively test all aspects of their security posture in real world conditions, through advanced penetration testing and threat intelligence modeling.

Implementation Group 1

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
Basic		**3**	**Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.**			*See the following descriptions at the 3.X level.*
	2	3.1	Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.	ResearchSOC Provides	VIS/VST	VIS scanning partially fulfills this control when done with firewall rules in place. VST can perform this task.
	2	3.2	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.	ResearchSOC Provides	VST	VIS is currently set up to do remote scanning only. VST can perform internal scanning for clients
	2	3.3	Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.	ResearchSOC Supports	VST	VST can assist client with drafting and enforcing relevant policy
	1	3.4	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	ResearchSOC Provides	VST	Patch management
	1	3.5	Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	ResearchSOC Provides	VST	Patch management
	2	3.6	Regularly compare the results from back-to-back vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.	ResearchSOC Provides	PL	Project Liaisons perform this task when reveiwing VIS scans and preparing client results.
	2	3.7	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.	ResearchSOC Provides	VST	Project Liaisons advise clients on mitigation of found vulnerabilities and can assist with the creation of a risk registry. VST can perform risk assessment and provide registry
Basic		**4**	**The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.**			*See the following descriptions at the 4.X level.*
	2	4.1	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.	Not Currently Offered		Consider as possible VST function for the future in more mature clients
	1	4.2	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	1	4.3	Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	4.4	Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	4.5	Use multi-factor authentication and encrypted channels for all administrative account access.	Not Currently Offered		
	1	4.6	Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	4.7	Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy

Implementation Group 1

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
	2	4.8	Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.	ResearchSOC Enables	OmniSOC	Ensure that security audit is being captured by Kafka and ingested to OmniSOC during the onboarding process.
	2	4.9	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.	ResearchSOC Enables	OmniSOC	Ensure that security audit is being captured by Kafka and ingested to OmniSOC during the onboarding process.
Basic		**5**	**Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.**			*See the following descriptions at the 5.X level.*
	1	5.1	Maintain documented, standard security configuration standards for all authorized operating systems and software.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	5.2	Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	5.3	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	5.4	Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.	Not Currently Offered		
	2	5.5	Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.	Not Currently Offered		
Basic		**6**	**Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.**			*See the following descriptions at the 6.X level.*
	2	6.1	Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	1	6.2	Ensure that local logging has been enabled on all systems and networking devices.	ResearchSOC Provides	OmniSOC	Should be actively tracked during the onboarding process so that clients are capturing logs from all identified assets and shipping to Kafka cluster.
	2	6.3	Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.	ResearchSOC Provides	OmniSOC	Ensure logging levels are accurate with client and OmniSOC during the onboarding process.
	2	6.4	Ensure that all systems that store logs have adequate storage space for the logs generated.	ResearchSOC Provides	OmniSOC	OmniSOC sizes the onsite appliance appropriately and maintains records of gathered logs for an extended period.
	2	6.5	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.	ResearchSOC Provides	OmniSOC	OmniSOC monitoring fulfills this requirement.
	2	6.6	Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.	ResearchSOC Provides	OmniSOC	OmniSOC monitoring fulfills this requirement.
	2	6.7	On a regular basis, review logs to identify anomalies or abnormal events.	ResearchSOC Provides	OmniSOC	OmniSOC provides 24/7/365 eyes on glass monitoring
	3	6.8	On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.	ResearchSOC Provides	OmniSOC	OmniSOC engineers tune and revisit site baselines on a regular basis.
Foundational		**7**	**Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.**			*See the following descriptions at the 7.X level.*

Implementation Group 1

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
	1	7.1	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	7.2	Uninstall or disable any unauthorized browser or email client plugins or add-on applications.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	7.3	Ensure that only authorized scripting languages are able to run in all web browsers and email clients.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	7.4	Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.	Not Currently Offered		
	2	7.5	Subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.	Not Currently Offered		
	2	7.6	Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.	ResearchSOC Provides	OmniSOC	OmniSOC can monitor web requests for malicious sites, but I'm not sure if that's something that is actively monitored/tracked.
	1	7.7	Use DNS filtering services to help block access to known malicious domains.	ResearchSOC Provides	STINGAR	STINGAR active blocking can block known bad IPs in real time using a client's IDS system or optional Black Hole Routing protocol with BGP router.
	2	7.8	To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail(DKIM) standards.	ResearchSOC Supports	VST	VST will work with system administrators to secure email services with client
	2	7.9	Block all e-mail attachments entering the organization's e-mail gateway if the file types are unnecessary for the organization's business.	Not Currently Offered		
	3	7.10	Use sandboxing to analyze and block inbound email attachments with malicious behavior.	Not Currently Offered		
Foundational		**8**	**Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.**			*See the following descriptions at the 8.X level.*
	2	8.1	Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.	Not Currently Offered		PL will assess client compliance with this control during onboardin and encourage them to adopt appropriate tools
	1	8.2	Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	8.3	Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	1	8.4	Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	1	8.5	Configure devices to not auto-run content from removable media.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	8.6	Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.	ResearchSOC Provides	OmniSOC	Configure monitoring of anti-malware during onboarding and capture logs for OmniSOC
	2	8.7	Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.	ResearchSOC Provides	OmniSOC	PL and OmniSOC will ensure adequate data is captured during onboarding

Implementation Group 1

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
	2	8.8	Enable command-line audit logging for command shells, such as Microsoft Powershell and Bash.	ResearchSOC Provides	OmniSOC	Possible future implementation vis elastic endpoint monitoring
Foundational		**9**	**Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.**			*See the following descriptions at the 9.X level.*
	2	9.1	Associate active ports, services and protocols to the hardware assets in the asset inventory.	ResearchSOC Provides	VST	
	2	9.2	Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	9.3	Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.	ResearchSOC Enables	VIS	VIS scans all ports on connected IPs, clients will need to implement their own monitoring/alerting
	1	9.4	Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	9.5	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.	Not Currently Offered		
Foundational		**10**	**The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.**			*See the following descriptions at the 10.X level.*
	1	10.1	Ensure that all system data is automatically backed up on regular basis.	Not Currently Offered		All Group 10 controls not offered at this time, PL should asses client's ability to enforce these controls operationally during onboarding and encourage them to implement group 1 and 2 controls where possible
	1	10.2	Ensure that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.	Not Currently Offered		
	2	10.3	Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.	Not Currently Offered		
	1	10.4	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.	Not Currently Offered		
	1	10.5	Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.	Not Currently Offered		
Foundational		**11**	**Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.**			*See the following descriptions at the 11.X level.*
	2	11.1	Maintain standard, documented security configuration standards for all authorized network devices.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	11.2	All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	11.3	Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	1	11.4	Install the latest stable version of any security-related updates on all network devices.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	11.5	Manage all network devices using multi-factor authentication and encrypted sessions.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
	2	11.6	Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	11.7	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
Foundational		**12**	**Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.**			*See the following descriptions at the 12.X level.*
	1	12.1	Maintain an up-to-date inventory of all of the organization's network boundaries.	ResearchSOC Supports	OmniSOC	OmniSOC onboarding process.
	2	12.2	Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.	ResearchSOC Provides	SIMSCI	This is dependent on the successful funding of the SIMSCI proposal, otherwise can be considere as "ResearchSOC Enables" and provided by the VST team.
	2	12.3	Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries,.	ResearchSOC Provides	STINGAR	Active blocking and policy enforcement
	1	12.4	Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	12.5	Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.	ResearchSOC Provides	OmniSOC	OmniSOC network monitoring fulfills this control.
	2	12.6	Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	12.7	Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	12.8	Enable the collection of NetFlow and logging data on all network boundary devices.	ResearchSOC Provides	OmniSOC	OmniSOC considers netflow data superflous if adequate monitoring is in place via Zeek/Corelight
	3	12.9	Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	12.10	Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.	Not Currently Offered		
	2	12.11	Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	12.12	Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.	Not Currently Offered		
Foundational		**13**	**The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.**			*See the following descriptions at the 13.X level.*

Implementation Group 1

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
	1	13.1	Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	1	13.2	Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	13.3	Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.	Not Currently Offered		
	2	13.4	Only allow access to authorized cloud storage or email providers.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	13.5	Monitor all traffic leaving the organization and detect any unauthorized use of encryption.	ResearchSOC Provides	OmniSOC	OmniSOC can detect unauthorized encryption if configured to do so.
	1	13.6	Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	13.7	If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	13.8	Configure systems not to write data to external removable media, if there is no business need for supporting such devices.	Not Currently Offered		
	3	13.9	If USB storage devices are required, all data stored on such devices must be encrypted while at rest.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
Foundational		**14**	**The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.**			*See the following descriptions at the 14.X level.*
	2	14.1	Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	14.2	Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	14.3	Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	14.4	Encrypt all sensitive information in transit.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	14.5	Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider and update the organization's sensitive information inventory.	Not Currently Offered		
	1	14.6	Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	14.7	Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.	Not Currently Offered		

Implementation Group 1

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
	2	14.8	Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.	Not Currently Offered		
	2	14.9	Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).	ResearchSOC Enables	OmniSOC	OmniSOC logs can capture and analyze this data if desired.
Foundational		**15**	**The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANs), access points, and wireless client systems.**			*See the following descriptions at the 15.X level.*
	2	15.1	Maintain an inventory of authorized wireless access points connected to the wired network.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	15.2	Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.	Not Currently Offered		
	2	15.3	Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network.	Not Currently Offered		
	3	15.4	Disable wireless access on devices that do not have a business purpose for wireless access.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	15.5	Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	15.6	Disable peer-to-peer (adhoc) wireless network capabilities on wireless clients.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	1	15.7	Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	15.8	Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), that requires mutual, multi-factor authentication.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	15.9	Disable wireless peripheral access of devices (such as Bluetooth and NFC), unless such access is required for a business purpose.	Not Currently Offered		
	1	15.10	Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
Foundational		**16**	**Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.**			*See the following descriptions at the 16.X level.*
	2	16.1	Maintain an inventory of each of the organization's authentication systems, including those located onsite or at a remote service provider.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	16.2	Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	16.3	Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	16.4	Encrypt or hash with a salt all authentication credentials when stored.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	16.5	Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.	ResearchSOC Enables	OmniSOC/VST	OmniSOC monitoring can detect unencrypted credentials and alert client.
	2	16.6	Maintain an inventory of all accounts organized by authentication system.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	16.7	Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy

Implementation Group 1

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
	1	16.8	Disable any account that cannot be associated with a business process or business owner.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	1	16.9	Automatically disable dormant accounts after a set period of inactivity.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	16.10	Ensure that all accounts have an expiration date that is monitored and enforced.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	1	16.11	Automatically lock workstation sessions after a standard period of inactivity.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	16.12	Monitor attempts to access deactivated accounts through audit logging.	ResearchSOC Provides	OmniSOC/Assessment	OmniSOC audit logs enabled during onboarding process.
	3	16.13	Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.	Not Currently Offered		
Organizational	**2**	**17**	**For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.**			*See the following descriptions at the 17.X level.*
	2	17.1	Perform a skills gap analysis to understand the skills and behaviors workforce members are not adhering to, using this information to build a baseline education roadmap.	ResearchSOC Provides	VST	The virtual security team will work to assess and improve client personnel preparedness and awareness
	2	17.2	Deliver training to address the skills gap identified to positively impact workforce members' security behavior.	ResearchSOC Provides	VST	RSOC provides webinars regularly, and can perform specific training and security exercises at clients to address specific controls and issues.
	1	17.3	Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.	ResearchSOC Provides	VST	RSOC provides webinars regularly, and can perform specific training and security exercises at clients to address specific controls and issues.
	2	17.4	Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards and business requirements.	ResearchSOC Provides	VST	The virtual security team will work to assess and improve client personnel preparedness and awareness
	1	17.5	Train workforce members on the importance of enabling and utilizing secure authentication.	ResearchSOC Provides	VST	The virtual security team will work to assess and improve client personnel preparedness and awareness
	1	17.6	Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams and impersonation calls.	ResearchSOC Provides	VST	The virtual security team will work to assess and improve client personnel preparedness and awareness
	1	17.7	Train workforce on how to identify and properly store, transfer, archive and destroy sensitive information.	ResearchSOC Provides	VST	The virtual security team will work to assess and improve client personnel preparedness and awareness
	1	17.8	Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.	ResearchSOC Provides	VST	The virtual security team will work to assess and improve client personnel preparedness and awareness
	1	17.9	Train employees to be able to identify the most common indicators of an incident and be able to report such an incident.	ResearchSOC Provides	VST	The virtual security team will work to assess and improve client personnel preparedness and awareness
Organizational		**18**	**Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.**			*See the following descriptions at the 18.X level.*
	2	18.1	Establish secure coding practices appropriate to the programming language and development environment being used.	Not Currently Offered		Direct clients to Trusted CI or partners such as SWAMP
	2	18.2	For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.	Not Currently Offered		Direct clients to Trusted CI or partners such as SWAMP

Implementation Group 1

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
	2	18.3	Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	18.4	Only use up-to-date and trusted third-party components for the software developed by the organization.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	18.5	Use only standardized and extensively reviewed encryption algorithms.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	18.6	Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	18.7	Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.	Not Currently Offered		Direct clients to Trusted CI or partners such as SWAMP
	2	18.8	Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group.	Not Currently Offered		Direct clients to Trusted CI or partners such as SWAMP
	2	18.9	Maintain separate environments for production and nonproduction systems. Developers should not have unmonitored access to production environments.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	18.10	Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.	Not Currently Offered		
	2	18.11	For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.	Not Currently Offered		
Organizational		**19**	**Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.**			*See the following descriptions at the 19.X level.*
	1	19.1	Ensure that there are written incident response plans that defines roles of personnel as well as phases of incident handling/management.	ResearchSOC Provides	VST	VST. Optional
	2	19.2	Assign job titles and duties for handling computer and network incidents to specific individuals and ensure tracking and documentation throughout the incident through resolution.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	1	19.3	Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	19.4	Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy

Implementation Group 1

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
	1	19.5	Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and ISAC partners.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	1	19.6	Publish information for all workforce members, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	19.7	Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real world threats. Exercises should test communication channels, decision making, and incident responders technical capabilities using tools and data available to them.	ResearchSOC Provides	VST	PL and VST will perform exercises with varying frequency and complexity depending on terms of service
	3	19.8	Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures.	ResearchSOC Provides	VST	PL and VST will perform exercises with varying frequency and complexity depending on terms of service
Organizational		**20**	**Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.**			*See the following descriptions at the 20.X level.*

Implementation Group 2

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
Basic	**2**	**1**	**Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.**			*See the following descriptions at the 1.X level.*
	2	1.1	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.	ResearchSOC Supports	VIS / VST	VST can run VIS internal scans in addition to the external scans normally provided by VIS to add another data gathering mechanism.
	2	1.3	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.	ResearchSOC Enables	OmniSOC	If this is logged on the client's network hardware and provided in feeds to ResearchSOC, it can be provided back as part of a regular (human- or machine-readable) report to the client for maintenance of their inventory.
	2	1.5	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.	Not Currently Offered		Possible future VST function at mature clients
	2	1.7	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.	Not Currently Offered		
Basic		**2**	**Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.**			*See the following descriptions at the 2.X level.*
	2	2.3	Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.	Not Currently Offered		
	2	2.4	The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.	Not Currently Offered		
Basic		**3**	**Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.**			*See the following descriptions at the 3.X level.*
	2	3.1	Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.	ResearchSOC Provides	VIS/VST	VIS scanning partially fulfills this control when done with firewall rules in place. VST can perform this task.
	2	3.2	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.	ResearchSOC Provides	VST	VIS is currently set up to do remote scanning only. VST can perform internal scanning for clients
	2	3.3	Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.	ResearchSOC Supports	VST	VST can assist client with drafting and enforcing relevant policy
	2	3.6	Regularly compare the results from back-to-back vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.	ResearchSOC Provides	PL	Project Liaisons perform this task when reveiwing VIS scans and preparing client results.
	2	3.7	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.	ResearchSOC Provides	VST	Project Liaisons advise clients on mitigation of found vulnerabilities and can assist with the creation of a risk registry. VST can perform risk assessment and provide registry
Basic		**4**	**The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.**			*See the following descriptions at the 4.X level.*

COLOR KEY

■ **ResearchSOC Provides**
ResearchSOC and their partners provide provide tools and services that meet this control with no burden on the client.

■ **ResearchSOC Enables**
ResearchSOC collects and/or provides information allowing the client to implement a control to meet the requirement (e.g. OmniSOC collects DNS query logs that can be used to build a passive device inventory).

■ **ResearchSOC Supports**
ResearchSOC will advise, coach, and/or train the client to implement and enforce controls.

■ **Not Currently Offered**
Controls which are not currently addressed by ResearchSOC in any form.

■ **VST (service add-on)**
ResearchSOC Virtual Security Team (VST) members act as an outsourced security team and can consult on, revise, create and enforce policies and procedures to help clients to meet policy or oversight based controls.

■ **SIMSCI**
Security Intrusion Modeling for Scientific CyberInfrastructure (SIMSCI) is a proposed red-team service operated by ResearchSOC. SIMSCI will allow organizations to comprehensively test all aspects of their security posture in real world conditions, through advanced penetration testing and threat intelligence modeling.

Implementation Group 2

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
	2	4.1	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.	Not Currently Offered		Consider as possible VST function for the future in more mature clients
	2	4.4	Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	4.5	Use multi-factor authentication and encrypted channels for all administrative account access.	Not Currently Offered		
	2	4.7	Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	4.8	Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.	ResearchSOC Enables	OmniSOC	Ensure that security audit is being captured by Kafka and ingested to OmniSOC during the onboarding process.
	2	4.9	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.	ResearchSOC Enables	OmniSOC	Ensure that security audit is being captured by Kafka and ingested to OmniSOC during the onboarding process.
Basic		**5**	**Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.**			*See the following descriptions at the 5.X level.*
	2	5.2	Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	5.3	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	5.4	Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.	Not Currently Offered		
	2	5.5	Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.	Not Currently Offered		
Basic		**6**	**Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.**			*See the following descriptions at the 6.X level.*
	2	6.1	Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	6.3	Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.	ResearchSOC Provides	OmniSOC	Ensure logging levels are accurate with client and OmniSOC during the onboarding process.
	2	6.4	Ensure that all systems that store logs have adequate storage space for the logs generated.	ResearchSOC Provides	OmniSOC	OmniSOC sizes the onsite appliance appropriately and maintains records of gathered logs for an extended period.
	2	6.5	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.	ResearchSOC Provides	OmniSOC	OmniSOC monitoring fulfills this requirement.
	2	6.6	Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.	ResearchSOC Provides	OmniSOC	OmniSOC monitoring fulfills this requirement.
	2	6.7	On a regular basis, review logs to identify anomalies or abnormal events.	ResearchSOC Provides	OmniSOC	OmniSOC provides 24/7/365 eyes on glass monitoring

Implementation Group 2

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
Foundational		**7**	**Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.**			*See the following descriptions at the 7.X level.*
	2	7.2	Uninstall or disable any unauthorized browser or email client plugins or add-on applications.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	7.3	Ensure that only authorized scripting languages are able to run in all web browsers and email clients.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	7.4	Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.	Not Currently Offered		
	2	7.5	Subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.	Not Currently Offered		
	2	7.6	Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.	ResearchSOC Provides	OmniSOC	OmniSOC can monitor web requests for malicious sites, but I'm not sure if that's something that is actively monitored/tracked.
	2	7.8	To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail(DKIM) standards.	ResearchSOC Supports	VST	VST will work with system administrators to secure email services with client
	2	7.9	Block all e-mail attachments entering the organization's e-mail gateway if the file types are unnecessary for the organization's business.	Not Currently Offered		
Foundational		**8**	**Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.**			*See the following descriptions at the 8.X level.*
	2	8.1	Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.	Not Currently Offered		PL will assess client compliance with this control during onboardin and encourage them to adopt appropriate tools
	2	8.3	Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	8.6	Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.	ResearchSOC Provides	OmniSOC	Configure monitoring of anti-malware during onboarding and capture logs for OmniSOC
	2	8.7	Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.	ResearchSOC Provides	OmniSOC	PL and OmniSOC will ensure adequate data is captured during onboarding
	2	8.8	Enable command-line audit logging for command shells, such as Microsoft Powershell and Bash.	ResearchSOC Provides	OmniSOC	Possible future implementation vis elastic endpoint monitoring
Foundational		**9**	**Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.**			*See the following descriptions at the 9.X level.*
	2	9.1	Associate active ports, services and protocols to the hardware assets in the asset inventory.	ResearchSOC Provides	VST	
	2	9.2	Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy

Implementation Group 2

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
	2	9.3	Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.	ResearchSOC Enables	VIS	VIS scans all ports on connected IPs, clients will need to implement their own monitoring/alerting
Foundational		**10**	**The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.**			*See the following descriptions at the 10.X level.*
	2	10.3	Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.	Not Currently Offered		
Foundational		**11**	**Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.**			*See the following descriptions at the 11.X level.*
	2	11.1	Maintain standard, documented security configuration standards for all authorized network devices.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	11.2	All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	11.3	Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	11.5	Manage all network devices using multi-factor authentication and encrypted sessions.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	11.6	Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	11.7	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
Foundational		**12**	**Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.**			*See the following descriptions at the 12.X level.*
	2	12.2	Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.	ResearchSOC Provides	SIMSCI	This is dependent on the successful funding of the SIMSCI proposal, otherwise can be consdidere as "ResearchSOC Enables" and provided by the VST team.
	2	12.3	Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries,.	ResearchSOC Provides	STINGAR	Active blocking and policy enforcement
	2	12.5	Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.	ResearchSOC Provides	OmniSOC	OmniSOC network monitoring fulfills this control.
	2	12.6	Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	12.8	Enable the collection of NetFlow and logging data on all network boundary devices.	ResearchSOC Provides	OmniSOC	OmniSOC considers netflow data superflous if adequate monitoring is in place via Zeek/Corelight
	2	12.11	Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy

Implementation Group 2

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
Foundational		**13**	**The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.**			*See the following descriptions at the 13.X level.*
	2	13.4	Only allow access to authorized cloud storage or email providers.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	13.7	If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
Foundational		**14**	**The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.**			*See the following descriptions at the 14.X level.*
	2	14.1	Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	14.2	Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	14.3	Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	14.4	Encrypt all sensitive information in transit.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	14.7	Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.	Not Currently Offered		
	2	14.8	Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.	Not Currently Offered		
	2	14.9	Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).	ResearchSOC Enables	OmniSOC	OmniSOC logs can capture and analyze this data if desired.
Foundational		**15**	**The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANs), access points, and wireless client systems.**			*See the following descriptions at the 15.X level.*
	2	15.1	Maintain an inventory of authorized wireless access points connected to the wired network.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	15.2	Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.	Not Currently Offered		
	2	15.3	Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network.	Not Currently Offered		
	2	15.8	Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), that requires mutual, multi-factor authentication.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
Foundational		**16**	**Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.**			*See the following descriptions at the 16.X level.*
	2	16.1	Maintain an inventory of each of the organization's authentication systems, including those located onsite or at a remote service provider.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy

Implementation Group 2

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
	2	16.2	Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	16.3	Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	16.4	Encrypt or hash with a salt all authentication credentials when stored.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	16.5	Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.	ResearchSOC Enables	OmniSOC/VST	OmniSOC monitoring can detect unencrypted credentials and alert client.
	2	16.6	Maintain an inventory of all accounts organized by authentication system.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	16.7	Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	16.10	Ensure that all accounts have an expiration date that is monitored and enforced.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	16.12	Monitor attempts to access deactivated accounts through audit logging.	ResearchSOC Provides	OmniSOC/Assessment	OmniSOC audit logs enabled during onboarding process.
Organizational	**2**	**17**	**For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.**			*See the following descriptions at the 17.X level.*
	2	17.1	Perform a skills gap analysis to understand the skills and behaviors workforce members are not adhering to, using this information to build a baseline education roadmap.	ResearchSOC Provides	VST	The virtual security team will work to assess and improve client personnel preparedness and awareness
	2	17.2	Deliver training to address the skills gap identified to positively impact workforce members' security behavior.	ResearchSOC Provides	VST	RSOC provides webinars regularly, and can perform specific training and security exercises at clients to address specific controls and issues.
	2	17.4	Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards and business requirements.	ResearchSOC Provides	VST	The virtual security team will work to assess and improve client personnel preparedness and awareness
Organizational		**18**	**Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.**			*See the following descriptions at the 18.X level.*
	2	18.1	Establish secure coding practices appropriate to the programming language and development environment being used.	Not Currently Offered		Direct clients to Trusted CI or partners such as SWAMP
	2	18.2	For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.	Not Currently Offered		Direct clients to Trusted CI or partners such as SWAMP
	2	18.3	Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	18.5	Use only standardized and extensively reviewed encryption algorithms.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	18.6	Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	18.7	Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.	Not Currently Offered		Direct clients to Trusted CI or partners such as SWAMP

Implementation Group 2

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
	2	18.8	Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group.	Not Currently Offered		Direct clients to Trusted CI or partners such as SWAMP
	2	18.9	Maintain separate environments for production and nonproduction systems. Developers should not have unmonitored access to production environments.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	18.10	Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.	Not Currently Offered		
	2	18.11	For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.	Not Currently Offered		
Organizational		**19**	**Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.**			*See the following descriptions at the 19.X level.*
	2	19.2	Assign job titles and duties for handling computer and network incidents to specific individuals and ensure tracking and documentation throughout the incident through resolution.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	19.4	Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	2	19.7	Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real world threats. Exercises should test communication channels, decision making, and incident responders technical capabilities using tools and data available to them.	ResearchSOC Provides	VST	PL and VST will perform exercises with varying frequency and complexity depending on terms of service
Organizational		**20**	**Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.**			*See the following descriptions at the 20.X level.*
	2	20.1	Establish a program for penetration tests that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks.	ResearchSOC Provides	SIMSCI	
	2	20.2	Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.	ResearchSOC Provides	SIMSCI	
	2	20.4	Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation.	ResearchSOC Provides	SIMSCI	

Implementation Group 2

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
	2	20.5	Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.	Not Currently Offered		
	2	20.6	Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.	ResearchSOC Provides	SIMSCI	VST. Optional
	2	20.8	Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy

Implementation Group 3

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
	3	1.2	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.	ResearchSOC Enables	OmniSOC	Logs from DNS servers and ARP tables from network devices can be analyzed to passively identify assets, producing a regular (human- or machine-readable) report to the client for maintenance of their inventory.
	3	1.8	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.	Not Currently Offered		
Basic		**2**	**Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.**			*See the following descriptions at the 2.X level.*
	3	2.5	The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.	Not Currently Offered		
	3	2.7	Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.	Not Currently Offered		
	3	2.8	The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc) are allowed to load into a system process.	Not Currently Offered		
	3	2.9	The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc) are allowed to run on a system.	Not Currently Offered		
	3	2.10	Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incur higher risk for the organization.	Not Currently Offered		
Basic		**3**	**Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.**			*See the following descriptions at the 3.X level.*
Basic		**4**	**The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.**			*See the following descriptions at the 4.X level.*
Basic		**5**	**Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.**			*See the following descriptions at the 5.X level.*
Basic		**6**	**Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.**			*See the following descriptions at the 6.X level.*
	3	6.8	On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.	ResearchSOC Provides	OmniSOC	OmniSOC engineers tune and revisit site baselines on a regular basis.
Foundational		**7**	**Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.**			*See the following descriptions at the 7.X level.*
	3	7.10	Use sandboxing to analyze and block inbound email attachments with malicious behavior.	Not Currently Offered		
Foundational		**8**	**Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.**			*See the following descriptions at the 8.X level.*

COLOR KEY

🟩	**ResearchSOC Provides** ResearchSOC and their partners provide provide tools and services that meet this control with no burden on the client.
🟩	**ResearchSOC Enables** ResearchSOC collects and/or provides information allowing the client to implement a control to meet the requirement (e.g. OmniSOC collects DNS query logs that can be used to build a passive device inventory).
🟦	**ResearchSOC Supports** ResearchSOC will advise, coach, and/or train the client to implement and enforce controls.
⬛	**Not Currently Offered** Controls which are not currently addressed by ResearchSOC in any form.
■	**VST (service add-on)** ResearchSOC Virtual Security Team (VST) members act as an outsourced security team and can consult on, revise, create and enforce policies and procedures to help clients to meet policy or oversight based controls.
🟩	**SIMSCI** Security Intrusion Modeling for Scientific CyberInfrastructure (SIMSCI) is a proposed red-team service operated by ResearchSOC. SIMSCI will allow organizations to comprehensively test all aspects of their security posture in real world conditions, through advanced penetration testing and threat intelligence modeling.

Implementation Group 3

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
Foundational		**9**	**Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.**			*See the following descriptions at the 9.X level.*
	3	9.5	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.	Not Currently Offered		
Foundational		**10**	**The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.**			*See the following descriptions at the 10.X level.*
Foundational		**11**	**Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.**			*See the following descriptions at the 11.X level.*
Foundational		**12**	**Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.**			*See the following descriptions at the 12.X level.*
	3	12.7	Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	12.9	Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	12.10	Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.	Not Currently Offered		
	3	12.12	Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.	Not Currently Offered		
Foundational		**13**	**The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.**			*See the following descriptions at the 13.X level.*
	3	13.3	Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.	Not Currently Offered		
	3	13.5	Monitor all traffic leaving the organization and detect any unauthorized use of encryption.	ResearchSOC Provides	OmniSOC	OmniSOC can detect unauthorized encryption if configured to do so.
	3	13.8	Configure systems not to write data to external removable media, if there is no business need for supporting such devices.	Not Currently Offered		
	3	13.9	If USB storage devices are required, all data stored on such devices must be encrypted while at rest.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
Foundational		**14**	**The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.**			*See the following descriptions at the 14.X level.*
	3	14.5	Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider and update the organization's sensitive information inventory.	Not Currently Offered		

Implementation Group 3

Type	Implementation Group	Control Number	Control Description	Covered by RSOC Services?	Relevant Service	Status of Implementation
Foundational		**15**	**The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANs), access points, and wireless client systems.**			*See the following descriptions at the 15.X level.*
	3	15.4	Disable wireless access on devices that do not have a business purpose for wireless access.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	15.5	Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	15.6	Disable peer-to-peer (adhoc) wireless network capabilities on wireless clients.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
	3	15.9	Disable wireless peripheral access of devices (such as Bluetooth and NFC), unless such access is required for a business purpose.	Not Currently Offered		
Foundational		**16**	**Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.**			*See the following descriptions at the 16.X level.*
	3	16.13	Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.	Not Currently Offered		
Organizational		**18**	**Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.**			*See the following descriptions at the 18.X level.*
	3	18.4	Only use up-to-date and trusted third-party components for the software developed by the organization.	ResearchSOC Supports	PL/VST	PL will advise client on enforcing this control, the VST will work with client to draft and actively enforce policy
Organizational		**19**	**Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.**			*See the following descriptions at the 19.X level.*
	3	19.8	Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures.	ResearchSOC Provides	VST	PL and VST will perform exercises with varying frequency and complexity depending on terms of service
Organizational		**20**	**Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.**			*See the following descriptions at the 20.X level.*
	3	20.3	Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.	ResearchSOC Provides	SIMSCI	
	3	20.7	Wherever possible, ensure that Red Teams results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.	ResearchSOC Provides	SIMSCI	VST. Optional