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 maintaing 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** : Tranfering 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 confedential 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 Activites
    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. **Ganning 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 occurence 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 tranmission 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 uncertainity or expectation that an adverse event may cause damage to the system.

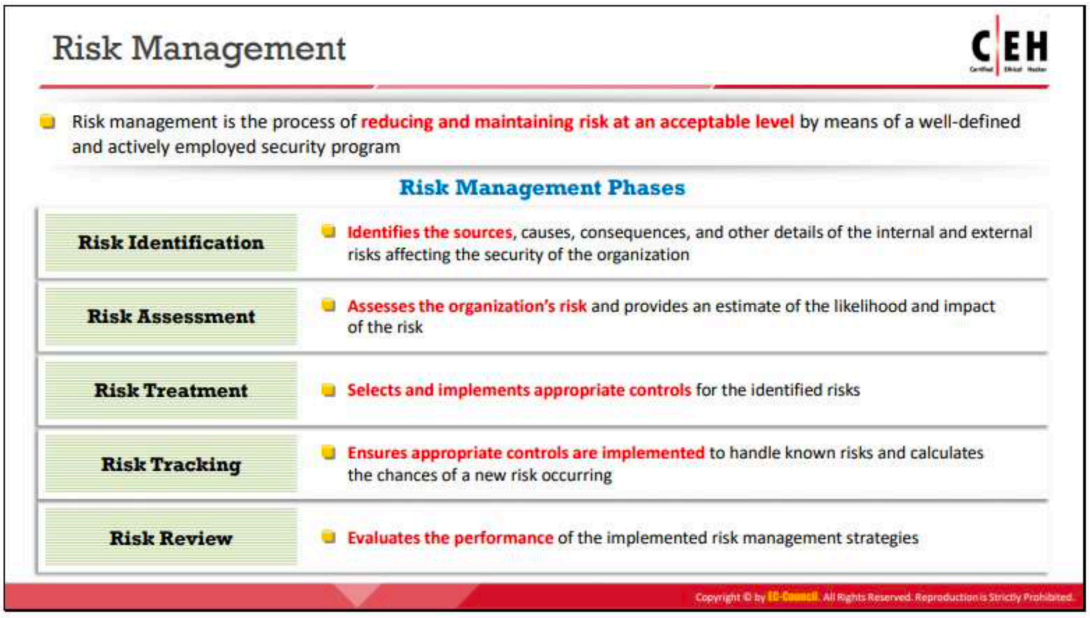
RISK = THREAT X VULNERABILITY X IMPACT
RISK = THREAT X VULNERABILITY X ASSET VALUE

25. **Risk Level** : It is an assesment of the resulted impact on the network.
Likelihood : The chance of the risk occuring,
Consequence : The severity of a risk events that occurs.

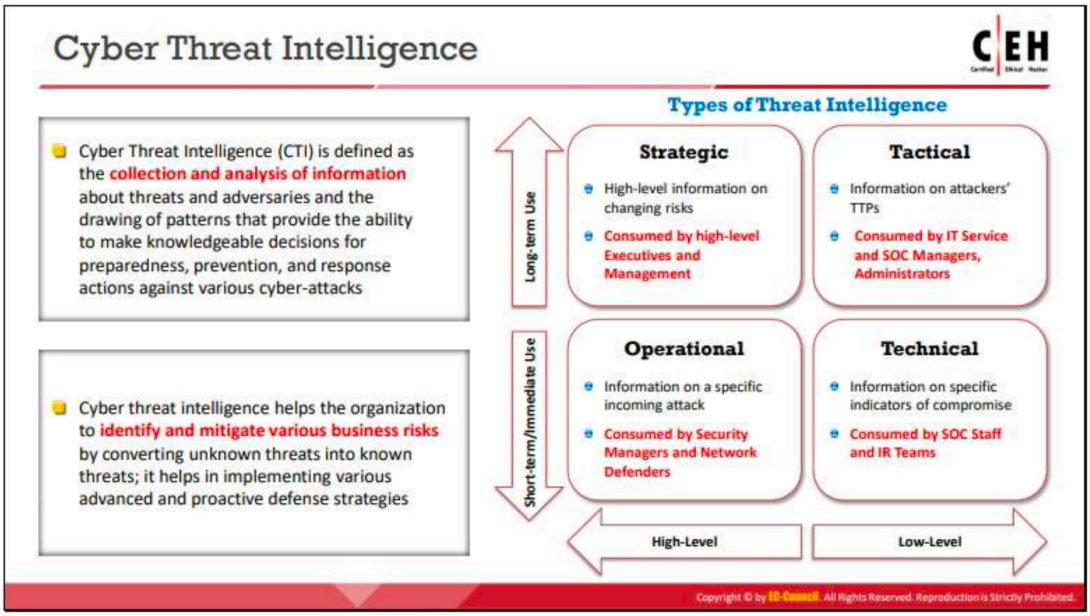
RISK LEVEL = CONSEQUENCE X LIKELIHOOD

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** :

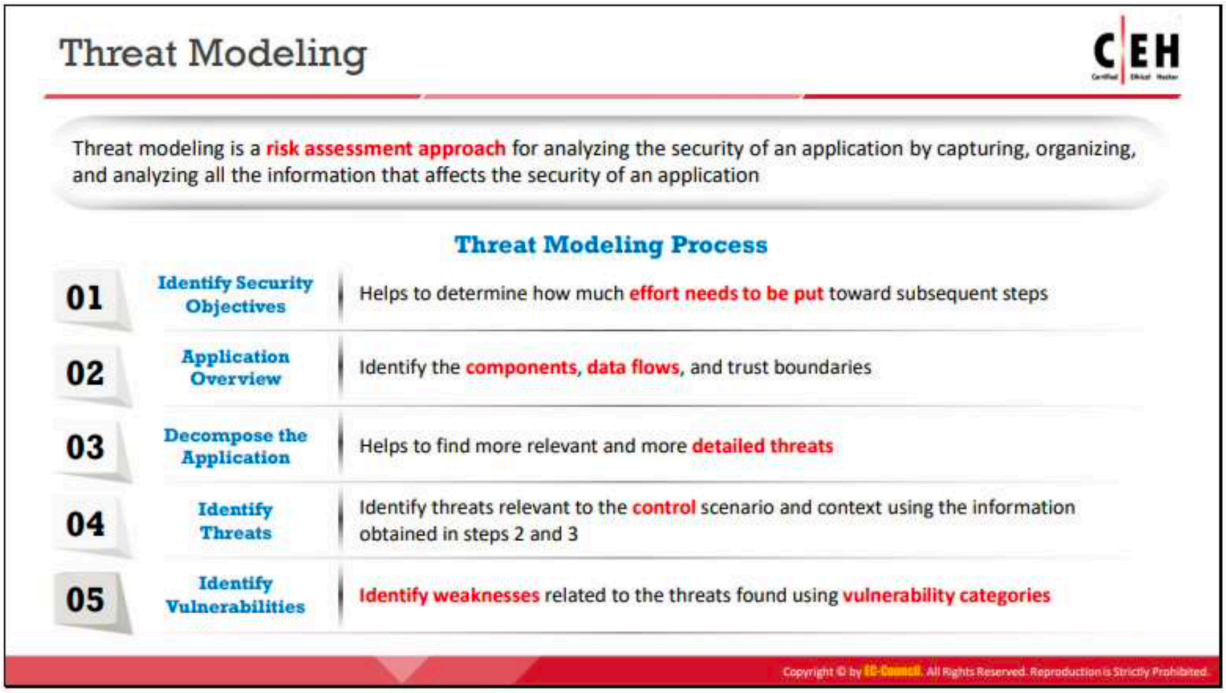


28. **Cyber Threat Intelligence** :

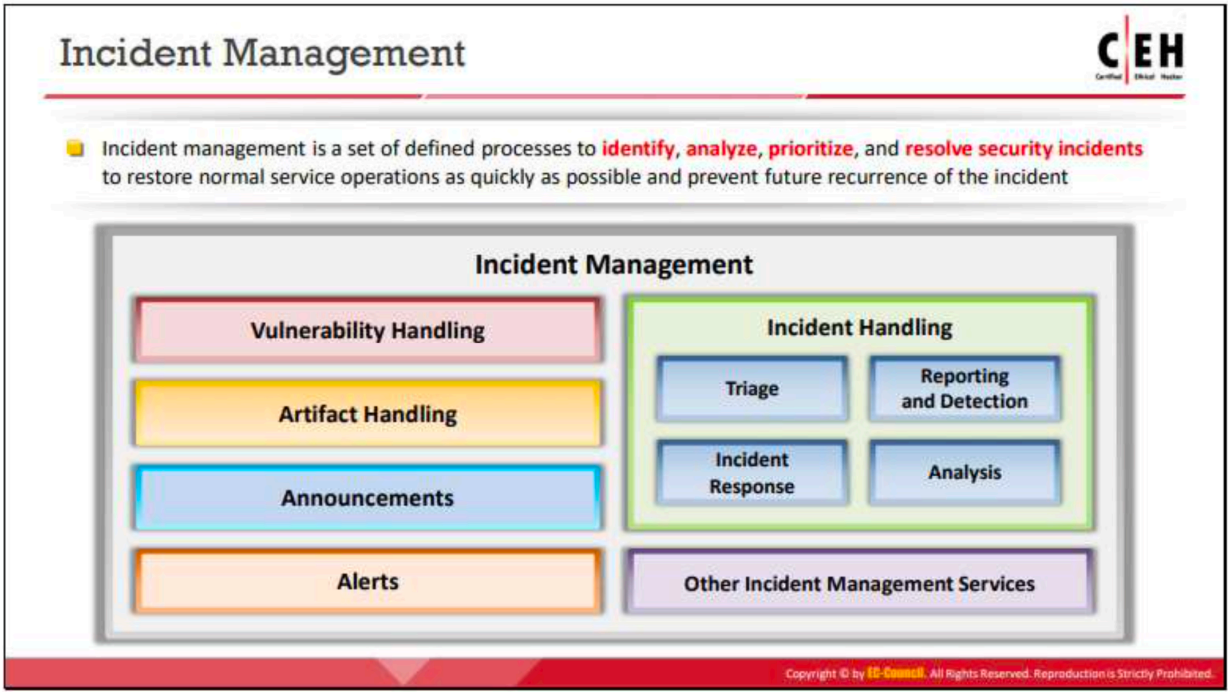


29. Threat : defined as “the possibility of a malicious attempt to damage or disrupt a computer network or system”

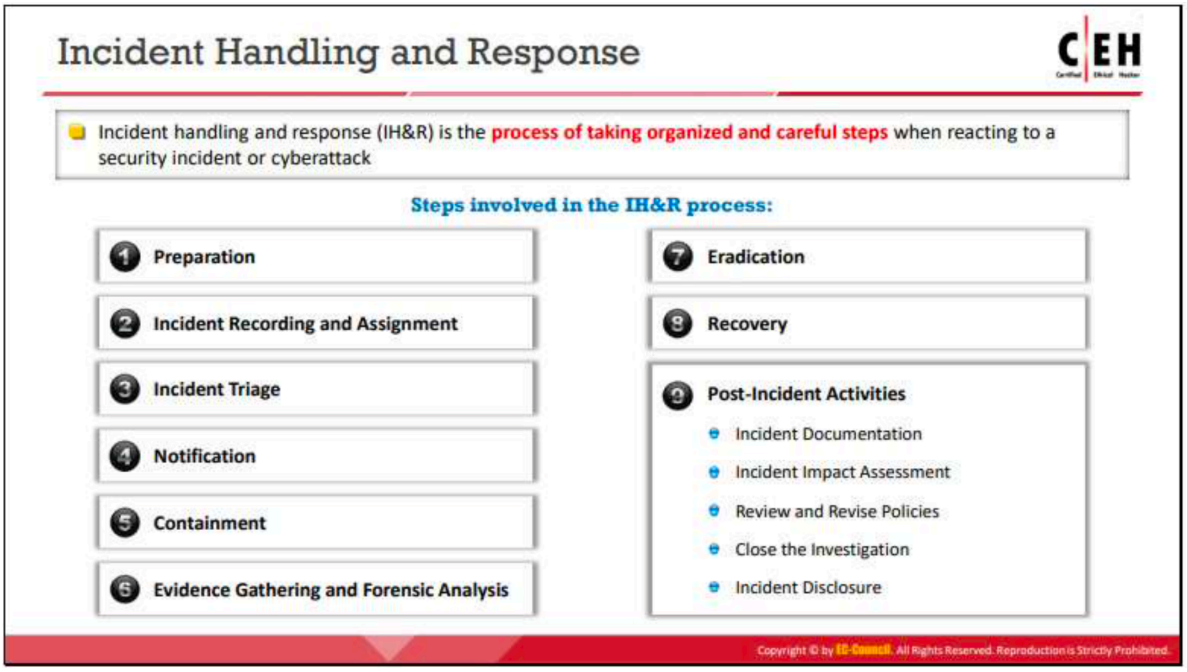
30. Threat Modeling :



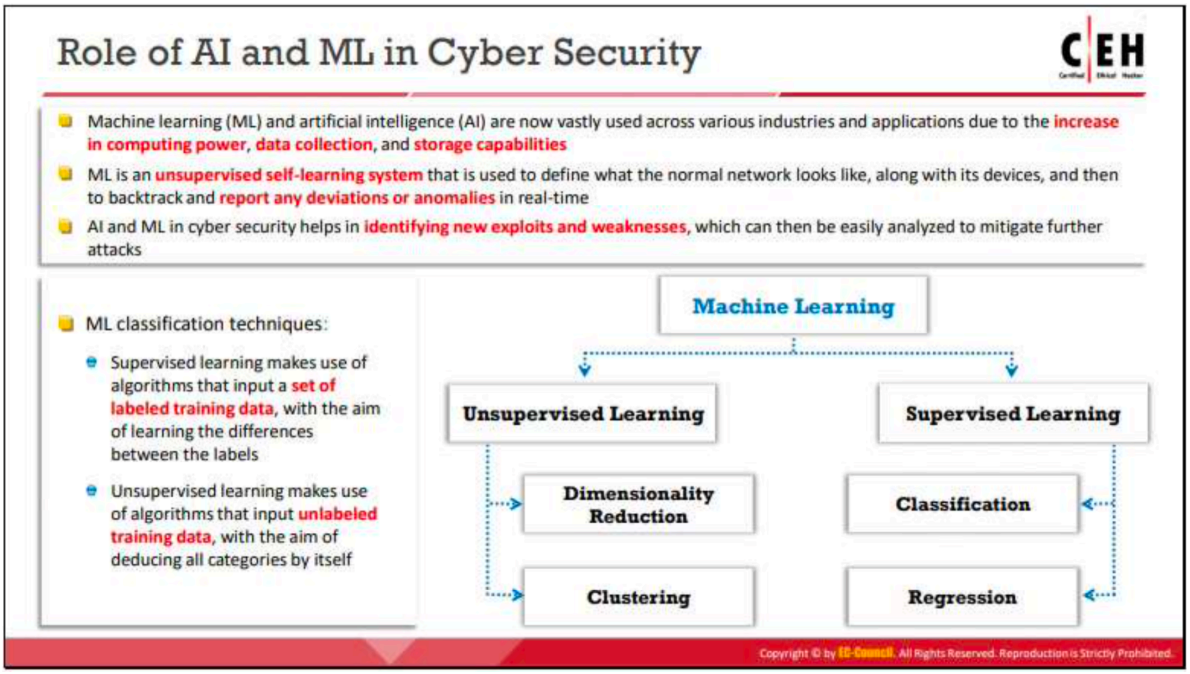
31. **Incident Management** :



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

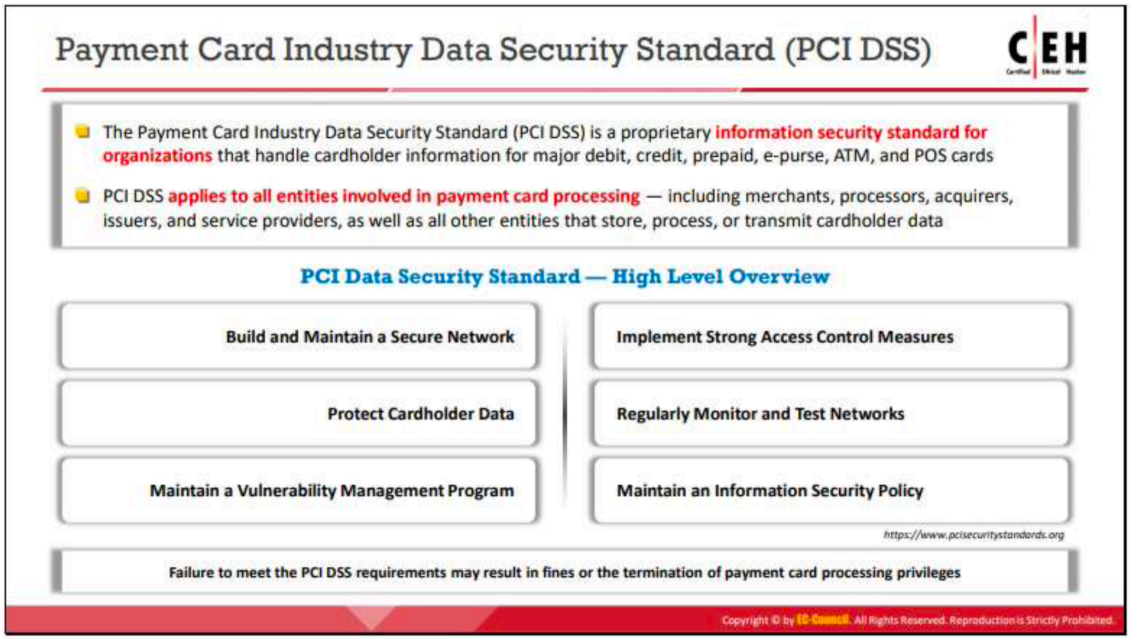


33. **Role of AI and ML in CyberSec** :

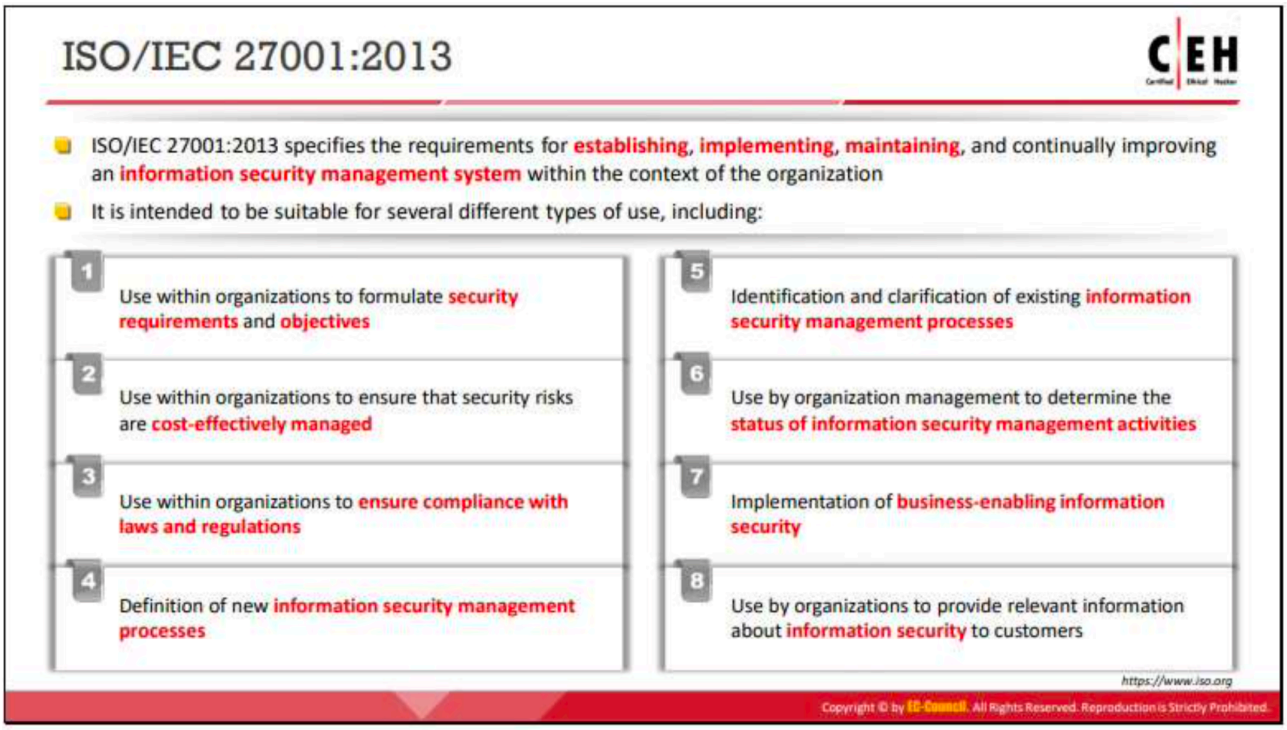


34. **How Do AI and ML Prevents cyber Attacks** :

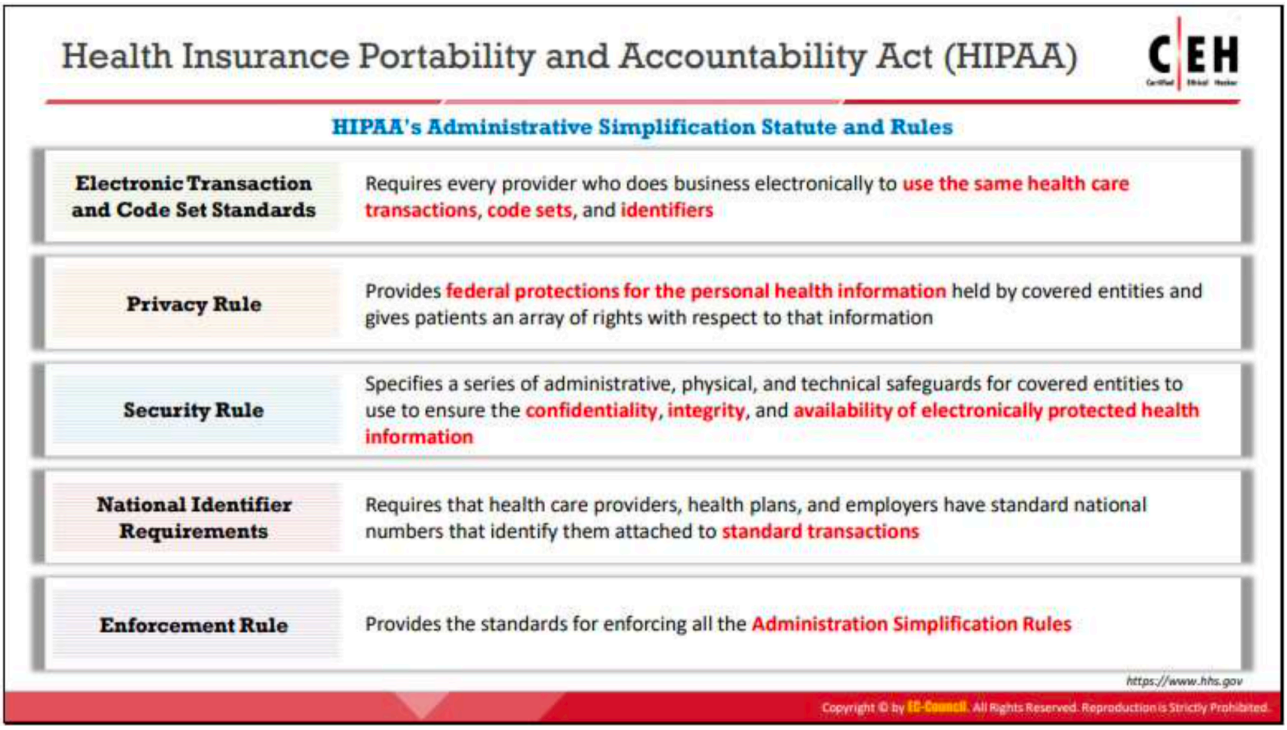
35. **Payment Card Industry Data security Standards (PCI-DSS)**:



36. **ISO / IEC 27001:2013**

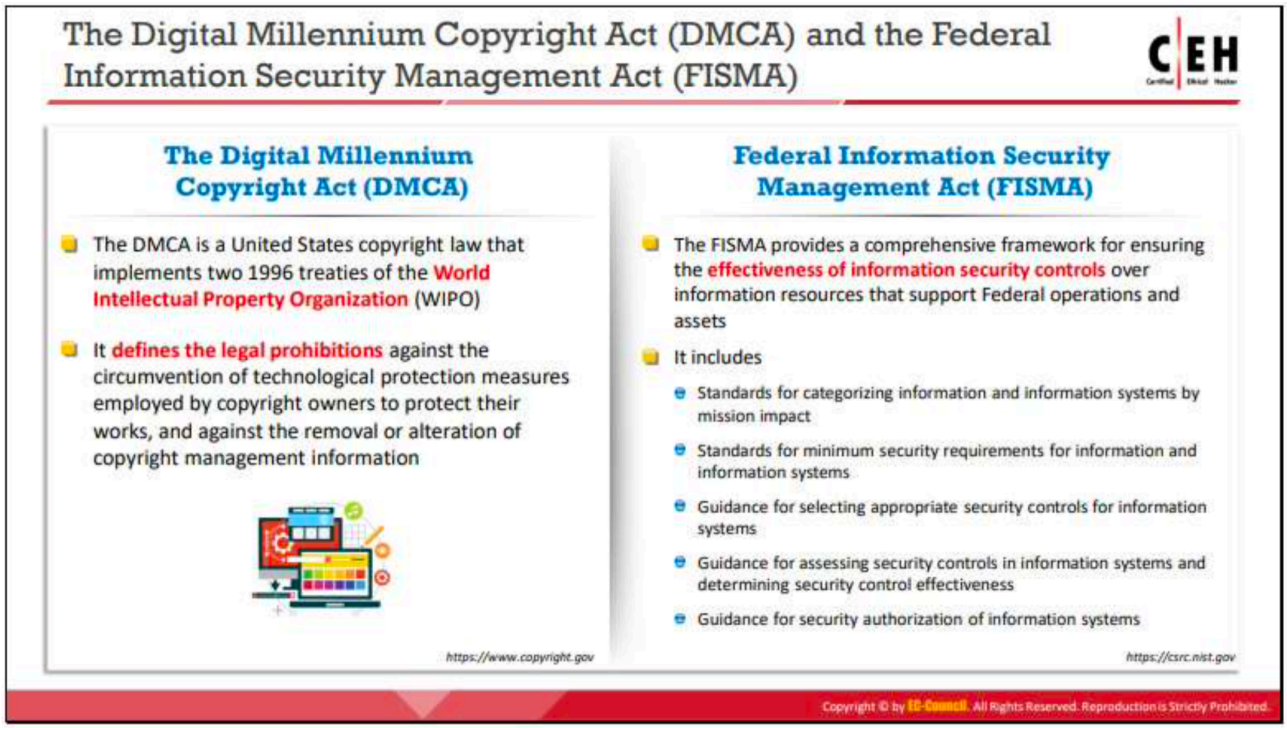


37. **HIPAA (Health Insurance Portability and Accountablity Act)**



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** :



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 **********
****