Cybersecurity Detective Controls—Monitoring to Identify and Respond to Threats

Fredric Greene, CISSP, is an experienced IT auditor specializing in technology infrastructure in the financial services industry. His main areas of focus are information and cybersecurity, IBM platforms (mainframe z/OS, AIX Power Systems), databases (DB2, Oracle), and a spectrum of systems and network technology. Another area of focus in recent years is cloud and virtualization technology including VMWare, Citrix and IBM cloud products and services. Greene worked for the legacy organization Bank of Tokyo (prior to its merger to form MUFG Union Bank), Depository Trust & Clearing Corporation (DTCC), and KPMG.

Detective controls are a key component of a cybersecurity program in providing visibility into malicious activity, breaches and attacks on an organization's IT environment. These controls include logging of events and the associated monitoring and alerting that facilitate effective IT management. Auditors should identify and assess these critical controls when auditing a cybersecurity program.

According to *Transforming Cybersecurity*, which applies the COBIT® 5 framework and its component publications toward transforming cybersecurity in a systemic way, a key cybersecurity objective is that "attacks and breaches are identified and treated in a timely and appropriate manner."[1]

COBIT 5 also provides the related audit objectives:

1. Confirm monitoring and specific technical attack recognition solutions.
2. Assess interfaces to security incident management and crisis management processes.
3. Evaluate the timeliness and adequacy of attack response.

Another excellent source of guidance for cybersecurity detective controls is the US National Institute for Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework).[2] The detect function is a key component of the NIST Cybersecurity Framework, which includes associated categories of anomalies and events and continuous security monitoring.

Cybersecurity detective controls should be designed to identify a range of threats. Lockheed Martin has introduced the Cyber Kill Chain framework, which can be used to detect cyberthreats and includes surveillance (e.g., scanning), weaponization and delivery (e.g., malware), exploitation (e.g., vulnerability), command and control (e.g., compromised administrator accounts), and exfiltration of data (e.g., intellectual property [IP]).[3]

While it is close to impossible to prevent all intrusions, early detection of adverse activity is essential to any cybersecurity regime. Organizations should also emphasize adaptability in their cybersecurity processes and tools to address the dynamic threat landscape.

CYBERSECURITY DETECTIVE CONTROLS

If designed well and operating effectively, specific cybersecurity detective controls should be able to halt the cyberthreats discussed previously. These controls are generally managed or performed by a security operations center (SOC) that is responsible for cybersecurity monitoring.

The security information and event management (SIEM) system is the central software platform that can integrate event logs aggregated from multiple sources with threat data sources (e.g., real-time feeds) and contextual information about assets and users.

There are alternatives to the SIEM approach discussed here, including intrusion detection systems (IDs)and intrusion prevention systems (IPS) that aggregate and analyze security data. There is also an option to outsource the security monitoring function altogether to a third-party vendor. However, this article discusses the SIEM approach, which is highly adaptable and flexible with an organization's requirements.

The SIEM aggregates, normalizes (standardizes format) and correlates event data to identify and prioritize threats, filter out false positives, and provide actionable threat intelligence. An organization's unique context (assets, users, risks) should be integrated into SIEM operations. The SIEM is the essential tool for security analysis, incident response, forensics and regulatory compliance (reporting). *Critical Capabilities for Security Information and Event Management*[4] enumerates many of the key controls in a generic SIEM, including real-time monitoring, threat intelligence, data and user monitoring, application monitoring, analytics, log management, and reporting.

FORUM

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article and choose the Comments tab to share your thoughts.

Go directly to the article:

Specific use cases may include detection of suspicious behavior (e.g., compromised privileged user accounts, access to sensitive data), detection of policy violations (e.g., change in server configurations), detection of advanced persistent threats (APTs) (e.g., outbound data flows to international destinations) and detection of fraud (e.g., change in trade volumes or money transfers). Auditors should assess the design and operating effectiveness of the SIEM functionality described.

Event log management is a critical component of the SIEM functionality. Event logs should be aggregated (e.g., pulled) from most or all deployed technology (e.g., source systems) in an organization, including security devices (e.g., firewalls, IDS/IPS, web proxy), network devices (e.g., routers, switches), systems (e.g., mainframe, midrange, distributed servers), applications, databases, storage devices, end-point desktops and mobile devices. Event log data may also be aggregated from various technology functions, such as performance and change management.

Configuring the source systems to send log data to the central SIEM system may require substantial effort. In larger organizations, the volume of event log data can be enormous, and the storage requirements may also be substantial.

A separate module, server or component (e.g., HP Arcsight Log Aggregator, IBM Security QRadar Log Manager) is generally required to manage the logs. Auditors will want to confirm a maximum level of SIEM coverage of logs from around an organization's IT environment.

SOURCES OF THREAT INTELLIGENCE

Gartner defines threat intelligence as "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."[5]

There is a wide range of threat intelligence vendors that can provide tactical or operational feeds of Internet Protocol (IP) reputation information (e.g., suspected malware sources by IP or uniform resource locator [URL]); malware profiles; indicators of compromise, command and control (C&C) patterns; and exfiltration approaches.

Here is a brief overview of the sources of threat intelligence categorized into current services available for ingestion into a SIEM system:

- SIEM vendors that offer threat intelligence feeds as part of a one-stop solution, e.g., IBM QRadar SIEM combined with IBM X-Force Threat Intelligence service
- Commercial aggregated and packaged threat intelligence from multiple sources—structured and unstructured, e.g., CyberSquared ThreatConnect[6] feed (partnered with Cisco Sourcefire) and AlienVault Open Threat Exchange (OTX), claimed to be the world's largest crowd-sourced repository of threat data
- Free threat intelligence feeds (e.g., Google Safe Browsing API, Zeus Tracker Blocklist) offered through the information security community mostly in the crystallographic information file (CIF) format, including blacklists of IP addresses and URLs suspected in malicious activity[7]
- Original threat intelligence offered as threat feeds, rules, blacklists and parsers (e.g., RSA FirstWatch,[8] which offers intelligence on advanced and emerging threats at the strategic and tactical level)

There are differences in threat information, which may be raw, unfiltered, unvalidated data with varying levels of credibility and intelligence, which are processed, sorted, distilled, accurate and timely, and from reliable sources. Thus, the clear preference is toward threat intelligence.

Threat intelligence becomes more useful when security analysts apply contextual knowledge and analysis to the threat intelligence (e.g., connecting the dots). Contextual knowledge here means the deeper meaning of events—past, present and future. Furthermore, this knowledge includes contextual linkage among tactics, techniques and procedures (TTPs) and the operational environment (e.g., infrastructure).[9]

Intelligence that is specific and enriched with context and actionable data also becomes useful in setting severity and priority ratings.

While this article does not cover the extensive ecosystem of threat data, intelligence and vendors, threat intelligence is, from an audit perspective, a key component of cybersecurity detective controls.

SEVERITY AND PRIORITY RATINGS

An inherent problem with monitoring security-related activity is the potential flood of events and alerts that may be created and transmitted into the SIEM system. FireEye estimates the typical cybersecurity deployment generates five alerts per second.[10] Few, if any, organizations have the resources to investigate such volume of activity.

The key metric of cybersecurity monitoring tools (e.g., SIEM) is not the volume of alerts, but the ability to detect real threats, filter out the meaningful alerts and enrich those alerts with context that facilitates action.[11]

This filtering, validating and correlating of incoming events and alerts is a key process in the overall detective capability. To focus resources (e.g., security analyst time) on the most significant threats, an organization should manage the flow of security events as follows:

- **Reduce the volume of alerts** by reducing the frequency of alerts from devices (e.g., change the frequency of an alert from every second to every minute); aggregate alerts with the same source and destination IP addresses; and remove meaningless indicators and false positives.
- **Prioritize the alerts** that matter most based on business risk. Set priorities by assets, impact on business function (e.g., core processes) and type of activity (e.g., beaconing, policy violation).

CONCLUSION

Detective controls are critical to an organization's cybersecurity posture. A SIEM system is the central component for integrating event logs with threat intelligence and contextual information (organization-specific user, asset and risk data). Event logs should be aggregated from most or all sources in a technology environment. Threat intelligence should be leveraged as tactical or operational feeds of real-time incoming threats. The potential flood of events and alerts should be filtered to enable efficient analysis and response to the most significant and relevant threats.

The net result of implementing these controls in alignment with COBIT 5 is the capability to identify and treat attacks and breaches in a timely and appropriate manner. By reviewing these controls, the auditor can get assurance on the design and operating effectiveness of an organization's cybersecurity detective capability.

ENDNOTES

[1] ISACA, *Transforming Cybersecurity*, USA, 2013, *www.isaca.org*

[2] National Institute for Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, USA, 2014, *www.nist.gov/cyberframework*

[3] Lockheed Martin, Cyber Kill Chain, *www.lockheedmartin.com/us/what-we-do/information-technology/cyber-security/cyber-kill-chain.html*

[4] Nicolett, Mark; Kelly M. Kavanagh; *Critical Capabilities for Security Information and Event Management*, Gartner, 2012, *www.gartner.com/doc/2022315/critical-capabilities-security-information-event*

[5] Chuvakin, Anton; "Made for Each Other: How to Use Threat Intelligence With SIEM," Gartner, *http://searchsecurity.techtarget.com/tip/Made-for-each-other-How-to-use-threat-intelligence-with-SIEM*

[6] CyberSquared, "ThreatConnect," Cisco Sourcefire, *www.sourcefire.com/partners/technology-partners/sourcefire-technology-partners/threatconnect*

[7] Chuvakin, Anton; "On Comparing Threat Intelligence Feeds," 7 January 2014, *http://blogs.gartner.com/anton-chuvakin/2014/01/07/on-comparing-threat-intelligence-feeds/*

[8] EMC Corp., FirstWatch, *www.emc.com/emc-plus/rsa-thought-leadership/firstwatch/index.htm*

[9] Hartley, Matt; "Cyber Threats: Information vs. Intelligence," 22 October 2014, *www.darkreading.com/analytics/threat-intelligence/cyber-threats-information-vs-intelligence/a/d-id/1316851?page_number=2*

[10] FireEye, "Speed Dating For Security Teams—Finding the Alerts That Lead to Compromise," webinar, August 2014

[11] FireEye, *The SIEM Who Cried Wolf: Focusing Your Cybersecurity Efforts on the Alerts That Matter,* white paper, 2014