Log Management as an Enabler for Data Protection and Automated Threat Detection

In August 2022, the US Federal Bureau of Investigations (FBI) alerted the South African Reserve Bank (SARB) that it was under attack. Although there are claims that some local agencies detected the breach as well, what is clear is the fact that the SARB did not detect this breach itself.

"The fact that the SARB had to be alerted to an attack by a third party tells us they were not adequately monitored and protected by their own systems," said World Wide Worx founder Arthur Goldstuck.[1]

Google subsidiary Mandiant, an American cybersecurity firm, reported that 41 percent of the incidents it investigated in 2020 stemmed from external notification.[2] Another way to interpret this is that 59 percent of organizations did not detect intrusion into their environments on their own, supporting Goldstuck's notion that an organization that must be alerted by an external party is not adequately monitored and protected by its own systems.

For a long time, the focus of security efforts was effective incident response and threat mitigation. As a result, organizations and vendors have matured significantly in these areas—so much so that security operations centers (SOCs) sometimes miss security incidents because there are just too many tools to monitor and data to process.

Log management is an important and foundational aspect of security; however, it is often overlooked.

It is common to view security logging and monitoring as one function—that is, logging-and-monitoring. It is easy to lose sight of the fact that security logging is distinctly different from security monitoring, although they are interdependent. Security event logging is a critical component that underpins many capabilities, including security monitoring. Similarly, automation, artificial intelligence (AI)-enabled tools, analytics, incident response, forensics and ediscovery are all dependent on proper event logging.

The threat landscape is constantly evolving, and as a result, organizations need to be more vigilant. Without a proper log management capability, organizations may not be able to detect and respond to potential threats in a timely and effective manner. Effective data protection and threat detection requires robust log management and monitoring capabilities; however, implementing and maturing these capabilities can be complex and challenging.

A proposed framework can be used to fast-track a log management program, which will ultimately improve the overall security and risk posture of any organization.

Using Data Security as a Trust Builder

Trust in the protection of employee and customer data privacy should underpin everything security professionals do. People do not work for organizations they do not trust, and customers do not buy from enterprises they do not trust.

The role of security teams is to support business objectives. Specifically, it is to ensure that security

GRANT HUGHES | CISA, CISM, CDPSE, CCSP, CEH, CISSP

Is principal security architect at Engen Oil in South Africa. He has more than 12 years of IT experience and a background in security strategy, architecture, cybersecurity risk and security operations. He can be contacted on LinkedIn at *https://www.linkedin.com/in/grant-hughes-52196569/.*

© 2023 ISACA. All rights reserved. *www.isaca.org*

The reality is that only a limited volume of data can be handled efficiently using traditional manual approaches, and this is where advanced analytics and AI-enabled solutions can add value.

does not adversely impact the customer experience and, above all else, that the trust of stakeholders is maintained. To this end, it is necessary to understand what trust is.

From a customer perspective, trust is a mental state comprised of three things:

1. **Expectancy**—The trustor expects a specific behavior from the trustee.
2. **Belief**—The trustor believes that the expected behavior will occur.
3. **Willingness to assume risk**—The trustor is willing to assume risk based on that belief.[3]

From an organization's perspective, trust is slightly more complex because several components must be balanced to maintain customer trust. According to the International Data Corporation (IDC) trust framework, the components of trust can broadly be categorized into foundational, compulsory and strategic elements.[4]

The foundation of trust is built on the element of risk, which depends on the likelihood and impact of an outcome. Any outcome, whether favorable or unfavorable, could affect an organization's confidentiality, integrity, availability, reputation, productivity or revenue. Therefore, all security decisions should follow a risk-based approach.[5]

Compulsory elements include risk, security, compliance and privacy. These elements can be self-imposed by organizations or mandated by regulations such as the Protection of Personal Information Act (POPIA), the EU General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS). Failure to adhere to regulations can lead to fines, loss of stakeholder trust, and reputational damage that ultimately can harm an organization's trustworthiness.

The strategic layer of trust should include privacy, ethics, assurance and convenience. Although privacy protection is mandated by several laws and regulations that prioritize data protection, organizations can demonstrate to consumers that they value their privacy and as a result generate goodwill, leading to increased loyalty and brand trust. Although not all strategic elements are explicitly mandated by regulatory bodies, organizations can leverage them as strategic initiatives with the aim of increased stakeholder trust and customer retention.

The Threat Landscape Is a Big Data Problem

As digital disruption and expansion continue, there are more attacks, and as a result, more signals, logs and telemetry than ever before, resulting in cybersecurity becoming a big data problem. This is supported by an experiment T-Mobile performed in 2022; T-Mobile placed a honeypot on the Internet to see how often adversaries would target it. It was targeted 65 million times a day.[6]

Threats have become so advanced that it is increasingly difficult to differentiate between authorized and unauthorized users. People can work from any location at any hour of the day. Traditional baselining is simply not enough. Security teams must correlate, normalize and sift through big data sets to find anomalies.

The reality is that only a limited volume of data can be handled efficiently using traditional manual approaches, and this is where advanced analytics and AI-enabled solutions can add value. According to the IDC, there will be 41.6 billion Internet of Things (IoT) devices by 2025,[7] all generating logs and telemetry. The challenge is no longer looking for a needle in a haystack—it is looking for a needle in a pile of needles.

Different Types of Logging Organizations

Historically, logging was rooted in the idea of collecting as much as possible in the hope of meeting future needs. The collect-everything mindset initially seems like an easy approach, but there are cost implications that make it unfeasible for many organizations. This problem is amplified by cloud security providers that make it easy to collect different types of logs, but expensive to collect and retain large volumes of logs.

According to the IBM *Cost of a Data Breach Report 2022*, for an organization with fully deployed AI

© 2023 ISACA. All rights reserved. www.isaca.org

capabilities, the average dwell time—the amount of time that a threat actor remains undetected within a network or system before being discovered—is 181 days.[8] With all the modern solutions provided by security vendors, why does it take so long to detect intruders in an organization's environment?

In *The Defender's Advantage*, Mandiant provides insight into extended dwell time:

> *The Defender's Advantage is based on the notion that organizations are defending against cyberattacks in their own environment. This provides a fundamental advantage arising from the fact that organizations have control over the landscape where they will meet their adversaries. Sadly, organizations struggle to capitalize on this advantage.*[9]

Inadequate security event logging is one of the biggest contributors to extended dwell time. At a high level, there are three categories of organizations when it comes to security logging:

1. **Leave it on default and hope for the best**—This approach is irresponsible and dangerous and will certainly result in blind spots for the security team.
2. **Log it all and let the analyst sort it out**—This is not financially feasible and will, at some point, result in an exorbitant bill (for a cloud-based log solution) or storage capacity challenges (for on-premises solutions).
3. **Purpose-driven logging**—This is a pragmatic and comprehensive approach, informed by use cases and attack models.

Taking a purpose-driven approach to logging is the only way to leverage existing security solutions to the fullest. An SOC and a security information and event management (SIEM) system simply cannot deliver if there are logging gaps.

Logging Gaps and Challenges

A logging gap occurs when one of four conditions arises:

1. **Insufficient logging**—Logs for an action were not captured.
2. **Insufficient verbosity**—Logs were captured, but the required level of detail was not recorded to support the investigation.
3. **Insufficient retention**—Logs were captured with the right level of verbosity, but they were not kept long enough.
4. **Inadequate parsing and normalization**—The correct events at the right level of verbosity were logged, but due to differences in how vendors log these events, security tools may have failed to attribute them to related incidents.

Organizations of all sizes struggle to develop and maintain a purpose-driven strategy and approach to logging and monitoring. This results in an increase in costs to collect, store and monitor logs as well as a fragmented approach to log management that is not aligned to the organization's risk exposure. Ultimately, this impacts the organization's ability to answer key investigative questions such as:

- How did the attacker gain access to the environment?
- How long has the organization been compromised?
- What were the attackers able to access or exfiltrate?

Gaps in logging can have far-reaching consequences if all dependencies are not understood. Consequences may include the inability to comply with ediscovery requests, failure to detect intrusions and inability to perform effective incident response.

Taking a purpose-driven approach to logging is the only way to leverage existing security solutions to the fullest.

A Purpose-Driven Event Logging Framework

A purpose-driven logging approach ensures that all logs being collected support a specific use case that is relevant to the organization. These use cases are underpinned by threat models and incident-response playbooks that clearly identify the required events, along with appropriate technical levels and retention periods. With this approach, it becomes clear which logs should be collected, at what level of verbosity and for how long they should be retained.

Figure 1 outlines a purpose-driven event logging framework that can be adopted by any organization to fast-track a log management program, regardless of the current level of maturity. The framework has nine steps:

1. **Obtain management support**—Security event logging is a significant undertaking and must

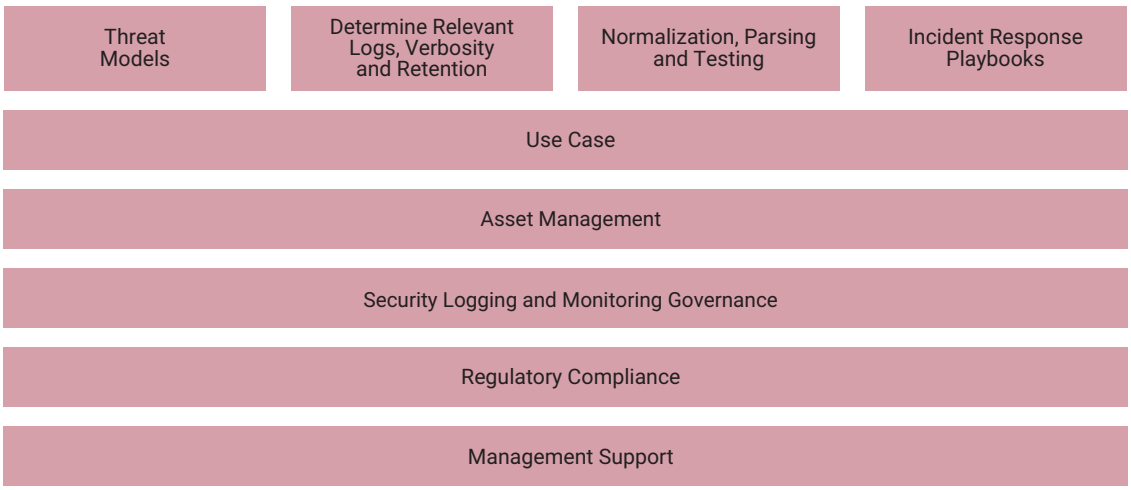
LOOKING FOR MORE?

- Read *Privacy as Design or Default: A Primer. www.isaca.org/Privacy-by-Design*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

© 2023 ISACA. All rights reserved. *www.isaca.org*

FIGURE 1

A Purpose-Driven Event Logging Framework



be justified with a business case. The business requirements for establishing security event logging must be articulated clearly and supported by an approved policy. Resources for training and tools must be made available to support the logging and monitoring strategy.

2. **Determine regulatory requirements**—Organizations must identify the requirements and regulatory obligations that may influence the retention period for event logs. These may include:
   - **Compliance**—Organizations are required to retain their event logs for a specific period as set out by legal and regulatory requirements.
   - **Ediscovery**—Finding and producing electronic documents, including event logs, may be required in response to litigation.
   - **Forensics**—Retention of event logs may be required to support future forensic investigations. In such cases, organizations may need to demonstrate the integrity of the logs as well (i.e., chain of custody).
3. **Establish security logging and monitoring governance**—An organization should have a policy and supporting standards in place for logging and monitoring security events. The policy should outline the systems and devices that should have event logging enabled, the types of events that should be logged (e.g., login attempts, system crashes), how logs should be protected (such as through encryption and access control) and how long the logs should be retained (which may be influenced by regulatory requirements and the need to support investigations).
4. **Asset management**—The first and second Center for Internet Security (CIS) controls (inventory and control of enterprise and software assets) emphasize the importance of asset management.[10] It is only when an organization knows what it has that it can protect and monitor it. The SOC must have access to updated asset inventory information. Establishing the best controls and monitoring practices is pointless if all assets have not been identified. For example, if a domain controller is not known to the SOC and the logs are not being ingested into a SIEM, this will impact the ability of the SOC to detect a security incident involving that specific domain controller.
5. **Define use cases**—The concept of defining or identifying security use cases is closely linked to attack models. A security use case is an attack scenario that a security control is intended to prevent or defend against. Examples include phishing, credential theft and malware infections. The MITRE ATT&CK framework provides a list of use cases from which to select.[11] Attack models should inform security use cases.
6. **Define threat models**—Threat models are created to identify and simulate attacks against security environments using likely adversary techniques and attack paths. By modeling attacks, defenders can better understand the behavior, tactics and objectives of adversaries, and they can take steps to remediate any vulnerabilities within their environments. This provides useful insights on the type of devices that should be in scope for logging and the level of verbosity that should be enabled for logging.

© 2023 ISACA. All rights reserved. www.isaca.org

7. **Determine relevant logs, verbosity and retention**—At this point, it should be clear which log sources should be in scope and which event logs are required, at what level of verbosity and for what retention periods. Once the log sources have been identified, the process of defining a logging standard per log source must be completed. This is a granular exercise that should include performance on the respective appliances. The level of verbosity can have a performance impact, while the local retention policy can have a storage impact. In some cases, this may automatically result in older logs being overwritten.
8. **Develop detection and response playbooks**—A playbook is a list of activities that should be performed in the event of a cyberincident. In most cases, it involves a review of log information. Therefore, it is imperative to ensure that all anticipated log information that could be required has been enabled with the appropriate retention period. A disconnect between the events being logged, the use cases being monitored, and the documented playbooks adversely impacts incident response activities.
9. **Normalize, parse and test**—The final step is to test and validate that event logs are being normalized and parsed correctly. Consider the example of the user field. Some common examples of the user field include User, Usr, Uname,Src_usr, Dst_user, User_name, Sys_created_by, Sys_updated_by. Different systems log this field differently, and if it is not being parsed and normalized correctly, context will be missed and detection rules will fail to alert.

It will take considerable time and effort to get to this level of detail for each use case. However, until that is done, no advanced SIEM, or AI-enabled security solution will save the day.

Effective Logging and Monitoring Strategy

An effective security monitoring strategy must be developed with clear scope and objectives. There are numerous benefits to proactive log management. Without a perceived business purpose, even the best technically designed architectures have no value. Before starting a log monitoring journey, it is necessary to identify, communicate and socialize the business benefits throughout the organization. Examples of objectives may include:

- Improving availability by an amount of time
- Reducing incident response and detection time by an amount of time
- Improving visibility

Before starting a log monitoring journey, it is necessary to identify, communicate and socialize the business benefits throughout the organization.

An effective strategy must be supported with sufficient resources. Cloud computing offers scale and convenience at a cost. An organization must be willing to invest in the program, and a business case will help the security team win buy-in.

Intelligence must also be used to support effective logging and monitoring strategies. Threat intelligence provides context to otherwise meaningless data. The platform that is ultimately used for centralizing log data must incorporate a threat intelligence feed for enrichment and context to enhance detection capabilities.

Metrics must be used as well. Metrics drive behavior. Therefore, it is important that metrics are both meaningful and aligned to the desired behaviors. For example, measuring time to resolution might result in analysts closing calls without following all the steps because there may be a rush to close calls. Examples of good metrics include measuring a managed security service provider (MSSP) on the time to detect and alert and the quality of the alert. Internal SOCs can be measured on the number and type of improvements that were made to processes over time.

To avoid fidelity drift, logging and monitoring must continuously improve. For example, rules might work well for specific times and then stop working due to a rearchitecture of the network or deployment of new technology. The goal of continuous improvement is to identify and learn from past incidents, with the aim of reducing the likelihood of future breaches using similar tactics.

Security Logging Benefits

A purpose-driven logging and monitoring program is likely to yield benefits to the organization, including:

- **Improved capacity planning**—Event logs can be leveraged to support the effective utilization of IT resources and in so doing support the availability

© 2023 ISACA. All rights reserved. *www.isaca.org*

of systems. For example, most hardware devices will issue warnings in the event logs when a hardware module starts failing.

- **Support for forensic investigations**—An important use case for event logs is to support internal and external investigations. When logging has been enabled at the correct level of verbosity, it can answer critical questions related to the types of unusual activity that have been performed; individuals responsible for initiating unusual activities; and the duration of unusual activity, which is critical for future investigations.
- **Improved cost management**—Event logs can be used to demonstrate a return on security investment by showing that security controls are working as expected and meeting business requirements. For example, showing the number of attacks prevented by an intrusion prevention system (IPS) or firewall.

Event logs can be used to identify and analyze threats to systems in near real time.

- **Compliance with regulations, industry standards and best practices**—Despite the obvious benefits and value security event logging provides to organizations, it remains one of the most overlooked areas in security. As a result, an increasing number of regulations and standards have been adopted to provide event logging requirements and guidance:
  - According to the CIS Critical Security Control 8, Audit Log Management, organizations should establish and maintain an audit log management process that defines the enterprise's logging requirements.[12]
  - The International Organization for Standardization (ISO) standard ISO 27001 covers logging and monitoring. The objective of the control is to record events and generate evidence for future investigations.[13]
  - Requirement 10 of PCI DSS 4.0 provides extensive requirements and guidelines for system logging and monitoring.[14]
  - In 2017, the Open Web Application Security Project (OWASP) noted insufficient logging and monitoring as a risk. In 2021, renamed "Security Logging and Monitoring Failures," it is still listed as number 9 on the OWASP Top 10.[15]
- **Support for automated threat detection and response**—Whether they like it or not, security professionals are in a race with the bad guys. In July 2022, Palo Alto Networks released a report stating that attackers scan for vulnerabilities within 15 minutes of common vulnerabilities and exposures (CVE) disclosure.[16] Event logs can be used to identify and analyze threats to systems in near real time. Security orchestration, automation and response (SOAR) technologies are considered a force multiplier; they allow security professionals to do what humans do at scale. SOAR technologies can improve detection and response processes by adding context and enrichment, and in so doing, improve downstream prioritization and efficiency.

Security Logging Challenges

In pursuit of implementing a purpose-driven logging strategy, an organization may face some challenges, including:

- **Lack of management support**—Lack of management support for security event logging initiatives can often be attributed to failures to articulate the link between security event logging and clear business objectives. There are few published examples of security logging resulting in significant business benefits, which may add to the perception that the cost of security logging efforts is disproportionate to the business benefits. Therefore, it is imperative that security professionals paint a clear picture to business leaders of the opportunities that can be realized if security logging has the right level of investment and management support.
- **Lack of asset management**—Incomplete and outdated IT inventory result in a lack of knowledge and visibility into where event logging should be enabled, which is likely to lead to monitoring blind spots. Organizations should establish a comprehensive IT inventory management process that includes regular updates and maintenance to have a clear understanding of all system components and to aid in effective security event logging, monitoring and incident response.
- **Technical complexities**—Technical considerations, such as an out-of-sync system clock, may introduce difficulties to match up events across different systems. Technical complexities could ultimately affect the integrity of the logs and could impact incident response and forensic efforts. Another issue is that logs from different solutions are often in different formats, making it challenging

© 2023 ISACA. All rights reserved. www.isaca.org

to normalize and parse logs. Security teams should be aware of technical complexities and develop strategies to address them.

- **Balance between privacy and regulatory requirements**—Maintaining a balance between privacy and regulatory compliance can be challenging. Organizations may want to collect certain logs and attributes that violate privacy laws in certain countries. This practice may impact forensic investigations and make it difficult for security solutions to present complete event timelines to security analysts.
- **Inadequate storage and network capacity**—Large quantities of event logs may impact storage and network capacity if planning is not done up front. This may have an unintended impact on other applications. When determining the optimal location for a central event logging server, privacy laws, bandwidth limitations and physical security should be considered.
- **Financial impact related to retention guidelines**—Laws and regulations often require organizations to store logs for extended time periods. Finding cost-effective solutions for long-term storage of large volumes of event logs can be challenging. Organizations must ensure that they have a thorough understanding of their log retention requirements and ensure that they apply optimal strategies.

Guidelines for Effective Log Management

To address logging gaps, capitalize on the benefits and improve overall detection and response capabilities, security professionals should focus on educating key stakeholders. It is crucial to educate the organization and the team on the importance of logging and monitoring by creating awareness about the requirements and obligations for logging and monitoring and referencing vendor-neutral and authoritative sources of information. They should also spend time defining attack models and use cases and mapping them to the required event logs.

Alignment with technology vendors is important. It is recommended that security teams proactively engage with their threat detection vendors for input on the mapping of required event logs to different cybersecurity use cases. The vendors should be asked for the mappings that pertain to the organization's technology stack.

Governance remains important and, to this end, policies, standards and guidelines should be documented to empower support teams. It is essential to document concise and easy-to-understand standards and guidelines to maintain continuity. If a new firewall is being installed, the logging and verbosity levels should be clear, and retention periods must be enabled to avoid ambiguity.

Organizations must ensure that they have a thorough understanding of their log retention requirements and ensure that they apply optimal strategies.

An important step is to regularly test the organization's technologies. Simulations should be performed to test whether the configured use cases are triggering alerts as expected. General IT changes may have unintended consequences that can impact previously working use cases and alerts.

Finally, regular and continued health checks must be built into the operating model. Health monitoring is critical because even a perfectly implemented SIEM or other threat detection solution is of no value if it stops working. Health monitoring should include the health of the solution and the health of the log sources. A key consideration includes health alerts and thresholds along with the extent of manual health checks compared to automated health checks. In many cases, automated health alerts require human action to remediate.

Conclusion

In 2015, CrowdStrike published an article titled, "The Importance of Logs." The opening line encapsulates the entire article: "Across all of the nation-state targeted attacks, insider thefts, and criminal enterprises that CrowdStrike has investigated, one thing is clear: logs are extremely important."[17]

In any investigation, the first thing incident response or forensic practitioners do is review the logs. In recent years, the importance of event logging has increased significantly due to the sophistication and volume of attacks. In addition, compliance regulations mandate logging and monitoring to support forensic investigations and to identify and respond to threats in real time.

However, there remains a host of complexities and challenges organizations must address to mature their logging and monitoring capabilities.

© 2023 ISACA. All rights reserved. *www.isaca.org*

In 2003, David Brailsford, a British cycler and coach, was hired to assist with improving performance in British Cycling.[18] At that point, no British cyclist had won the Tour de France in 110 years. Brailsford applied the concept of "tiny gains" by making small incremental changes consistently. As a result, from 2007 to 2017, British cyclists won 178 world championships, 66 Olympic or Paralympic gold medals and five Tour de France victories.

From a security perspective, there is a lesson to be learned from this. It is unlikely that any organization will mature its security logging capability overnight. Starting with small consistent actions—that is, tiny gains—security teams will ultimately move the needle and mature capabilities over time. This will have a positive downstream effect, as all existing and future security capabilities will deliver a better return on security investment (ROSI) as a result.

Endnotes

1 Maliti, S.; "FBI Beat Security Cluster in Identifying Cyber Hack of the SA Reserve Bank, Says Godongwana," *Independent Online*, 15 December 2022, *https://www.iol.co.za/capeargus/news/fbi-beat-security-cluster-in-identifying-cyber-hack-of-the-sa-reserve-bank-says-godongwana-0c5e9af6-00e2-45bd-9867-a386cd351db7*

2 FireEye Mandiant Services, *M-Trends 2021*, USA, 2021, *https://mandiant.widen.net/s/rphjwkvzgp/rpt-mtrends-2021-3*

3 Huang, J.; D. Nicol; "Evidence-Based Trust Reasoning," Information Trust Institute, University of Illinois Urbana-Champaign, USA, April 2014, *https://assured-cloud-computing.illinois.edu/files/2015/08/Evidence-Based-Trust-Reasoning.pdf*

4 Shivhare, Y.; "Building Trust Across the Organization as Cyberattacks Continue to Rise in Canada," International Data Corporation, *https://www.idc.com/ca/blog/detail?id=8b0ed89907914d5933ce*

5 Dickson, F.; "The Five Elements of the Future of Trust," IDC Blog, 22 April 2020, *https://blogs.idc.com/2020/04/22/the-five-elements-of-the-future-of-trust/*

6 Kapko, M.; "T-Mobile CSO: One Wrong Decision Can Wreak Havoc," Cybersecurity Dive, 11 January 2023, *https://www.cybersecuritydive.com/news/tmobile-cso-strategy/640228/*

7 Clements, C.; "IoT: The Internet of Threats and How Users Can Defend Themselves," *Security Magazine*, 24 August 2020, *https://www.securitymagazine.com/articles/93136-iot-the-internet-of-threats-and-how-users-can-defend-themselves*

8 Ponemon Institute and IBM, *Cost of a Data Breach Report 2022*, USA, 2022, *https://www.ibm.com/reports/data-breach*

9 Mandiant, *The Defender's Advantage: A Guide to Activating Cyber Defense*, USA, *https://experience.mandiant.com/defenders-advantage-landing-page/p/1*

10 Center for Internet Security (CIS), "CIS Critical Security Controls Version 8," USA, *https://www.cisecurity.org/controls/v8*

11 MITRE ATT&CK, *https://attack.mitre.org/*

12 Center for Internet Security (CIS), "CIS Critical Security Control 8: Audit Log Management," USA, *https://www.cisecurity.org/controls/audit-log-management*

13 Infocerts, "ISO 27001 Annex: A.12.4 Logging and Monitoring," *https://infocerts.com/iso-27001-annex-a-12-4-logging-and-monitoring/*

14 Baykara, S.; "PCI DSS Logging and Monitoring Requirements," PCI DSS Guide, 20 April 2020, *https://www.pcidssguide.com/pci-dss-logging-requirements/*

15 The Open Worldwide Application Security Project (OWASP), "A09 Security Logging and Monitoring Failures," OWASP Top 10, 2021, *https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/*

16 Swotinsky, E.; "Report: Attackers Scan for Vulnerabilities Within 15 Minutes of CVE Disclosure," Acronis, 30 July 2022, *https://www.acronis.com/en-us/cyber-protection-center/posts/report-attackers-scan-for-vulnerabilities-within-15-minutes-of-cve-disclosure/*

17 Churchill, M.; "The Importance of Logs," CrowdStrike Blog, 16 December 2015, *https://www.crowdstrike.com/blog/the-importance-of-logs/*

18 Clear, J.; " This Coach Improved Every Tiny Thing by 1 Percent and Here's What Happened," James Clear, USA, 2018, *https://jamesclear.com/marginal-gains*

© 2023 ISACA. All rights reserved. *www.isaca.org*