- Incident: an occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
- Event: an observable occurrence on a network, system, or device.
- All incidents are events, but not vice versa.
- **The 5 W's of an incident:**
  - Who triggered the incident?
  - What happened?
  - When the incident took place?
  - Where the incident took place?
  - Why the incident happened?
- Incident handler's journal: a form of documentation used in incident response.
- **NIST incident response life cycle stages:**
  - Preparation.
  - Detection and Analysis.
  - Containment, eradication, and recovery.
  - Post-incident activity.

- Computer Security Incident Response Teams (CSIRT): a specialized group of security professionals that are trained in incident management and response.
- CSIRT can also be referred as SIRT and IHT (Incident Handling Team).
- **Roles in CSIRT:**
  - Security Analyst: investigate security alerts to determine if an incident has occurred. If an incident has been detected, the analyst will determine the criticality rating of the incident.
  - Technical Lead: provides technical leadership by guiding security incidents through their lifecycle
  - Incident Coordinator: tracks and manages the activities of the CSIRT and other teams involved in the response effort. Their job is to ensure that incident response processes are followed and that teams are regularly updated on the incident status.
- Incident Response Plan: a document that outlines the procedures to take in each step of incident response.
- Security Information and Event Management (SIEM) tool: an application that collects and analyzes log data to monitor critical activities in an organization.
- **SIEM Process:**
  - Collect and aggregate data
  - Normalize data
  - Analyze data
- Security Orchestration, Automation, and Response (SOAR): a collection of applications, tools, and workflows that uses automation to respond to security events.

- Intrusion Detection System (IDS): an application that monitors system activity and alerts on possible intrusions.
- **IDS Detections types:**
  - True positive: correctly detects the presence of an attack
  - True negative: no malicious activity exists and no alert is triggered
  - False positive: identifies an activity as malicious, but it isn't.
  - False negative: malicious activity happens but an IDS fails to detect it
- Intrusion Prevention System (IPS): an application that monitors system activity to detect and alert on intrusions, and it also takes action to prevent the activity and minimize its effects.
- Endpoint Detection and Response (EDR): an application that monitors an endpoint for malicious activity. EDR tools monitor, record, and analyze endpoint system activity to identify, alert, and respond to suspicious activity.

Capability	IDS	IPS	EDR
Detects malicious activity	✓	✓	✓
Prevents intrusions	N/A	✓	✓
Logs activity	✓	✓	✓
Generates alerts	✓	✓	✓
Performs behavioral analysis	N/A	N/A	✓