📄 Types of Logs Every SOC Analyst Must Understand

🎯 Objective of This Guide

To help aspiring SOC Analysts understand the different types of logs, their purpose, and how to analyze them in a real-world Security Operations Center (SOC).

🔍 Why Logs Matter in SOC

Logs are the backbone of threat detection. SIEM tools like Splunk, ELK, and QRadar ingest logs to detect anomalies and trigger alerts.

🔹 **Every alert starts with a log**

🔹 Logs allow us to reconstruct attack chains

🔹 Logs help with incident investigation, compliance, and monitoring

🧩 Key Logs Every SOC Analyst Must Master

1□ Syslog

🖥️ OS-level log for Unix/Linux systems.

💬 Captures kernel messages, cron jobs, system reboots.

✅ Use Case: Detect system crashes, unauthorized cron jobs, privilege escalation.

📍 Path: /var/log/syslog

2□ Auth.log

🔐 Tracks authentication events: logins, sudo, SSH.

🔍 Crucial for investigating brute-force attacks or suspicious login attempts.

📍 Path: /var/log/auth.log

✅ **Detects**:

- Failed login attempts
- Privilege escalation attempts
- New user creation

3□ Firewall Logs

- Shows incoming/outgoing traffic and blocked connections.
- Identifies port scans, IP blocks, DoS attempts.

✅ **Use Cases:**

- Detect reconnaissance
- Spot outbound C2 traffic
- Alert on denied access
- Location: Depends on firewall (iptables, pfSense, Cisco ASA)

4□ Web Server Logs

🌐 Apache/Nginx log HTTP/S requests.

🔍 Helps detect application-layer attacks like SQLi, XSS, path traversal.

✅ **Key Elements:**

- Request type (GET/POST)
- URL path

◆ HTTP response code (403, 500, etc.)

◆ Referrer & User-Agent

📍 **Paths:**

◆ Apache: /var/log/apache2/access.log

◆ Nginx: /var/log/nginx/access.log

5□ Windows Event Logs

◆ Security Log (e.g., Event ID 4625: Failed Login)

◆ System Log (hardware or service failures)

◆ Application Log

✅ Detect:

◆ Failed RDP login

◆ Suspicious PowerShell usage

◆ DLL injections or registry tampering

📍 View via: Event Viewer → Windows Logs

6□ Antivirus / EDR Logs

🛡️ Tracks malware detections, hashes, blocked files.

🖥️ Key for identifying compromised endpoints.

✅ Info Captured:

◆ Threat names

- File hashes
- Process ID
- Remediation status

🔄 Real SOC Use-Cases With Logs

✅ **Brute Force Attack Detection**

Analyze auth.log or Windows Security Log (Event ID 4625) for repeated login failures from same IP.

✅ **Lateral Movement**

Use Windows Event Logs + Sysmon to trace account logins across multiple hosts.

✅ **Malware Execution**

Cross-reference antivirus logs with process execution logs (Sysmon or EDR) to detect malware spreading.

✅ **Internal Threat Monitoring**

Look for unusual access in firewall logs, USB insertions (event ID 4663), or strange system reboots.

🧑‍💻 **Author: Afroz Shaikh**

📧 **afrozshaikh8086@gmail.com**

🎯 **SOC Analyst | Log Monitoring | Blue Team | Cybersecurity**