Manage Cloud Logs for Effective Threat Hunting

Executive summary

The many ways of accessing and managing a cloud tenant (often from anywhere in the world) can complicate the problem of security monitoring. Since cloud networks are virtualized, getting to “ground truth” can be difficult. Defense of a cloud tenant hinges on maintaining logs that record the right level of detail on security-relevant events. It also depends on logs that cannot be modified by actors to cover their tracks, even when they can act as administrators. Cloud access policies, system logs, and administrative audits must be controlled and monitored by security engineers and system administrators to prevent access abuse.

Cloud Service Providers (CSP) must have a strong focus on security to maintain reliable business models and to help secure cloud infrastructure. Organizations need to know what should be logged and how those logs should be managed, stored, and analyzed. Security logs can help in several ways, including threat hunting, investigating security incidents, and meeting compliance and audit requirements.

Cloud log benefits

Appropriate cloud logging can provide several benefits for an organization, including for:

- **Threat hunting operations** - Cloud security logs provide a detailed record of activity, which can be used to detect security threats early on. Under MITRE’s D3FEND™ matrix, the use of logs is broadly applicable under the Detect category. [1] By monitoring security logs, organizations can identify suspicious activity, such as command and control activity, lateral movement, or other techniques as described in MITRE’s ATT&CK® matrix. [2] Detection would then allow network defenders to take appropriate mitigation actions against the threat.

D3FEND Tactic	Countermeasures
Detect	Network Traffic Analysis [D3-NTA]
Detect	Platform Monitoring [D3-PM]
Detect	Process Analysis [D3-PA]

D3FEND Tactic	Countermeasures
Detect	User Behavior Analysis [D3-UBA]

ATT&CK Tactic	Technique
Command and Control	Non-Application Layer Protocol [T1095]
Lateral Movement	Remote Services [T1021]

- **Investigation of security incidents** - Cloud security logs can provide context about a potential security incident and the root cause. Logs can be used to reconstruct the sequence of events leading up to the incident, identify sources, and determine the extent of the exposure.
- **Compliance and audit requirements** - Regulatory and compliance requirements are prevalent, and cloud security logs can help organizations comply with regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), PCI Data Security Standard (PCI-DSS), and European Union's General Data Protection Regulation (GDPR).

What should be logged in the cloud?

Organizations cannot realistically log, organize, and analyze everything in an environment as the operational cost prevents that. However, CSPs may not enable critical logs by default or require critical logs to be configured to work properly with collection mechanisms, leading to a dearth of information during investigations and threat hunting operations. [3] Organizations must find a balance between logging requirements and resource constraints. Organizations should also prioritize choosing CSPs that embrace secure by design principles and provide appropriate logging. [4], [5]

Logging requirements will vary among organizations depending on things such as business needs, known threats, and relevant regulations. Resource constraints invariably include costs, product and tool interoperability, network speed and bandwidth, and other complex restrictions. Therefore, prioritizing which logs to collect and analyze must be part of a thorough cloud security plan. Start with two questions:

1. From what sources should logs be collected?
2. What types of logs should be collected from those sources?

Log sources

During the SolarWinds incidents, Russian actors were able to use cloud APIs to exfiltrate data from their targets' cloud environments. They were also able to add credentials, authenticate to cloud services, add permissions to applications, and move laterally throughout the cloud using specific cloud APIs, which prevented their activity from being logged in conventional web console logs. The SolarWinds incident served as a wake-up call to the industry on how malicious agents might exploit cloud operations in ways that are difficult to detect. [6], [7]

To help detect similar breaches in cloud networks, organizations need to enable or add logging capabilities for business critical applications, hosts, networks, and cloud API calls. Cloud logs for the security of infrastructure include:

- **Authentication and authorization** - User and service events, such as login, authentication, and authorization attempts, and changes to user roles or permissions along with the creation of new users.
- **Network and security** - Networking related events, such as firewall services blocking incoming network connections, network flows, intrusion detection system events, and network configuration changes.
- **System and application** - System and application security events, such as changes to system configurations and security policy violations.
- **Audit and compliance** - Events for audit and compliance requirements, such as for data access, data protection, and compliance with regulatory standards.
- **Application programming interface (API)** - Events in a cloud platform, such as resource provisioning, usage and cost analysis, and service configuration changes.
- **Short-term cloud resources** - Resource events, such as virtual machines, containers, or other services that are rapidly spun up or down.

Analyzing these logs helps to identify security risks, detect incidents and anomalies, and respond to events quickly. However, many applications and data sources that handle critical information produce logs with few details and security context. Organizations must prioritize logs based on their value and completeness.

Event types

Cloud event types depend on the services and actions being performed, including:

1) **User and resource actions** - Events or actions by users and applications, such as user logins, account creation, API calls, and configuration changes, or actions taken on cloud resources, such as launching a resizable computing capacity instance, modifying a database, or deleting a storage resource.
2) **Security, error, and performance events** - Security-related activities, such as attempts to access a resource without authorization, changes to security settings, or the detection of a threat; as well as, events related to errors and performance issues, such as failed API calls, resource timeouts, or service disruptions.
3) **Compliance and billing events** - Events related to costs, policy compliance, and privacy, such as changes to access policies, data privacy violations, or audit-related events; as well as billing and cost-related activities, such as changes to pricing plans, usage-based billing events, or cost optimization recommendations.

Logging of these event types is critical for understanding actions within a cloud environment and for detecting and responding to threats, performance issues, compliance violations, and other important events.

Cloud log management

Due to the potential for an immense amount of data to come in from logs, a robust log management strategy is vital. The use of Security Information and Event Management (SIEM) and/or Security Orchestration, Automation, and Response (SOAR) tools to efficiently manage and process the data into actionable alerts will likely prove to be imperative. Even in short-lived resource environments where traditional SIEMs do not have significant visibility, a number of offerings exist from vendors who have the capability to handle logs in temporary environments. In addition to SIEM and SOAR products, CSPs often offer log centralization services where logs can be sent to a centralized location for any related analysis.

Logs stored in a centralized location make log monitoring and analysis easier. Retention guidelines vary among organizations based on what is logged and the regulations that the data is subject to. Limits may be placed on a CSP’s log retention based on policy or

pricing. Managing cloud logs correctly can prevent inundation by implementing the following strategies, including:

- **Log filtering** - Filter logs to remove noise and reduce the data volume. Logs can be filtered on criteria such as type, severity, IP address, or keywords.
- **Log sampling** - Sample logs to reduce the data being retrieved or analyzed. This takes a representative sample of logs rather than every event.
- **Log aggregation** - Aggregate logs from multiple sources into a single stream, which can reduce the volume of log data being stored and analyzed.
- **Log compression** - Compress logs to reduce the file size, the data transmitted, and also allow for longer retention.
- **Log streaming** - Stream logs to an analysis tool for processing as they are generated rather than storing them locally, to reduce stored data.
- **Log retention** - Define retention policies that specify log storage and deletion. This can reduce the amount of log data being stored over time.

These strategies should be applied differently to different log sources and event types as appropriate. For example, sampling of network metadata logs may be appropriate, while sampling user authentication logs may not.

Preventing inundation requires strategies that balance the need for capturing important events while reducing the log volume. The location and storage method of security logs can vary depending on the cloud platform and the logging service being used, but some common storage options include:

1. **Cloud-based storage service** - Cloud platforms offer storage for security logs. These can store large amounts and offer features such as versioning, access control, and data durability.
2. **Cloud-native logging services** - Platforms offer services that are specifically designed for storing and analyzing logs generated within a cloud environment.
3. **Third-party log management** - In some cases, organizations may choose to use third-party log management tools to store and analyze security logs generated within the cloud environment.

Security logs must be stored and protected from unauthorized access and prevent any editing, alteration, or deletion. This includes employing measures such as encrypting, restricting access, and implementing monitoring and alerting to detect any suspicious activity related to the logs.

Cloud log analysis

As previously described, the use of a SIEM and SOAR solution is important, as vast amounts of data and information could come in at any time. Cloud platforms often have internal tools that collect and analyze data from various sources, including cloud provider resources, associated operating systems, and applications to provide insights on the health, performance, and security of system resources and services.

The following steps help with log collection and analysis in cloud platforms:

1. **Identify sources** - Find sources that generate security events. Sources such as virtual machines, storage accounts, databases, security groups and more. An administrator defines the criteria for analysis, such as unusual or suspicious activity, failed login attempts, unauthorized access attempts, and so on.
2. **Enable, review, and adjust settings** - Enable and configure the logging settings to capture, analyze, and store data, such as user and application activity, transactions, and changes to configurations. Regularly review and adjust these log settings and tools to ensure that a system is capturing all relevant data and that the analysis techniques are effective.
3. **Collect and store logs** - Collect and store logs from different sources in a centralized location. Use log management tools to collect and store logs.
4. **Normalize and enrich logs** - Normalize the logs from different sources to a common format and enrich them with context and metadata, such as IP addresses, user identities, and timestamps. Adhere to a public standard for log formats, such as the NCSA Log Format for web services or the Open Cybersecurity Schema Framework. [8], [9]
5. **Analyze logs** - Choose a primary log analysis tool for log formatting and custom queries. This tool can be used to investigate and analyze the root cause of an incident and identify any suspicious or anomalous activity. Look for events that

could indicate security risks, such as unauthorized access attempts, changes to configurations, and unusual patterns of behavior.

6. **Correlate logs** - Correlate logs from different sources to identify patterns that could indicate a security incident. For example, multiple failed login attempts from different IP's for the same user account could indicate brute force attempts.
7. **Perform active threat hunting** - Investigate security incidents by reviewing the relevant logs and taking appropriate actions, such as revoking user access.
8. **Support vulnerability assessment and penetration testing** - Use logs to help identify exposed cloud resources and weaknesses in the cloud environment.
9. **Create queries and alerts** - Once security logs are collected and stored, create queries to retrieve and analyze the data. SIEM and SOAR products, as well as CSP tools, may aid in creating useful queries. Use these to gain insights into alerts, vulnerabilities, and compliance status. Custom queries help to make security processes much more efficient when data targets are previously known. A user can configure alerts when certain events or conditions occur in the security logs.

Analyzing security logs to gain insight into an organization's security posture requires a combination of technical expertise, analytical skills, and an understanding of the environment. These steps help a user to analyze cloud platform security logs, hunt threats, and respond to incidents in the cloud environment.

Cloud log security

When a system does not implement controls to track and log user actions, it opens itself to manipulation, forging, or deletion of not only data and files, but also the logs that would reveal such activity.

For example, in 2016 Russian actors hacked the Democratic National Convention and wiped away traces of their operations by destroying system logs. [10], [11] MITRE's ATT&CK matrix documents how potential malicious actors could manipulate logs to their advantage. Examples include 'Indicator Removal' where adversaries remove logs showing evidence of their actions or 'Impair Defenses' in which logs could be disabled entirely. Allowing for these malicious log manipulations can degrade security and allow for impersonation and spoofing.

ATT&CK Tactic	Technique
Defense Evasion	Impair Defenses: Disable Cloud Logs [T1562.008]
Defense Evasion	Indicator Removal [T1070]

Unauthorized alteration or deletion of logs will invalidate any operations based on those logs. Organizations should take the security of their logs just as seriously as that of their critical applications.

An inability to properly control logs allows for manipulation of identities and actions, and prevents user-action accountability. Maintaining accountability is vital in any setting; however, the communal nature of the public cloud stresses the need for security and accountability to keep records and to prevent any false accusations, as seen in the STRIDE threats: [12], [13]

- Spoofing identity – to impersonate an entity during authentication.
- Tampering with data – unauthorized data alteration.
- Repudiation – denying and/or covering up one's own actions.
- Information disclosure – the unauthorized release of system information.
- Denial of service – forced service unavailability.
- Elevation of privilege – illicit acquisition of additional higher-level privileges.

For example, repudiation refers to when malicious actors are able to deny attribution of any actions. The countermeasure to repudiation is to establish accountability mechanisms that verify that a user performed a specific action. Cloud logs help protect against repudiation by providing a trail of evidence that can be used to verify the authenticity and integrity of transactions and events. Events, such as user actions that are inconsistent with the expected behavior or unauthorized changes to configurations, can indicate tampering of data. Logs help to generate audit trails for a complete and accurate record of actions, including information such as user identity, time stamps, and transaction details. Users with cloud access cannot falsely deny performing an action. Not only does this allow a host to track individual actions, but maintaining proper logs will also help prevent false accusations of users' actions. [14]

Best practices

Cloud logs can help protect networks by providing visibility into network activity and detecting and alerting on potential security threats. Cloud administrators should implement the following as a baseline:

1. **Log as much security relevant information as possible** - Organizations need to determine their logging capabilities, log everything possible up to that extent that is security relevant, and should prioritize the event sources and types listed in the "What should be logged in the cloud?" section.
2. **Implement a management plan for the logs** - Poorly managed logs will hinder an organization and make forensic and hunting operations infeasible. Establish good log management plans and practices, including, but not limited to, centrally aggregating logs, applying filters, and following a retention plan suitable for whatever regulations and practices apply. Many CSPs provide log aggregation tools that can ease log collection and management for organizations.
3. **Use a SIEM and/or SOAR to analyze logs and improve hunt and forensic operations** - Cloud defenders will be easily overwhelmed if they were to manually search through logs for hunt and forensic operations. Organizations should use a SIEM to help organize and process log data so that defenders can properly analyze events to discover and respond to threats. Most CSPs offer machine-learning-based log analytic tools. This can be beneficial, as traditional SIEM tools may not effectively map actions across cloud resources.
4. **Protect the logs** - Malicious agents can target logs and logging infrastructure to hide their presence, erase evidence, or otherwise repudiate their actions. Controls on who may access and modify logs, primarily using a log administrator role that is distinct and isolated from other administrator roles, should be established. Network communications with log data should be encrypted to help protect the integrity of logs. Ensure that the logs and the logging service are available when they are needed by using a robust logging service and by hardening the central logging appliance or repository.

Cloud logs are an essential tool for defending networks by providing visibility into network activity, identifying security threats, and supporting swift incident response. By

using cloud logs effectively, organizations can develop their security posture and defend their networks from cyber threats.

Additional references

Readers can obtain additional details and guidance from the following publications:

- NIST Special Publication 800-92: Guide to Computer Security Log Management
- Guidance for Implementing M-21-31: Improving the Federal Government's Investigative and Remediation Capabilities
- https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf

Works cited

[1] The MITRE Corporation. MITRE D3FEND: A knowledge graph of cybersecurity countermeasures. 2023. https://d3fend.mitre.org

[2] The MITRE Corporation. MITRE ATT&CK: ATT&CK Matrix for Enterprise. 2024. https://attack.mitre.org/

[3] SANS Institute. A SANS 2021 DFIR Cloud Report: Partly Cloudy with a Bunch of DFIR. 2021. https://www.sans.org/white-papers/sans-2021-dfir-cloud-report-partly-cloudy-with-bunch-dfir/

[4] Cybersecurity and Infrastructure Security Agency et al. Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software. https://www.cisa.gov/resources-tools/resources/secure-by-design

[5] Cybersecurity and Infrastructure Security Agency. When Tech Vendors Make Important Logging Info Available for Free, Everyone Wins. 2023. https://www.cisa.gov/news-events/news/when-tech-vendors-make-important-logging-info-available-free-everyone-wins

[6] Cybersecurity and Infrastructure Security Agency. AA21-008A: Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments. 2021. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-008a

[7] Cybersecurity and Infrastructure Security Agency. AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a

[8] Microsoft. NCSA Logging. 2019. https://learn.microsoft.com/en-us/windows/win32/http/ncsa-logging

[9] Open Cybersecurity Schema Framework. OCSF Schema. 2024. https://schema.ocsf.io/

[10] U.S. Department of Justice. United States of America v. Viktor Borisovich Netyksho et al. 2018. https://www.justice.gov/file/1080281/download

[11] CrowdStrike. CrowdStrike's work with the Democratic National Committee: Setting the record straight. 2020. https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

[12] Microsoft Corporation. Microsoft Threat Modeling Tool threats. 2022. https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats

[13] Open Worldwide Application Security Project (OWASP). Threat Modeling Process. 2023. https://owasp.org/www-community/Threat_Modeling_Process#stride

[14] Open Worldwide Application Security Project (OWASP). Repudiation Attack. 2020. https://owasp.org/www-community/attacks/Repudiation_Attack

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Trademarks

ATT&CK and MITRE and are registered trademarks of The MITRE Corporation. D3FEND is a trademark of The MITRE Corporation.

Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
General Cybersecurity Inquiries or Customer Requests: Cybersecurity_Requests@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov