- Threat Hunting: the proactive search for threats on a network. Security professionals use it to uncover malicious activity that was not identified by detection tools and as a way to do further analysis on detection.
- Threat Intelligence: evidence-based threat information that provides context about existing or emerging threats.
- **Threat Intelligence resources:**
  - Industry reports: this often include attacker's tactics, techniques, and procedures (TTP).
  - Government advisories: similar to industry reports.
  - Threat data feeds: provide a stream of threat-related data that can be used to help protect against sophisticated attackers like advanced persistent threats (APTs).
- Threat Intelligence Platform (TIP): an application that collects, centralizes, and analyzes threat intelligence from different resources.
- Cyber deception: involves techniques that deliberately deceive malicious actors with the goal of increasing detection and improving defensive strategies.
- Honeypots: systems or resources that are created as decoys vulnerable to attacks with purpose of attracting potential intruders.
- Indicators of Compromise (IoCs): obxservable evidence that suggests signs of potential security incident.
- Indicators of Attack (IoAs): the series of observed events that indicate a real-time incident.
- Essentially, IoCs help to identify the who and what of an attack after it's taken place, while IoAs focus on finding the why and how of an ongoing or unknown attack
- Indicators of compromise are not always a confirmation that a security incident has happened. IoCs may be the result of human error, system malfunctions, and other reasons not related to security

- Pyramid of Pain: captures the relationship between indicators of compromise and the level of difficulty that malicious actors experience when indicators of compromise are blocked by security teams.
- **Pyramid of Pain levels:**
  - Hash values (Trivial): Hashes that correspond to known malicious files.
  - IP Addresses (Easy): An internet protocol address.
  - Domain names (Simple): A web address.
  - Network artifacts (Annoying): Observable evidence created by malicious actors on a network. For example, information found in network protocols such as User-Agent strings
  - Host artifacts (Annoying): Observable evidence created by malicious actors on a host. A host is any device that's connected on a network. For example, the name of a file created by malware.
  - Tools (Challenging): Software that's used by a malicious actor to achieve their goal. For example, attackers can use password cracking tools like John the Ripper to perform password attacks to gain access into an account.
  - Tactics, Techniques, and Procedures "TTP" (Tough): the behavior of a malicious actor. Tactics refer to the high-level overview of the behavior. Techniques provide detailed descriptions of the behavior relating to the tactic. Procedures are highly detailed descriptions of the technique. TTPs are the hardest to detect.

- **Benefits of documentation:**
  - Transparency.
  - Standardization.
  - Clarity.
- Chain of custody: the process of documenting evidence possession and control during an incident lifecycle.
- **Chain of custody establishes:**
  - Integrity.
  - Reliability.
  - Accuracy.
- Broken chain of custody: inconsistencies in the collection and logging of the evidence in the chain of custody.
- **Types of Playbooks:**
  - Non-Automated: requires step-by-step actions performed by an analyst
  - Automated: automate tasks in incident response processes.
  - Semi-Automated: combines a person's action with automation.
- Containment: the act of limiting and preventing additional damage caused by an incident.
- Eradication: the complete removal of the incident elements from all affected systems.
- Recovery: the process of returning affected systems back to normal operations.
- Business Continuity Plan (BCP): a document that outlines the procedures to sustain business operations during and after a significant disruption. A BCP helps organizations ensure that critical business functions can resume or can be quickly restored when an incident occurs.

- Triage: the prioritizing of incidents according to their level of importance or urgency.
- **Triage process:**
  - Receive and assess: involves gathering as much information as possible about the alert, including details about the activity that triggered the alert, the systems and assets involved, and more
  - Assign priority: there are some factors to consider when determining the priority of an incident:
    - Functional impact: Security incidents that target information technology systems impact the service that these systems provide to its users
    - Information impact: Incidents can affect the confidentiality, integrity, and availability of an organization's data and information.
    - Recoverability: How an organization recovers from an incident depends on the size and scope of the incident and the amount of resources available
  - Collect and analyze: involves the security analyst performing a comprehensive analysis of the incident. The goal of this step is to gather enough information to make an informed decision to address it.

- Resilience: the ability to prepare for, respond to, and recover from disruptions.
- **Types of site resilience:**
  - Hot sites: A fully operational facility that is a duplicate of an organization's primary environment. Hot sites can be activated immediately when an organization's primary site experiences failure or disruption
  - Warm sites: A facility that contains a fully updated and configured version of the hot site. Unlike hot sites, warm sites are not fully operational and available for immediate use but can quickly be made operational when a failure or disruption occurs
  - Cold sites: A backup facility equipped with some of the necessary infrastructure required to operate an organization's site. When a disruption or failure occurs, cold sites might not be ready for immediate use and might need additional work to be operational.
- Post-incident activity phase: the process of reviewing an incident to identify areas for improvement during incident handling.
- Final report: documentation that provides a comprehensive review of an incident.