Cybersecurity Incident Response – Key Terms & Concepts

Introduction

In cybersecurity, effective incident response depends on clear processes, trained teams, and specialized tools. This document explains the **core incident response concepts, tools, teams, and terminology** used in modern security operations.

---

1. Incident Response Teams & Planning

Computer Security Incident Response Team (CSIRT)

A **specialized group of security professionals** trained to:

- Detect security incidents
- Respond to and manage incidents
- Reduce impact and restore systems

Incident Response Plan (IRP)

A **formal document** that outlines:

- Step-by-step procedures for handling incidents
- Roles and responsibilities
- Communication and recovery actions

Purpose: Acts as a **blueprint** for effective incident response.

Playbook

A **manual** that provides **detailed instructions** for specific operational actions, such as:

- Responding to phishing

- Handling malware
- Managing ransomware incidents

---

2. Monitoring, Detection & Response Tools

Endpoint Detection and Response (EDR)

An application that:

- Monitors endpoints (laptops, desktops, servers)
- Detects malicious behavior
- Supports investigation and response

Intrusion Detection System (IDS)

An application that:

- Monitors system or network activity
- **Alerts** when suspicious activity is detected
- Does **not block** the attack

Intrusion Prevention System (IPS)

An application that:

- Monitors system or network activity
- **Detects and blocks** malicious activity automatically

Security Information and Event Management (SIEM)

An application that:

- Collects and analyzes log data
- Correlates events from multiple sources
- Helps detect security incidents

Security Orchestration, Automation, and Response (SOAR)

A collection of tools and workflows that:

- Automates incident response
- Orchestrates actions across security tools
- Reduces manual effort for analysts

---

3. Security Operations & Monitoring

Security Operations Center (SOC)

A dedicated organizational unit responsible for:

- Monitoring networks, systems, and devices
- Detecting and responding to security threats
- Managing incidents 24/7

---

4. Events, Incidents & Documentation

Event

An **observable occurrence** on a network, system, or device.
➡️ *Not every event is an incident.*

Incident

An occurrence that:

- Jeopardizes the **confidentiality, integrity, or availability (CIA)** of information
- Violates security policies or laws
- Represents an actual or imminent threat

Documentation

Any form of **recorded content** used for a specific purpose, such as:

- Incident reports
- Logs
- Journals
- Playbooks

Incident Handler's Journal

A form of documentation used to:

- Record incident details
- Track actions taken
- Capture lessons learned

---

5. Detection Accuracy Terms (Alerts)

Term	Meaning
True Positive	Alert correctly detects an actual attack

False Positive	Alert incorrectly detects a threat
True Negative	No malicious activity and no alert
False Negative	Malicious activity exists but is not detected

---

6. NIST Incident Response Framework

NIST Incident Response Lifecycle

A structured framework consisting of **four phases**:

1. **Preparation**
2. **Detection and Analysis**
3. **Containment, Eradication, and Recovery**
4. **Post-Incident Activity**

Simple Diagram

```
[ Preparation ]

        ↓
```

```
[ Detection & Analysis ]
        ↓
[ Containment, Eradication & Recovery ]
        ↓
[ Post-Incident Activity ]
```

---

7. Tool Comparison Table

Tool	Main Purpose
IDS	Detect & alert suspicious activity
IPS	Detect and block threats
EDR	Monitor and respond on endpoints
SIEM	Collect and analyze logs

SOAR	Automate and orchestrate response

Conclusion

Incident response relies on **people (CSIRT, SOC)**, **processes (IRP, NIST framework)**, and **technology (IDS, IPS, SIEM, SOAR, EDR)**. Proper documentation and accurate detection are essential for reducing risk and improving security posture.