Event Logging & Threat Detection

Why are proper logging practices so important?

An institution's system event logging practices can provide increased visibility into system performance and compliance with established institutional security policies. In addition, strong logging practices often provide the first indicators of system incidents and compromise and can provide valuable support to incident response efforts. Visibility through logging should be considered immutable; without it, organizations cannot attribute or respond to cyber threats proactively, nor can they effectively investigate and reconstruct incidents after they occur. Ransomware and nation-state threat actors leverage **"living off the land"**, or **LOTL**, techniques to maintain hard-to-detect persistence in systems - sometimes for months at a time. The increased prevalence of malicious actors employing LOTL techniques further highlights the importance of implementing and maintaining an effective event logging solution.[1]

What are "living off the land" (LOTL) techniques?

In simple terms, "living off the land", or LOTL, techniques allow threat actors to leverage and abuse native tools and processes on systems, such as existing, legitimate binaries, that are already trusted in the institution's environment. Once a system or network has been compromised, these LOTL techniques allow the threat actor to conduct their operations discreetly by blending with typical system and network behavior, potentially eluding basic endpoint security capabilities. These techniques work very well for the threat actor because (a.) "many organizations lack effective security and network management practices (i.e., established baselines) that support detection of malicious LOTL activity; (b.) there is a general lack of conventional indicators of compromise (IOCs) associated with the activity, complicating network defenders' efforts to identify, track, and categorize malicious behavior; and (c.) it enables cyber threat actors to avoid investing in developing and deploying custom tools." Default logging configurations often do not comprehensively log indicators of LOTL techniques or provide sufficiently detailed information to differentiate malicious activity from normal, legitimate activity. In addition, system defenders may also find it difficult to identify a relatively small volume of malicious activity contained within vast amounts of log data.[2]

Countering LOTL techniques and improving logging and threat detection practices

There are four best practices identified to improve logging and threat detection practices and defend against the use of LOTL techniques associated with cloud services, enterprise networks, enterprise mobility, and operational technology (OT) networks: *Enterprise-approved event logging policy*, *centralized event log collection and correlation, secure storage and event log integrity,* and *detection strategy for relevant threats*.[3]

Enterprise-approved event logging policy

An enterprise-approved event logging policy increases consistency of logging practices throughout the organization and increases the chances of detecting malicious behaviors. This policy should consider any

[1] CISA (Jointly with NSA, FBI, and others). *Best Practices for Event Logging and Threat Detection.* August 22, 2024.
[2] CISA (Jointly with NSA, FBI, and others). *Joint Guidance: Identifying and Mitigating Living off The Land Techniques.* February 7, 2024.
[3] CISA, August 22, 2024.

shared responsibilities between the institution and its service providers and should include "details of the events to be logged, event logging facilities to be used, how event logs will be monitored, event log retention durations, and when to reassess which logs are worthy of collection". The policy should focus on enabling the capture of "high quality cybersecurity events to aid network defenders in correctly identifying cybersecurity incidents". The policy should also address requirements that event logs be sufficiently detailed to enable forensic investigations and assist network defenders and incident responders. While developed as guidance for U.S. Federal Civilian Executive Branch agencies, the guidelines found in *US Office of Management and Budget's M-21-31 (OMB M-21-31)* document can provide useful guidance to financial institutions regarding specific data event logs should capture.[4] Logging practices should consider an appropriate degree of logging for OT devices and aim for consistency in content, format, and timestamping. Finally, log retention periods should ideally be driven by risk assessment of the subject system, and logs should be retained "long enough to support cybersecurity incident investigations". Effective logging solutions aim to reduce alert noise to increase savings on costs associated with storage and query time.[5] Prevailing guidelines for Federal agencies, as reflected in OMB M-21-31, require the retention of logs for 12 months (active storage) and 18 months (cold data storage).[6] Longer retention periods often equate to greater success in evaluating the scope of a cybersecurity incident.[7]

Centralized event log collection and correlation

The effectiveness of log monitoring can be enhanced through the centralization and correlation of event logs produced by various areas of the organization. *This enables prompt, efficient organization and identification of deviations from baselines, as well as cybersecurity events and incidents, through one continuous, centralized process.* Prioritization of logs from enterprise networks ideally focuses on logs from sources including, but not limited to, critical systems and data most likely to be targeted in an attack, internet-facing services, identity and domain servers, edge devices such as boundary routers and firewalls, admin workstations, and highly privileged systems and data repositories. In the OT environment (i.e., security systems, ATMs, point-of-sale systems, card personalization equipment, network-connected smart devices, etc.), areas for prioritization include those OT devices critical to safety and service delivery, internet-facing OT devices, and OT devices accessible via network boundaries. For mobile devices, logs from web proxies used by organizational users, organization operated DNS services, device security and behavior of organizationally managed devices, and user account behavior (e.g., sign-ins) should be prioritized in the organization's mobility solution. Finally, for cloud environments, organizations should adjust logging practices in line with the cloud service being administered (i.e., IaaS, SaaS, PaaS, etc.). Logs from critical systems and data most likely to be targeted; internet-facing services; tenant accounts that access and administer cloud services; logs for admin configuration changes; and logs for creating, modifying, and deleting security principles, including setting and changing permissions, should be prioritized.[8]

[4] US Office of Management and Budget. *Memo M-21-31: Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*. August 27, 2021.
[5] CISA. August 22, 2024.
[6] US Office of Management and Budget. August 27, 2021.
[7] CISA. August 22, 2024.
[8] Ibid.

Secure storage and event log integrity

Cyber threat actors are known to target local system event logs for deletion or modification to "avoid detection and to delay or degrade the efficacy of cybersecurity incident response". Any log forwarding agents used by the institution should be properly secured and monitored. In addition, CISA recommends the use of cryptographic verification to ensure the integrity of event logs in-transit and at rest, prioritizing those records that have a justified requirement to record sensitive data. Access to delete, modify, or review audit logs should be limited to personnel with a justified requirement. Logs should ideally be stored in a separate or segmented network with additional security controls to help lessen the risk of tampering in the event of a network or system incident. Secure backup and data practices should also be implemented, and SIEMs should ideally be hardened and segmented from the general IT environment.[9]

Detection strategy for relevant threats

CISA also recommends that organizations consider the implementation of user and entity behavioral analytics to better detect anomalous behavior on networks, devices, and accounts. A SIEM (security information and event management system) can detect unusual activity in the areas through the comparison of event logs to normal baseline business activity and traffic. The use of behavioral analytics can also be very helpful in detecting the use of LOTL techniques.[10]

[9] Ibid.
[10] Ibid.