Evaluating and Improving Logging and SIEM Programs

Why logging matters

Logs are not just compliance evidence. They are often the fastest way to detect malicious activity, reconstruct an incident, determine scope, and prove recovery actions. CIS Control 8 defines the goal clearly: collect, alert, review, and retain audit logs for events that help detect, understand, or recover from an attack. Source: https://www.cisecurity.org/controls/audit-log-management

What to evaluate in a logging or SIEM solution

Area	What to look for	Why it matters
Coverage	Endpoints, servers, cloud, identity providers, network devices, DNS, web proxy, EDR, firewalls, SaaS, and service provider logs	Blind spots become attacker hiding places. CIS recommends enabling audit logging across enterprise assets and collecting service provider logs where supported.
Centralization	Ability to aggregate logs from multiple sources into one searchable platform	CIS recommends centralizing audit log collection and retention, with SIEM as a common implementation
Detection quality	Correlation rules, behavioral analytics, threat intelligence, entity context, and MITRE ATT&CK-style mapping	A SIEM should turn events into actionable detections, not just store logs. CIS Control 13 recommends centralized security event alerting for log correlation and analysis.
Log detail	Event source, date, username, timestamp, source address, destination address, command-line activity, DNS queries, and URL requests	CIS recommends detailed logging for sensitive assets and specifically calls out DNS, URL, and command-line audit logs
Retention and storage	Hot, warm, and cold storage options with clear retention, searchability, and legal hold capabilities	CIS recommends retaining audit logs for at least 90 days and ensuring logging destinations have adequate storage.
Time accuracy	NTP support, normalized timestamps, and timezone consistency	CIS recommends at least two synchronized time sources where supported, which is essential for incident timelines.

Usability	Fast search, dashboards, role-based access, simple investigations, case management, and clear alert context	Tools fail when analysts cannot use them quickly during an incident.
Operations	Rule tuning, health monitoring, parser management, source onboarding, change control, and ownership model	CIS recommends weekly or more frequent log reviews and monthly or more frequent alert threshold tuning.

Quick self-assessment

Ask these questions before buying a new tool or renewing the current one:

1. What critical systems are not sending logs today?
2. Can we detect misuse of privileged accounts within minutes?
3. Can we reconstruct a ransomware timeline from initial access to encryption?
4. Are DNS, URL, identity, endpoint, cloud, and command-line logs searchable in one place?
5. Do we review and tune detections on a defined schedule?
6. Are logs protected from tampering and retained long enough to support investigations?

Useful Tools

Sigma is a generic, open, and structured detection format that allows security teams to detect relevant log events in a simple and shareable way. repository offers more than 3000 detection rules of different types and aims to make reliable detections accessible to all at no cost. https://sigmahq.io/ and https://github.com/SigmaHQ/sigma

Sysmon is a Microsoft Tool that provides detailed information about process creations, network connections, and changes to file creation time by writing that information to the event log. https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

Winlogbeat reads from one or more event logs using Windows APIs, filters the events based on user-configured criteria, then sends the event data to the configured outputs (Elasticsearch or Logstash). https://www.elastic.co/docs/reference/beats/winlogbeat

Actionable takeaways for improving your current environment

- **Document the logging standard:** Define what must be logged, where logs go, who reviews them, how long they are retained, and what events require alerting. CIS recommends a documented audit log management process covering collection, review, and retention.
- **Inventory your log sources:** Compare asset inventory against SIEM ingestion. Identify systems that can produce logs but are not sending them.
- **Prioritize high-value sources:** Start with identity, privileged access, EDR, firewalls, DNS, cloud control plane, VPN, email security, and critical applications.
- **Normalize time:** Validate NTP configuration and timestamp consistency before the next incident.
- **Collect richer telemetry:** Add DNS, URL, command-line, authentication, authorization, user management, and sensitive data access events where supported.
- **Retain enough data to investigate:** Use tiered storage so critical security logs remain searchable while meeting at least the CIS 90-day minimum.
- **Tune for actionability:** Review noisy alerts monthly, suppress low-value events, add context, and track alert fidelity using true positive and false positive rates.
- **Review logs on a schedule:** Assign ownership for weekly anomaly review, daily alert triage, and periodic control testing.
- **Protect the logs:** Restrict access, prevent unauthorized modification or deletion, and monitor for logging failures or disabled agents.
- **Test with real scenarios:** Run tabletop exercises and detection tests for ransomware, credential abuse, impossible travel, privilege escalation, lateral movement, and data exfiltration.

Sources for CIS Recommendations

https://cas.docs.cisecurity.org/en/latest/source/Controls8/

https://www.cisecurity.org/controls/cis-controls-navigator

Closing message

The best SIEM is not the one with the most data. It is the one that gives your team the right data, at the right time, with enough context to act.