# Building Alert Prioritization & Incident Response Capabilities

This report outlines a structured learning and practical implementation plan for mastering Security Operations Center (SOC) core competencies. The program focuses on three critical areas: Alert Priority Levels, Incident Classification, and Basic Incident Response. Through theoretical study and hands-on exercises, this framework develops the skills necessary to efficiently triage, classify, and respond to security incidents using industry-standard frameworks and tools.

## Alert Priority Levels:

When you work in a **Security Operations Center (SOC)**, you receive many alerts from SIEM tools (Splunk, Wazuh, QRadar, etc). Some are urgent and dangerous; others are harmless or false positives. To manage them, we use **Alert Priority Levels**.

## Core Concepts:

- **Priority Definitions**: Mastered severity classification (Critical, High, Medium, Low) based on impact (data breach, service disruption) and urgency (active exploitation).
  - Every alert is categorized into:
    - **Critical** → Indicates an ongoing attack that can cause **massive damage.** Needs **immediate action.**
    - **High** → Very important but not as immediate as Critical. Usually means **potential compromise.**
    - **Medium** → Suspicious, needs investigation but **not urgent.** Could turn into a high or critical issue if ignored.
    - **Low → No immediate threat. Often for monitoring and tuning.**

## Assignment Criteria:

- **Asset Criticality** → How important is the system?
  - Production Server → High priority
- Exploit likelihood → Is the vulnerability actually exploitable?
  - CVE with public exploit.
- Business Impact → If this alert is real, what will happen?
  - Financial loss and Reputation loss

## Scoring Systems:

Understood CVSS (Common Vulnerability Scoring System) for risk quantification and SOC tool scoring (Splunk risk scoring).

**Used for grading vulnerabilities:**

| Score | Severity |
|---|---|
| 9.0–10 | Critical |
| 7.0–8.9 | High |
| 4.0–6.9 | Medium |
| 0.1–3.9 | Low |

## SOC Tools risk scoring for alert prioritization:

- Each alert is given a risk score
  - Eg. 20, 50, 80, 100
- Higher the Risk score Higher the Chance of Compromise.
- SOC analysts use this score to filter the most important alerts first.

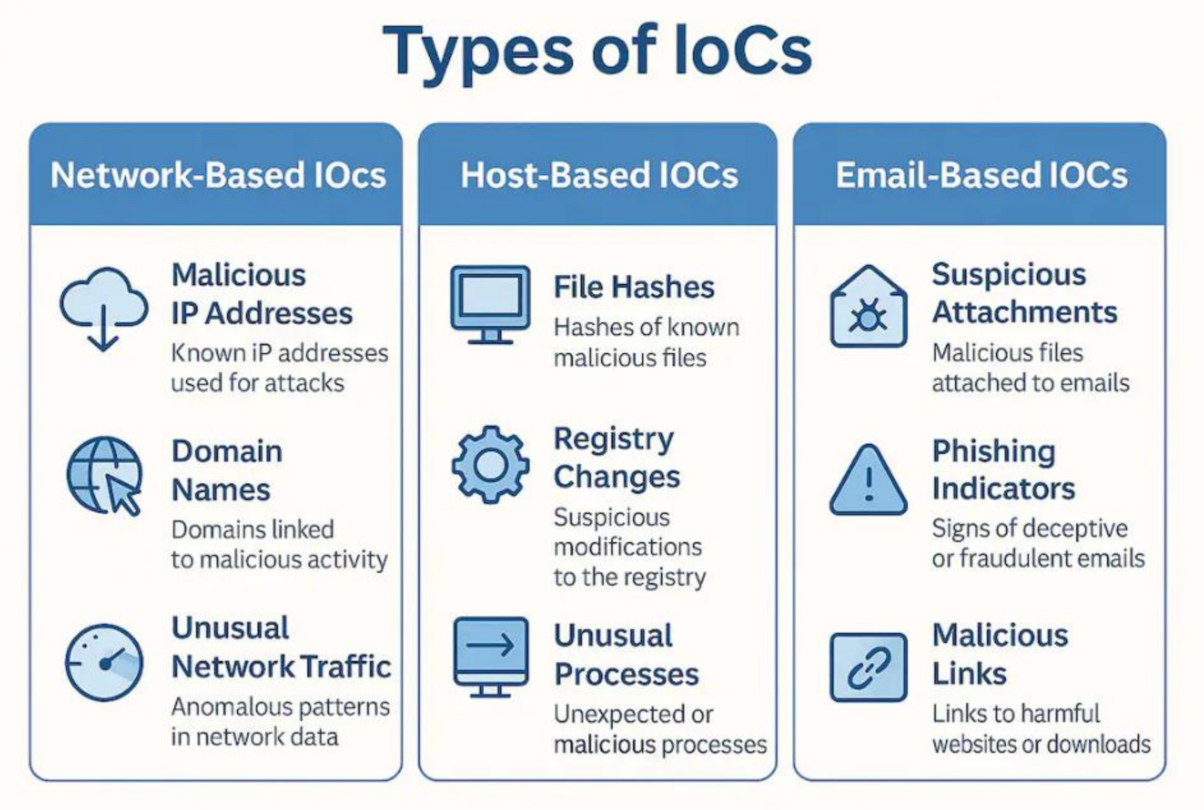
## Incident Classification:

Incident Classification means identifying what type of security event has occurred so that you know how to respond, which team to involve, and how serious the situation is.

- **Core Concept:**
  - **Incident Categories contains:**
    - Malware,
    - Phishing,
    - DDoS Attack,
    - Insider threats,
    - Data exfiltration,
    - Unauthorized Access / Account Compromise,
    - Vulnerability Exploitation
  - **Taxonomy:**
    - MITRE ATT&CK → Global framework of attacker **tactics** and **techniques**. Global framework of attacker **tactics** and **techniques**.
    - ENISA Incident Taxonomy → Used in Europe for cyber incident reporting.
    - VERIS → Vocabulary for Event Recording and Incident Sharing Used for breach analysis. It also focuses on:
      - Action
      - Assets
      - Attributes

## Contextual Metadata:

Enriched incidents with affected systems, timestamps, source IPs, and IOCs (indicators of compromise).



Types of IoCs

**Network-Based IOcs**

Malicious IP Addresses
Known iP addresses used for attacks

Domain Names
Domains linked to malicious activity

Unusual Network Traffic
Anomalous patterns in network data

**Host-Based IOCs**

File Hashes
Hashes of known malicious files

Registry Changes
Suspicious modifications to the registry

Unusual Processes
Unexpected or malicious processes

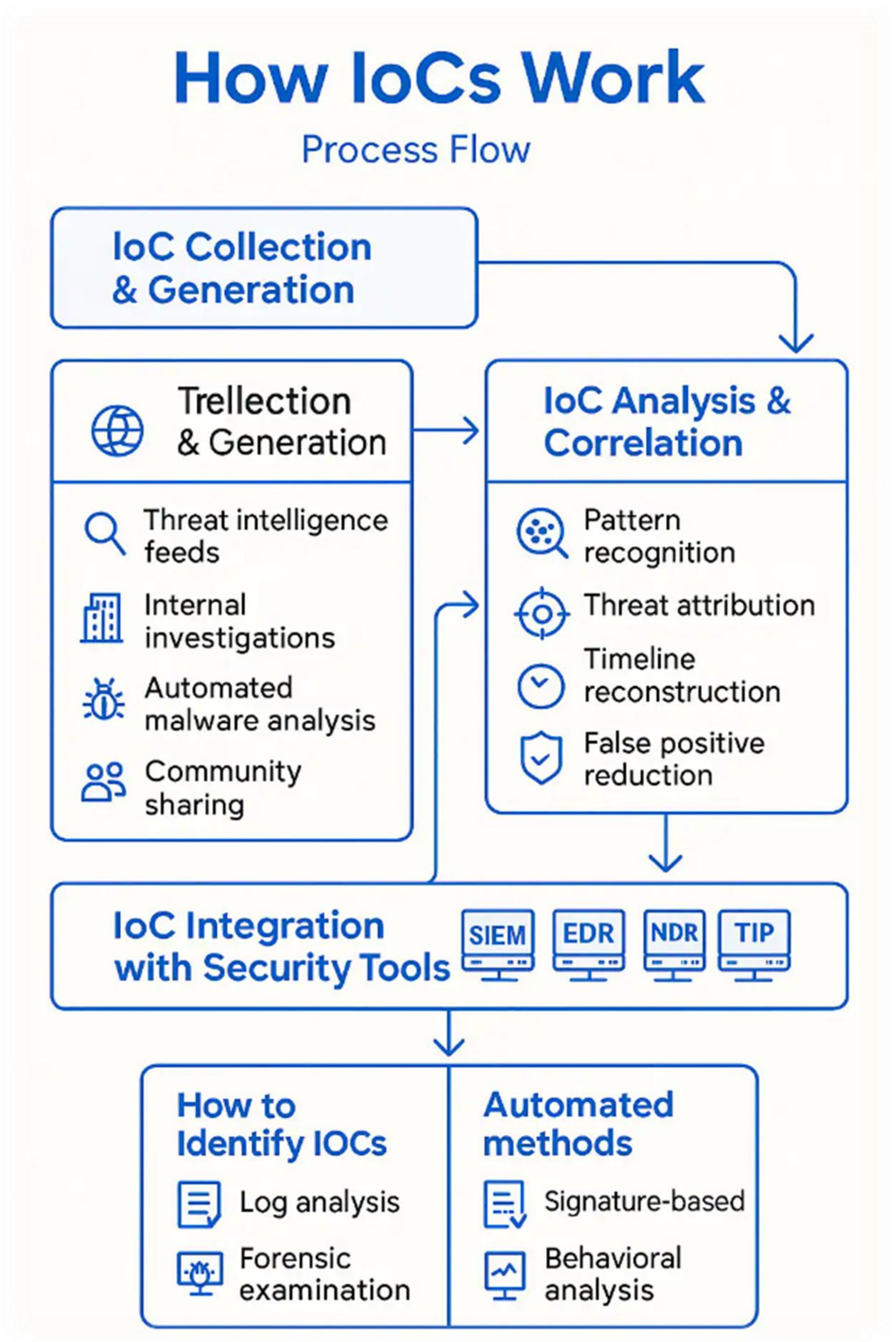
**Email-Based IOCs**

Suspicious Attachments
Malicious files attached to emails

Phishing Indicators
Signs of deceptive or fraudulent emails

Malicious Links
Links to harmful websites or downloads

**Work Flow**



How IoCs Work

Process Flow

IoC Collection & Generation

Trellection & Generation

- Threat intelligence feeds
- Internal investigations
- Automated malware analysis
- Community sharing

IoC Analysis & Correlation

- Pattern recognition
- Threat attribution
- Timeline reconstruction
- False positive reduction

IoC Integration with Security Tools

How to Identify IOCs

- Log analysis
- Forensic examination

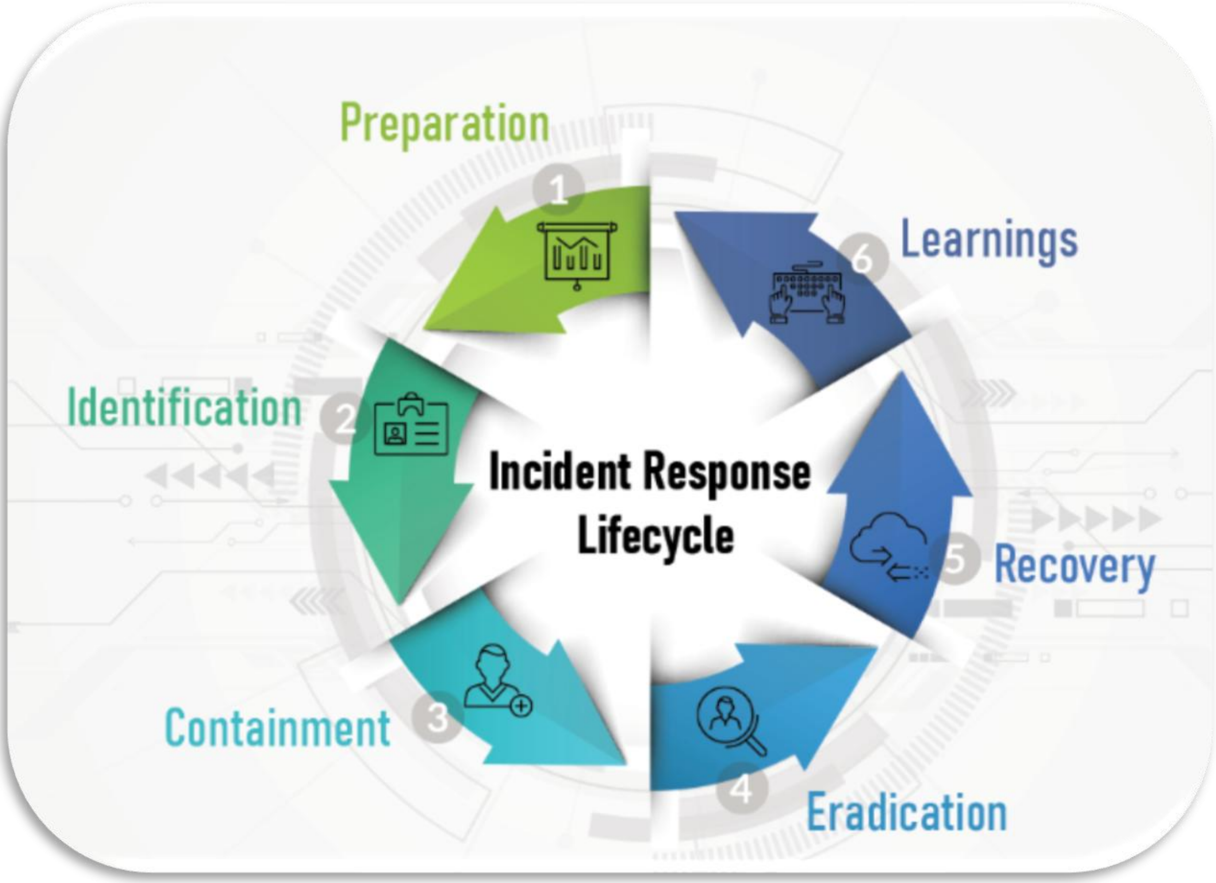
Automated methods

- Signature-based
- Behavioral analysis

## Basic Incident Response:

Incident Response (IR) is the structured process SOC teams follow when a security incident happens. It ensures quick detection, controlled response, and minimal business impact.

The Life cycle of Incident Response,



## Core Concept:

❖ **Incident Lifecycle (NIST SP 800-61 Standard):**

- **Preparation** → This is everything done *before* an incident happens.
- **Identification** → This is where the SOC detects and analyzes suspicious events.
- **Containment** → Goal is to Stop the damage immediately.
- **Eradication** → Goal is to Remove the threat completely.
- **Recovery** → Goal is to Return systems to normal and ensure no re-infection.
- **Lessons Learned** → After the incident, the team documents and discusses,
  - What happened?
  - What worked well?
  - What failed?
  - How do we prevent this next time?

## ❖ Procedures:

We must know how to handle incidents technically and professionally by Implementing:

- System isolation,
  - Disconnect from wired/wireless network
  - Use EDR tools to quarantine endpoint
  - Block VPN session
  - Prevent lateral movement
- Evidence preservation → Never Delete any data.
  - Collect
    - Memory dump (RAM)
    - Disk images
    - Network logs
    - Browser history
    - Process list (e.g., `ps`, `tasklist`)
    - File hashes for forensics (SHA256/MD5)
- Communication protocols,
  - Notify IR Team Lead
  - Avoid discussing details on email (attacker might have access)
  - Communicate via secure channels (Slack IR room, MS Teams IR channel)
  - Avoid unnecessary panic among employees
- SOAR automation concepts.
  - Use of SOAR Tools
    - Splunk Phantom
    - Cortex XSOAR
    - IBM Resilient