**Elements of information security**

* Confidentiality
* Integrity
* Availability
* Authentication
* Non-Repudiation

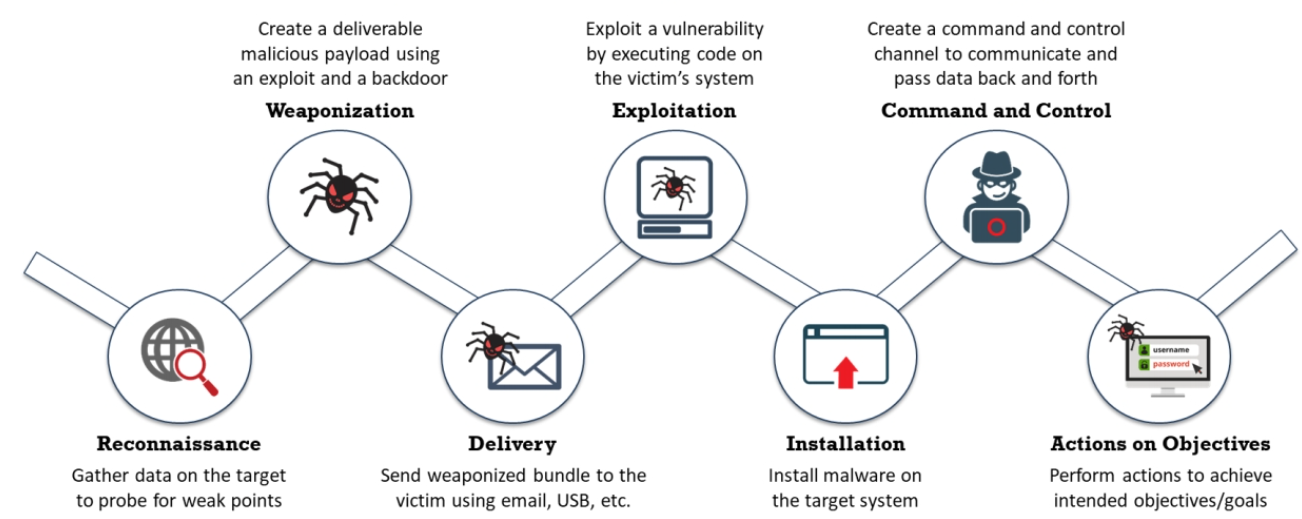
**Attacks = Motive (Goal) + Method + Vulnerability**

**Classification of Attacks**

* **Passive attacks:** It involve intercepting and monitoring network traffic and data flow on the target network and do not tamper with the data.
* **Active Attacks:** It tamper with the data in transit or disrupt communication or services between the systems to bypass or break into secured systems.
* **Close-in attacks:** These attacks are performed when the attacker is in close physical proximity with the target system or network.
* **Insider attacks:** These attacks are performed by trusted persons who have physical access to the critical assets of the target.
* **Distribution attacks:** It occur when attackers tamper with hardware or software prior to installation.

**Information Warfare**

* **Command and control warfare (C2 warfare):** C2 warfare refers to the impact an attacker possesses over a compromised system or network that they control.
* **Intelligence-based warfare:** Intelligence-based warfare is a sensor-based technology that directly corrupts technological systems.
* **Electronic warfare:** It uses radio-electronic and cryptographic techniques to degrade communication.
* **Psychological warfare:** Psychological warfare is the use of various techniques such as propaganda and terror to demoralize one’s adversary in an attempt to succeed in battle.
* **Hacker warfare:** The purpose of this type of warfare can vary from the shutdown of systems, data errors, theft of information, theft of services, system monitoring, false messaging, and access to data.
* **Economic warfare:** It can affect the economy of a business or nation by blocking the flow of information.
* **Cyberwarfare:** It is the use of information systems against the virtual personas of individuals or groups.
* **Defensive Information Warfare:** Involves all strategies and actions to defend against attacks on ICT assets.
* **Offensive Information Warfare:** Involves attacks against the ICT assets of an opponent.

**Cyber Kill Chain**

**TTP 🡺 Tactic, Technique, Procedures**

* **Tactics:** describes the way an attacker performs their attack from beginning to end.
* **Techniques:** technical methods used by an attacker to achieve intermediate results during attack.
* **Procedures:** organizational approach followed by the threat actors to launch their attack.

**Adversary Behaviours**

* Internal reconnaissance
* Use of PowerShell
* Unspecified Proxy Activities
* Use of Command-Line Activities
* HTTP User Agent
* Command & Control Server
* Use of DNS Tunnelling
* Use of Web Shell
* Data Stagging

**Indicators of Compromise (IoC’s)**

An IoC is

* Atomic indicators are those that cannot be segmented into smaller parts, and whose meaning is not changed in the context of an intrusion. Examples of atomic indicators are IP addresses and email addresses.
* Computed indicators are obtained from the data extracted from a security incident. Examples of computed indicators are hash values and regular expressions.
* Behavioural indicators refer to a grouping of both atomic and computed indicators, combined on the basis of some logic.

**An IoC is categorised into:**

* **Email Indicators:** Attackers usually prefer email services to send malicious data to the target organization or individual.
* **Network Indicators:** Network indicators are useful for command and control, malware delivery, and identifying details.
* **Host-Based Indicators:** Host-based indicators are found by performing an analysis of the infected system within the organizational network.
* **Behavioural Indicators:** Behavioural IoC’s are used to identify specific behavior related to malicious activities such as code injection into the memory or running the scripts of an application.

**Hacking Phases**

* **Reconnaissance:** Reconnaissance refers to the preparatory phase in which an attacker gathers as much information as possible
* **Scanning:** The attacker uses the details gathered during reconnaissance to scan the network for specific information. Scanning is a logical extension of active reconnaissance.
* **Gaining Access:**
* **Maintaining Access:**
* **Clearing Tracks:**

**Information Assurance** refers to the assurance of the integrity, availability, confidentiality, and authenticity of information and information systems during the usage, processing, storage, and transmission of information. Security experts accomplish information assurance with the help of physical, technical, and administrative controls.

**Defense-in-depth** is a security strategy in which security professionals use several protection layers throughout an information system.

**Risk** is the probability of the occurrence of a threat or an event that will damage, cause loss to, or have other negative impacts on the organization, either from internal or external liabilities.

**RISK = Threats x Vulnerabilities x Impact Impact can be Asset Value**

**Risk level** is an assessment of the resulted impact on the network. Working out the frequency or probability of an incident happening (likelihood) and its possible consequences is necessary to analyze risks. **Level of Risk = Consequence x Likelihood**

**Risk Matrix** defines various levels of risk and categorizes them as the product of negative probability and negative severity.

**Risk management** is the process of identifying, assessing, responding to, and implementing the activities that control how the organization manages the potential effects of risk.

**risk management phases**

* Risk Identification
* Risk Assessment
* Risk Treatment
* Risk Tracking and Review

**Cyber threat intelligence**, usually known as CTI, is the collection and analysis of information about threats and adversaries and the drawing up of patterns that provide an ability to make knowledgeable decisions for preparedness, prevention, and response actions against various cyberattacks. It is the process of recognizing or discovering any “unknown threats” that an organization may face so that necessary defense mechanisms can be applied to avoid such occurrences.

**Types:**

**Strategic threat intelligence** provides high-level information regarding cybersecurity posture, threats, details about the financial impact of various cyber activities, attack trends, and the impact of high-level business decisions.

**Tactical threat intelligence** plays a major role in protecting the resources of the organization. It provides information related to the TTPs used by threat actors (attackers) to perform attacks.

**Operational threat intelligence** provides information about specific threats against the organization. It provides contextual information about security events and incidents that help defenders disclose potential risks, provide greater insight into attacker methodologies, identify past malicious activities, and perform investigations on malicious activity in a more efficient way.

**Technical threat intelligence** provides information about resources an attacker uses to perform an attack; this includes command and control channels, tools, and other items. It has a shorter lifespan compared to tactical threat intelligence and mainly focuses on a specific IoC.

**Threat modelling** is a risk assessment approach for analysing the security of an application by capturing, organizing, and analysing all the information that affects it. The threat model consists of three major building blocks: understanding the adversary’s perspective, characterizing the security of the system, and determining threats.

**Threat modelling process:**

* Identify Security Objectives
* Application Overview
* Identify Roles
* Identify Key Usage Scenarios
* Identify Technologies
* Identify Application Security Mechanisms
* Decompose the Application
* Identify Trust Boundaries
* Identify Data Flows
* Identify Entry Points
* Identify Exit Points
* Identify Threats
* Identify Vulnerabilities

**Incident management** is a set of defined processes to identify, analyze, prioritize, and resolve security incidents to restore the system to normal service operations as soon as possible, and prevent recurrence of the incident. It involves not only responding to incidents but also triggering alerts to prevent potential risks and threats.

Incident management includes

* Vulnerability analysis
* Artifact analysis
* Security awareness training
* Intrusion detection
* Public or technology monitoring

**Incident handling and response (IH&R)** is the process of taking organized and careful steps when reacting to a security incident or cyberattack. It is a set of procedures, actions, and measures taken against an unexpected event occurrence. It involves logging, recording, and resolving incidents that take place in the organization. It notes the incident, when it occurred, its impact, and its cause. It is the practice of managing the incident response processes, such as preparation, detection, containment, eradication, and recovery, to overcome the impact of an incident quickly and efficiently.

**Steps:**

* Preparation
* Incident Recording &Assignment
* Incident Triage
* Notification
* Containment
* Evidence Gathering & Forensic Analysis
* Eradication
* Recovery
* Post-Incident Activities