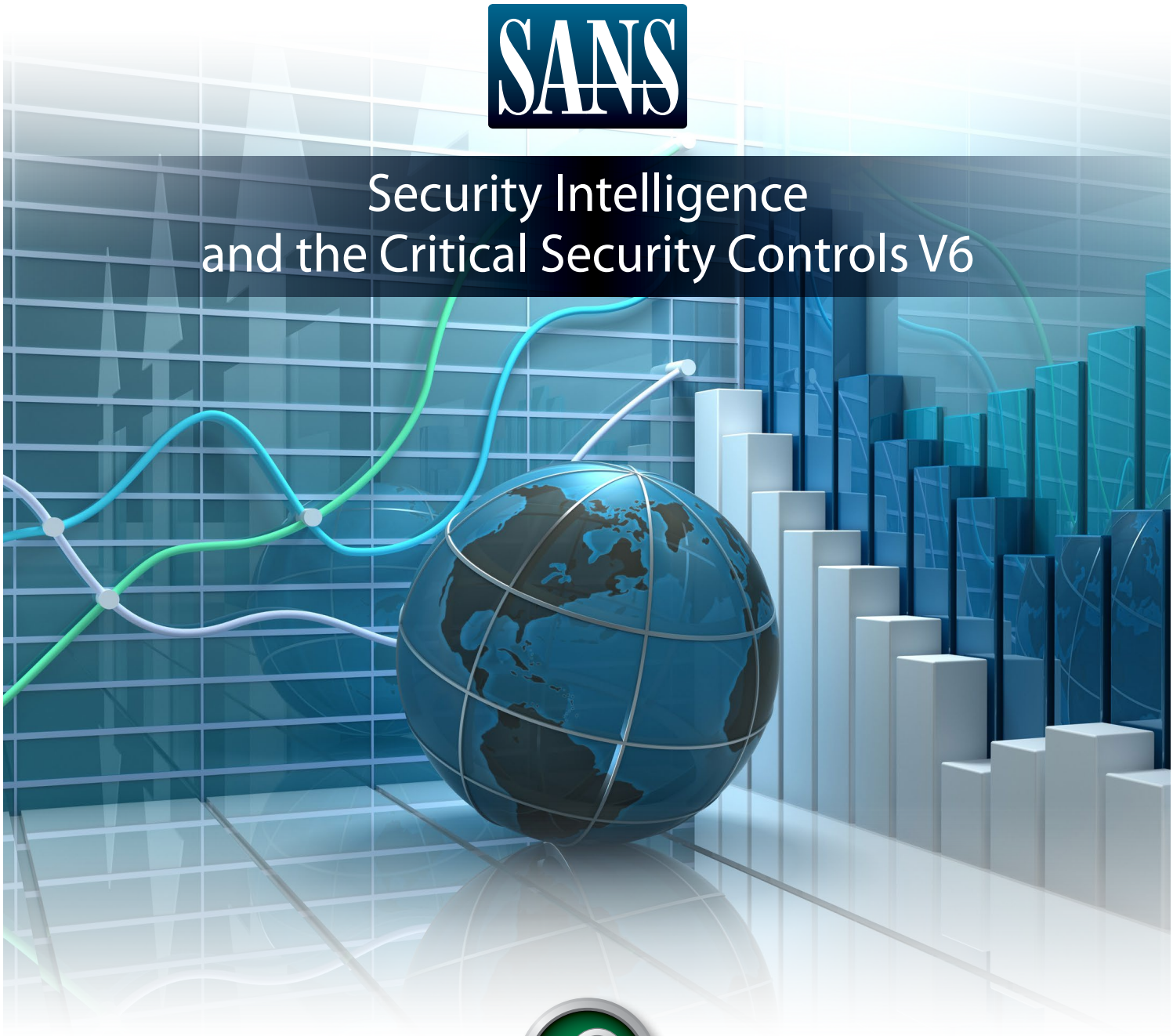
Interested in learning more about security?

SANS Institute InfoSec Reading Room

Security Intelligence and the Critical Security Controls v6

Security data is everywhere in our logs, feeds from security devices (IDS/IPS/ rewalls, whitelists, etc.), network and endpoint systems, anomaly reports, access records, network tra c data, security incident and event monitoring (SIEM) systems, and even in applications hosted in the cloud. All of this data and the processes that use them combine to form an organization s security intelligence ecosystem. The major challenge of managing this ecosystem of security data is tying all these bits of data together and autom...



Security Intelligence and the Critical Security Controls V6

A SANS Spotlight Paper

Written by G. W. Ray Davidson, PhD

September 2016

Sponsored by LogRhythm

Security data is everywhere—in our logs, feeds from security devices (IDS/IPS/firewalls, whitelists, etc.), network and endpoint systems, anomaly reports, access records, network traffic data, security incident and event monitoring (SIEM) systems, and even in applications hosted in the cloud. All of this data—and the processes that use them—combine to form an organization's security intelligence ecosystem.

The major challenge of managing this ecosystem of security data is tying all these bits of data together and automating their correlation and use, with the goal of faster detection, prevention, continued security improvement and ultimately, reduced risk.[1] The key to success is through automation and integration, according to the CIS Critical Security Controls, which is now in version 6.[2]

Security Intelligence Through CIS Controls

Unifying security intelligence processes through automation and integration is key to successfully integrating security-related data into the workflow of detection, prevention and response/remediation.

Unfortunately, in SANS' most recent survey on security analytics and intelligence, 32 percent of respondents had no automation at all, and only 3 percent said their processes were "fully automated."[3] The rest fell somewhere in between, reporting only partial automation, while many responders reported their desire to unify their security-related data for better cross-functional visibility and control over events. Often this security intelligence ecosystem is unified under a platform or SIEM, according to respondents.

Automated security intelligence addresses most, if not all, of the CIS Controls. Table 1 calls out some of the key aspects of the security intelligence ecosystem that should be made available through a platform or SIEM to prevent, detect and respond swiftly and accurately to threats.

Table 1. The Role of Security Intelligence in CIS Critical Security Controls

Control	Actions to Automate	Security Intelligence Applied
CIS Control 1: Inventory of Authorized and Unauthorized Devices	Use an asset inventory system to compare devices accessing the network against the inventory of known and approved devices. Use DHCP logs or other data to detect new/unauthorized systems. Deny access or quarantine unknown devices.	Visibility into the asset and inventory data combined with "normal" network monitoring data provide a baseline of the known and authorized devices on the network (and their attributes). Continuous monitoring (a key component of security intelligence) enables the organization to quickly identify, locate and remediate anomalies as needed.
CIS Control 2: Inventory of Authorized and Unauthorized Software	Detect and prevent attempts to install unauthorized software or uninstall required software. If execution of unauthorized software is detected, terminate the process. Quarantine the device if that is unsuccessful.	Security intelligence systems make use of approved whitelists and blacklists, provide a baseline of the known and authorized applications and processes on the network (and their attributes), support workflow and remediation, and report when unauthorized systems are detected.

[1] Average time to detect and respond is most often due to lack of automation/integration, according to the SANS 2015 Analytics and Intelligence Survey, www.sans.org/reading-room/whitepapers/analyst/2015-analytics-intelligence-survey-36432

[2] CIS Critical Security Controls, Center for Internet Security, www.cisecurity.org/critical-controls.cfm

[3] "SANS 2015 Analytics and Intelligence Survey," Table 2, page 6, www.sans.org/reading-room/whitepapers/analyst/2015-analytics-intelligence-survey-36432

Table 1 (continued)

Control	Actions to Automate	Security Intelligence Applied
CIS Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Maintain an inventory of approved software and hardware configurations, and monitor network and endpoint devices for changes in ports, services, files, registry keys, etc. Remediate unauthorized changes, or quarantine the device automatically using network access control (NAC), mobile device management (MDM) or other endpoint or network device management tools.	Utilize the baseline configuration available in these records, such as a configuration management database (CMDB), along with output from continuous monitoring through the security intelligence platform to detect excursions from "normal" and changes in configuration of devices and applications on the network.
CIS Control 4: Continuous Vulnerability Assessment and Remediation	Regularly scan for vulnerabilities in the environment using a continuously updated tool to identify missed patch installations. Use vulnerability scan data to determine relevance of detected threats and adjust risk profiles accordingly.	Apply real-time security analytics and vulnerability assessment data to create a dynamic risk profile to detect cyber attacks that seek to exploit those vulnerabilities, and adjust existing defensive capability. Supplement real-time vulnerability data with additional change information that may not be included in standard vulnerability assessments. This feedback loop is a key aspect of the security intelligence ecosystem.
CIS Control 5: Controlled Use of Administrative Privileges	Minimize administrative privileges and use them only when required. Change default passwords, and use secure, multifactor authentication for administrative duties. Monitor access and event logs for attempts to access password files, escalate privilege or add accounts.	Monitor for account misuse through the application of behavioral analytic techniques to proactively detect anomalous privileged account behavior. The security intelligence system serves to automate baselining of normal admin activity so that anomalous behavior can be detected early in the threat lifecycle.
CIS Control 6: Maintenance, Monitoring, and Analysis of Audit Logs	Collect and analyze logs from monitoring systems to identify suspicious activity and implement remediation. Do that automatically where possible. Periodically validate that devices are still generating logs and forwarding them to the appropriate location.	Real-time data ingestion through automated collection, normalization and analytics is a characteristic of a mature security intelligence platform. Automated collection, processing, monitoring and analysis of log data helps in developing behavioral heuristics, proactively identifying risk and responding to incidents.
CIS Control 8: Malware Defenses	Use relevant input from external threat feeds combined with indicators of compromise developed from internal logs to detect malicious activity and update defense capabilities. Update the organizational risk profile in response to changes in the external threat environment as well. Do that automatically if possible.	The security intelligence platform should automatically combine security intelligence from external feeds with information from internal malware defense systems to support real-time, accurate and actionable detection. The intelligence system should also work with and tune malware defenses for better future protection.
CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services	Monitor networking devices and endpoints using port scanners and other tools. Detect open ports and running services and protocols, and compare them against the baseline for deviations. Remediate automatically where possible.	Correlate output from network monitors to detect and facilitate remediation of any deviations from the baseline. In a mature intelligence ecosystem, these activities will be automated and performed in real time to reduce the mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR).

Employ a security intelligence platform to achieve end-to-end threat lifecycle management to improve prevention, detection, response and neutralization of cyber threats that pose a risk to your organization.

Table 1 (continued)

Control	Actions to Automate	Security Intelligence Applied
CIS Control 10: Data Recovery Capability	Use regular automated scans to ensure backup technology is installed and working correctly. Analyze logs to determine previous backup time, and remediate automatically when backups are missed. Test restore capability as well.	Monitor backup logs to detect modifications to backup files, which may be an indicator of ransomware that can render backups useless. Security intelligence systems should automatically digest information from backup logs to detect failures in backup execution and automatically support remediation.
CIS Control 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Monitor and compare configurations of these devices against standard/gold build, and alert change attempts and unusual network attempts.	Network monitoring output, combined with vulnerability data, provides better visibility into threats attempting to exploit vulnerable network devices that are misconfigured. The platform should make this vulnerability data readily available for use during threats and remediation.
CIS Control 12: Boundary Defense	Collect and utilize network flow data and data (including device logs) from boundary devices to detect anomalies and add context to other activities happening on the network. Combine this edge data with internal data to decrease the information that must be examined within the network for network behavior anomaly detection (NBAD).	Security intelligence processes should correlate data from real-time network monitoring with baseline data to adjust and tune boundary defenses on a real-time basis. The system should also include visibility into automated remediation actions (e.g., issue an access control list (ACL) rule to block an IP address from which an attack is originating).
CIS Control 13: Data Protection	Apply protection at both the endpoints and the network to detect and prevent access and to exfiltrate data based on the organizational risk management policy. Detect access to sensitive data, and monitor for violations of policy.	Monitor logs and other data from data protection systems (including access control systems, endpoint systems, boundary defenses, network perimeter devices, proxies, email servers, etc.) to provide additional context when investigating potential exfiltration attempts. This additional context is a hallmark of a mature security intelligence ecosystem.
CIS Control 15: Wireless Access Control	Detect when new devices request access to the network and when access points come online. Deny access or quarantine automatically when the device is not present in the approved list or doesn't conform to specs.	Utilize network monitoring and analytics to detect when rogue or unknown devices connect to the network, as well as when unauthorized or unknown applications are used over wireless access points. The system must also support responders.
CIS Control 16: Account Monitoring and Control	Monitor all accounts and usage. Review and disable system accounts that cannot be associated with business processes or dormant accounts. Alert when previously dormant accounts are used. Maintain audit trails to support changes. Maintain updated account and activity log listings, subject to change control.	Monitor user and system behavior for unauthorized or deviant activity. Employ immediate and, when appropriate, automated responses based on policy through the security intelligence system. Correlate the output of monitoring processes to produce behavioral information for detecting anomalies in real time and responding quickly to indicators of account misuse to reduce the risk of data loss.
CIS Control 19: Incident Response and Management	Ensure written procedures to deal with incidents. Conduct periodic incident scenarios. Utilize lessons learned to identify indicators of compromise, aid investigations and support continuous process improvement.	Utilize security intelligence systems to make data automatically available to incident responders so they can identify, scope and react appropriately. A mature security intelligence system should support full incident response orchestration, including remediation workflow.

As this table shows, security intelligence automation helps realize the true threat management potential of the CIS Controls.

Keys to Effectiveness

Start by surveying what machine data exists in your enterprise, and develop a classification scheme to determine what data is most valuable and important to protect, along with models describing the threats to that data. On an ongoing basis, collect, process, store and analyze machine data from across the enterprise, and monitor the segments most closely tied to the most critical assets.

Reduce Risk and Contain Damage

Create your own customized security intelligence ecosystem. Develop and implement processes specific to your business to create a detection and response framework that does the following:

- Concentrates on high-risk areas
- Discovers attacks quickly
- Contains damage effectively
- Completely eradicates the attacker's footprints
- Restores the integrity of the network and systems in a timely fashion
- Utilizes any new security data for future prevention, detection and remediation

Utilize security intelligence data to expand risk scoring of other areas of the enterprise. For instance, if regular vulnerability monitoring (CIS Control 4) detects an unpatched device that is included in the scope of monitoring, that device deserves a higher risk score until it is patched and the automated workflow system has alerted the security intelligence platform the patches are completed and tested.

Standards for consuming and normalizing the information, along with automated workflow for detecting and disseminating new threat information, are critical to making these moving parts work together.

By designing and implementing the appropriate security intelligence architecture and having appropriate communication standards and staffing, security intelligence improves visibility, detection and response, according to the SANS survey on security intelligence and analytics.[4]

[4] "SANS 2015 Analytics and Intelligence Survey," www.sans.org/reading-room/whitepapers/analyst/2015-analytics-intelligence-survey-36432

About the Author

G. W. Ray Davidson, PhD, is the former dean of academic affairs for the SANS Technology Institute. He continues to serve as a mentor, subject matter expert and technical reviewer for the SANS Institute and holds several GIAC certifications. Ray started his career as a research scientist and subsequently led global security projects for a major pharmaceutical company. He has taught at the college level and worked at a security startup. Ray currently works with clients to develop and implement network security monitoring and threat intelligence capabilities. He is also active in the leadership of the Michigan Cyber Civilian Corps.

Sponsor

SANS would like to thank this paper's sponsor:

LogRhythm®
The Security Intelligence Company

Last Updated: June 27th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, AU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, DK	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, GB	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, COUS	Sep 25, 2017 - Sep 30, 2017	Live Event
Data Breach Summit & Training	Chicago, ILUS	Sep 25, 2017 - Oct 02, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, NL	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MDUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SEC564:Red Team Ops	OnlineCAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced