# Advanced Log Analysis

Advanced Log Analysis moves beyond viewing logs as isolated records of events and instead treats them as the digital nervous system of an organization. No single log source tells the full story; the truth is revealed through relationships and deviations from established norms.

## Core concept:

- **Log Correlation:**
  - This is the process of establishing meaningful relationships between discrete log entries from disparate sources.
    Eg: A single failed login (Windows Event 4625) is noise. That same failed login, correlated with a successful login from a foreign geo-location minutes later (from a VPN or proxy log), followed by anomalous outbound SMB traffic (from a network sensor) to a rare external IP, forms a high-fidelity signal of a potential credential compromise and data exfiltration attempt. Correlation reduces entropy (disorder) in the data, transforming it into information.
- **Anomaly Detection:**
  - This operates on the principle of **baselining "normal"** behavior to identify statistical outliers. The theory distinguishes between:
    - Rule-Based Detection
    - Statistical/Behavioral Anomaly Detection
- **Log Enrichment:**
  - This is the process of adding contextual metadata to raw log data to increase its analytical value. Theoretically, it's about reducing the time for an analyst's cognitive processing.
- **Theoretical Objective:**
  - To develop a probabilistic model of security events. By correlating, finding anomalies, and enriching, the analyst moves from asking "What happened?" to "What is likely happening, and how confident are we?" This is the shift from reactive log review to proactive security monitoring.

# Threat Intelligence Integration

Threat Intelligence (TI) is external context applied to internal observations. TI integration provides the "who," "why," and "what next" behind the "what" discovered in log analysis. It's the difference between seeing a suspicious process and knowing it's part of "FIN7's latest ransomware deployment, which typically moves laterally via RDP after initial access."

## Core Concept:

- **Threat Intelligence Types:**
  - Indicators of Compromise (IOCs):
    - Atomic, observable data (IPs, hashes, domains). These are tactical and often short-lived. they are the "lowest level" of intelligence, useful for automated blocking but easy for adversaries to change.
  - Tactics, Techniques, and Procedures (TTPs):
    - The adversary's behavior pattern. This is the most valuable construct. Instead of blocking a single malicious hash (which changes), you detect the technique (e.g., T1055 - Process Injection) regardless of the tool's hash. This raises the attacker's cost to evade detection.
  - Strategic & Operational Intelligence:
    - Understanding adversary goals, campaigns, and motivations. This informs broader defensive strategy.
- **Integration in SOC:**
  - It is **automated enrichment and prioritization**. When your SIEM sees an internal IP scanning, it's a medium-priority alert. If that same IP is automatically enriched via a threat feed and matches a known **APT29** C2 server, the alert's **fidelity** and **priority** skyrocket. This is the practical application of the "cyber kill chain" or **MITRE ATT&CK** framework—placing isolated events into an adversary's known playbook.
- **Threat Hunting with Intelligence:**
  - This is a proactive, hypothesis-driven search based on intelligence. The theory is "assume breach." A hunter receives intelligence that a new malware variant exploits a specific vulnerability (CVE). Instead of waiting for an alert, they proactively query all logs across the enterprise (e.g., EDR, proxies) for behavioral patterns associated with that exploitation (TTPs), even if no IOCs match. It's searching for the signal of the behavior, not just the signature of the tool.

# Incident Escalation Workflows

Escalation workflows are the formalized decision-making and communication protocols that govern an incident's lifecycle. The theory recognizes that incident response is not just a technical challenge but a socio-technical process involving coordination, authority, and timely information flow under stress.

## Core Concept:

- **Escalation Tiers & Criteria:**
  - Tier 1 (Triage/Initial Response):
    - Volume handling and noise reduction. They follow predefined runbooks to validate alerts, perform initial enrichment, and filter out false positives. Escalation criteria are typically rule-based. e.g., severity >= High, involves critical asset, matches known TTP
  - Tier 2 (Investigation/Incident Response):
    - Deep-dive analysis and containment. They investigate escalated incidents, determine scope/impact, and execute initial containment. They escalate based on complexity, scope, or strategic impact
  - Tier 3 (Advanced/Threat Hunt):
    - Expert analysis and strategic improvement. They handle the most complex intrusions, perform forensic analysis, lead threat hunts based on findings, and develop new detection logic to close gaps.
- **Communication Protocols:**
  - Standardized communication reduces ambiguity and accelerates response. Protocols like **SITREPs** (Situation Reports) provide a structured format (e.g., Executive Summary, Current Status, Action Items, Next Update) to ensure all stakeholders (technical teams, management, legal, PR) have the information they need, when they need it, without information overload.
- **Automation in Escalation (SOAR):**
  - Remove human latency and error from repetitive, rule-based processes. SOAR platforms theoretically codify escalation workflows into playbooks.
    Eg: An alert meeting "Critical" severity and tagging "Ransomware" can automatically: enrich IOCs from 3 threat feeds, isolate the infected host via EDR API, create a ticket in the ITSM system, assign it to the Tier 2 on-call analyst, and post a message to the SOC chat channel. This ensures consistency and frees analysts for higher-order cognitive tasks.

THANK YOU!