Logging and monitoring: which logs do you need, and which alerts deserve a person?

This month, send Entra, Microsoft 365, cloud and server logs to a store that your everyday admin accounts can't change or delete, and keep 12 months of them, the first 6 searchable, matching the new baseline for US federal agencies[2]. Then alert on the few events that are rarely harmless, give each alert a named owner and deputy, and prove every month that the alerts still reach them.

Reviewed	Next review	Version
4 Nov 2026	**4 Dec 2026**	**1.0**

Written for
IT and security teams in small and mid-size organizations without a 24/7 SOC, many on Microsoft 365 and Entra ID with some on-premises servers and cloud workloads

Latest version
sheets.einblick.dev/logging/

If you only do five things

1. **Get logs out of their default stores.** Entra keeps sign-in and audit logs 7 days on Free and 30 on P1 or P2[8]; the Azure Activity log[10] and CloudTrail event history[11] keep 90 days. Export each one this month.
2. **Keep the copy where your admins can't delete it.** Attackers delete local logs to hide[1]. Use a separate AWS log archive account[11] or Azure subscription with its own admins, on immutable storage that even account administrators can't delete[13].
3. **Turn on the Windows logging that's off by default.** Enable **Audit Process Creation** with command lines[14] and **PowerShell Script Block Logging**[15], plus at least the minimum audit policy for Windows Event Forwarding[16].
4. **Name who answers each alert.** Send alerts to a shared mailbox and a phone, with a named person and deputy each week. If nobody answers at night, pay a managed detection service before buying tools.
5. **Alert when a source goes quiet, and test monthly.** Alert on unexpected log termination, as Mandiant advises[4]. Monthly, run Defender for Endpoint's detection test on a server, which raises an alert in about 10 minutes[24], and check that a person saw it.

Check whether your logging would hold up

1. **Could you see an admin sign-in from 10 months ago?** If not, extend retention. In some cases it takes up to 18 months to discover an incident[1], and Mandiant calls standard 90-day retention insufficient for scoping intrusions[4].
2. **Who could erase the central copy?** List every account that can delete logs or stop collection. If any of them is an everyday admin account, separate the store.
3. **Do all clocks agree?** Point the PDC emulator in the forest root at a reliable external source; domain members follow the domain hierarchy[18]. Store timestamps in UTC as ISO 8601 and use more than one time source[1].
4. **Is every planned source arriving?** Compare the asset list with the sources that sent data this week. The BSI's federal standard requires this check after rollout, including data formats and time sync[6].
5. **When did an alert last reach someone after hours?** If nobody knows, raise a test alert on a Sunday evening and time the response.

Logs to collect first

- **Rank by what attackers want.** ASD's top three are critical systems and data, internet-facing services, and identity servers[1].
- **Entra ID.** Export sign-in logs, including non-interactive and service principal ones, audit logs and Graph activity logs (P1 or P2)[9], kept only if exported[8]. For Microsoft 365, see the incident response sheet.
- **Linux.** On RHEL, copy one set of sample rules, such as the STIG set, from `/usr/share/audit/sample-rules` to `/etc/audit/rules.d/` and run `augenrules --load`[19]. Log use of curl, systemctl and python[1].
- **Cloud.** In AWS, use a multi-Region trail with log file integrity validation[11]. In Azure, add an Activity log diagnostic setting per subscription; a management group setting misses some events[10].
- **Hypervisors.** Forward their logs too: Mandiant calls them the only way to detect snapshot tampering or rogue virtual machines[4].

Retention and cost

- **Keep 12 months, 6 of them searchable.** That's the minimum for US federal agencies since May 2026[2], and a sound default.
- **Tier the storage.** Keep recent logs hot and older ones cold[1]. Sentinel's first 90 days of retention are free, and its lake tier is cheaper[20].

Alerts worth a person's time

- **Logging stopped or cleared.** Windows events 1102 and 104 mean a log was cleared[16]. Also alert on deleted diagnostic settings and stopped trails.
- **New admin rights.** Use the privileged access sheet's list for AD groups and Entra roles, and the edge devices sheet's for firewalls and VPNs.
- **Mail forwarded outside.** The default policy **Suspicious email forwarding activity** is High severity and on by default in E1, E3 and E5[22]. Add your alert mailbox as a recipient.
- **Security tools changed.** Alert when someone changes Defender or logging settings or disables monitoring services[1].
- **High-severity incidents.** Create a Defender XDR email rule for High and Medium incidents and use **Send test email**[23].
- **Large data exports.** ASD advises alerting on large or continuous exports by default[1].

What changed in 2026

- **The US federal baseline was cut.** In May 2026, OMB's M-26-14 replaced M-21-31, whose retention of vast log volumes without clear utility proved neither feasible nor cost-effective for most agencies[2].

- **Start with what's free.** Sentinel ingests Azure Activity, Office 365 audit logs and Defender alerts free; raw Entra ID and Defender logs cost extra[20].
- **Filter at the source.** Collect Windows security events with the Common or Minimal set, and keep non-security data in a separate workspace[21].
- **Write the period down.** NIS2 rules for digital providers require one[5]. The BSI suggests 90 days for federal logs, then requires deletion, except for attack-related events and security events without personal data[6].

What you can skip

- **Sending everything to the SIEM.** CISA notes that SIEM-first designs often get costly as volume grows[3]. Keep bulky logs in cheaper storage.
- **Microsoft service principal sign-in logs.** Microsoft calls this preview log high-volume and not essential for security investigations[9].
- **Data access logs everywhere.** Google Cloud leaves them off, except for BigQuery, because of their volume[12]. Enable them only for sensitive data.
- **Hundreds of imported rules.** Ten answered alerts beat hundreds ignored.
- **CISA published a logging reference architecture.** Its August 2026 guide calls for health monitoring, synthetic tests and threat emulation[3].
- **CISA retired Logging Made Easy.** Support ended on 22 May 2026 and the repository is read-only[7]. If you run it, plan a replacement.
- **Sysmon is built into Windows.** Windows 11 and Windows Server 2025 include it as an optional feature. Uninstall standalone Sysmon first, and parse the XML, as event text is now localized[17].

Mistakes that cost the most

- **Basic audit policy overwriting the advanced one.** Enable **Audit: Force audit policy subcategory settings**; event 4719 shows an overwrite[14].
- **Local logs too small.** Events overwritten before they are forwarded are lost without notice[16]. Raise maximum log sizes[1].
- **Counting on a license upgrade.** It won't bring back expired Entra logs[8].
- **Letting everyone read the logs.** Command lines and script blocks can expose passwords and other credentials[14,15]. Limit who can read them.

What this looks like at your size

Small team, no security staff

- Send Defender XDR incident emails for High and Medium severity to a shared mailbox[23].
- Archive Entra logs to a storage account in its own subscription, and lock its immutability policy once logs arrive[13].
- Ask your IT provider for the last alert it acted on.

Growing, with IT or security staff

- Run one SIEM workspace: free sources first, then Entra sign-ins and server security events.
- Write one rule per item in the alert list, each with an owner, and test them monthly.
- Buy managed detection for nights and weekends.

Enterprise or regulated

- Under NIS2, digital providers must sync clocks where feasible and monitor logging availability independently[5].
- Keep a year or more in a cheaper lake tier and only recent data in analytics[20].
- Inject synthetic events[3] for each source monthly.

Version history

4 Nov 2026, version 1.0 Published after a copy edit and a source-by-source fact check, which narrowed 10 statements to what the sources say.

Sources

1. Best practices for event logging and threat detection. ASD's ACSC, CISA, FBI, NSA and partners, Aug 2024. ic3.gov
2. M-26-14: Ensuring Effective and Efficient Agency Logging and Network Visibility. OMB (US), 22 May 2026. whitehouse.gov
3. Logging Reference Architecture. CISA, 20 Aug 2026. cisa.gov
4. M-Trends 2026 Executive Edition. Google Cloud (Mandiant), Mar 2026. services.google.com
5. NIS2 technical implementation guidance (Implementing Regulation 2024/2690), v1.0. ENISA, 26 Jun 2025. enisa.europa.eu
6. Mindeststandard Protokollierung und Detektion von Cyberangriffen, Version 2.1. BSI, 11 Nov 2024. bsi.bund.de
7. Logging Made Easy (archived repository). CISA on GitHub, archived 22 May 2026. github.com
8. Microsoft Entra data retention. Microsoft Learn, 6 Jan 2026. learn.microsoft.com
9. Logs available for streaming from Microsoft Entra ID. Microsoft Learn, 16 Apr 2025. learn.microsoft.com
10. Activity log in Azure Monitor. Microsoft Learn, 19 Oct 2026. learn.microsoft.com
11. Security best practices in AWS CloudTrail. AWS Documentation, checked 4 Nov 2026. docs.aws.amazon.com
12. Cloud Audit Logs overview. Google Cloud Documentation, updated 30 Oct 2026. docs.cloud.google.com
13. Immutable storage for blob data overview. Microsoft Learn, 18 Aug 2026. learn.microsoft.com
14. Command line process auditing. Microsoft Learn, 12 May 2025. learn.microsoft.com
15. about_Logging (Windows PowerShell 5.1). Microsoft Learn, 9 Jan 2024. learn.microsoft.com
16. Use Windows Event Forwarding to help with intrusion detection. Microsoft Learn, 18 Aug 2025. learn.microsoft.com
17. Sysmon overview. Microsoft Learn, 24 Feb 2026. learn.microsoft.com
18. How the Windows Time service works. Microsoft Learn, 25 Jul 2025. learn.microsoft.com
19. Auditing the system (RHEL 9 Security hardening). Red Hat Documentation, checked 4 Nov 2026. docs.redhat.com
20. Plan costs and understand pricing and billing (Microsoft Sentinel). Microsoft Learn, 1 Apr 2026. learn.microsoft.com
21. Reduce costs for Microsoft Sentinel. Microsoft Learn, 14 Jun 2025. learn.microsoft.com
22. Alert policies in the Microsoft Defender portal. Microsoft Learn, 3 Aug 2026. learn.microsoft.com
23. Get incident notifications by email. Microsoft Learn, 2 Jul 2026. learn.microsoft.com
24. Run a detection test on a newly onboarded device. Microsoft Learn, 2 Jul 2026. learn.microsoft.com