SANS "Top 20" Critical Controls for Effective Cyber Defense

SANS "Top 20" Critical Controls for Effective Cyber Defense

Summary

In a rapidly evolving threat landscape, organizations must protect their entire IT environment against both external and internal attacks. Threats and risks arrive from many angles, requiring security professionals to use a wide variety of methods to defend against attacks. As a result, many organizations are now adopting the 20 Critical Security Controls developed by the SANS Institute. These controls help organizations prioritize the most effective methods and policies for safeguarding their assets, information and infrastructure.

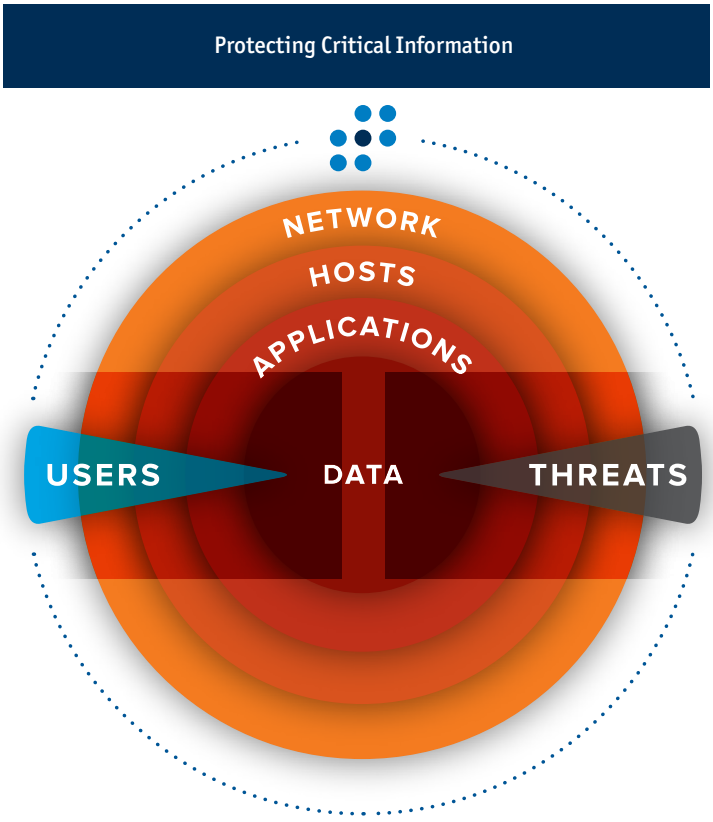
This paper outlines how LogRhythm's Security Intelligence Platform maps directly to each of the 20 Critical Security Controls. The LogRhythm Platform has been specifically designed to provide real-time, continuous monitoring at the log layer. LogRhythm collects, normalizes and analyzes all available log and machine data in real time. All data is immediately forwarded to the AI Engine, LogRhythm's patented Machine Analytics technology, for advanced behavioral and statistical analysis to deliver true visibility into all activity observed within the environment.

By combining machine data with both external and internal context such as geographic location and user logins, LogRhythm is able to establish normal behavioral patterns, thus enabling real-time detection of abnormal behavior. And LogRhythm goes beyond monitoring and detection by providing automated, intelligent remediation capabilities via Smart**Response**™ . This combination of capabilities delivers greater accuracy in threat detection and automates key components of the response process, accelerating remediation times. LogRhythm empowers organizations to manage risk more effectively while also reducing the Total Cost of Ownership for their Security Intelligence program.

LogRhythm provides a broad range of out-of-the-box advanced alerts, investigations, and reports that map directly to various components of the SANS Critical Controls in an effort to help organizations maintain a secure network. Alerts can be sent to groups or individuals, and can also be suppressed for a configurable period of time while investigations are carried out. Reports for manual review can be generated either on-demand or scheduled for delivery. For additional ease of deployment and streamlined administration, multiple list management templates are provided that enable organizations to simplify the process of aligning specific components to individual organizational requirements.

The SANS Critical Controls are listed in the table below, with an outline of how LogRhythm can support the implementation of each control.

This document has been created based on version 4.1 of the Critical Controls.



SANS Top 20 Critical Controls for Cyber Security

Critical Control	Description	LogRhythm Supporting Capability
1 Inventory of Authorized and Unauthorized Devices	The processes and tools used to track/control/prevent/correct network access by devices (computers, network components, printers, anything with IP addresses) based on an asset inventory of which devices are allowed to connect to the network.	LogRhythm can import from asset databases, and correlate actual devices present on the network against lists of approved devices. LogRhythm can also collect logs from DHCP servers to help detect unknown or unauthorized systems. LogRhythm supports the Control 1 Metric by identifying new unauthorized devices being connected to the network in near real time (for example via DHCP logs). LogRhythm offers the ability through Smart**Response**™ to automatically isolate the system from the network (for example by disabling the appropriate switch port) once an approval process has been completed.
2 Inventory of Authorized and Unauthorized Software	The processes and tools organizations use to track/control/prevent/correct installation and execution of software on computers based on an asset inventory of approved software.	LogRhythm monitors for the installation or execution of unauthorized software. LogRhythm can also create and maintain dynamic lists of approved software based on behavioral monitoring that may be operated in the environment. LogRhythm supports the Control 2 Metric by identifying attempts to install unauthorized software (for example via Windows application logs), by identifying attempts to execute unauthorized software (by monitoring process startups). LogRhythm offers the ability through Smart**Response**™ to automatically terminate execution of unauthorized software, or otherwise quarantine the affected system once an approval process has been completed.
3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	The processes and tools organizations use to track/control/prevent/correct security weaknesses in the configurations of the hardware and software of mobile devices, laptops, workstations, and servers based on a formal configuration management and change control process.	LogRhythm monitors the use of privileged or generic accounts, the startup of services, the use of ports, and the application of patches. LogRhythm can also detect changes to key files through its File Integrity Monitor. LogRhythm supports the Control 3 Metric by identifying changes to key files, services, ports, configuration files, or software installed on the system. LogRhythm has the ability through Smart**Response**™ to automatically respond to file or service changes, or otherwise quarantine the affected system.
4 Continuous Vulnerability Assessment and Remediation	The processes and tools used to detect/prevent/correct security vulnerabilities in the configurations of devices that are listed and approved in the asset inventory database.	LogRhythm collects logs from vulnerability scanners. It is able to correlate event logs with data from vulnerability scans. LogRhythm can monitor the use of the account that was used to perform the vulnerability scan. LogRhythm supports the Control 4 Metric by collecting logs and data from vulnerability scans. This enables LogRhythm to correlate both the data from the scan and the logs about the scan, providing the basis to report on progress of the vulnerability scan, and of any devices where the scan did not take place. LogRhythm can also collect logs relating to patch installation, and can trigger an alert based on successful completion.

Critical Control	Description	LogRhythm Supporting Capability
5 Malware Defenses	The processes and tools used to detect/prevent/correct installation and execution of malicious software on all devices.	LogRhythm collects logs from malware detection tools and correlate those logs with other data collected in real time to eliminate false positives and detect blended threats. LogRhythm can also collect logs from email and web-content filtering tools. Via its advanced Agent, LogRhythm can detect and report data copied to removable storage devices. LogRhythm is tightly integrated with industry-leading security vendors including FireEye, Sourcefire, Fortinet and Palo Alto among many others. LogRhythm supports the Control 5 Metric by continually collecting and monitoring logs from a wide variety of malware detection tools, in addition to its own agent technology. LogRhythm has the ability through Smart**Response**™ to automatically terminate the execution of unauthorized software and quarantine any affected systems.
6 Application Software Security	The processes and tools organizations use to detect/prevent/correct security weaknesses in the development and acquisition of software applications.	LogRhythm collects logs from web application firewalls, and from vulnerability scanners. LogRhythm also offers a built-in Web Application Defense Module via its knowledge base. LogRhythm supports the Control 6 Metric through the LogRhythm Web Application Defense Module which is designed to leverage web log data with a focus on detection, identification, and prevention of security related issues. By design, this module can be used in combination with Intrusion Detection Systems and Web Application Firewalls or on its own. Because of LogRhythm's ability to correlate across various applications and device logs at once, it is especially well positioned to create meaningful, relevant alerts around suspicious web log data. The Web Application Defense Module provides out-of-the-box alerts for detecting Suspicious URL Characters and malicious user agent strings, in addition to automatically populating an "attacking IPs list." This list enables reporting to be done on source IPs that are attacking web applications. LogRhythm collects logs from WAFs and IDS/IPS systems, in addition to vulnerability scanners. All security event logs are correlated in real time. LogRhythm has the ability through Smart**Response**™ to automatically push a new configuration to a firewall (for example via the Palo Alto API), or otherwise quarantine the affected system.
7 Wireless Device Control	The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.	LogRhythm collects logs from a variety of wireless devices and management systems. In conjunction with logs collected from DHCP servers, wireless clients may be detected connecting to the organization's network. LogRhythm supports the Control 7 Metric by collecting logs from wireless devices, wireless management systems, and DHCP. Real time correlation of these logs enables the identification of unauthorized wireless devices or configurations. LogRhythm has the ability through Smart**Response**™ to automatically isolate the system from the network (for example by disabling the appropriate switch port).

Critical Control	Description	LogRhythm Supporting Capability
8 Data Recovery Capability	The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.	LogRhythm collects logs from Windows and other backup systems. Through the AI Engine, LogRhythm can detect backups that did not successfully complete, or backups that did not start. There is no Metric for Control 8.
9 Security Skills Assessment and Appropriate Training to Fill Gaps	The process and tools to make sure an organization understands the technical skill gaps within its workforce, including an integrated plan to fill the gaps through policy, training, and awareness.	SANS Control 9 is policy based and focuses on skills and training. LogRhythm is able to monitor user compliance with policy and send alerts in real time where credentials are used in an abnormal manner. Since all user activity is logged and collected, correlation and reporting are effective methods for monitoring adherence to policy. There is no Metric for Control 9.
10 Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	The processes and tools used to track/control/prevent/correct security weaknesses in the configurations in network devices such as firewalls, routers, and switches based on formal configuration management and change control processes.	LogRhythm collects logs from any network device that generates syslog or SNMP. LogRhythm supports the Control 10 Metric by collecting logs from network devices and correlating changes against a change control system to identify and alert on any unauthorized changes. LogRhythm has the ability through Smart**Response**™ to automatically shut down any services performing unauthorized changes.
11 Limitation and Control of Network Ports, Protocols, and Services	The processes and tools used to track/control/prevent/correct use of ports, protocols, and services on networked devices.	By collecting logs from port scanners, LogRhythm is able to detect open ports on the network. LogRhythm can also collect logs on protocols in use and services starting up on individual devices. LogRhythm supports the Control 11 Metric by collecting logs from across the environment and baselining the behavior patterns observed over a period of time. Using this baseline, deviations from normal or expected behavior can be detected and alerts generated. LogRhythm's AI Engine and list management capabilities can alert on the use of non-authorized ports in the environment in real time.
12 Controlled Use of Administrative Privileges	The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.	LogRhythm collects logs from almost any device and can monitor the use of default, generic, service and other privileged accounts. LogRhythm supports the Control 11 Metric by collecting logs on administrative activity from across the infrastructure. LogRhythm offers an out-of-the-box Privileged User Monitoring Module, which simplifies the task of tracking and monitoring accounts with elevated privileges and automates a number of tasks that are generally done manually. By design, this module can be used in combination with multiple operating systems (various Linux distributions, Windows, Solaris, etc.) in addition to MS Exchange server 2007 and 2010. LogRhythm's unique ability to simultaneously correlate data across multiple applications and devices strengthens privileged user monitoring and exposes suspicious activity performed by administrative accounts.

Critical Control	Description	LogRhythm Supporting Capability
13 Boundary Defense	The processes and tools used to detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.	LogRhythm collects logs from a wide variety of boundary defense devices for correlation or compliance purposes. LogRhythm supports the Control 12 Metric by collecting logs from boundary defense devices in addition to NetFlow data. LogRhythm can build trends of data flows based on observed behavior and alert on deviations from normal behavior. By understanding the internal network infrastructure, internal and external context can be added to alerts, helping identify unexpected traffic flows such as a website in the DMZ communicating directly with a SQL database, rather than communicating via the application layer. LogRhythm also offers out-of-the-box support for third party threat lists and custom IP address blacklists and can alert in real- time when connections are made to any blacklisted IP address or host.
14 Maintenance, Monitoring, and Analysis of Audit Logs	The processes and tools used to detect/prevent/correct the use of systems and information based on audit logs of events that are considered significant or could impact the security of an organization.	LogRhythm provides a comprehensive platform for the maintenance, monitoring and analysis of audit logs. LogRhythm supports the Control 14 Metric by collecting all events from across the network. LogRhythm offers silent log source detection in order to validate that devices are still generating logs, and has comprehensive time normalization abilities to ensure that the SIEM engine sees the logs in the actual order they occurred. LogRhythm performs extensive processing of every log that is collected, assigning a common event and establishing a risk based priority for each log. LogRhythm's patented real-time analytics technology, the AI Engine, can baseline behavior of users, hosts and data from across the network. Once a baseline is established, abnormal behavior can be detected and alarmed on.
15 Controlled Access Based on the Need to Know	The processes and tools used to track/control/prevent/correct secure access to information according to the formal determination of which persons, computers, and applications have a need and right to access information based on an approved classification.	LogRhythm collects audit logs from across the network. Fully integrated File Integrity Monitoring capabilities monitor for and alert on a variety of malicious behaviors, including improper user access of confidential files to botnet related breaches and transmittal of sensitive data. LogRhythm supports the Control 15 Metric by collecting logs of all attempts by users to access files on local systems or network accessible file shares without the appropriate privileges. LogRhythm's File Integrity Monitor can also be used to establish a baseline of normal behavior against a file or fileset, and can alert on deviations from that behavioral baseline.

Critical Control	Description	LogRhythm Supporting Capability
16 Account Monitoring and Control	The processes and tools used to track/control/ prevent/correct the use of system and application accounts.	LogRhythm collects audit logs from across the network for both local and network accounts. LogRhythm supports the Control 16 Metric by collecting logs of all user activity and correlating this with lists of privileged, generic, and service accounts, and also with lists of accounts for users that are terminated. Using a Smart**Response**™ plug-in, lists can be automatically maintained when changes take place in the environment. LogRhythm can alert when the use of terminated accounts are observed, and offers extensive reporting capabilities in this area. LogRhythm can also establish baselines of normal account behavior. For example, LogRhythm can track which servers a user normally connects to, and alert on deviation from that norm.
17 Data Loss Prevention	The processes and tools used to track/control/ prevent/correct data transmission and storage, based on the data's content and associated classification.	LogRhythm collects logs from both endpoints and network perimeter devices in order to assist in the detection of data loss incidents. LogRhythm also provides basic Data Loss Detection functionality in its advanced agent technology. LogRhythm supports the Control 17 Metric by collecting logs from endpoints, authentication systems, boundary defense devices, proxies and email servers amongst others. LogRhythm is able to detect abnormal activity (e.g. upload of large number of files to Internet based file sharing facilities) in real time and take immediate action via a Smart**Response**™ plug-in that can block user access, or terminate the process that is exfiltrating the data. LogRhythm's patented real-time analytics technology, the AI Engine, is able to establish baselines of behavior. For example, AI Engine can observe how users work with a certain set of documents, and alert on deviations from that behavior.
18 Incident Response and Management	The process and tools to make sure an organization has a properly tested plan with appropriate trained resources for dealing with any adverse events or threats of adverse events.	SANS Control 18 is policy based and focuses on having a clear Incident Response policy. LogRhythm has an integrated incident management capability providing real-time updates on an incident's status (i.e., working, closed, etc.). Status and commentary can be attached to each alert and progress reports can be generated on demand. There is no Metric for Control 18.
19 Secure Network Engineering	The process and tools used to build, update, and validate a network infrastructure that can properly withstand attacks from advanced threats.	SANS Control 19 is focused on the design of the network. By bringing understanding of the internal network design into LogRhythm, this information can be used to identify unexpected traffic flows such as sensitive systems being accessed directly from the Internet. There is no Metric for Control 19.

Critical Control	Description	LogRhythm Supporting Capability
20 Penetration Tests and Red Team Exercises	The process and tools used to simulate attacks against a network to validate the overall security of an organization.	LogRhythm collects logs from across the environment. It is a valuable monitoring tool during any penetration test, or red team exercise. LogRhythm enables the accounts used in the penetration test to be automatically monitored for legitimate use. LogRhythm also enables the detection of unusual behavior and may be used to detect the attempts to exploit the enterprise systems during penetration testing. There is no Metric for Control 20.