



10 Logs Type
every
SOC Analyst
should know

1 OPERATING SYSTEM LOGS

Windows Logs:

- Security Logs (Logon events, process creation)
- System Logs (Service failures, hardware errors)
- Application Logs (App crashes, .NET errors)
- PowerShell Logs
- Sysmon Logs (Advanced process/network telemetry)

Linux Logs:

- /var/log/auth.log (Authentication attempts)
- /var/log/syslog or /var/log/messages (System activity)
- /var/log/secure (Security-related messages)
- Bash History Logs
- Auditd Logs (SELinux, user actions)



2 NETWORK LOGS

- Firewall Logs (Deny/allow actions, NAT, connection states)
- IDS/IPS Logs (e.g., Suricata, Snort alerts)
- DNS Query Logs (Domain resolutions)
- Proxy Logs (URL access, categories)
- NetFlow/sFlow Logs (Traffic flow summaries)



3 ENDPOINT SECURITY LOGS

- Antivirus/EDR Logs (Detection, quarantine, scan results)
- Device Control Logs (USB insert/removal)
- Application Whitelisting Logs
- Exploit Prevention/Behavioral Analysis Logs



4

WEB & APPLICATION LOGS

- Web Server Logs (Apache/Nginx access/error logs)
- Application Logs (Custom app logs, API calls)
- Web Proxy Logs (Squid, Zscaler, Bluecoat)
- WAF Logs (Blocked SQLi, XSS attempts)



5

EMAIL & MESSAGING LOGS

- Email Gateway Logs (Phishing, spam detections)
- SMTP Logs (Sent/received metadata)
- Microsoft 365 or Google Workspace Audit Logs
- Email Header Analysis Logs



6 AUTHENTICATION & IDENTITY LOGS

- Active Directory Logs (User logon, group changes)
- LDAP Logs
- SSO/SAML Logs (Okta, Azure AD)
- MFA Logs (Success/failure of token validations)
- VPN Logs (Logins, location info, durations)



7

CLOUD SERVICE LOGS

AWS:

- CloudTrail (API calls, user activity)
- GuardDuty (Threat detections)
- VPC Flow Logs (Network traffic)

Azure:

- Azure Activity Logs
- Azure Sign-in & Audit Logs
- Microsoft Defender for Cloud Logs

GCP:

- Audit Logs
- VPC Flow Logs
- Cloud Armor Logs



8

SECURITY APPLIANCE LOGS

- Firewall Logs (Palo Alto, Fortinet, Cisco ASA)
- IDS/IPS Logs (Suricata, Zeek, Snort)
- VPN Appliance Logs
- NAC Logs (Cisco ISE, Aruba ClearPass)



9 IAM & PRIVILEGED ACCESS LOGS

- Privileged Access Management (PAM) Logs (CyberArk, BeyondTrust)
- Role Elevation Logs
- Password Vault Access Logs
- Session Recording Logs



10

SIEM LOGS

- Correlation Rule Matches
- Alert Generation Logs
- Log Ingestion Status (Parsing errors, delays)
- Use Case Execution Logs (Rule triggers, false positives)

Next Step?

Ultimate SOC Analyst Course

- 12+ Hands-on modules
- 35+ Labs
- 45+ Hours of Video
- Job Assistance
- Community Access

**DM “Ultimate SOC” to
get **50%** discount
Coupon**

