📘 Essential Logs for Every SOC Analyst

🎯 *Purpose of This Guide*

To empower aspiring SOC Analysts with a clear understanding of various log types, their functions, and how to effectively analyze them within a real-world Security Operations Center (SOC) environment.

🔎 Why Logs Are Crucial in SOC

Logs are the **foundation of threat detection**. SIEM platforms like **Splunk, ELK Stack, and IBM QRadar** analyze logs to uncover anomalies and raise alerts.

- 📌 Every alert originates from a log
- 🔄 Logs help reconstruct the attack timeline
- 🕵️ Useful for incident response, auditing, compliance, and real-time monitoring

---

📚 Core Log Types for Every SOC Analyst

1: System Activity Log

🗄️ Records OS-level events like kernel alerts, system reboots, and scheduled tasks.
🗂️ **Path:** `/var/log/syslog`

✅ **Use Case:**

- Detect system failures
- Spot unauthorized cron jobs
- Monitor privilege escalation attempts

2: Login & Access Log

🔐 Tracks user authentication such as SSH logins, sudo usage, and account switching.
🗂️ **Path:** `/var/log/auth.log`

✅ **Use Case:**

- Investigate brute-force attacks
- Detect failed logins or new user creation
- Monitor root access escalation

3: Network Traffic Log

🌐 Captures incoming/outgoing network connections and blocked IPs.
🗂 **Location:** Based on the firewall (e.g., iptables, pfSense, Cisco ASA)

✅ **Use Case:**

- Detect port scans or IP blocks
- Alert on denied access
- Identify suspicious outbound traffic

4: Web Request Log

🌍 Logs details of user interactions with a web server (Apache/Nginx).
🗂 **Paths:**

- Apache: `/var/log/apache2/access.log`
- Nginx: `/var/log/nginx/access.log`

✅ **Use Case:**

- Detect SQL injection, XSS attacks
- Monitor traffic spikes or broken links
- Spot bot activity

5:Windows System Log

□ Includes user actions, system errors, and application warnings on Windows machines.
🗂 **View via:** Event Viewer → Windows Logs

✅ **Use Case:**

- Monitor failed login attempts (Event ID 4625)
- Detect PowerShell abuse
- Spot suspicious DLL injection

6: Threat Detection Log

 Shows malware detections, blocked processes, and endpoint protection activities.
🗁 **Location:** Varies based on the security product (e.g., Defender, SentinelOne, CrowdStrike)

✅ **Use Case:**

- Track threat names and file hashes
- Investigate malicious activity
- Confirm remediation actions

👤 **Author:** *Tausif Pathan*
✉ tausifpathan8086@gmail.com
🎯 *SOC Analyst | Log Monitoring | Blue Team | Cybersecurity Enthusiast*