



Top 10 Must-Know Logs for SOC Analysts



What are Logs?

Digital records of system, application, network, and security events — capturing activities like logins, configuration changes, traffic flows, and alerts.

Why Important for SOC Analysts?

- Detect threats early (malware, brute force, unauthorized access).
- Reconstruct incidents and trace attacker actions.
- Provide forensic evidence for investigations.
- Meet compliance requirements (GDPR, ISO, PCI DSS).
- Assist in troubleshooting and performance monitoring.
- Identify insider threats through abnormal activity patterns.

How They Help SOC Operations:

- Give real-time visibility across IT infrastructure.
- Correlate events from multiple sources to uncover attack patterns.
- Support audits, reporting, and policy enforcement.
- Aid in improving detection rules and security controls.

1. Windows Event Logs

Description: Core Windows OS logs containing system, security, and application events

Importance: Essential for detecting authentication failures, policy changes, privilege escalation, and malicious activity on Windows systems

File Locations:

C:\Windows\System32\winevt\Logs\Security.evtx (Security events)

C:\Windows\System32\winevt\Logs\System.evtx (System events)

C:\Windows\System32\winevt\Logs\Application.evtx (Application events)

Process: Generated by Windows Event Log service, accessed via Event Viewer or PowerShell

Example: Event ID 4624 (successful logon) followed by Event ID 4625 (failed logon) indicating potential brute force attack

STATEMENT OF CONFIDENTIALITY

This document is Confidential. No part of this document shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise without prior permission. Other logos, trademarks and service marks depicted in this document are the property of their respective owners.

2. Linux System Logs

Description: Core Linux system activity, authentication, and kernel events

Importance: Foundation for Linux server security monitoring and incident response

File Locations:

/var/log/auth.log (Authentication attempts)

/var/log/syslog or /var/log/messages (System activity)

/var/log/secure (Security-related messages)

Bash History: ~/.bash_history (Command history)

Auditd: /var/log/audit/audit.log (SELinux, user actions)

Process: System daemons and kernel logging via syslog/rsyslog

Example: Multiple failed SSH attempts: Failed password for root from 192.168.1.100

3. Firewall Logs

Description: Network traffic allow/deny decisions with source/destination details

Importance: Critical for identifying unauthorized access attempts, port scans, and network anomalies

File Locations:

Windows: C:\Windows\System32\LogFiles\Firewall\pfirewall.log

Linux iptables: /var/log/messages or /var/log/kern.log

pfSense: /var/log/filter.log

Process: Generated by firewall engines when packets match rules

Example: Multiple blocked connections to port 22 from same IP indicating SSH brute force attempt

STATEMENT OF CONFIDENTIALITY

This document is Confidential. No part of this document shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise without prior permission. Other logos, trademarks and service marks depicted in this document are the property of their respective owners.

4. Proxy Server Logs

Description: Web traffic requests, URLs accessed, and user browsing behavior

Importance: Monitors data exfiltration, malicious websites, and policy violations

File Locations:

Squid: /var/log/squid/access.log

IBM Proxy: install/logs/proxy-n.log

Microsoft ISA: Custom configured location

Process: HTTP/HTTPS requests logged with timestamps and user context

Example: Large POST requests to external cloud storage indicating potential data exfiltration

5. Antivirus/EDR Logs

Description: Malware detections, quarantine actions, and endpoint behavioral analysis

Importance: First line of defense against malware, ransomware, and advanced threats

File Locations:

Windows Defender: C:\ProgramData\Microsoft\Windows Defender\Support\

Symantec: C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\Logs\AV

CrowdStrike/SentinelOne: Cloud-based with local agent logs

Process: Real-time file scanning and behavioral monitoring

Example: Ransomware behavior detected: file encryption attempts blocked on multiple files

STATEMENT OF CONFIDENTIALITY

This document is Confidential. No part of this document shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise without prior permission. Other logos, trademarks and service marks depicted in this document are the property of their respective owners.

6. Active Directory Logs

Description: Domain authentication, user/group changes, and directory service access

Importance: Critical for detecting credential theft, privilege escalation, and insider threats

File Locations:

Event Logs: C:\Windows\System32\winevt\Logs\Security.evtx

Database: C:\Windows\NTDS\ntds.dit

Debug: C:\Windows\Debug\netlogon.log

Process: Domain controller activities and authentication events

Example: Event 4728 - User added to security-enabled global group (potential privilege escalation)

7. VPN Logs

Description: Remote access connections, authentication attempts, and session details

Importance: Monitor unauthorized remote access and unusual connection patterns

File Locations:

OpenVPN: /var/log/openvpn.log or client-specific paths

Windows: C:\Program Files\OpenVPN\log\

AWS Site-to-Site: CloudWatch Logs /aws/vpn/

Process: VPN gateway authentication and tunnel establishment

Example: Multiple failed VPN connections from geographically impossible locations

STATEMENT OF CONFIDENTIALITY

This document is Confidential. No part of this document shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise without prior permission. Other logos, trademarks and service marks depicted in this document are the property of their respective owners.

8. Cloud Security Logs

Description: Cloud service API calls, resource changes, and access patterns

Importance: Essential for cloud security monitoring and compliance in hybrid environments

File Locations:

AWS CloudTrail: S3 buckets (JSON format)

Azure Activity: Event Hub or Log Analytics workspace

GCP Cloud Logging: Stackdriver logs

Process: API activity logging and resource audit trails

Example: Unusual resource deletion or privilege escalation in cloud environment

9. DNS Logs

Description: Domain name resolution requests and responses

Importance: Detect command & control traffic, data exfiltration, and malicious domains

File Locations:

Windows DNS: C:\dnslogs\dns.log

Linux BIND: /var/log/named/queries.log

pfSense: /var/log/resolver.log

Process: DNS queries logged with source IP and requested domains

Example: Frequent queries to algorithmically generated domains indicating DGA malware

STATEMENT OF CONFIDENTIALITY

This document is Confidential. No part of this document shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise without prior permission. Other logos, trademarks and service marks depicted in this document are the property of their respective owners.

10. IDS/IPS Logs=

Description: Intrusion detection and prevention system alerts and blocked threats

Importance: Early warning system for cyber attacks, malware, and network intrusions

File Locations:

NSX-T: /var/log/nsx-idps/nsx-idps-events.log

Cisco IPS: Retrieved via SDEE protocol

Snort: /var/log/snort/alert

Process: Pattern matching against threat signatures and behavioral analysis

Example: SQL injection payload detected: ALERT TCP 192.168.1.100 -> 10.0.0.50
[SQL Injection Attempt]

11. Database Logs (BONUS)

Description: Database queries, transactions, authentication, and access patterns

Importance: Protect sensitive data from SQL injection, unauthorized access, and data breaches

File Locations:

MySQL: /var/log/mysql/error.log, /var/log/mysql/mysql.log

PostgreSQL: /var/lib/postgresql/data/log/postgresql-*.log

SQL Server: Windows Event Logs and SQL Server logs

Process: Database engine activity and transaction logging

Example: Unusual bulk SELECT queries on sensitive tables or failed authentication attempts

STATEMENT OF CONFIDENTIALITY

This document is Confidential. No part of this document shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise without prior permission. Other logos, trademarks and service marks depicted in this document are the property of their respective owners.