

Cybersecurity Frameworks and SOC Operations

Core Frameworks

Cyber Kill Chain

The Cyber Kill Chain describes the typical lifecycle of a cyberattack through seven stages:

1. **Reconnaissance** - Gathering information about targets
2. **Weaponization** - Creating malicious payloads
3. **Delivery** - Transmitting the payload to the target
4. **Exploitation** - Executing code to gain initial foothold
5. **Installation** - Establishing persistent presence
6. **Command & Control (C2)** - Maintaining communication channels
7. **Action on Objectives** - Achieving strategic goals (data exfiltration, privilege escalation, lateral movement)

MITRE ATT&CK Framework

A practical knowledge base cataloging attacker behaviors rather than specific malware or tools. It encompasses 14 tactics with varying techniques, including:

- Reconnaissance (11 techniques)
- Initial Access (11 techniques)
- Execution (17 techniques)
- Persistence (23 techniques)
- Defense Evasion (47 techniques)
- Credential Access (17 techniques)
- Lateral Movement (9 techniques)
- Exfiltration (9 techniques)

TTPs vs IOCs

Tactics, Techniques, and Procedures (TTPs) describe how attackers think, act, and operate. They reveal the "how" and "why" behind attacks, enabling SOC analysts to detect threats even when IOCs change and build better detection playbooks.

Indicators of Compromise (IOCs) are observable evidence of system compromise, categorized as:

1. **Network-Based** - Malicious IPs, suspicious domains, C2 communications
2. **Host/Endpoint-Based** - Suspicious processes, registry changes, scheduled tasks
3. **File-Based** - File hashes, name patterns, size anomalies
4. **Email-Based** - Malicious sender emails, phishing subject lines

Key Difference: IOCs show "what happened" (short-lived evidence), while TTPs show "how it happened" (long-lived behavior patterns).

Alert Triage Process

Alert triage is the structured process of quickly analyzing security alerts to separate real attacks from false alarms.

Prioritization Rules:

1. Filter alerts - Take only new, unassigned alerts
2. Sort by severity - Critical, High, Medium, Low
3. Sort by time - Address oldest alerts first

Initial Actions:

- Assign alert to yourself
- Move to "in-progress" status
- Review alert details, description, and key indicators

Alert Properties: Include alert time, name, severity, status, verdict (True/False Positive), assignee, description, and relevant contextual fields.

Workflow: Event occurs → System logs event → Logs sent to SIEM/EDR → Alert generated → SOC analyst triages → Decision: True Positive or False Positive → Escalation or Closure

Effective triage reduces false positives, catches real threats early, and ensures SOC efficiency and business protection.