Event Logging & Threat Detection
Questions Board Members Should Ask

Below are some questions you may ask management to ensure that event logging and threat detection processes are sufficient to address ongoing and emerging threats against the institution.

1. ***Does the institution have an enterprise-approved event logging policy?***

   WHY THIS IS IMPORTANT: According to CISA, an enterprise-approved event logging policy increases consistency of logging practices throughout the organization and increases the chances of detecting malicious behaviors. For financial institutions, this policy should:

   - *Consider any **shared responsibilities** between the institution and its service providers;*
   - *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;*
   - *Focus on **capturing high quality cybersecurity events** to aid network defenders in correctly identifying cybersecurity incidents;*
   - *Address requirements that event logs contain **sufficient detail to aid network defenders and incident responders**;*
   - *Consider an appropriate degree of **logging for any network-connected operational technology (OT) devices** (i.e., security systems, ATMs, point-of-sale systems, card personalization equipment, network-connected smart devices, etc.) and aim for consistency in content, format, and timestamping; and*
   - *Ideally be driven by **risk assessment of the subject system**.*

   Event logs should be detailed and retained long enough to support cybersecurity incident investigations and assist network defenders and incident responders. Longer retention periods often equate to greater success in evaluating the scope of a cybersecurity incident. The most effective logging solutions will aim to reduce alert noise to increase savings on costs associated with storage and query time.[1]

2. ***Does the institution have a process for the centralized collection and correlation of event logs produced from various areas of the institution (e.g., enterprise networks, operational technology (OT) networks, mobile devices, cloud environments)?***

   WHY THIS IS IMPORTANT: 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. This centralization and correlation of log data considers inputs from areas such as enterprise networks, OT networks, mobile devices, and cloud environments. Moreover, within these areas, the institution should consider risk-based prioritization of inputs based on, but not limited to, logs for critical systems and data most likely to be attacked, areas considered critical to services and

[1] CISA (Jointly with NSA, FBI, and others). *Best Practices for Event Logging and Threat Detection.* August 22, 2024.

operations, internet-facing services, and logs for configuration changes and other administrative activity.[2]

3. ***Does the institution have a process to assure the security and integrity of local system event logs?***

   WHY THIS IS IMPORTANT: Cyber threat actors are known to target local system event logs for deletion or modification to elude detection and to delay or degrade the efficacy of the institution's incident response efforts.

   - ***Maintaining Data Integrity:*** *CISA recommends the use of cryptographic verification techniques 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 Control:*** *Access to delete, modify, or review audit logs should be limited to personnel with a justified requirement.*
   - ***Log Storage:*** *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.*
   - ***Log Backups and Security:*** *Secure backup and data practices should also be implemented, and security information and event management systems (SIEMs) should ideally be hardened and segmented from the general IT environment.*[3]

4. ***Does the institution utilize user and entity behavioral analytics to detect anomalous behavior or activity on networks, devices, and accounts?***

   WHY THIS IS IMPORTANT: CISA recommends that organizations consider the implementation of user and entity behavioral analytics to better detect anomalous behavior on networks, devices, and accounts. A SIEM 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 "living off the land", or "LOTL" techniques, which are increasingly being used by both ransomware and nation-state threat actors to evade detection.

   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.[4]

[2] Ibid.
[3] Ibid.
[4] CISA (Jointly with NSA, FBI, and others). *Joint Guidance: Identifying and Mitigating Living off The Land Techniques.* February 7, 2024.