

1. **Close-In Attacks** : Close In Attacks Are performed when the attacker is in physical proximity with the target system or network. Ex :
 - Social engineering (Eavesdropping, shoulder surfing, dumpster Driving)
2. **Distribution Attack** : Distribution Attacks occurs when attacker tamper with hardware and software prior to installation. Attackers tamper the hardware or software at its source or when it is in transit.
 - > Modification of Software and Hardware during Distribution
 - > Modification of Software and Hardware during Production
3. **Information Warfare** : The Term information warfare or infowar refers to the use of Information and communication Technology (ICT) to gain competitive advantages over an opponent
 - Ex : virus, worm, trojan horse, logic bombs, trap doors
4. **Semantic Attacks** : Similar to Hacker Warfare, but instead of harming a system, it Takes over the system while maintaining the perception that it is operating correctly.
5. **Types of Information Warfare** :
 1. Command and Control Warfare
 2. Intelligence Based Warfare
 3. Electronic Warfare
 4. Psychological Warfare
 5. Hacker Warfare
 6. Economic Warfare
 7. CyberWarfare
6. **Defensive information warfare** : Involves all the strategies and action to defend against attacks on ICT assets.
7. **Offensive Information Warfare** : Involves attacks against the ICT assets of an opponent.
8. **Cyber Kill Chain Concept** : The Cyber kill chain is an efficient and effective way of illustrating how an adversary can attack the organization. This model helps organization understands the various possible threats at every stage of an attack and the necessary countermeasure to defend against such attacks.
 - It is a component of Intelligence -driven defence for the identification and Prevention of malicious intrusion activities.
9. **7 Stages of Cyber Kill Methodology** :
 1. **Reconnaissance** : Gathering Information
 2. **Weaponization** : creating Payload According to Information gathered
 3. **Delivery** : Transferring payload to Victim
 - Delivery is the key stage that measure the effectiveness of the defence strategies.
 4. **Exploitation** : run the malicious code
 5. **Installation** : Install more malicious code to maintain access to the target
 6. **Command and Control** : two way communication between attacker and victim
 7. **Actions on Objectives** : Attacker gains access to confidential Data, compromise more systems linked to that machine.
10. **Tactics, Techniques, and Procedure (TTPs)** : refers to the pattern of activities and methods associated with specific threat actor or group of threat actor.
 - Tactics** : Way an attacker performs an attack, tactics for info gathering
 - Techniques** : technical methods used by an attacker
 - Procedure** : Organizational approach that attacker follow to launch the attack
11. **Attacker Behaviour Identification** : It involves the identification of the common methods or techniques followed by an attacker.

12. Attacker / Adversary Behaviours :

1. Internal reconnaissance
2. Use of PowerShell
3. Unspecified Proxy Activities
4. Use of Command Line Interface
5. HTTP User Agent
6. Command and Control Server
7. Use of DNS Tunneling
8. Use of a Web Shell
9. Data staging : data staging techniques to collect and combine as much as possible

13. Indicator of Compromise (IOCs) : clues, artifact and piece of forensics data found on the network or OS of an organization that indicate the malicious activity on the network. Act as a good source of information regarding the threat.

14. Indicators : **Atomic Indicator** - cannot be segmented into smaller parts, whose meaning is not changed in the context of an intrusion. **Computed Indicator** : obtained from the data extracted from a security incident. **Behavioural Indicators** : grouping of both Atomic and computed.

15. Categories of IOCs :

1. **Email Indicator** : use for mails
2. **Network Indicator** : uses for URLs, Domain Names, IP address.
3. **Host Indicator** : file name , File Hashes, DLL
4. **Behavioral Indicator** : document executing powershell script.

16. Dumpster Diving : Dumpster Diving is simply enough , looking through an organization's trash for any discarded sensitive information.

17. Hacking Phase :

1. Reconnaissance :

- 1.1 Active
- 1.2 Passive

Methods of Reconnaissance :

- 1.1 Social engineering
- 1.2 Dumpster Diving

2. Scanning

3. Gaining Access
4. Maintaining Access
5. Clearing Tracks

18. Smurf Attack : Smurf Attack attempt to cause users on a network to flood each other with data. Making It appear as if everyone is attacking each other, and leaving the hacker anonymous.

19. Steganography : It is the process of hiding data in other data, in image and sound file.

20. Tunneling takes advantage of the transmission protocol by carrying one protocol over another.

21. Information Security Controls : This prevent the occurrence of unwanted events and reduce risk to the organization's information assets.

This section Deals with Information Assurance (IA), defence-in-depth, risk management, cyber threat intelligence, threat Modeling, incident Management, and AI and ML concepts.

22. Information Assurance (IA) : refer to the assurance of integrity, confidentiality, availability, and authenticity of information and information system is protected during the usage of, processing storage, and transmission of information.

23. Defence in Depth : It is a security strategy in which several protection Layer are placed throughout an information system. It helps to prevent direct attacks against the system and its data because a break in one layer only leads to attacker to the next layer.

24. Risk : refer to the degree of uncertainty or expectation that an adverse event may cause damage to the system.

$$\text{RISK} = \text{THREAT} \times \text{VULNERABILITY} \times \text{IMPACT}$$

$$\text{RISK} = \text{THREAT} \times \text{VULNERABILITY} \times \text{ASSET VALUE}$$

25. Risk Level : It is an assesment of the resulted impact on the network.

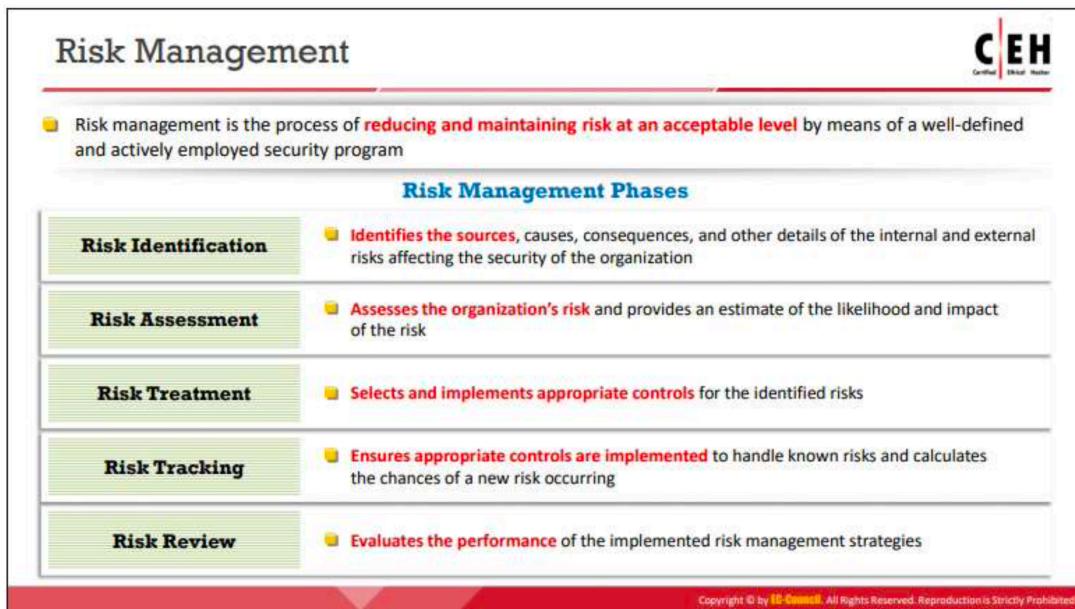
Likelihood : The chance of the risk occurring,

Consequence : The severity of a risk events that occurs.

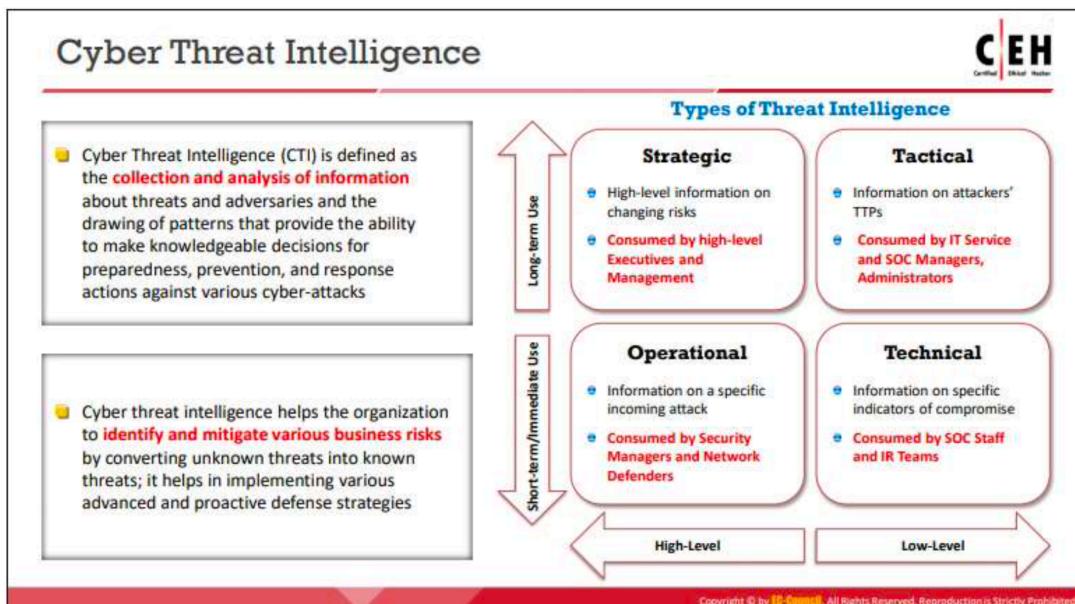
$$\text{RISK LEVEL} = \text{CONSEQUENCE} \times \text{LIKELIHOOD}$$

26. Risk Matrix : scales the risk of occurence or likelihood probability, along with its consequences or impact. It is the graphical representation of risk severity and the extent to which the controls can or mitigate it.

27. Risk Management :



28. Cyber Threat Intelligence :



29. Threat : defined as “the possibility of a malicious attempt to damage or disrupt a computer network or system”

30. Threat Modeling :

Threat Modeling



Threat modeling is a **risk assessment approach** for analyzing the security of an application by capturing, organizing, and analyzing all the information that affects the security of an application

Threat Modeling Process	
01	Identify Security Objectives Helps to determine how much effort needs to be put toward subsequent steps
02	Application Overview Identify the components, data flows , and trust boundaries
03	Decompose the Application Helps to find more relevant and more detailed threats
04	Identify Threats Identify threats relevant to the control scenario and context using the information obtained in steps 2 and 3
05	Identify Vulnerabilities Identify weaknesses related to the threats found using vulnerability categories

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

31. Incident Management :

Incident Management



- Incident management is a set of defined processes to **identify, analyze, prioritize, and resolve security incidents** to restore normal service operations as quickly as possible and prevent future recurrence of the incident

Incident Management	
Vulnerability Handling	Incident Handling
Artifact Handling	Triage Reporting and Detection
Announcements	Incident Response Analysis
Alerts	Other Incident Management Services

Copyright © by IC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

32. Incident handling and Response (IH & R) :

Incident Handling and Response

CEH
Certified Ethical Hacker

- Incident handling and response (IH&R) is the **process of taking organized and careful steps** when reacting to a security incident or cyberattack

Steps involved in the IH&R process:

1 Preparation	7 Eradication
2 Incident Recording and Assignment	8 Recovery
3 Incident Triage	9 Post-Incident Activities
4 Notification	<ul style="list-style-type: none"> Incident Documentation Incident Impact Assessment Review and Revise Policies Close the Investigation Incident Disclosure
5 Containment	
6 Evidence Gathering and Forensic Analysis	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

33. Role of AI and ML in CyberSec :

Role of AI and ML in Cyber Security

CEH
Certified Ethical Hacker

- Machine learning (ML) and artificial intelligence (AI) are now vastly used across various industries and applications due to the **increase in computing power, data collection, and storage capabilities**
- ML is an **unsupervised self-learning system** that is used to define what the normal network looks like, along with its devices, and then to backtrack and **report any deviations or anomalies** in real-time
- AI and ML in cyber security helps in **identifying new exploits and weaknesses**, which can then be easily analyzed to mitigate further attacks

ML classification techniques:

- Supervised learning makes use of algorithms that input a **set of labeled training data**, with the aim of learning the differences between the labels
- Unsupervised learning makes use of algorithms that input **unlabeled training data**, with the aim of deducing all categories by itself

```

graph TD
    ML[Machine Learning] --> UL[Unsupervised Learning]
    ML --> SL[Supervised Learning]
    UL --> DR[Dimensionality Reduction]
    UL --> CL[Clustering]
    SL --> CLS[Classification]
    SL --> REG[Regression]
  
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

34. How Do AI and ML Prevents cyber Attacks :



35. Payment Card Industry Data security Standards (PCI-DSS):

Payment Card Industry Data Security Standard (PCI DSS)

The infographic highlights the following about PCI DSS:

- The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary **information security standard for organizations** that handle cardholder information for major debit, credit, prepaid, e-purse, ATM, and POS cards
- PCI DSS **applies to all entities involved in payment card processing** — including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process, or transmit cardholder data

PCI Data Security Standard — High Level Overview

Build and Maintain a Secure Network	Implement Strong Access Control Measures
Protect Cardholder Data	Regularly Monitor and Test Networks
Maintain a Vulnerability Management Program	Maintain an Information Security Policy

<https://www.pcisecuritystandards.org>

Failure to meet the PCI DSS requirements may result in fines or the termination of payment card processing privileges

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network	<ul style="list-style-type: none"> ▪ Install and maintain a firewall configuration to protect cardholder data ▪ Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ul style="list-style-type: none"> ▪ Protect stored cardholder data ▪ Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ul style="list-style-type: none"> ▪ Use and regularly update anti-virus software or programs ▪ Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ul style="list-style-type: none"> ▪ Restrict access to cardholder data by business need to know ▪ Assign a unique ID to each person with computer access ▪ Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ul style="list-style-type: none"> ▪ Track and monitor all access to network resources and cardholder data ▪ Regularly test security systems and processes
Maintain an Information Security Policy	<ul style="list-style-type: none"> ▪ Maintain a policy that addresses information security for all personnel

36. ISO / IEC 27001:2013

ISO/IEC 27001:2013

CEH
Certified Ethical Hacker

- ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining, and continually improving an **information security management system** within the context of the organization
- It is intended to be suitable for several different types of use, including:

<ol style="list-style-type: none"> 1 Use within organizations to formulate security requirements and objectives 2 Use within organizations to ensure that security risks are cost-effectively managed 3 Use within organizations to ensure compliance with laws and regulations 4 Definition of new information security management processes 	<ol style="list-style-type: none"> 5 Identification and clarification of existing information security management processes 6 Use by organization management to determine the status of information security management activities 7 Implementation of business-enabling information security 8 Use by organizations to provide relevant information about information security to customers
--	--

<https://www.iso.org>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

37. HIPAA (Health Insurance Portability and Accountability Act)

Health Insurance Portability and Accountability Act (HIPAA)

CEH
Certified Ethical Hacker

HIPAA's Administrative Simplification Statute and Rules

Electronic Transaction and Code Set Standards	Requires every provider who does business electronically to use the same health care transactions, code sets, and identifiers
Privacy Rule	Provides federal protections for the personal health information held by covered entities and gives patients an array of rights with respect to that information
Security Rule	Specifies a series of administrative, physical, and technical safeguards for covered entities to use to ensure the confidentiality, integrity, and availability of electronically protected health information
National Identifier Requirements	Requires that health care providers, health plans, and employers have standard national numbers that identify them attached to standard transactions
Enforcement Rule	Provides the standards for enforcing all the Administration Simplification Rules

<https://www.hhs.gov>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The HIPAA Privacy Rule provides federal protections for the individually identifiable health information held by covered entities and their business associates and gives patients an array of rights to that information. At the same time, the Privacy Rule permits the disclosure of health information needed for patient care and other necessary purposes.

38. DMCA & FISMA :

The Digital Millennium Copyright Act (DMCA) and the Federal Information Security Management Act (FISMA)



The Digital Millennium Copyright Act (DMCA)

- The DMCA is a United States copyright law that implements two 1996 treaties of the **World Intellectual Property Organization (WIPO)**
- It **defines the legal prohibitions** against the circumvention of technological protection measures employed by copyright owners to protect their works, and against the removal or alteration of copyright management information



<https://www.copyright.gov>

Federal Information Security Management Act (FISMA)

- The FISMA provides a comprehensive framework for ensuring the **effectiveness of information security controls** over information resources that support Federal operations and assets
- It includes
 - Standards for categorizing information and information systems by mission impact
 - Standards for minimum security requirements for information and information systems
 - Guidance for selecting appropriate security controls for information systems
 - Guidance for assessing security controls in information systems and determining security control effectiveness
 - Guidance for security authorization of information systems

<https://csrc.nist.gov>

Copyright © by EC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Short Forms :

1. ICT : Information and Communication Technology
2. IOCs : Indicator of Compromise
3. TTPs : Tactics, Techniques, and Procedure
4. IA : Information Assurance
5. IRM : Information Risk Management
6. C&A : Certification & Accreditation
7. CTI : Cyber Threat Intelligence
8. Incident handling and Response (IH & R)
9. DMCA : Digital millennium copyright act
10. FISMA : Federal Information Security Management act
11. WIPO : World Intellectual Property Organization

***** END OF MODULE - 1 *****