CIS TOP 20 CONTROLS

with RedSeal

THE FOUNDATION FOR RESILIENCE

CYBERSECURITY BEST PRACTICES

The Center for Internet Security's Critical Security Controls (CIS Controls) represent global industry best practices for cybersecurity. They are a prioritized and focused set of just 20 recommended cybersecurity actions. These 20 foundational and advanced actions provide the highest pay off to protect against the most common attacks.

While no one product can help with all 20 of the controls, RedSeal's platform can help you implement aspects of 17 of the 20 controls. RedSeal unique ability to model your network and understand all access paths are the foundation for a strong CIS Top 20 based security program.

What follows is a description of how RedSeal maps to each of the CIS Top 20 controls.

THE CENTER FOR INTERNET SECURITY
Critical Security Controls Version 6.1

FAMILY	CONTROL	CONTROL DESCRIPTION	REDSEAL CAPABILITY
Critical Security Control #1: Inventory of Authorized and Unauthorized Devices			
System	**1.1**	Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.	RedSeal's assisted modeling capability actively discovers network devices and determines how they are connected by evaluating their configuration files. From there, RedSeal computes a network model, uncovering previously unknown subnets and devices.
System	**1.3**	Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.	RedSeal can passively and automatically detect new network devices by signaling when anyone modifies existing network configurations (such as new router interfaces and new static routes). With its assisted modeling feature, RedSeal explores your network to identify assets that it doesn't currently know about. It will attempt to add them to the model using known logins. RedSeal also works with vulnerability scanners to put new hosts in the correct network context and assess their risk posture.

CIS TOP 20 CONTROLS WITH REDSEAL

FAMILY	CONTROL	CONTROL DESCRIPTION	REDSEAL CAPABILITY
System	**1.4**	Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.	See Control 1.3
System	**1.5**	Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. The 802.1x must be tied into the inventory data to determine authorized versus unauthorized systems.	Using RedSeal's best practice checks, you can ensure that 802.1X is enabled at the management plane, which interfaces (example, user interfaces) are permitted, and report on violations of this policy.
Critical Security Control #3: Secure Configurations for Hardware and Software			
System	**3.4**	Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.	RedSeal can identify network devices that have protocols such as TELNET and SNMPv1 enabled and listening, and create a report for mitigation. RedSeal's zones and policy feature can also test whether insecure protocols like Telnet or RDP exist in the clear between network zones.

CIS TOP 20 CONTROLS WITH REDSEAL

FAMILY	CONTROL	CONTROL DESCRIPTION	REDSEAL CAPABILITY
System	**3.5**	Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. The reporting system should: have the ability to account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command). These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).	RedSeal can identify when a network device's configuration changes. It uses the term "modified" to represent a change to the configuration. RedSeal maintains a history of configuration files and provides RedSeal users with the opportunity to perform a "diff" on the current configuration with any of the historical configurations.
System	**3.6**	Implement and test an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur. This includes detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system. Whenever possible use tools compliant with the Security Content Automation Protocol (SCAP) in order to streamline reporting and integration.	RedSeal can leverage your organizaton's trusted configuration templates to create custom best practice checks. You'll be able to continuously monitor network devices and identify any deviations from your templates.
Critical Security Control #4: Continuous Vulnerability Assessment and Remediation			
System	**4.1**	Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).	RedSeal ingests vulnerabilty scan data from SCAP compliant and other scanners and adds critical information to the scanner priorities. To severity, asset value, and threats, RedSeal adds access paths and vulnerability location. It can send the resulting prioritized list of your most critical vulnerabilties—along with risk scores—to each responsible system adminstrator.

CIS TOP 20 CONTROLS WITH REDSEAL

FAMILY	CONTROL	CONTROL DESCRIPTION	REDSEAL CAPABILITY
System	**4.2**	Correlate event logs with information from vulnerability scans to fulfill two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools is itself logged. Second, personnel should be able to correlate attack detection events with prior vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable.	For Test 2, RedSeal automatically correlates access from an untrusted network to a given vulnerability. This is referenced as "attack depth" scoring. A system at AD=1 is directly accessible and has a vulnerability listening on the port. If the vulnerability is pivotable, RedSeal automatically calculates downstream risk (DSR). Systems that are accessible to the first system and have a listening vulnerability would be score as AD=2 and so on. An incident responder or forensics expert can use RedSeal's model to reconstruct an attack, identify the accesssible vulnerabilities, and compute potential next targets to establish a potential blast radius for an event. RedSeal's model of your existing network is the fastest way to validate if activity seen in a log is correlated with a known vulnerability along an open network path.
System	**4.7**	Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk. Such acceptance of business risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed, increasing the risk.	RedSeal can compare back to back scanning results to verify that vulnerabilities were addressed by either patching, implementing a compensating control or documenting an exception. RedSeal's vulnerability surpression feature allows you to document and accept a reasonable business risk. The feature can also send automatic reminders for periodic review so you can re-evaluate your decisions as circumstances change. RedSeal's known attack surface report shows change in the known attack surface over time.
System	**4.8**	Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets (example, DMZ servers, internal network servers, desktops, laptops). Apply patches for the riskiest vulnerabilities first. A phased rollout can be used to minimize the impact to the organization. Establish expected patching timelines based on the risk rating level.	RedSeal allows you to segment assets by groups based on topology, asset type, or other criteria. You have access to a number of vulnerability prioritization reports. RedSeal adds the context of location and accessability to a particular system and vulnerability.

CIS TOP 20 CONTROLS WITH REDSEAL

FAMILY	CONTROL	CONTROL DESCRIPTION	REDSEAL CAPABILITY
Critical Security Control #5: Controlled Use of Administrative Privileges			
System	**5.1**	Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.	RedSeal can audit the number of local adminstrative accounts with admin rights. It also automatically audits default admin accounts for the presence of system default passwords. Custom checks can further ensure that devices are using remote access, authorization, and accounting (AAA) services (such as TACACs), and that configurations are aligned with your organization's standard.
System	**5.3**	Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.	RedSeal automatically checks device configurations for the presence of default passwords — and identifies them for administrators to change.
System	**5.5**	Configure systems to issue a log entry and alert on any unsuccessful login to an administrative account.	RedSeal has a custom best practice check to verify login security settings. This is routine practice for customers using a standard secure template.
System	**5.9**	Administrators shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated 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.	This requirement is most often met by dedicating a network segment to machines with administrative access. This zone has specialized access inside the network and no internet access. RedSeal's zones and policy feature can assess whether this has been done correctly.
Critical Security Control #6: Maintenance, Monitoring, and Analysis of Audit Logs			
System	**6.1**	Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.	RedSeal can validate that your team has specified two time sources in the configuration of each network device.
System	**6.2**	Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.	RedSeal can ensure that the audit log settings on each device are consistent with your organization's policies.

CIS TOP 20 CONTROLS WITH REDSEAL

FAMILY	CONTROL	CONTROL DESCRIPTION	REDSEAL CAPABILITY
System	**6.5**	Configure network boundary devices, including firewalls, network-based IPS, and inbound and outbound proxies, to verbosely log all traffic (both allowed and blocked) arriving at the device.	RedSeal can monitor device configurations to make sure they're logging traffic. RedSeal rule check and usage analysis manager, along with audit reports, will flag any ACL that is not logged. The logging configuration for each ACL is available in table format at any time.
System	**6.6**	Deploy a SIEM (Security Information and Event Management) or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis. Using the SIEM tool, system administrators and security personnel should devise profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.	While RedSeal is not an active logging agent, it accelerates incident response after an indicator of compromise has been identifed. With its knowledge of all network paths, RedSeal dramatically reduces the time it takes for incident investigation and containment.
Critical Security Control #7: Email and Web Browser Protections			
System	**7.6**	The organization shall maintain and enforce network based URL filters that limit a system's ability to connect to websites not approved by the organization. The organization shall 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. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.	RedSeal can monitor zone segmentation to ensure that web traffic traverses web proxies. It will send an alert if it finds access that doesn't.
System	**7.8**	Scan and block all e-mail attachments entering the organization's e-mail gateway if they contain malicious code or file types that are unnecessary for the organization's business. This scanning should be done before the e-mail is placed in the user's inbox. This includes e-mail content filtering and web content filtering.	Similar to Control 7.6, RedSeal can ensure that proxy and other devices are "in path" and no access exists that would defeat a monitoring device.
Critical Security Control #8: Malware Defenses			
System	**8.6**	Enable domain name system (DNS) query logging to detect hostname lookup for known malicious C2 domains.	RedSeal can ensure that network objects support a standard configuration profile, including settings for DNS.

CIS TOP 20 CONTROLS WITH REDSEAL

FAMILY	CONTROL	CONTROL DESCRIPTION	REDSEAL CAPABILITY
Critical Security Control #9: Limitation and Control of Network Ports			
System	**9.1**	Ensure that only ports, protocols, and services with validated business needs are running on each system.	The RedSeal model identifies all access paths, including those without current network traffic, by port and protocol. It allows users to query any path based on source, destination, port and protocol. The RedSeal zones and policy feature allows users to create network segmentation and access policies to define, alert, and enforce any access violations of this policy.
System	**9.3**	Perform automated port scans on a regular basis against all key servers and compared to a known effective baseline. If a change that is not listed on the organization's approved baseline is discovered, an alert should be generated and reviewed.	RedSeal can monitor for newly provisioned access to key assets. An increase in network access (ports, protocols, addresses) generates both a policy violation report and an email to a distribution list. This network access analysis is more accurate than an active network port scan, which can miss spots not visible from the scan's location or access opened to an unresponsive service.
System	**9.4**	Verify any server that is visible from the Internet or an untrusted network, and if it is not required for business purposes, move it to an internal VLAN and give it a private address.	RedSeal's access query, whether used ad hoc or as a zone policy, can easily identify hosts exposed to an untrusted network—including the internet, third party vendors, and SaaS services. With these results, you can determine if the access is required for business purposes.
System	**9.5**	Operate critical services on separate physical or logical host machines, such as DNS, file, mail, web, and database servers.	RedSeal can group internal systems by the services they are running and build a segmentation policy from there. You can review reports to ensure that systems are not running multiple services (per the control), and apply access modeling to the policy group to ensure that network controls prohibit other services in the zone from being accessed. For example, a customer can group the web servers together into segmentation zone "Web Servers" and have rules to ensure that SMTP, FTP and SSH are blocked from originating from that zone.

CIS TOP 20 CONTROLS WITH REDSEAL

FAMILY	CONTROL	CONTROL DESCRIPTION	REDSEAL CAPABILITY
System	**9.6**	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized services or traffic should be blocked and an alert generated.	Building on RedSeal's support for Control 9.5, customers can include a rule to ensure that a firewall exists between one zone and another. This is a standard segmentation test that can be applied on inter-zone access policies. You can extend it with an option to ensure the firewalls "must pass all best practice checks". Additionally, RedSeal can help ensure that the firewalls are provisioned with options such as application filtering (Layer 7).
Critical Security Control #10: Data Recovery Capability			
System	**10.1**	Ensure that each system is automatically backed up on at least a weekly basis, and more often for systems storing sensitive information. To help ensure the ability to rapidly restore a system from backup, the operating system, application software, and data on a machine should each be included in the overall backup procedure. These three components of a system do not have to be included in the same backup file or use the same backup software. There should be multiple backups over time, so that in the event of malware infection, restoration can be from a version that is believed to predate the original infection. All backup policies should be compliant with any regulatory or official requirements.	When network devices support automated backup, a RedSeal custom check can ensure compliance with the mandate.
Critical Security Control #11: Secure Configurations for Network Devices			
Network	**11.1**	Compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the organization. The security configuration of such devices should be documented, reviewed, and approved by an organization change control board. Any deviations from the standard configuration or updates to the standard configuration should be documented and approved in a change control system.	RedSeal conducts configuration checks on routers, firewalls and switches. These checks include pre-defined best practices, STIGs and customized checks. The results of each check are fully documented. You can approve these checks and document exceptions with a suppression feature. RedSeal can leverage your organization's trusted configuration templates as a base for custom best practice checks. This enables continuous monitoring of network devices for deviation from your trusted template configurations. Reports of any deviations can be sent to the teams responsible for managing the asset. The report will include the expected settings (remediation) for technicians to implement.

CIS TOP 20 CONTROLS WITH REDSEAL

FAMILY	CONTROL	CONTROL DESCRIPTION	REDSEAL CAPABILITY
Network	**11.2**	All new configuration rules beyond a baseline-hardened configuration that allow traffic to flow through network security devices, such as firewalls and network-based IPS, should be documented and recorded in a configuration management system, with a specific business reason for each change, a specific individual's name responsible for that business need, and an expected duration of the need.	RedSeal's zones and policy feature is designed to track the business justification for all network layer access between zones.
Network	**11.3**	Use automated tools to verify standard device configurations and detect changes. All alterations to such files should be logged and automatically reported to security personnel.	RedSeal's best practices feature allows organizations to define baseline configurations and automatically detect deviations. The results are available in .pdf reports and the RedSeal UI. See Control 11.1
Network	**11.4**	Manage network devices using two-factor authentication and encrypted sessions.	RedSeal custom best practice checks (and STIG checks) can validate that the configuration for an AAA server, such as TACACs, is enabled. The two-factor configuration is on the AAA server. RedSeal can also alert you to devices using non-secure protocols such as TELNET or SNMPv1. RedSeal checks look for unsecure protocols plus access to those protocols from external networks.
Network	**11.5**	Install the latest stable version of any security-related updates on all network devices.	RedSeal can check network devices for the latest stable versions of security updates.
Network	**11.6**	Network engineers shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated 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.	RedSeal can validate that a management segment doesn't have excess access or access to the internet.
Network	**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.	RedSeal can validate that the management network infrastructure across network connections is separated from the business use of that network.

CIS TOP 20 CONTROLS WITH REDSEAL

FAMILY	CONTROL	CONTROL DESCRIPTION	REDSEAL CAPABILITY
Critical Security Control #12: Boundary Defense			
Network	**12.1**	Deny communications with (or limit data flow to) known malicious IP addresses (black lists), or limit access only to trusted sites (whitelists). Tests can be periodically carried out by sending packets from bogon source IP addresses (non-routable or otherwise unused IP addresses) into the network to verify that they are not transmitted through network perimeters. Lists of bogon addresses are publicly available on the Internet from various sources, and indicate a series of IP addresses that should not be used for legitimate traffic traversing the Internet.	RedSeal's zones and policy feature can maintain a list of all blacklisted IP addresses and validate that they do not have access to the network. Since the list of bogon addresses changes over time, organizations can choose to separate this process into three steps: first, making sure that perimeter devices enforce a filter for bogons (via a custom best practice check), second, making sure the bogon content is up to date (either via custom check, or manually), and third, making sure no exit pathways have been missed. The third step is best done as an access query from internal subnets out to the edges. This is much more thorough than injecting sample bits of traffic into the live traffic, which can only cover a tiny fraction of the possible pathways.
Network	**12.2**	On DMZ networks, configure monitoring systems (which may be built in to the IDS sensors or deployed as a separate technology) to record at least packet header information, and preferably full packet header and payloads of the traffic destined for or passing through the network border. This traffic should be sent to a properly configured Security Information Event Management (SIEM) or log analytics system so that events can be correlated from all devices on the network.	RedSeal can ensure that network devices are properly configured to support deployed sensors. This includes determining if commands for SPAN ports and NetFlow (or other flow sampling) are configured. Second, RedSeal's network model enables you to optimally place network sensors and IPS systems to prevent covert or back channels from escaping monitoring.
Network	**12.3**	Deploy network-based IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These network-based IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic.	See Control 12.2

CIS TOP 20 CONTROLS WITH REDSEAL

FAMILY	CONTROL	CONTROL DESCRIPTION	REDSEAL CAPABILITY
Network	**12.5**	Design and implement network perimeters so that all outgoing network traffic to the Internet must pass through at least one application layer filtering proxy server. The proxy should support decrypting network traffic, logging individual TCP sessions, blocking specific URLs, domain names, and IP addresses to implement a black list, and applying whitelists of allowed sites that can be accessed through the proxy while blocking all other sites. Organizations should force outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter.	RedSeal identifies egress points that may not appear on inventory charts, and can identify long-forgotten links. RedSeal identifies which internal networks can reach the different network egress points. This enables security architects to optimally place mitigation and monitoring tools such as an IPS, and to ensure there are no access paths that evade the sensors. Monitoring with RedSeal ensures that no internal networks have external access, that internal networks have access to the proxy, and that the proxy has access to both internal and external networks.
Network	**12.6**	Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication.	RedSeal can validate that VPN termination points (routers, firewalls) are configured for remote authentication and that the remote authentication parameters match the intended servers. RedSeal can identify local accounts that would bypass a remote AAA system and not be compliant with two-factor authentication.
Network	**12.8**	Periodically scan for back-channel connections to the Internet that bypass the DMZ, including unauthorized VPN connections and dual-homed hosts connected to the enterprise network and to other networks via wireless, dial-up modems, or other mechanisms.	As specified in response to Control 12.5, RedSeal can continuously monitor a network for connections that bypass controls. RedSeal model checking heuristics will identify potential “new” egress points (new ISP interface configured) and alert the RedSeal system administrator to classify them as an egress point or a new internal network.
Network	**12.9**	Deploy NetFlow collection and analysis to DMZ network flows to detect anomalous activity.	See Control 12.2
Network	**12.10**	To help identify covert channels exfiltrating data through a firewall, configure the built-in firewall session tracking mechanisms included in many commercial firewalls to identify TCP sessions that last an unusually long time for the given organization and firewall device, alerting personnel about the source and destination addresses associated with these long sessions.	RedSeal can ensure that firewall configuration parameters are set up to detect and alert on long TCP sessions.
FAMILY	**CONTROL**	**CONTROL DESCRIPTION**	**REDSEAL CAPABILITY**

CIS TOP 20 CONTROLS WITH REDSEAL

FAMILY	CONTROL	CONTROL DESCRIPTION	REDSEAL CAPABILITY
Critical Security Control #13: Data Protection			
Network	**13.3**	Deploy an automated tool on network perimeters that monitors for sensitive information (e.g., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel.	RedSeal creates a model of your network and its controls. This includes a visual map of network egress points so your audit teams can efficiently and accurately place sensors. RedSeal can identify if controls are maintained to ensure that sensors can monitor traffic. For example, RedSeal can monitor perimeter devices to ensure that SPAN ports are properly configured to send traffic to monitoring systems.
Network	**13.8**	Block access to known file transfer and e-mail exfiltration websites.	If the control is a network ACL with known addresses, RedSeal can do a tracked access query from internal networks to a list of specific addresses. Changes in the query results can trigger an event. Additionally, if there is a configuration command on a network device (e.g. firewall) that implements a block list, RedSeal can determine if this control is accurately configured on the device.
Critical Security Control #14: Controlled Access Based on the Need to Know			
Application	**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 VLANS with firewall filtering to ensure that only authorized individuals are only able to communicate with systems necessary to fulfill their specific responsibilities.	One of RedSeal's core functions is zone segmentation, specifying controls and verifying that your network is enforcing the intended controls. RedSeal identifies variations in the controls and paths that are in violation (devices, ACLs, routes that circumvent the rule) for remediation.
Application	**14.3**	All network switches will enable Private Virtual Local Area Networks (VLANs) for segmented workstation networks to limit the ability of devices on a network to directly communicate with other devices on the subnet and limit an attackers ability to laterally move to compromise neighboring systems.	RedSeal can verify that: - User space has no access to protected space - VPN server has access to protected space - User space has access to VPN server Any access between user space and protected space is identified with detail on the paths and the controls that enable that path. This information can be shared with teams to correct the network and enforce the intended design.

CIS TOP 20 CONTROLS WITH REDSEAL

FAMILY	CONTROL	CONTROL DESCRIPTION	REDSEAL CAPABILITY
Application	**14.4**	All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principal that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	You can model your network segmentation in RedSeal
Application	**14.7**	Archived data sets or systems not regularly accessed by the organization shall be removed from the organization's 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.	RedSeal can create and monitor an access policy for systems that are identified as “archived systems” to ensure the systems remain off the network.
Critical Security Control #15: Wireless Access Control			
Network	**15.5**	Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection.	RedSeal can verify the configuration of access points and determine if they: - Have AES or better encryption specified - Don’t have unencrypted options provisioned
Network	**15.6**	Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), which provide credential protection and mutual authentication.	See Control 15.5
Network	**15.9**	Create separate virtual local area networks (VLANs) for BYOD systems or other untrusted devices. Internet access from this VLAN should go through at least the same border as corporate traffic. Enterprise access from this VLAN should be treated as untrusted and filtered and audited accordingly.	RedSeal’s network model can validate that virtual local networks for BYOD exist and the VLAN goes through the same border routing as corporate traffic.
Critical Security Control #16: Account Monitoring and Control			
Application	**16.4**	Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.	RedSeal can verify that account logout settings are uniformly configured across the network. Checks can be customized for each account created in a device’s configuration file. For example, logging out a console login after 2 minutes and a remote user (SSH) after 5 minutes. The checks are fully customizable. This allows customers to have tighter or looser controls on their firewalls and switches as needed.

CIS TOP 20 CONTROLS WITH REDSEAL

FAMILY	CONTROL	CONTROL DESCRIPTION	REDSEAL CAPABILITY
Application	**16.7**	Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.	As with Control 16.4, you can configure RedSeal to monitor and alert if a command instruction is incomplete, missing, or not to the agreed parameter. Several network device manufacturers have controls for the number of attempted logins, and RedSeal can monitor them.
Application	**16.13**	Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.	See Control 16.7
Application	**16.14**	Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.	RedSeal can verify that encryption is used in a device configuration and can check to see if the device's password algorithm is weak or strong.
Critical Security Control #18: Application Software Security			
Application	**18.2**	Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks, including but not limited to cross-site scripting, SQL injection, command injection, and directory traversal 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.	RedSeal can validate that no path around WAFs exists.
Application	**18.6**	Maintain separate environments for production and nonproduction systems. Developers should not typically have unmonitored access to production environments.	With RedSeal, you can model your segmentation to validate that network security controls prohibit developers from accessing production systems.
Critical Security Control #20: Penetration Tests and Red Team Exercises			
Application	**20.1**	Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. Penetration testing should occur from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization) as well as from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks.	Customers use RedSeal's network model to conduct virtual penetration testing from both external and internal sources. RedSeal also identifies attack vectors that can be used to exploit enterprise systems. RedSeal can simulate an internal attack, then identify and prioritize all possible vectors an attacker can traverse.

CIS TOP 20 CONTROLS WITH REDSEAL

FAMILY	CONTROL	CONTROL DESCRIPTION	REDSEAL CAPABILITY
Application	**20.2**	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.	RedSeal can monitor the addition of user accounts to a device's configuration (e.g. a user account created for a Red Team test on a firewall.) After the test, RedSeal can monitor configurations to ensure that these accounts are removed. RedSeal will supply a daily list of devices that have these accounts active, and can automatically email the list to the team(s) responsible.
Application	**20.3**	Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.	Maintaining RedSeal and properly defining reports to indicate changes to perimeter access, exposed vulnerabilities, and more, demonstrates your organization's commitment to continuous monitoring. While not a full replacement for Red Team testing, RedSeal allows organizations to perform White Box testing of their organization's security architecture on a daily basis.
Application	**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.	RedSeal creates network diagrams that identify the 'dark' areas of the network that can be used by attackers. It also indentifies configration issues on network devices that can be exploited by attackers.
Application	**20.5**	Plan clear goals of the penetration test itself with blended attacks in mind, identifying the goal machine or target asset. Many APT-style attacks deploy multiple vectors—often social engineering combined with web or network exploitation. Red Team manual or automated testing that captures pivoted and multi-vector attacks offers a more realistic assessment of security posture and risk to critical assets.	Both internal and external attack simulation can be done with RedSeal. RedSeal identifies all possible vulnerable targets from an external network. From inside the network RedSeal can identify all the possible targets an attacker can traverse to.
Application	**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.	By combining RedSeal data with vulnerability data, RedSeal can assist Red Teams in focusing their efforts on vulnerable assets that are accessible from an outisde network. RedSeal also provides the abilility to direct Red Teams by identying all access and vulnerabilities on all systems from any point inside the network.

CIS TOP 20 CONTROLS WITH REDSEAL

Application	**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.	RedSeal comes pre-configured with a number of tracked queries that run and are logged with each analysis. The RedSeal user can create additional tracked queries to evaluate access over a given portion of the network. RedSeal includes known and potential attack surface queries, along with pre-packaged historical trending reports. These allow a RedSeal user to track how changes to network controls impact access from external networks to internal networks and hosts within the RedSeal model. An increase in attack surface does not immediately correspond to an increase in risk, but it is something that warrants investigation. This information is not in a standard format, such as SCAP, but it is exportable in a number of standard formats (CSV, XML, etc) to be incorporated into other systems. RedSeal also provides a Digitial Resilience Score to improve operational risk metrics and resiliency. This is also tracked over time.
Application	**20.8**	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.	RedSeal mimics a production environment and can be used to test elements typically not tested in production.