🛡️ what is logs (simple)

📌 1. Introduction to Logs

Definition:
A **log** is a chronological record of events generated by devices, applications, operating systems, or security tools.

Purpose:
Helps **SOC Analysts** monitor, investigate, and respond to security incidents effectively.

Example:

- 🔹 Firewall log: Blocked connection from 192.168.1.5 to port 22

🌐 2. Why Logs Are Important in SOC

- 🔹 **Visibility:** Gain insights into user activities, network traffic, and system changes.
- 🔹 **Evidence:** Logs support digital forensics and compliance reporting.
- 🔹 **Detection:** Identify threats like brute-force attacks, malware, phishing, and insider threats.
- 🔹 **Compliance:** Logs help meet standards like **PCI-DSS, HIPAA, GDPR**.

Example:

- ⚡ Failed login attempts in **Windows Event Viewer** can indicate a brute-force attack.

🖥️ 3. Sources of Logs

- **Operating Systems:**
  - Windows Event Viewer (Application, Security, System logs)
  - Linux Syslog (/var/log/auth.log, /var/log/messages)
- **Network Devices:**
  - Routers, Switches, Firewalls (e.g., Cisco ASA logs)

- **Applications:**
  - Web servers (Apache, Nginx)
  - Email servers
- **Security Tools:**
  - IDS/IPS (Snort, Suricata)
  - Antivirus, EDR solutions
- **Cloud Platforms:**
  - AWS CloudTrail, Azure Monitor

📊 4. Types of Logs

- 📝 **System Logs:** OS events, kernel activities
- 🌐 **Network Logs:** IP traffic, routing changes
- 🔑 **Authentication Logs:** Successful & failed logins
- 🔒 **Security Logs:** Firewall blocks, IDS alerts
- ⚡ **Application Logs:** Software crashes, user actions
- ☁️ **Cloud Logs:** API calls, resource creation/deletion

Example:

- 🔹 Authentication log → Failed password for root from 10.10.1.5 port 2222 ssh2

🛠️ 5. Log Lifecycle

1. 🟢 **Generation:** Devices or services create logs automatically when events occur.
2. 📩 **Collection:** Logs are forwarded securely to a **SIEM or central log server**.
3. 🔄 **Normalization:** Raw logs are converted into a **common, structured format** for easy analysis.
4. 💾 **Storage:** Logs are stored in **databases or log management systems**, often in hot/warm/cold tiers.

5. 🔍 **Analysis:** Logs are **correlated and examined** to detect threats, anomalies, or suspicious activity.
6. 🗄️ **Retention & Archival:** Logs are **stored long-term** to meet **compliance, audit, and forensic requirements**.

🧠 6. Key Log Formats

- 📄 **Syslog (RFC 5424):** Standard for UNIX/Linux devices
- 🔹 **Windows Event Logs:** Proprietary format used in Event Viewer
- ⚙️ **JSON / XML Logs:** Structured logs for modern applications
- 📑 **CEF (Common Event Format):** Used in ArcSight & other SIEMs
- 🛡️ **LEEF (Log Event Extended Format):** IBM QRadar specific

---

📐 7. Log Analysis in SOC

- 🔹 **Correlation:** Combine multiple logs to detect attack patterns
- 🔔 **Alerting:** Trigger alerts based on rules (e.g., 5 failed logins in 1 min)
- 🕵️ **Threat Hunting:** Proactively search historical log data for IOCs
- ⚠️ **Anomaly Detection:** Identify unusual or suspicious behaviors

Examples:

- ⚡ Multiple failed logins from a single IP → **brute-force attack**
- ⚡ Unusual outbound traffic → **potential data exfiltration**