# Alert Triage, TTPs & Threat IOCs

Tactics, Techniques & Procedures

Indicators of Compromise

Alert Triage Process

#CyberSecurity #SOC
#ThreatDetection

2026-02-07

SECTION 01

# Tactics, Techniques & Procedures

# What Are TTPs?

TTPs describe how attackers think, act, and operate during a cyber-attack

**If an IOC tells you WHAT happened,**

**TTPs tell you HOW and WHY it happened**

**SOC Analysts Use TTPs To:**

- Build better detection alerts and response playbooks
- Understand attacker intent and methodology
- Detect threats even when IOCs change

# Breaking Down TTPs

## The Three Layers of Attacker Behavior

LAYER 01

### Tactics: The Goals

WHY an attacker is doing something — each tactic represents a phase of the attack lifecycle

**Common Attacker Goals:**

- Gain Initial Access
- Steal Credentials
- Move Laterally
- Maintain Persistence
- Exfiltrate Data

LAYER 02

### Techniques: The Methods

HOW the attacker achieves a tactic — specific attack methods

**Example: Credential Access**

Tactic (the goal): Credential Access

**Techniques (methods to achieve it):**

- Credential dumping (LSASS)
- Browser password theft
- Keylogging
- Phishing for credentials

LAYER 03

### Procedures: The Exact Steps

The attacker's exact implementation in the real world — where tools, commands, and timing come into play

**Example Procedure:**

Technique: Credential dumping

```
procdump.exe -accepteula -m
lsass.exe lsass.dmp
```

# TTP Frameworks

Two Major Approaches to Understanding Attacker Behavior

## Cyber Kill Chain

Describes the typical lifecycle of a cyberattack — the stages an attacker goes through to launch an attack

| | |
|---|---|
| 1 | Reconnaissance |
| 2 | Weaponization |
| 3 | Delivery |
| 4 | Exploitation |
| 5 | Installation |
| 6 | Command & Control |
| 7 | Action on Objectives |

→ **Linear 7-stage attack lifecycle**

## MITRE ATT&CK

A practical guide that catalogs attacker behaviors instead of focusing on malware and tools which constantly change

| | | | |
|---|---|---|---|
| **Reconnaissance** | 11 techniques | **Resource Dev.** | 8 techniques |
| **Initial Access** | 11 techniques | **Execution** | 17 techniques |
| **Persistence** | 23 techniques | **Privilege Esc.** | 14 techniques |
| **Defense Evasion** | 47 techniques | **Credential Access** | 17 techniques |
| **Discovery** | 18 techniques | **Lateral Movement** | 17 techniques |
| **Collection** | 34 techniques | **Command & Control** | 9 techniques |
| **Exfiltration** | 15 techniques | **Impact** | 9 techniques |

→ **14 tactics, 239+ techniques total**

# IOCs vs TTPs

Understanding The Fundamental Difference

## IOCs

Evidence

**What happened**

Specific artifacts left behind by attackers

**Examples**

`192.168.1.100 • evil.com • abc123.exe • SHA256:d4f8a...`

**Easy to change**

New server, new hash, new domain = new IOC

**Short-lived**

Attackers change IPs, domains, file hashes frequently

**Used for alerts**

Trigger immediate detection rules in SIEM/EDR

## TTPs

Behavior

**How it happened**

Methods and patterns attackers use

**Examples**

Credential dumping • Lateral movement • C2 beaconing

**Hard to change**

Changing behavior requires retooling entire operations

**Long-lived**

Attack methods stay consistent over time

**Used for detection logic**

Build behavioral detection rules that survive IOC changes

**Bottom Line: IOCs tell you a breach occurred. TTPs tell you how to stop the next one.**

SECTION 02

# Indicators of Compromise

# What Are IOCs?

Observable evidence that suggests a system may be compromised or under attack

**If TTPs describe attacker behavior,**

**IOCs are the footprints attackers leave behind**

SOC Analysts hunt, detect, correlate, and respond using IOCs every single day

**IOCs = "Something bad happened here and we can prove it with data"**

**In a real SOC environment, IOCs help you:**

- Confirm malicious activity
- Trigger alerts in SIEM
- Respond quickly (block, isolate)
- Correlate attacks across systems

# Types of IOCs

## Four Critical Categories SOC Analysts Monitor

### Network-Based

Show what happened inside a network

**Examples:**

- Malicious IP addresses
- Suspicious domains
- C2 server communication
- Unusual ports or protocols

Firewall logs • Proxy logs • DNS logs • IDS/IPS alerts

### Host/Endpoint-Based

Show what happened inside the system

**Examples:**

- Suspicious processes
- Unexpected services
- Registry changes
- New scheduled tasks

EDR/XDR • Windows Event Logs • Sysmon • Linux audit logs

### File-Based

Relate to malicious files

**Examples:**

- File hash (MD5, SHA256)
- File name patterns
- File size anomalies
- Suspicious file locations

Antivirus • EDR • Email security gateways • Sandboxes

### Email-Based

Relate to malicious emails

**Examples:**

- Malicious sender email
- Phishing subject lines
- Malicious URLs
- Header anomalies

Email security tools • Microsoft Defender • Proofpoint • Mimecast

# IOC Confidence Levels

Not All Indicators Are Created Equal

| Confidence Level | Example | SOC Response |
|---|---|---|
| **LOW**<br>Single data point | Single suspicious IP with no other context | Monitor, investigate context |
| **MEDIUM**<br>Known threat signature | Known phishing domain from threat intel feed | Block domain, review logs |
| **HIGH**<br>Active malicious activity | Malware hash detected + execution confirmed | Isolate host, begin IR |
| **VERY HIGH**<br>Correlated attack chain | Multiple IOCs across network + lateral movement | Full incident response, escalate |

**Key Principle: Context is everything. A single IOC might be noise, but multiple correlated IOCs across different data sources significantly increase confidence.**

SOC analysts build confidence by correlating IOCs with TTPs to understand the full attack picture.

SECTION 03

# Alert Triage

# What Is Alert Triage?

The structured process of quickly analyzing security alerts to decide whether they are real threats, false alarms, or need escalation

**Alert triage = separating real attacks from noise, fast and accurately**

SOC environments generate thousands of alerts daily. Only a small percentage are real incidents. Your job as a SOC analyst is to filter, prioritize, and act.

# Why Alert Triage Is Critical

The Difference Between Chaos and Control

## Without Proper Triage

**SOC Teams Drown in Alerts**

Alert fatigue leads to burnout and missed threats

**Real Attacks Get Missed**

Critical threats hidden in noise go undetected

**Response Is Delayed**

Slow triage = attackers gain more time and access

**Business Impact Increases**

More time for data exfiltration, lateral movement, damage

## With Good Triage

**Real Threats Caught Early**

Accurate triage identifies true positives before damage

**SOC Becomes Efficient**

Better signal-to-noise ratio = focused investigations

**False Positives Reduced**

Resources focused on real incidents, not noise

**Trust Is Built**

Stakeholders trust SOC decisions and recommendations

**Alert Triage separates real threats from noise through structured analysis**

# The Alert Generation Process

1 Event occurs (login, process launch, file download)

2 System logs the event (OS, firewall, cloud provider)

3 Logs sent to security solution (SIEM or EDR)

4 Detection rule triggered, alert created with severity

5 Analyst triages dozens of alerts instead of millions of logs

> **"Alerts save SOC teams from manual log review by highlighting only suspicious, anomalous events"**
>
> Without alerts, analysts would drown in millions of raw logs per day from thousands of systems

# Alert Properties

## Understanding The Anatomy of a Security Alert

| Property | Meaning (SOC L1) | Example |
|---|---|---|
| **Alert Name** | Summary of what triggered | Unusual Login Location Detected |
| **Alert Time** | When the alert was generated | `2026-02-07 15:35:42 UTC` |
| **Alert Severity** | Urgency assigned by detection | Low Medium High Critical |
| **Alert Status** | Current lifecycle state | New / In-Progress / Closed |
| **Alert Verdict** | L1 classification outcome | True Positive False Positive |
| **Alert Assignee** | Analyst handling the alert | SOC Analyst - John Smith |
| **Alert Description** | Explanation of what the alert means | User logged in from geographically impossible location within short timeframe |
| **Alert Fields** | Contextual values that led to alert | `user: jsmith \| source_ip: 203.0.113.45 \| hostname: WIN-PC-001` |

# Alert Prioritization

The process of deciding which alerts to take first

**Why Prioritization Matters:**

Without a clear prioritization system, analysts waste time on low-impact alerts while critical threats go unaddressed. Every SOC team decides its own prioritization rules and usually automates them by setting appropriate alert sorting logic in SIEM or EDR.

### 1 Filter Alerts

Make sure you don't take alerts that other analysts have already reviewed or that are being investigated by teammates

→ **Only take new, yet unseen and unresolved alerts**

### 2 Sort by Severity

Start with critical alerts, then high, medium, and finally low

CRITICAL HIGH MEDIUM LOW

Critical alerts are much more likely to be real, major threats and cause much more impact than medium and low

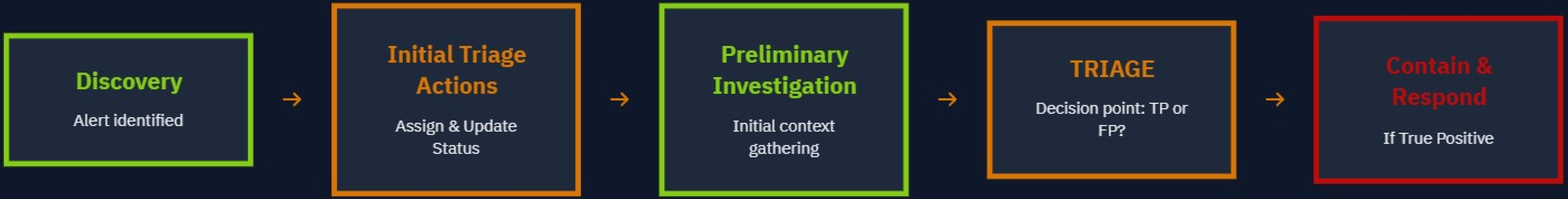
### 3 Sort by Time

Start with the oldest alerts and end with the newest ones

If both alerts are about breaches, the attacker from the older breach is likely already dumping your data, while the "newcomer" has just started discovery

# Alert Triage Workflow

From Discovery to Response



**Discovery**
Alert identified

→

**Initial Triage Actions**
Assign & Update Status

→

**Preliminary Investigation**
Initial context gathering

→

**TRIAGE**
Decision point: TP or FP?

→

**Contain & Respond**
If True Positive

## Initial Triage Actions

The initial steps ensure you take ownership of the assigned alert and avoid interfering with alerts being handled by other analysts

- Assign the alert to yourself
- Familiarize with alert name and description
- Move status to "In-Progress"
- Review key indicators and contextual fields

# Real SOC Flow

**IOC Detection → Alert → TTP Mapping → Decision**

**1** **IOC Detected**

IP, Hash, Process, Domain, or other indicator flagged

**2** **SIEM Generates Alert**

Detection rule triggered, alert created with severity

**3** **SOC L1 Validates IOCs**

Analyst reviews context: source, destination, timing, user

**4** **SOC Maps to TTP**

Link IOC to attacker tactic/technique (MITRE ATT&CK)

**5** **Decision**

Based on IOC validation + TTP context

**TRUE POSITIVE**
→ Escalate to L2/IR

**FALSE POSITIVE**
→ Close with notes

**Key Integration**

Alert triage decisions are based on understanding both:

→ The specific IOCs present
→ The broader TTP patterns they indicate

- IOCs are the evidence — the footprints attackers leave behind
- TTPs reveal attacker behavior — the how and why behind attacks
- **"SOC analysts are promoted based on triage quality, not number of alerts closed"**