Essential Log Sources for Your SIEM

A SIEM can only detect what it can see. Collecting everything is expensive and noisy, so start with the sources that reveal the most attacker activity, then expand. This guide ranks them by priority and lists what to watch in each.

How to use the tiers. `Tier 1` sources cover the most common attack paths: identity, endpoints and email. Onboard them first. `Tier 2` adds network and cloud visibility. `Tier 3` fills remaining gaps for mature programmes.

Identity and endpoints

Source	Tier	Why it matters	Key events to monitor
Windows Security log (domain controllers first)	1	Shows who logged on where, privilege use and changes to accounts and groups.	4624/4625 logon success/failure · 4672 special privileges · 4688 process creation (enable command line) · 4720 account created · 4728/4732/4756 added to privileged group · 4768/4769 Kerberos tickets · 4698 scheduled task · 1102 log cleared
EDR telemetry and alerts	1	The richest view of what actually ran on each device.	Alerts, process trees, suspicious parent/child processes, credential access (e.g. LSASS), isolation actions.
Sysmon (if no full EDR)	1	Free, detailed process and network telemetry on Windows.	1 process create · 3 network connection · 10 process access · 11 file create · 13 registry set · 22 DNS query
PowerShell logging	1	PowerShell is a favourite attacker tool; script logging reveals what was run.	4104 script block logging · 4103 module logging
Microsoft Entra ID (Azure AD) sign-in and audit logs	1	Cloud identity is the new perimeter; account takeover shows up here first.	Risky and impossible-travel sign-ins, MFA failures and fatigue, legacy authentication, new role assignments, app consent grants, MFA method changes.
Linux auth and audit logs	2	Covers servers that Windows-focused monitoring misses.	`auth.log`/`secure`: SSH logons, `sudo` use · `auditd`: command execution, changes to sensitive files.

Email and collaboration

Source	Tier	Why it matters	Key events to monitor
Email security gateway	1	Phishing is still the most common way in.	Delivered malicious messages, clicked URLs, blocked attachments, user-reported phishing.
Microsoft 365 unified audit log	1	Reveals business email compromise and data theft.	New inbox rules and forwarding, mailbox access by unusual IPs, mass downloads or external sharing in SharePoint and OneDrive.

© 2026 Scarlet Dragonfly · scarlet-dragonfly.com · Free to use and share with attribution

Network

Source	Tier	Why it matters	Key events to monitor
VPN and remote access	1	A common entry point using stolen credentials.	Logons from new countries or at odd hours, concurrent sessions, brute-force attempts.
Firewall	2	Shows connections in and out of your network.	Outbound traffic to rare destinations, unusual ports, large data transfers, denied inbound scans.
DNS	2	Almost all malware uses DNS; it exposes command-and-control traffic.	Queries to newly registered or rare domains, very long or random names (tunnelling), high query volumes.
Web proxy	2	Records which websites users and systems reach.	Uncategorised sites, file downloads, uploads to personal cloud storage.
DHCP	3	Maps IP addresses to devices so you can investigate alerts.	Lease assignments, unknown devices joining the network.
Web servers and WAF	3	Detects attacks on public applications.	Injection attempts, scanning, spikes in errors, access to admin paths.

Cloud platforms

Source	Tier	Why it matters	Key events to monitor
AWS CloudTrail and GuardDuty	2	Records every API call in your AWS accounts.	Root account use, console logins without MFA, new access keys, policy changes, `StopLogging`/`DeleteTrail`, public S3 bucket policies, GuardDuty findings.
Azure Activity log and Defender for Cloud	2	Tracks changes to Azure resources.	Role assignments, resource deletion, key vault access, security alerts.
Google Cloud Audit Logs	2	Admin and data access across GCP projects.	IAM policy changes, service account key creation, data access to sensitive buckets.

Five tips for getting it right

- [ ] **Check it's really arriving.** Alert when a critical source goes quiet. A silent log source is a blind spot attackers love.
- [ ] **Normalise fields.** Map user, host and IP fields consistently so you can correlate across sources.
- [ ] **Sync clocks.** Use NTP everywhere and store times in UTC, or timelines won't line up.
- [ ] **Keep enough history.** Aim for at least 12 months of retention, with the most recent 90 days quickly searchable. Intrusions are often discovered months after they start.
- [ ] **Map coverage to MITRE ATT&CK.** Track which attacker techniques each source and detection covers, and close the biggest gaps first.

Written by the team behind the SANS SEC555 course on detection engineering and SIEM analytics. For help onboarding sources or building detections, contact Scarlet Dragonfly at scarlet-dragonfly.com.

© 2026 Scarlet Dragonfly · scarlet-dragonfly.com · Free to use and share with attribution