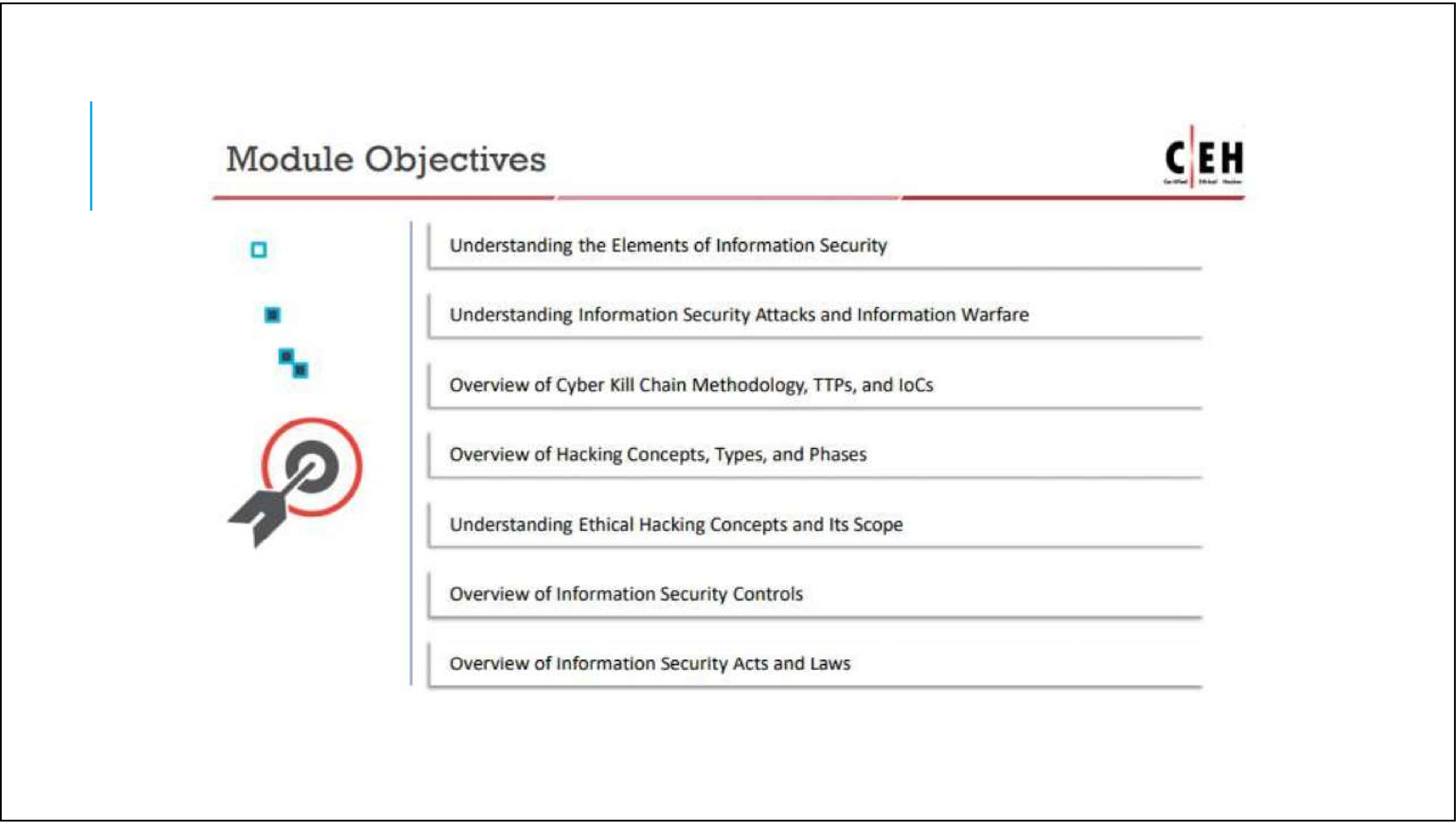
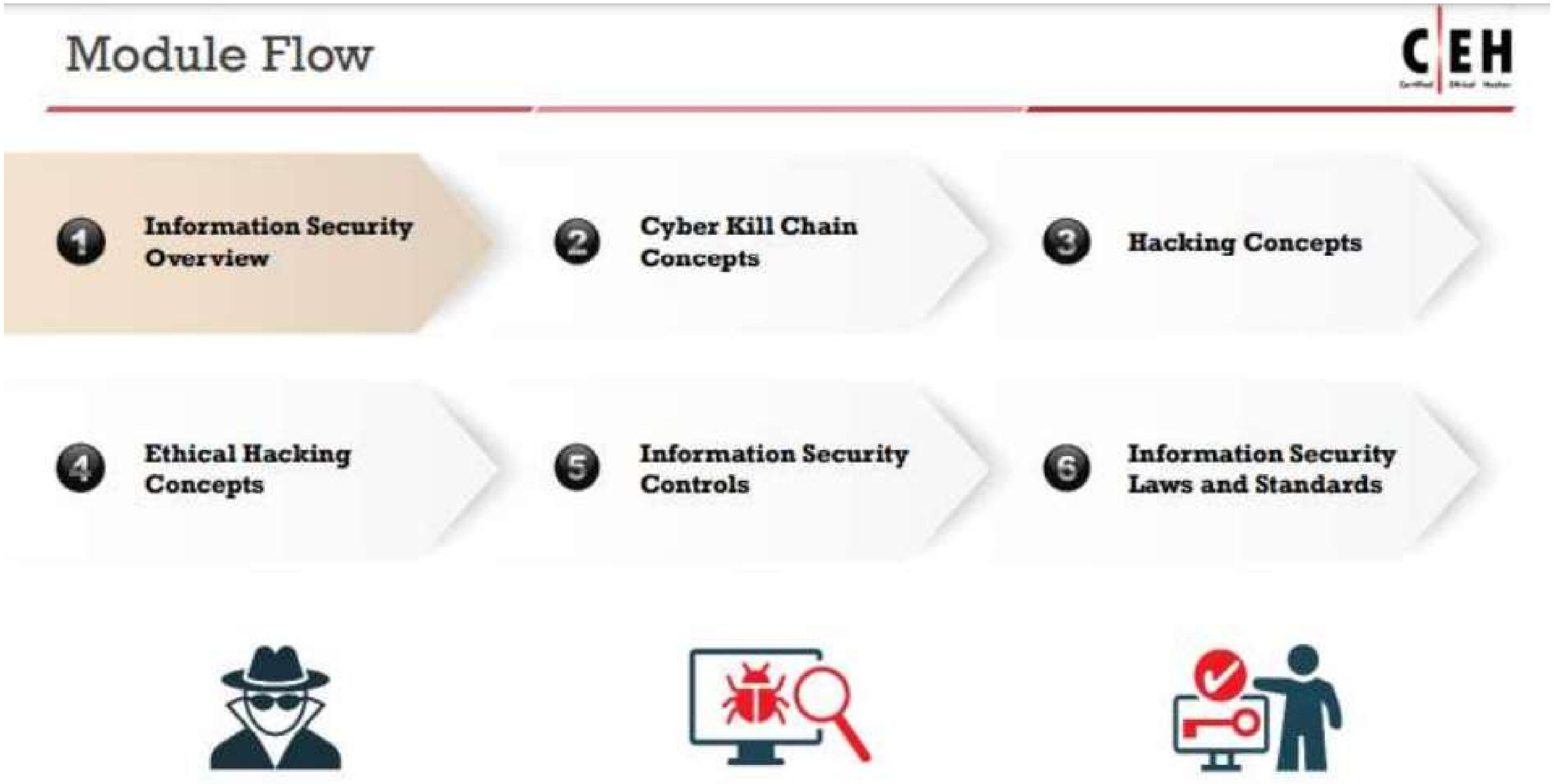
INTRODUCTION TO ETHICAL HACKING



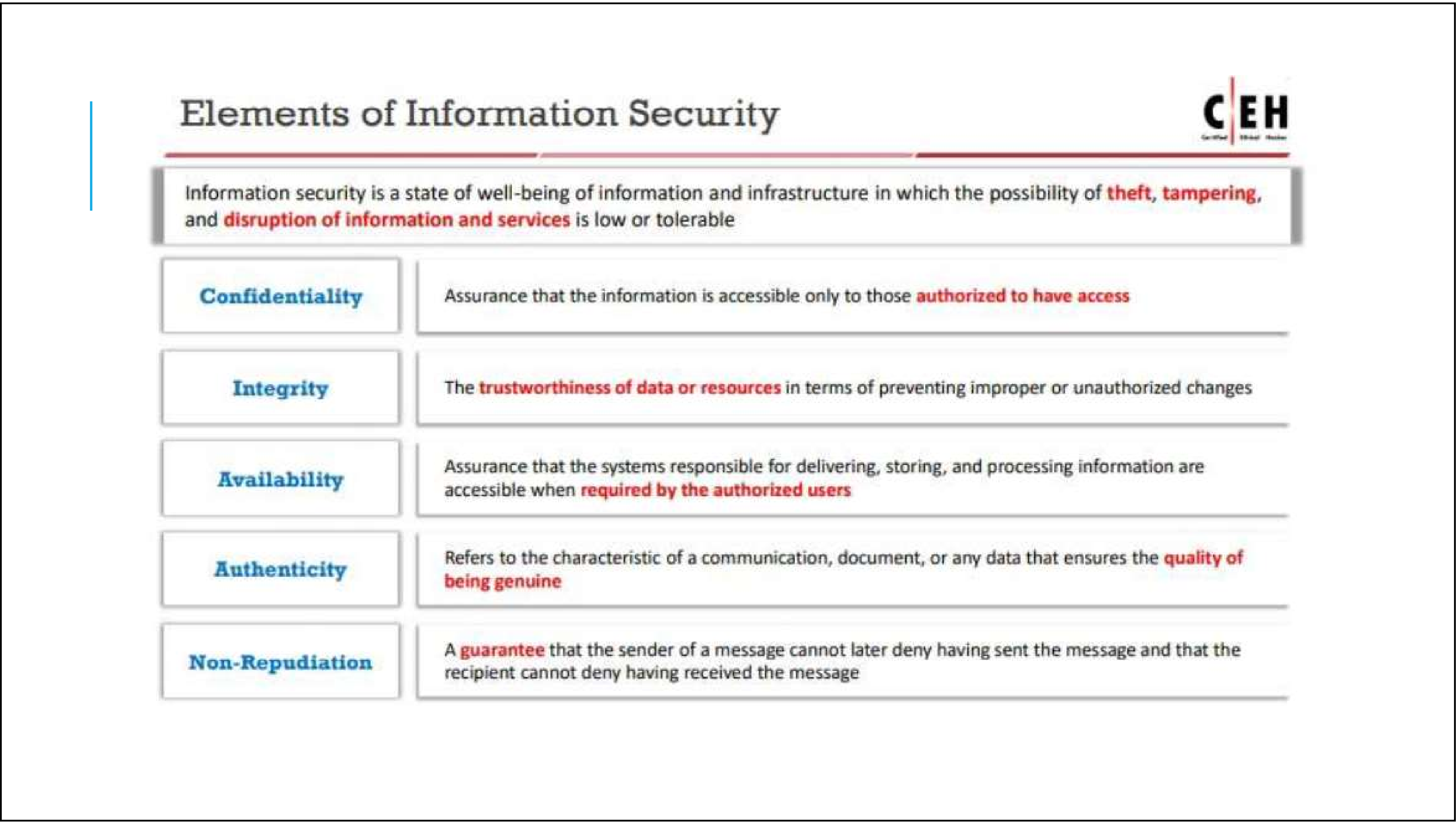
Module Objectives

- Understanding the Elements of Information Security
- Understanding Information Security Attacks and Information Warfare
- Overview of Cyber Kill Chain Methodology, TTPs, and IoCs
- Overview of Hacking Concepts, Types, and Phases
- Understanding Ethical Hacking Concepts and Its Scope
- Overview of Information Security Controls
- Overview of Information Security Acts and Laws



Module Flow

1. Information Security Overview
2. Cyber Kill Chain Concepts
3. Hacking Concepts
4. Ethical Hacking Concepts
5. Information Security Controls
6. Information Security Laws and Standards



Elements of Information Security

Information security is a state of well-being of information and infrastructure in which the possibility of **theft**, **tampering**, and **disruption of information and services** is low or tolerable

Confidentiality

Assurance that the information is accessible only to those **authorized to have access**

Integrity

The **trustworthiness of data or resources** in terms of preventing improper or unauthorized changes

Availability

Assurance that the systems responsible for delivering, storing, and processing information are accessible when **required by the authorized users**

Authenticity

Refers to the characteristic of a communication, document, or any data that ensures the **quality of being genuine**

Non-Repudiation

A **guarantee** that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message

In class activity :

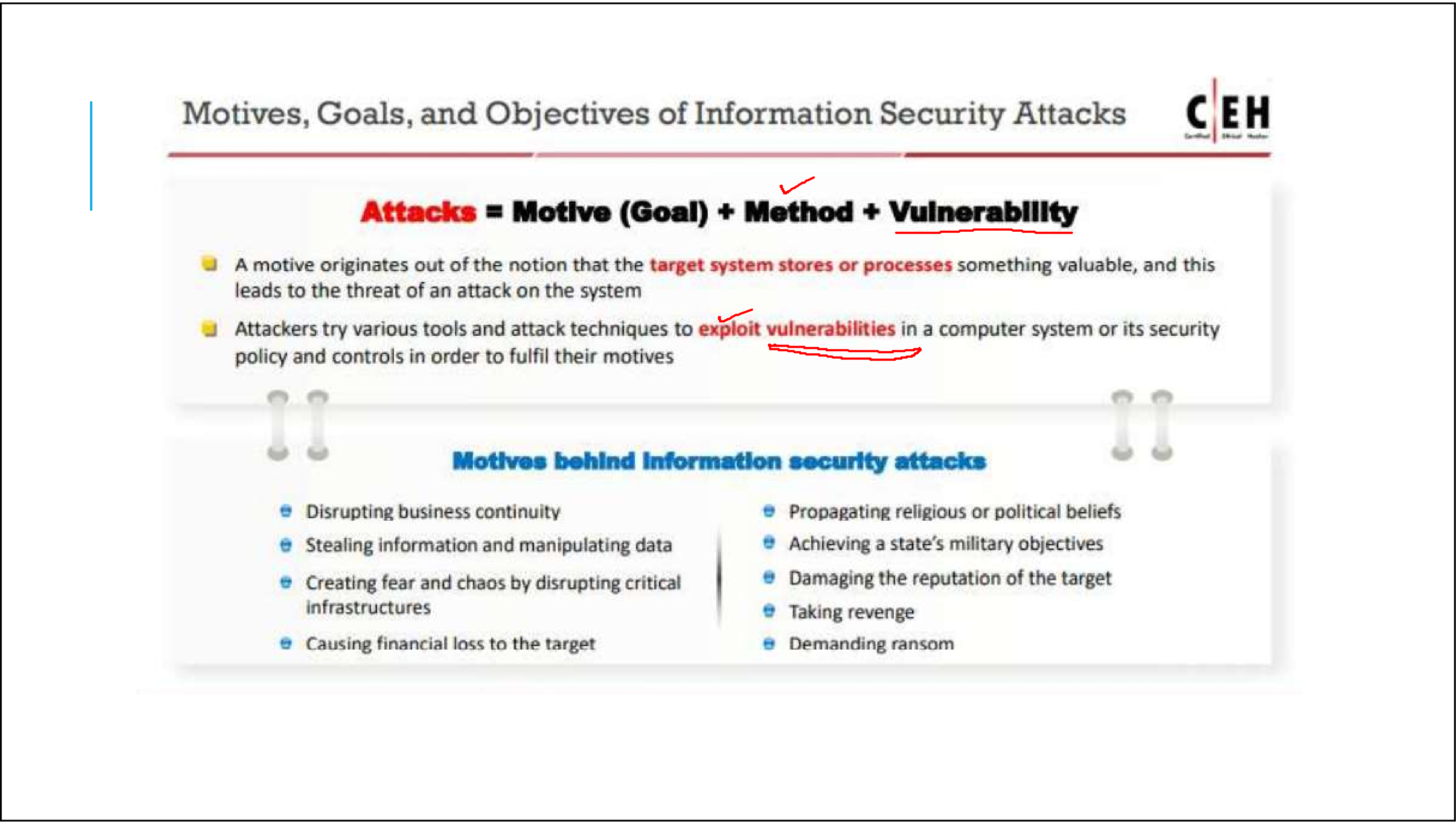
Identify real time application & infer how the elements of information security is implemented.

- Confidentiality
- Integrity
- Availability
- Authenticity
- Non-repudiation.

① in what feature — element is implemented

② how — element is implemented

⊛ we will continue our discussion by 5:05 pm



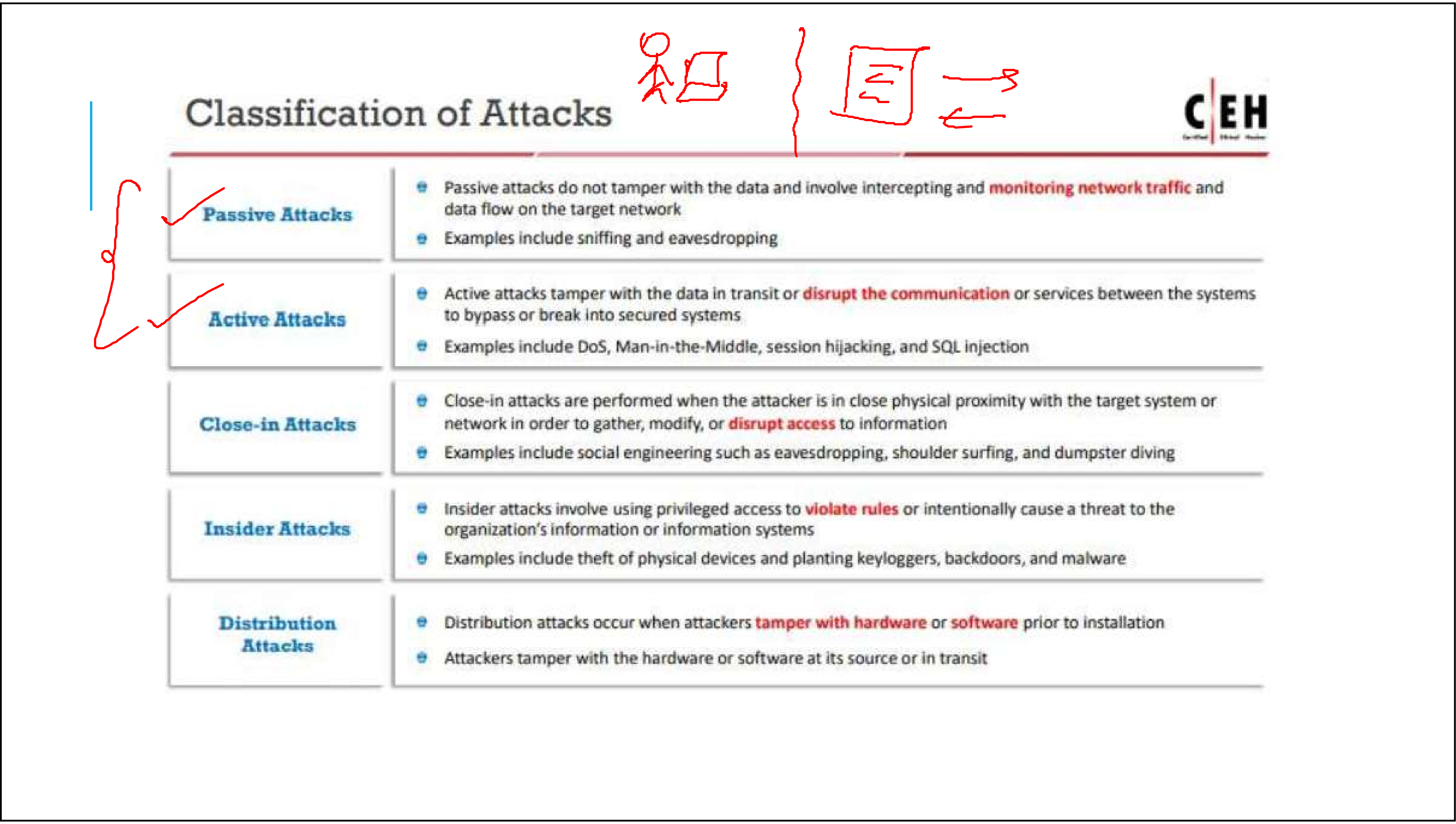
Motives, Goals, and Objectives of Information Security Attacks

Attacks = Motive (Goal) + Method + Vulnerability

- A motive originates out of the notion that the **target system stores or processes** something valuable, and this leads to the threat of an attack on the system
- Attackers try various tools and attack techniques to **exploit vulnerabilities** in a computer system or its security policy and controls in order to fulfil their motives

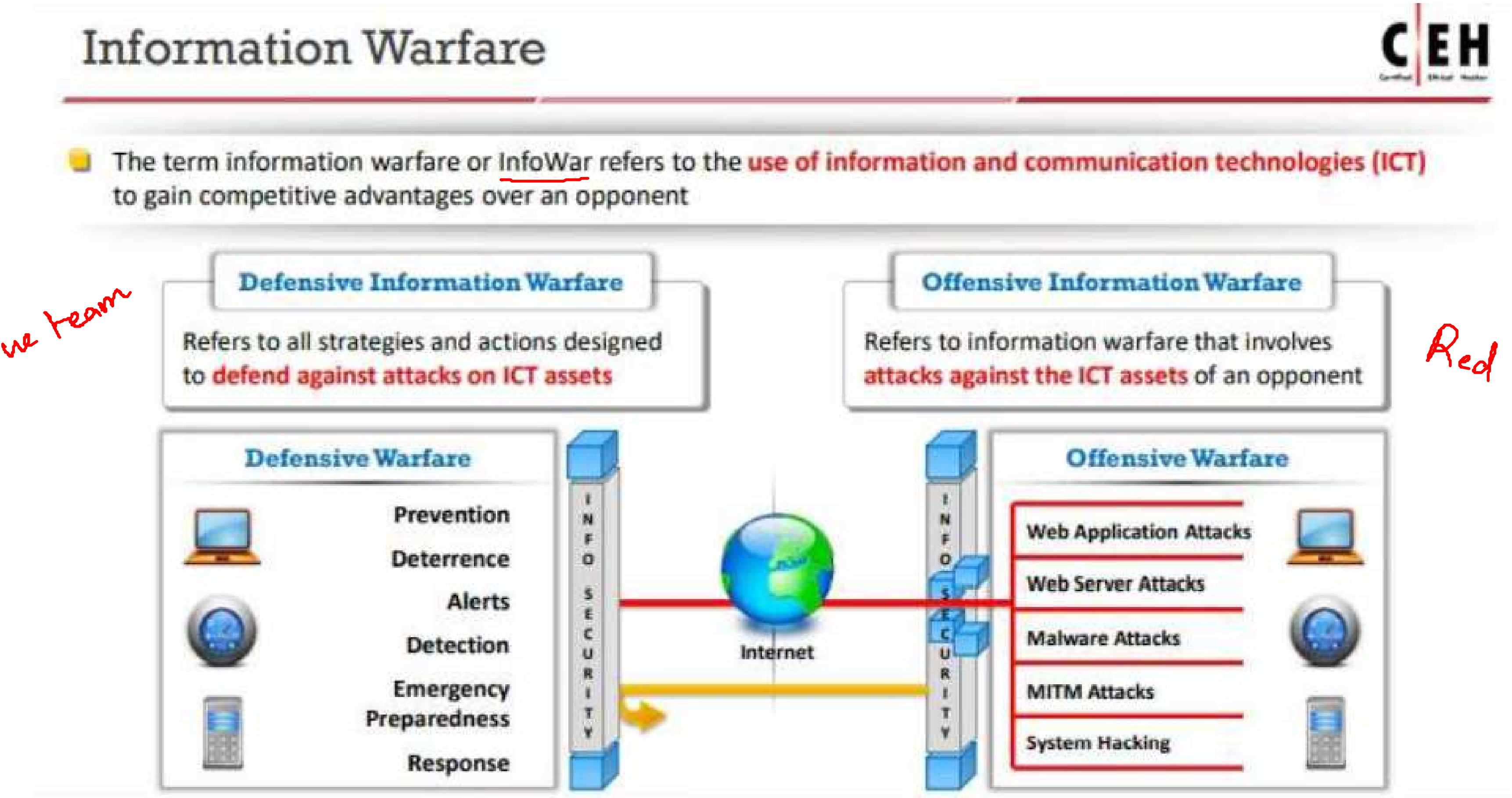
Motives behind information security attacks

- Disrupting business continuity
- Stealing information and manipulating data
- Creating fear and chaos by disrupting critical infrastructures
- Causing financial loss to the target
- Propagating religious or political beliefs
- Achieving a state's military objectives
- Damaging the reputation of the target
- Taking revenge
- Demanding ransom



Classification of Attacks

Passive Attacks	Passive attacks do not tamper with the data and involve intercepting and **monitoring network traffic** and data flow on the target network Examples include sniffing and eavesdropping
Active Attacks	Active attacks tamper with the data in transit or **disrupt the communication** or services between the systems to bypass or break into secured systems Examples include DoS, Man-in-the-Middle, session hijacking, and SQL injection
Close-in Attacks	Close-in attacks are performed when the attacker is in close physical proximity with the target system or network in order to gather, modify, or **disrupt access** to information Examples include social engineering such as eavesdropping, shoulder surfing, and dumpster diving
Insider Attacks	Insider attacks involve using privileged access to **violate rules** or intentionally cause a threat to the organization's information or information systems Examples include theft of physical devices and planting keyloggers, backdoors, and malware
Distribution Attacks	Distribution attacks occur when attackers **tamper with hardware** or **software** prior to installation Attackers tamper with the hardware or software at its source or in transit



Information Warfare

CEH

- The term information warfare or InfoWar refers to the **use of information and communication technologies (ICT)** to gain competitive advantages over an opponent

Blue team

Defensive Information Warfare

Refers to all strategies and actions designed to **defend against attacks on ICT assets**

Offensive Information Warfare

Refers to information warfare that involves **attacks against the ICT assets** of an opponent

Red team

Defensive Warfare

- Prevention
- Deterrence
- Alerts
- Detection
- Emergency Preparedness
- Response

Offensive Warfare

- Web Application Attacks
- Web Server Attacks
- Malware Attacks
- MITM Attacks
- System Hacking

Module Flow

1 Information Security Overview

2 Cyber Kill Chain Concepts

3 Hacking Concepts

4 Ethical Hacking Concepts

5 Information Security Controls

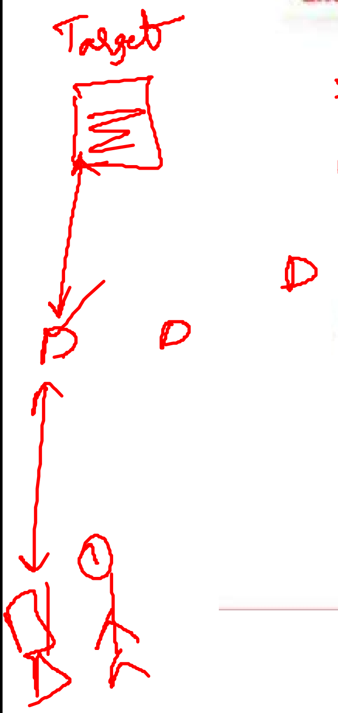
6 Information Security Laws and Standards

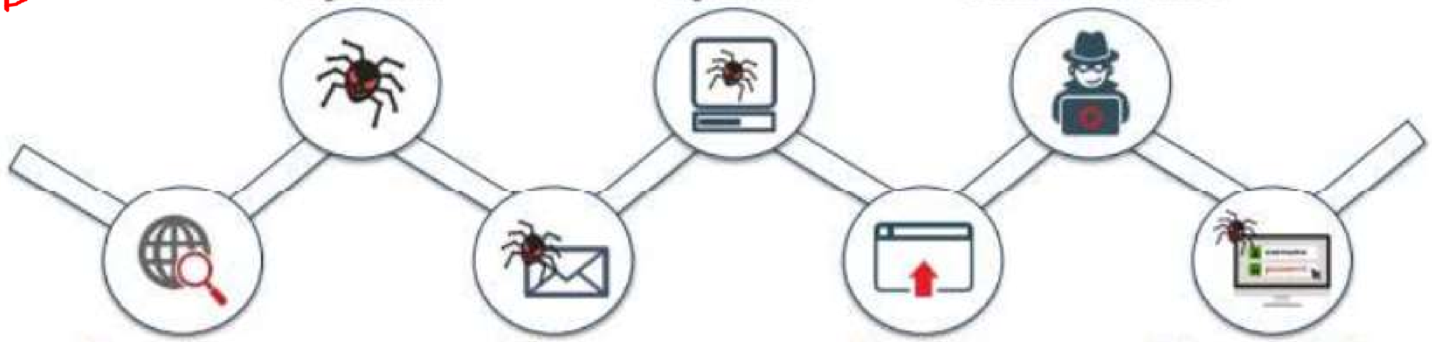
Zero day attack

Cyber Kill Chain Methodology

C|EH

- The cyber kill chain methodology is a component of intelligence-driven defense for the identification and **prevention of malicious intrusion activities**
- It provides greater insight into attack phases, which helps security professionals to understand the **adversary's tactics, techniques, and procedures beforehand**





Reconnaissance
Gather data on the target to probe for weak points

Weaponization
Create a deliverable malicious payload using an exploit and a backdoor

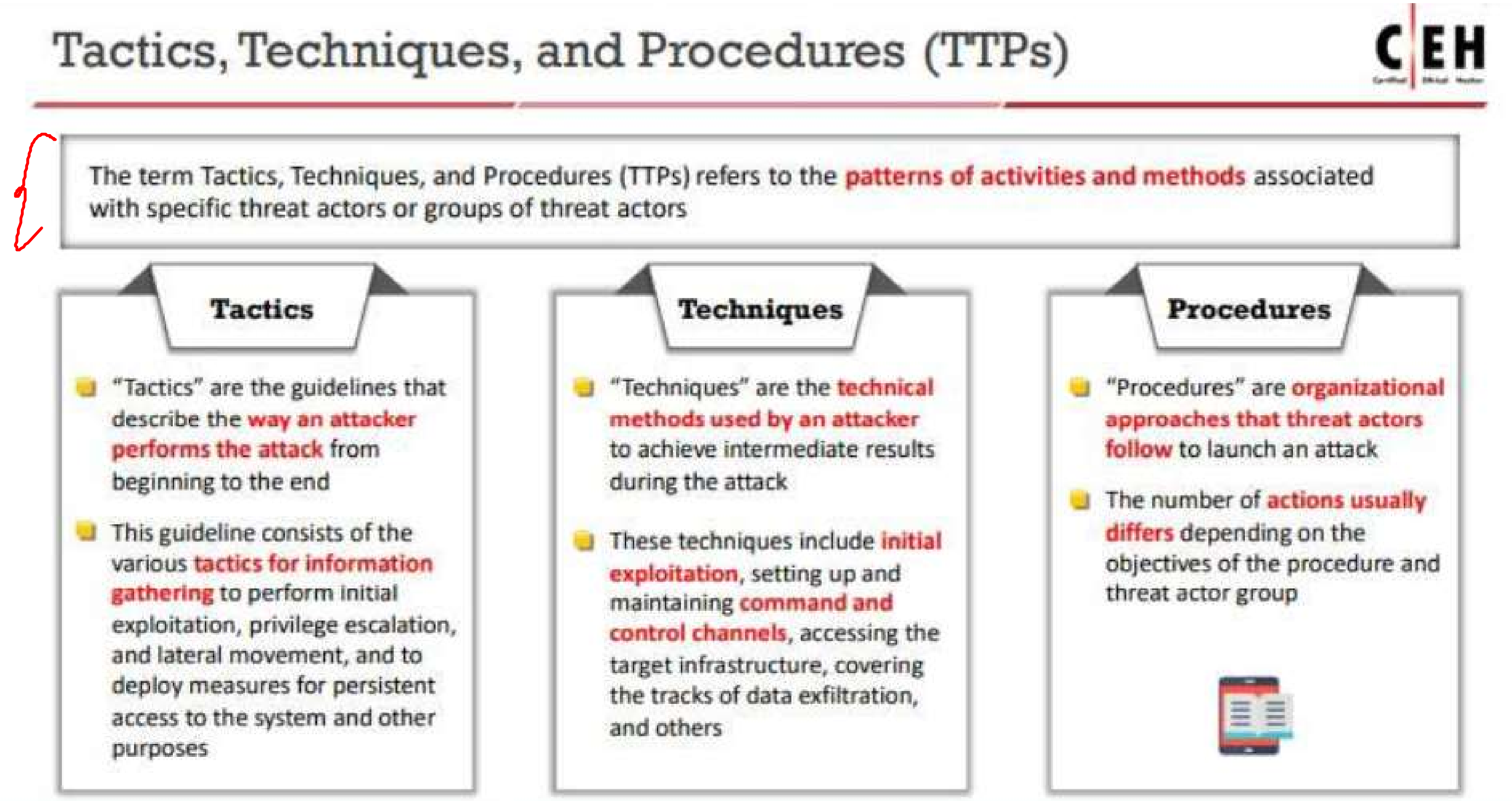
Delivery
Send weaponized bundle to the victim using email, USB, etc.

Exploitation
Exploit a vulnerability by executing code on the victim's system

Installation
Install malware on the target system

Command and Control
Create a command and control channel to communicate and pass data back and forth

Actions on Objectives
Perform actions to achieve intended objectives/goals



Tactics, Techniques, and Procedures (TTPs)

C|EH

The term Tactics, Techniques, and Procedures (TTPs) refers to the **patterns of activities and methods** associated with specific threat actors or groups of threat actors

Tactics

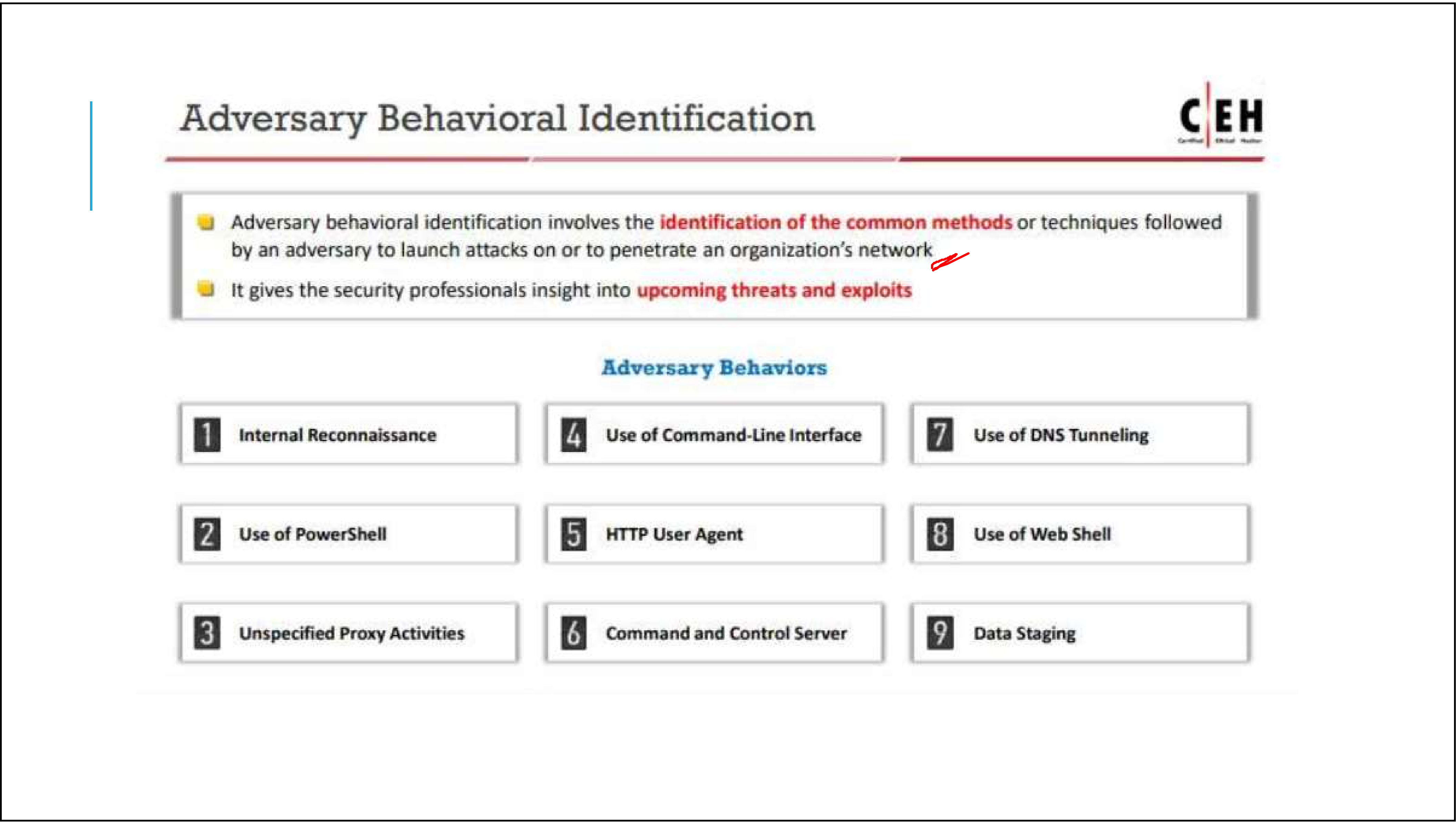
- "Tactics" are the guidelines that describe the **way an attacker performs the attack** from beginning to the end
- This guideline consists of the various **tactics for information gathering** to perform initial exploitation, privilege escalation, and lateral movement, and to deploy measures for persistent access to the system and other purposes

Techniques

- "Techniques" are the **technical methods used by an attacker** to achieve intermediate results during the attack
- These techniques include **initial exploitation**, setting up and maintaining **command and control channels**, accessing the target infrastructure, covering the tracks of data exfiltration, and others

Procedures

- "Procedures" are **organizational approaches that threat actors follow** to launch an attack
- The number of **actions usually differs** depending on the objectives of the procedure and threat actor group



Adversary Behavioral Identification

C|EH

- Adversary behavioral identification involves the **identification of the common methods** or techniques followed by an adversary to launch attacks on or to penetrate an organization's network
- It gives the security professionals insight into **upcoming threats and exploits**

Adversary Behaviors

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 Web Shell**

9 **Data Staging**

Indicators of Compromise (IoCs)

- Indicators of Compromise (IoCs) are the **clues**, **artifacts**, and **pieces of forensic data** found on the network or operating system of an organization that indicate a potential intrusion or malicious activity in the organization's infrastructure

- IoCs are not intelligence, although they do **act as a good source of information** regarding the threats that serve as data points in the intelligence process

- Security professionals need to **perform continuous monitoring** of IoCs to effectively and efficiently detect and **respond to evolving cyber threats**

Categories of Indicators of Compromise

- Understanding IoCs helps security professionals to **quickly detect the threats** against the organization and protect the organization from evolving threats

For this purpose, IoCs are divided into four categories:

Email Indicators

- Email indicators are used to send malicious data to the target organization or individual
- Examples include the sender's email address, email subject, and attachments or links

Network Indicators

- Network indicators are useful for command and control, malware delivery, identifying the operating system, and other tasks
- Examples include URLs, domain names, and IP addresses

Host-Based Indicators

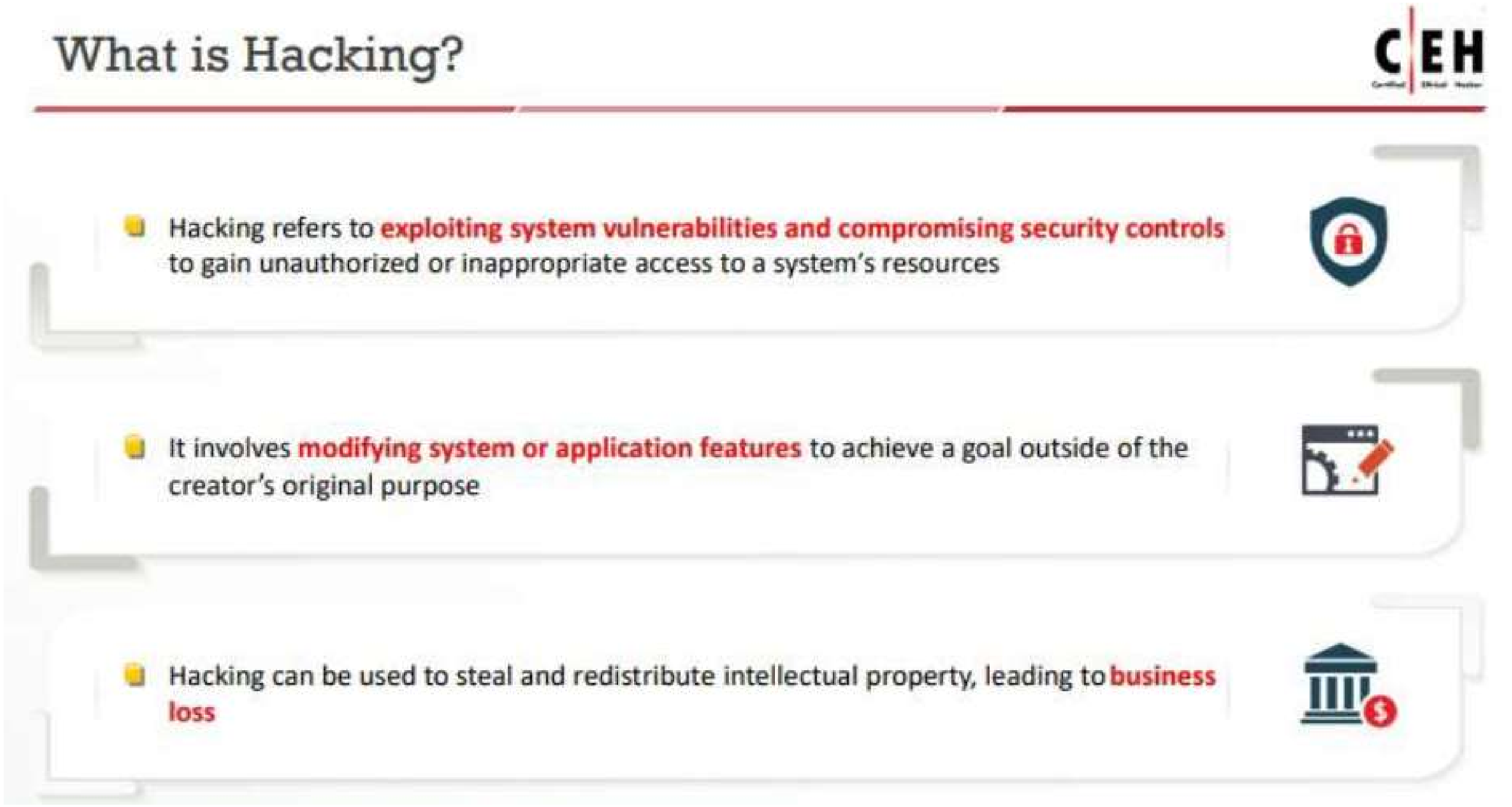
- Host-based indicators are found by performing an analysis of the infected system within the organizational network
- Examples include filenames, file hashes, registry keys, DLLs, and mutex

Behavioral Indicators

- Behavioral indicators of compromise are used to identify specific behavior related to malicious activities
- Examples of behavioral indicators include document executing PowerShell script, and remote command execution

Module Flow

1. Information Security Overview
2. Cyber Kill Chain Concepts
3. Hacking Concepts
4. Ethical Hacking Concepts
5. Information Security Controls
6. Information Security Laws and Standards

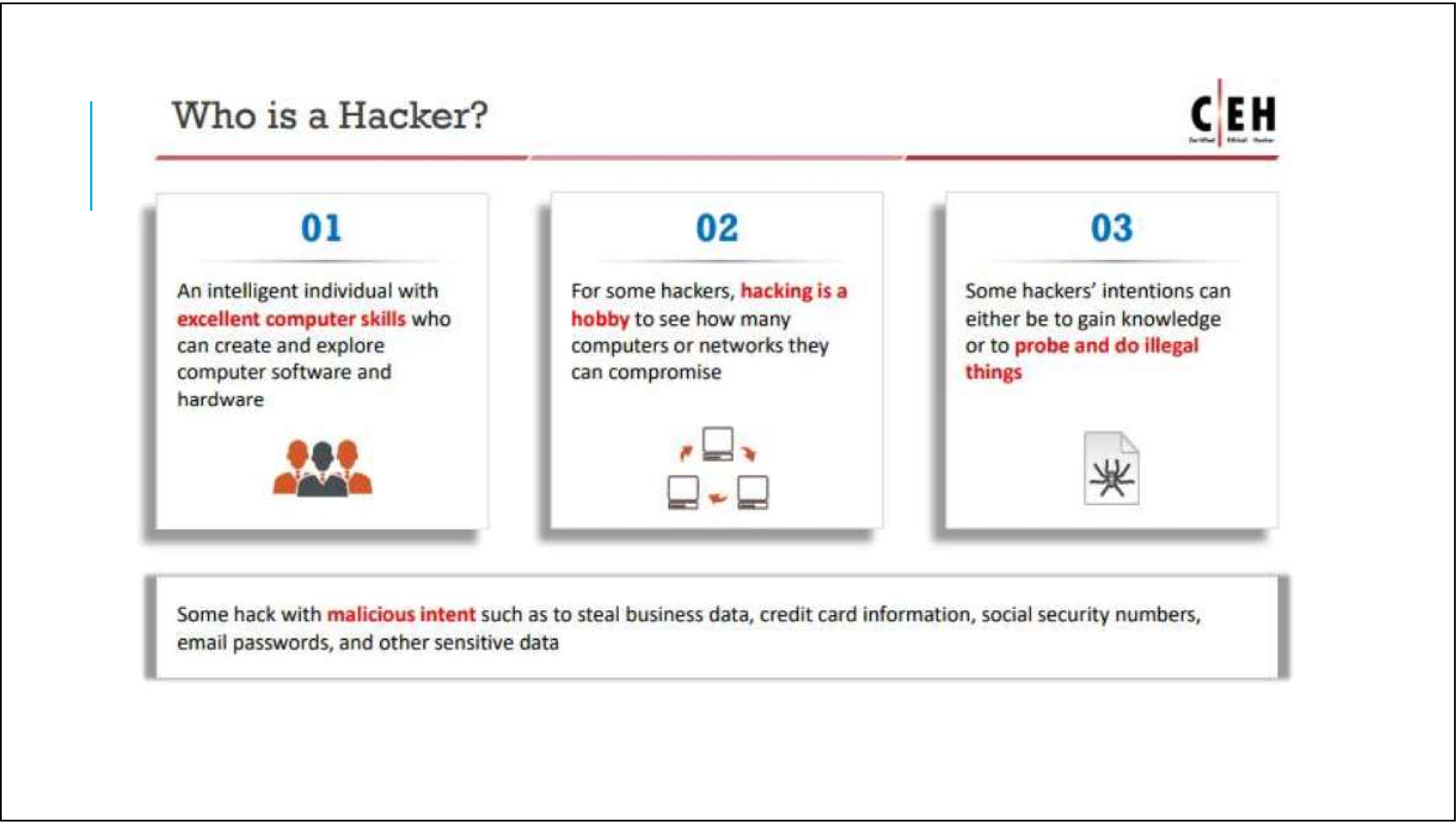


What is Hacking?

- Hacking refers to **exploiting system vulnerabilities and compromising security controls** to gain unauthorized or inappropriate access to a system's resources

- It involves **modifying system or application features** to achieve a goal outside of the creator's original purpose

- Hacking can be used to steal and redistribute intellectual property, leading to **business loss**



Who is a Hacker?

01

An intelligent individual with **excellent computer skills** who can create and explore computer software and hardware

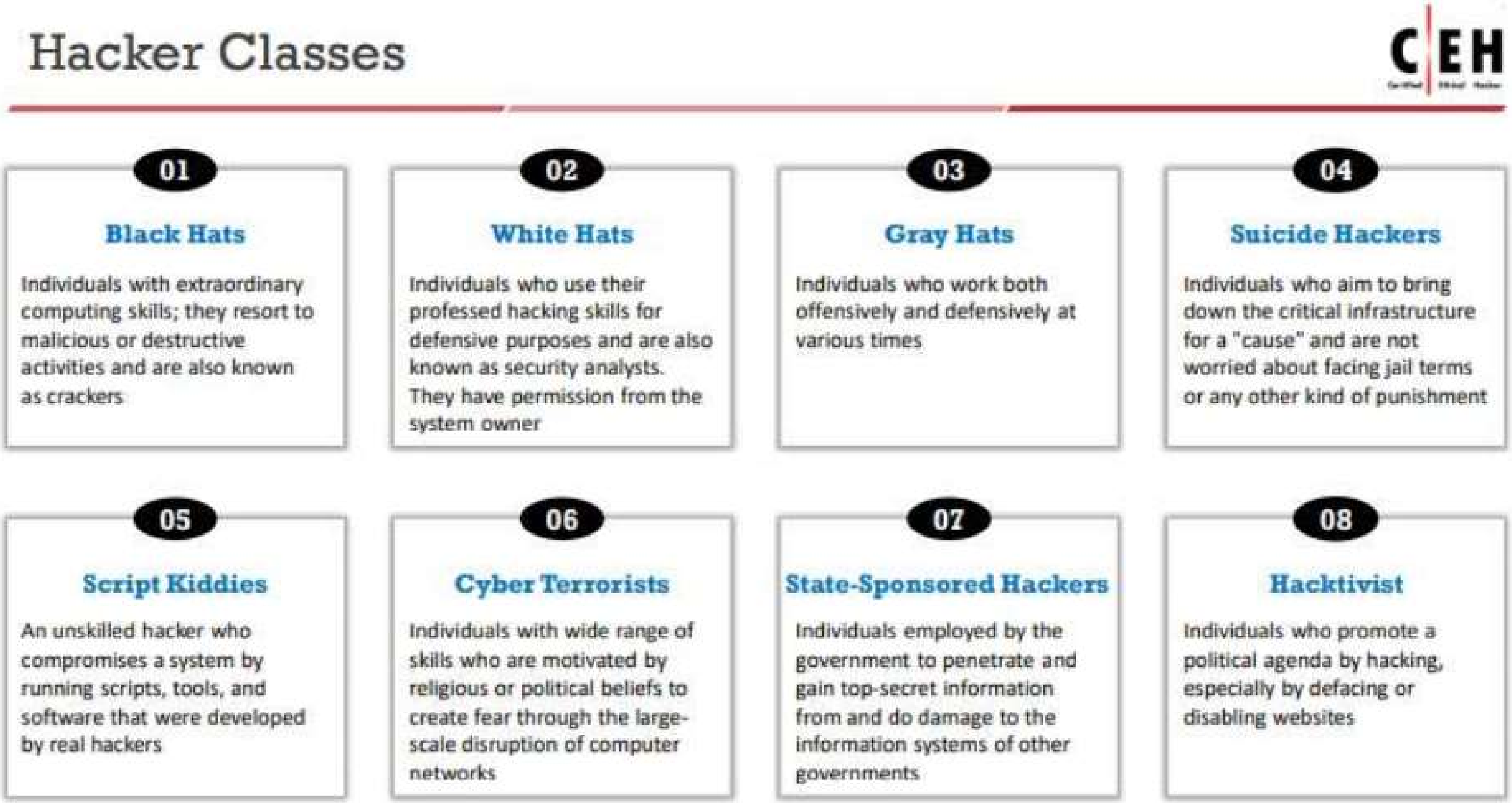
02

For some hackers, **hacking is a hobby** to see how many computers or networks they can compromise

03

Some hackers' intentions can either be to gain knowledge or to **probe and do illegal things**

Some hack with **malicious intent** such as to steal business data, credit card information, social security numbers, email passwords, and other sensitive data



Hacker Classes

01

Black Hats

Individuals with extraordinary computing skills; they resort to malicious or destructive activities and are also known as crackers

02

White Hats

Individuals who use their professed hacking skills for defensive purposes and are also known as security analysts. They have permission from the system owner

03

Gray Hats

Individuals who work both offensively and defensively at various times

04

Suicide Hackers

Individuals who aim to bring down the critical infrastructure for a "cause" and are not worried about facing jail terms or any other kind of punishment

05

Script Kiddies

An unskilled hacker who compromises a system by running scripts, tools, and software that were developed by real hackers

06

Cyber Terrorists

Individuals with wide range of skills who are motivated by religious or political beliefs to create fear through the large-scale disruption of computer networks

07

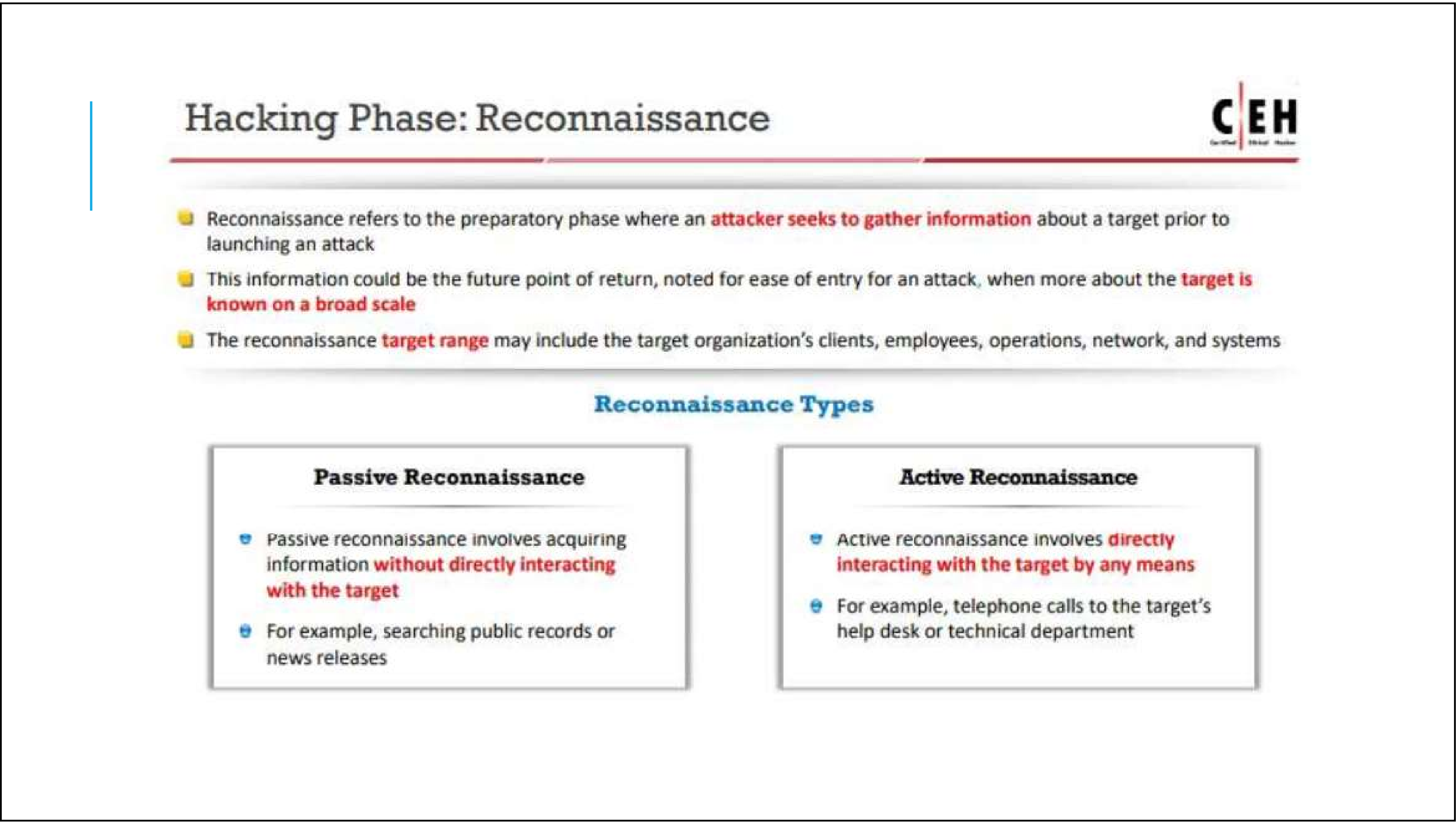
State-Sponsored Hackers

Individuals employed by the government to penetrate and gain top-secret information from and do damage to the information systems of other governments

08

Hacktivist

Individuals who promote a political agenda by hacking, especially by defacing or disabling websites



Hacking Phase: Reconnaissance

- Reconnaissance refers to the preparatory phase where an **attacker seeks to gather information** about a target prior to launching an attack
- This information could be the future point of return, noted for ease of entry for an attack, when more about the **target is known on a broad scale**
- The reconnaissance **target range** may include the target organization's clients, employees, operations, network, and systems

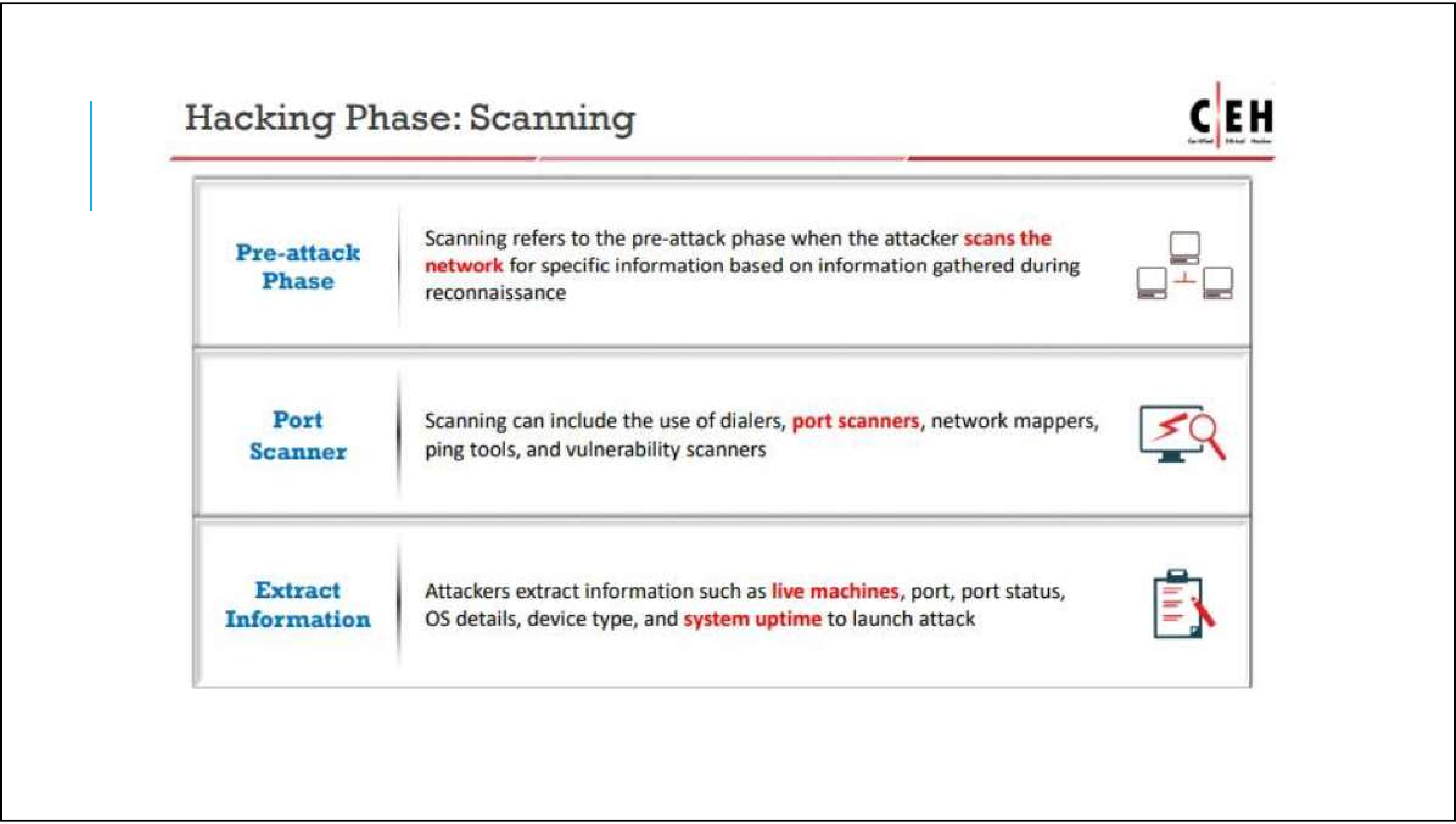
Reconnaissance Types

Passive Reconnaissance

- Passive reconnaissance involves acquiring information **without directly interacting with the target**
- For example, searching public records or news releases

Active Reconnaissance

- Active reconnaissance involves **directly interacting with the target by any means**
- For example, telephone calls to the target's help desk or technical department



Hacking Phase: Scanning

Pre-attack Phase

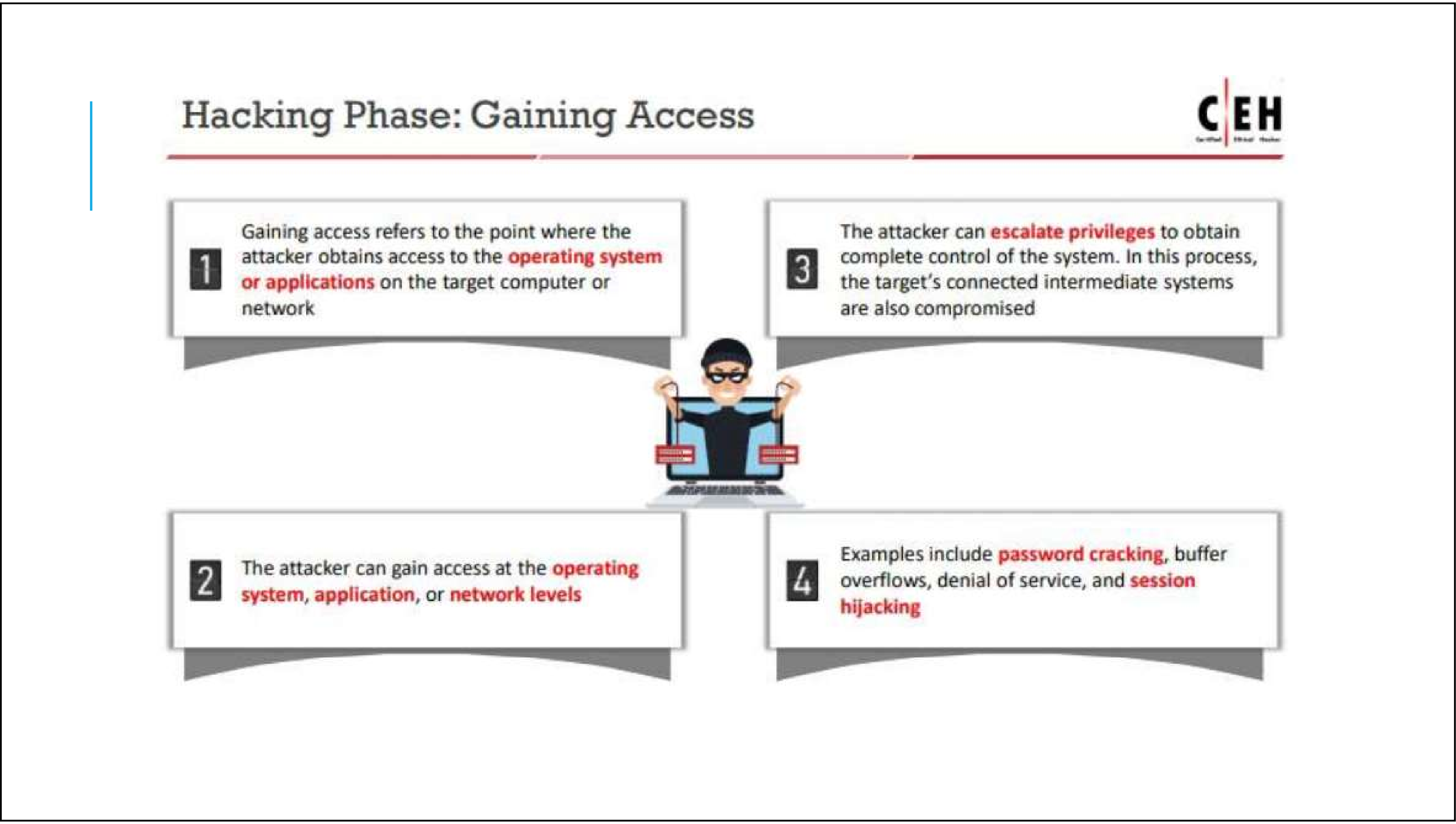
Scanning refers to the pre-attack phase when the attacker **scans the network** for specific information based on information gathered during reconnaissance

Port Scanner

Scanning can include the use of dialers, **port scanners**, network mappers, ping tools, and vulnerability scanners

Extract Information

Attackers extract information such as **live machines**, port, port status, OS details, device type, and **system uptime** to launch attack



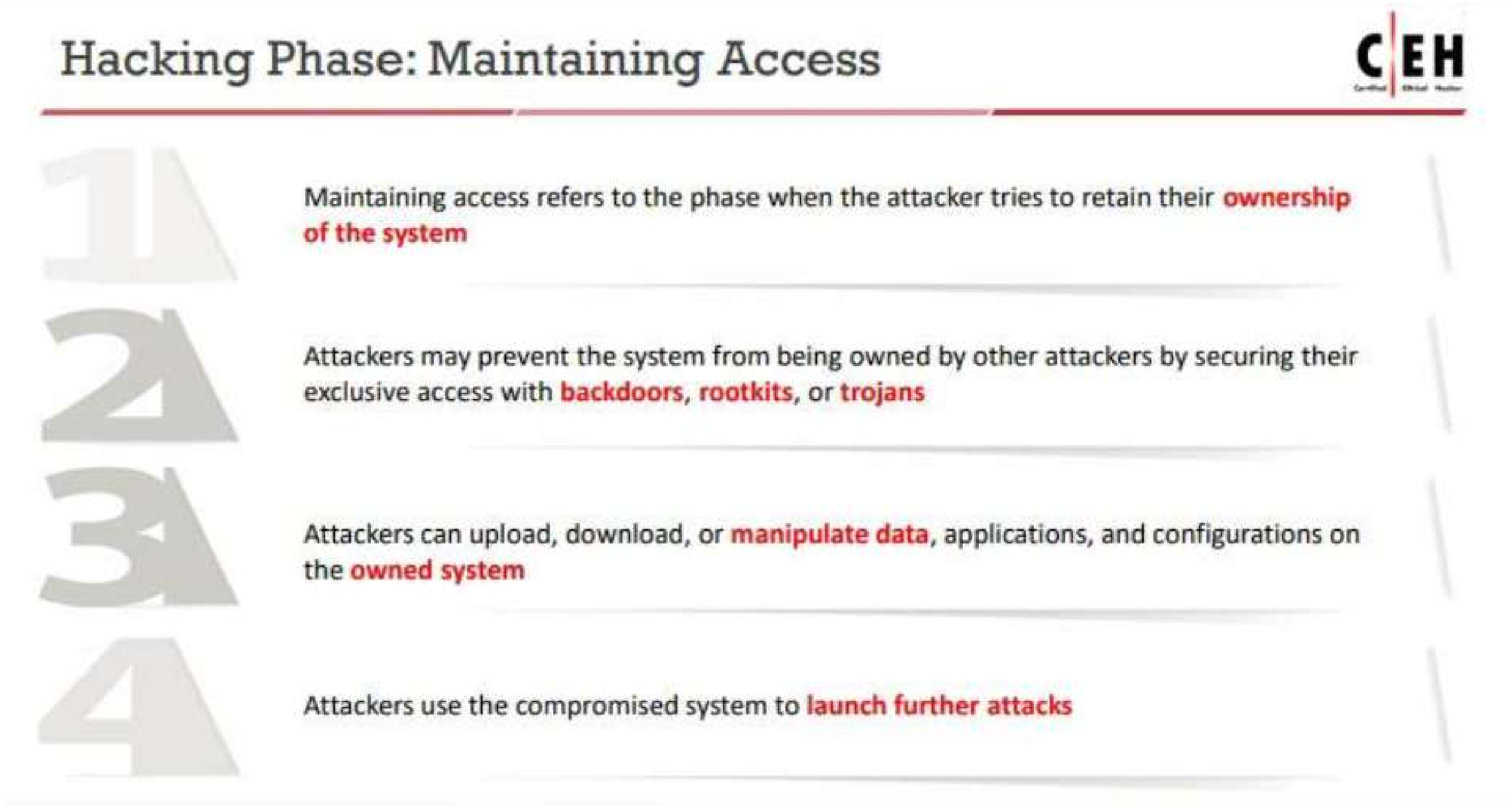
Hacking Phase: Gaining Access

1 Gaining access refers to the point where the attacker obtains access to the **operating system or applications** on the target computer or network

2 The attacker can gain access at the **operating system**, **application**, or **network levels**

3 The attacker can **escalate privileges** to obtain complete control of the system. In this process, the target's connected intermediate systems are also compromised

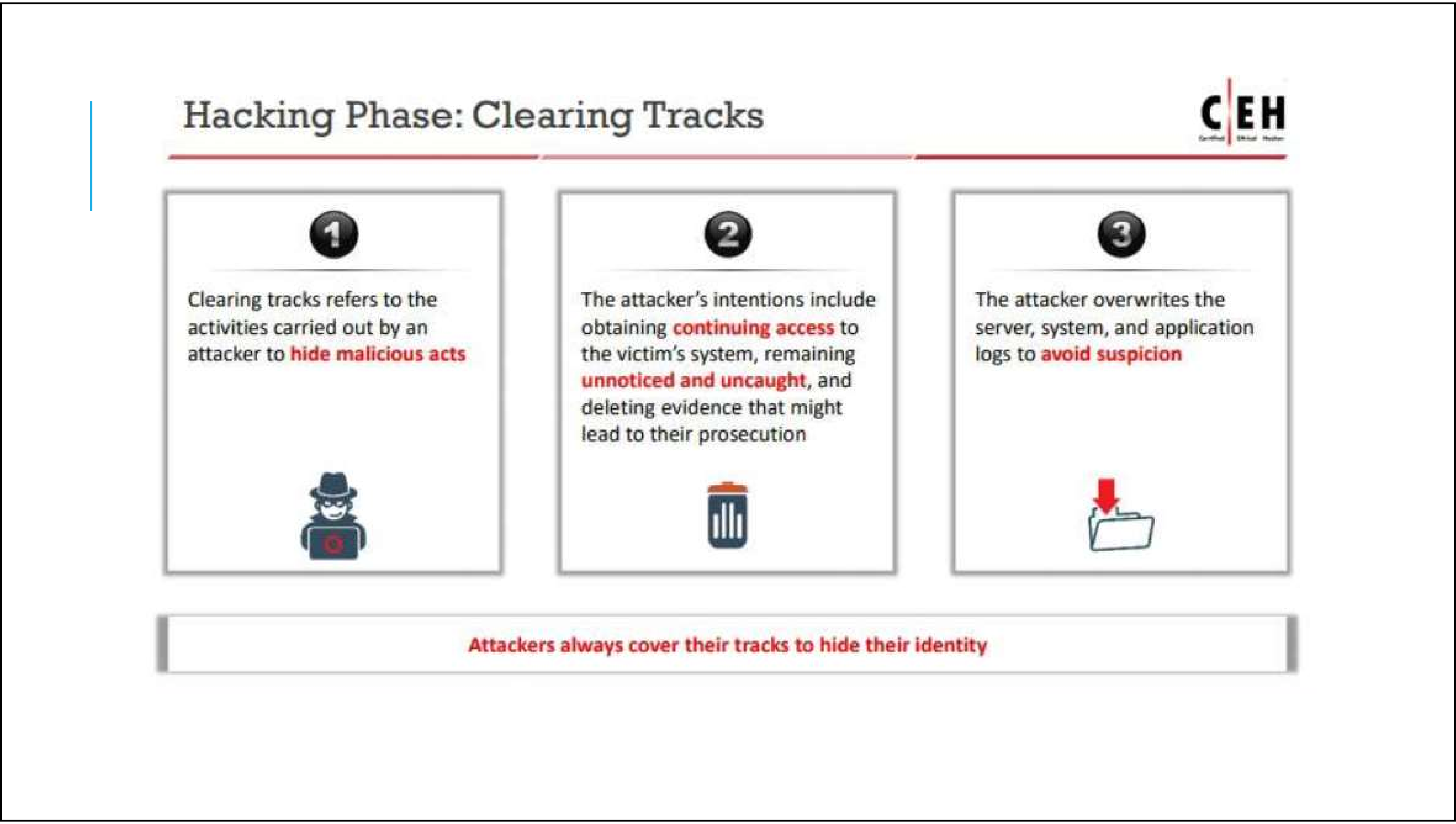
4 Examples include **password cracking**, buffer overflows, denial of service, and **session hijacking**



Hacking Phase: Maintaining Access

C|EH

1. Maintaining access refers to the phase when the attacker tries to retain their **ownership of the system**
2. Attackers may prevent the system from being owned by other attackers by securing their exclusive access with **backdoors**, **rootkits**, or **trojans**
3. Attackers can upload, download, or **manipulate data**, applications, and configurations on the **owned system**
4. Attackers use the compromised system to **launch further attacks**



Hacking Phase: Clearing Tracks

1. Clearing tracks refers to the activities carried out by an attacker to **hide malicious acts**

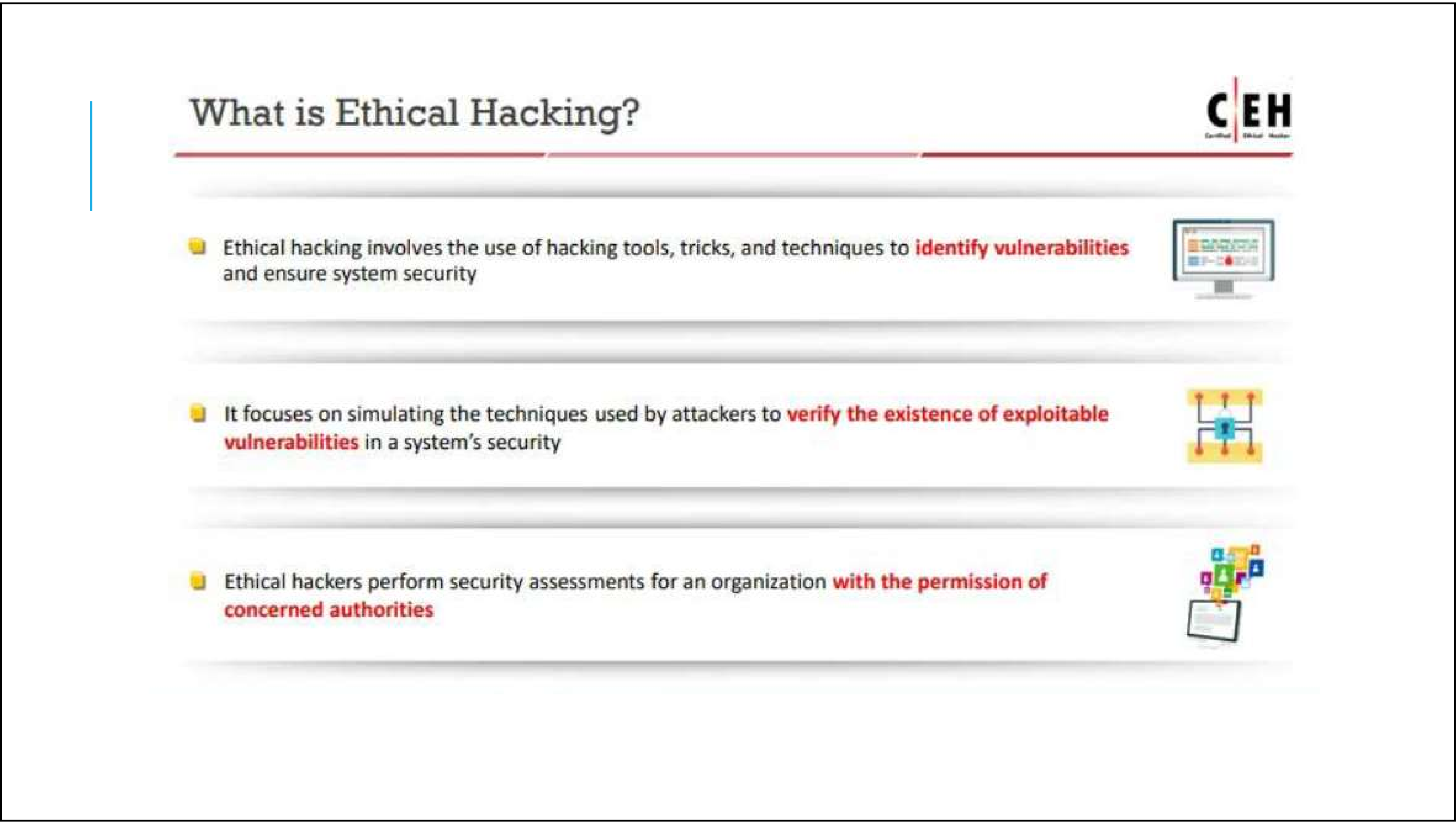
2. The attacker's intentions include obtaining **continuing access** to the victim's system, remaining **unnoticed and uncaught**, and deleting evidence that might lead to their prosecution

3. The attacker overwrites the server, system, and application logs to **avoid suspicion**

Attackers always cover their tracks to hide their identity

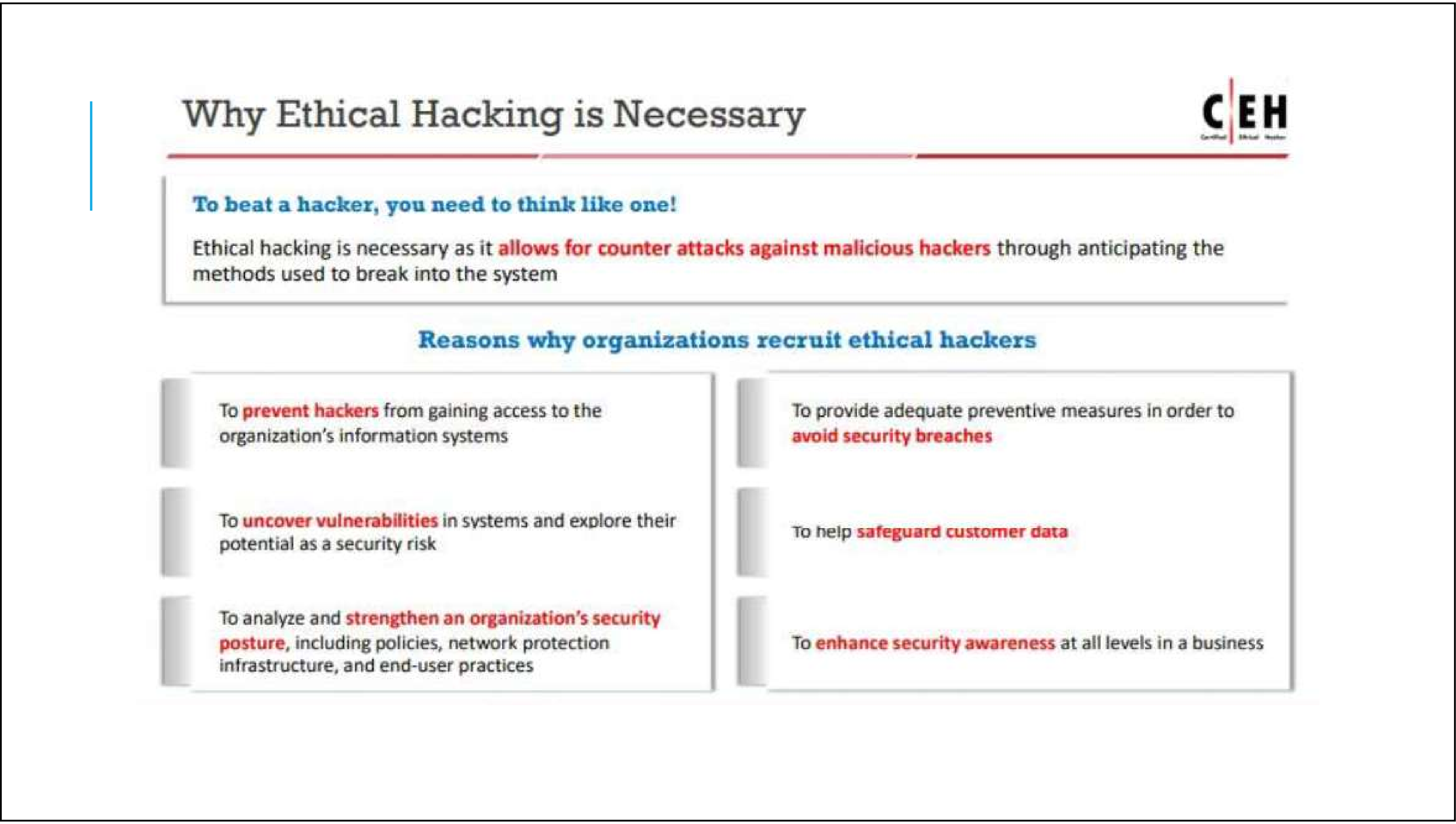
Module Flow

1. Information Security Overview
2. Cyber Kill Chain Concepts
3. Hacking Concepts
4. Ethical Hacking Concepts
5. Information Security Controls
6. Information Security Laws and Standards



What is Ethical Hacking?

- Ethical hacking involves the use of hacking tools, tricks, and techniques to **identify vulnerabilities** and ensure system security
- It focuses on simulating the techniques used by attackers to **verify the existence of exploitable vulnerabilities** in a system's security
- Ethical hackers perform security assessments for an organization **with the permission of concerned authorities**



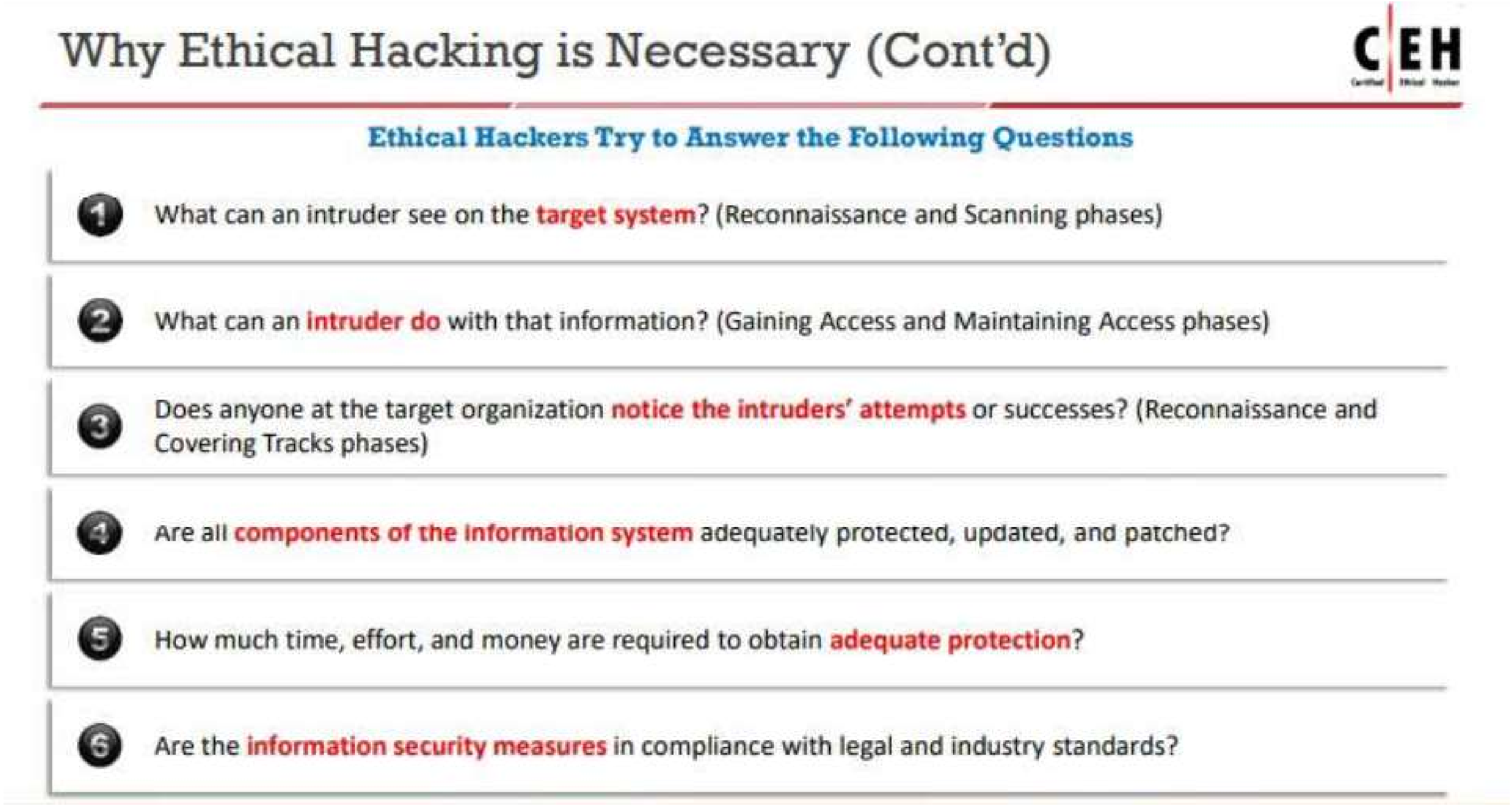
Why Ethical Hacking is Necessary

To beat a hacker, you need to think like one!

Ethical hacking is necessary as it **allows for counter attacks against malicious hackers** through anticipating the methods used to break into the system

Reasons why organizations recruit ethical hackers

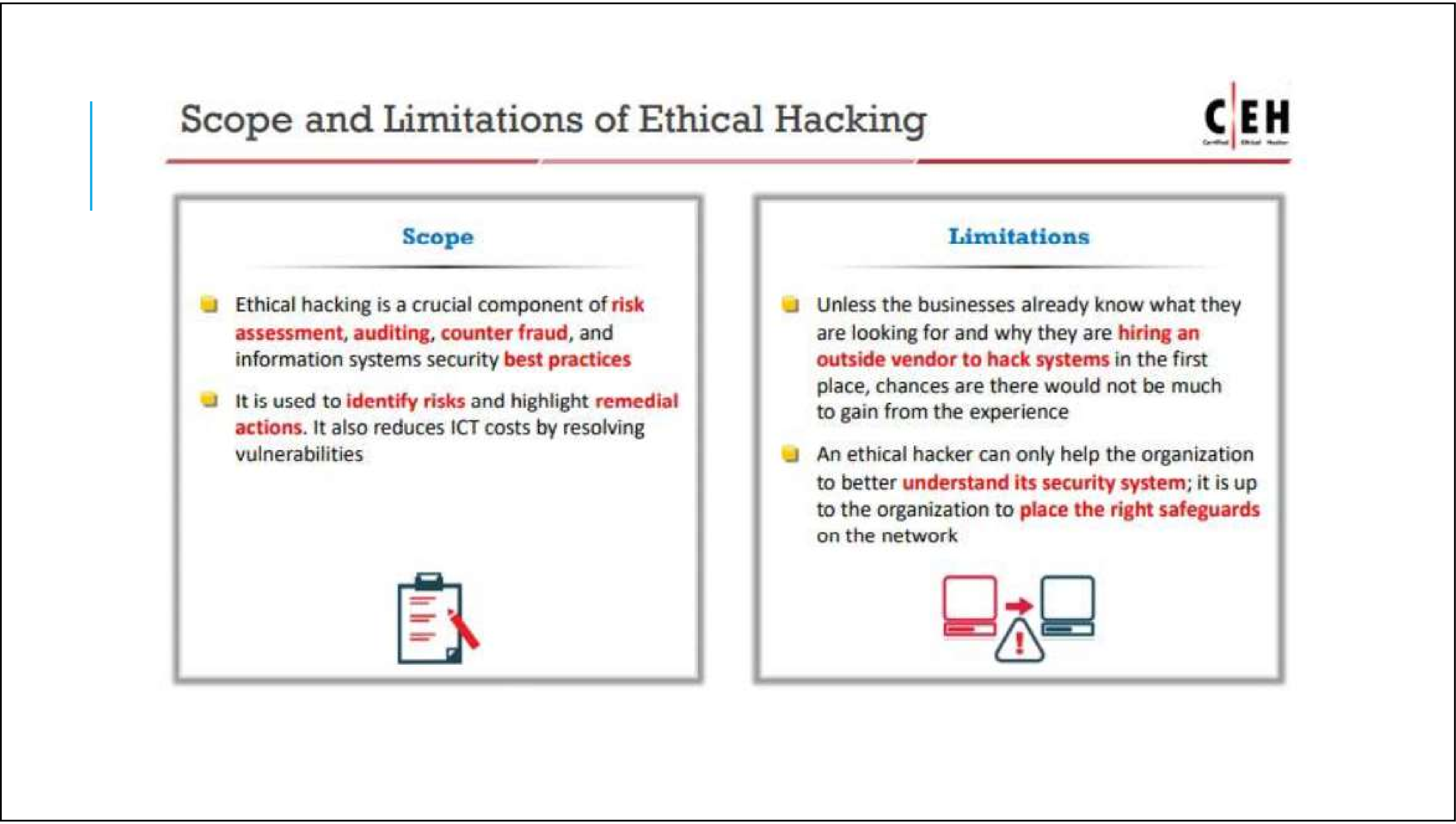
- To **prevent hackers** from gaining access to the organization's information systems
- To **uncover vulnerabilities** in systems and explore their potential as a security risk
- To analyze and **strengthen an organization's security posture**, including policies, network protection infrastructure, and end-user practices
- To provide adequate preventive measures in order to **avoid security breaches**
- To help **safeguard customer data**
- To **enhance security awareness** at all levels in a business



Why Ethical Hacking is Necessary (Cont'd)

Ethical Hackers Try to Answer the Following Questions

1. What can an intruder see on the **target system**? (Reconnaissance and Scanning phases)
2. What can an **intruder do** with that information? (Gaining Access and Maintaining Access phases)
3. Does anyone at the target organization **notice the intruders' attempts** or successes? (Reconnaissance and Covering Tracks phases)
4. Are all **components of the information system** adequately protected, updated, and patched?
5. How much time, effort, and money are required to obtain **adequate protection**?
6. Are the **information security measures** in compliance with legal and industry standards?



Scope and Limitations of Ethical Hacking

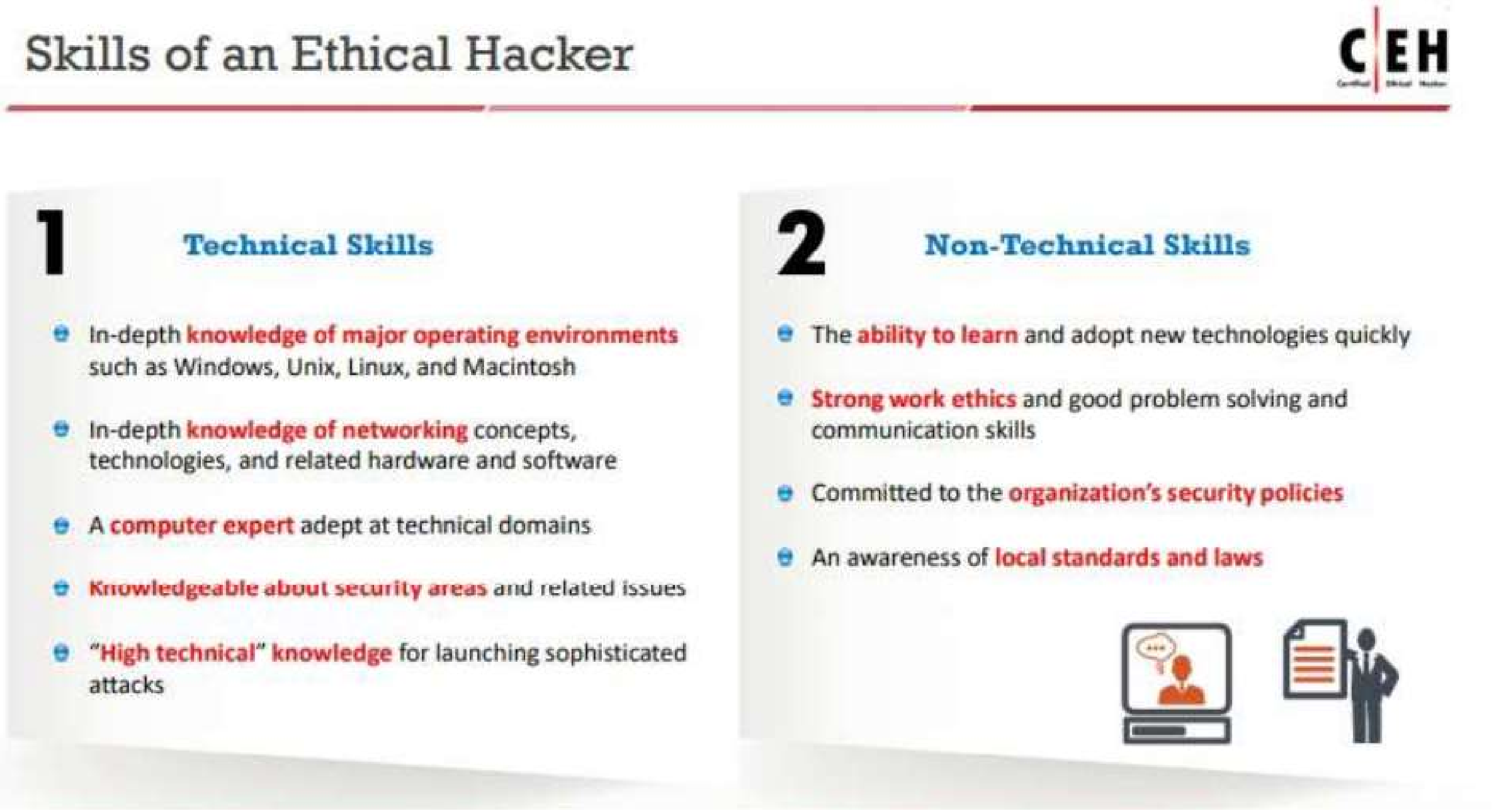
CEH
Certified Ethical Hacker

Scope

- Ethical hacking is a crucial component of **risk assessment**, **auditing**, **counter fraud**, and information systems security **best practices**
- It is used to **identify risks** and highlight **remedial actions**. It also reduces ICT costs by resolving vulnerabilities

Limitations

- Unless the businesses already know what they are looking for and why they are **hiring an outside vendor to hack systems** in the first place, chances are there would not be much to gain from the experience
- An ethical hacker can only help the organization to better **understand its security system**; it is up to the organization to **place the right safeguards** on the network



Skills of an Ethical Hacker

C|EH

1 Technical Skills

- In-depth **knowledge of major operating environments** such as Windows, Unix, Linux, and Macintosh
- In-depth **knowledge of networking** concepts, technologies, and related hardware and software
- A **computer expert** adept at technical domains
- **Knowledgeable about security areas** and related issues
- **"High technical" knowledge** for launching sophisticated attacks

2 Non-Technical Skills

- The **ability to learn** and adopt new technologies quickly
- **Strong work ethics** and good problem solving and communication skills
- Committed to the **organization's security policies**
- An awareness of **local standards and laws**

In class activity :

Identify hacking events of real time application.

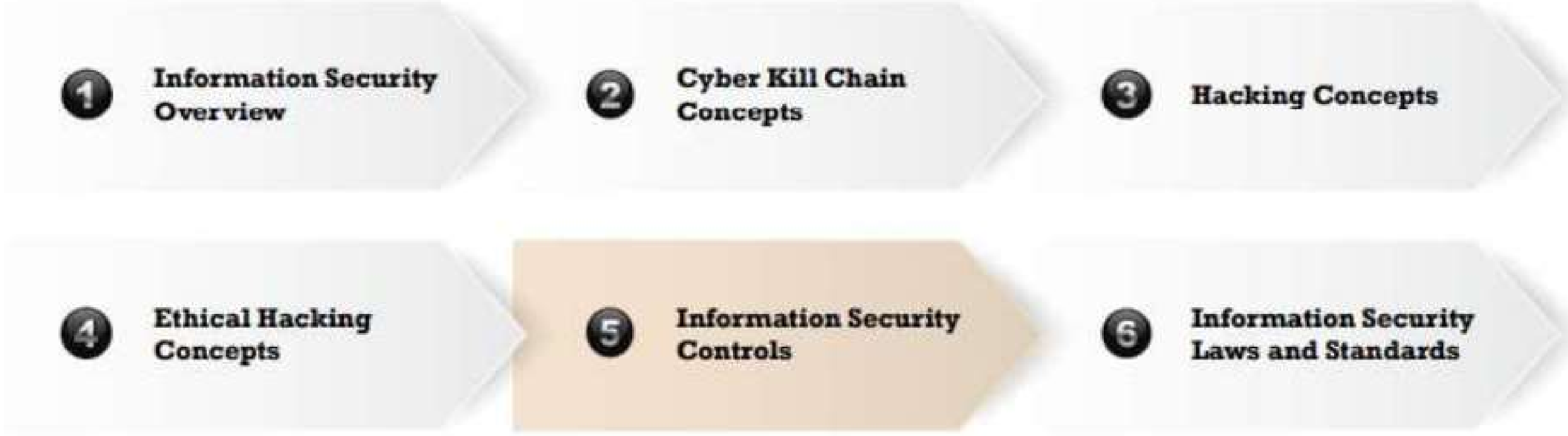
-'2' hacking events

- What hacking?
- How hacking?
- what loss?

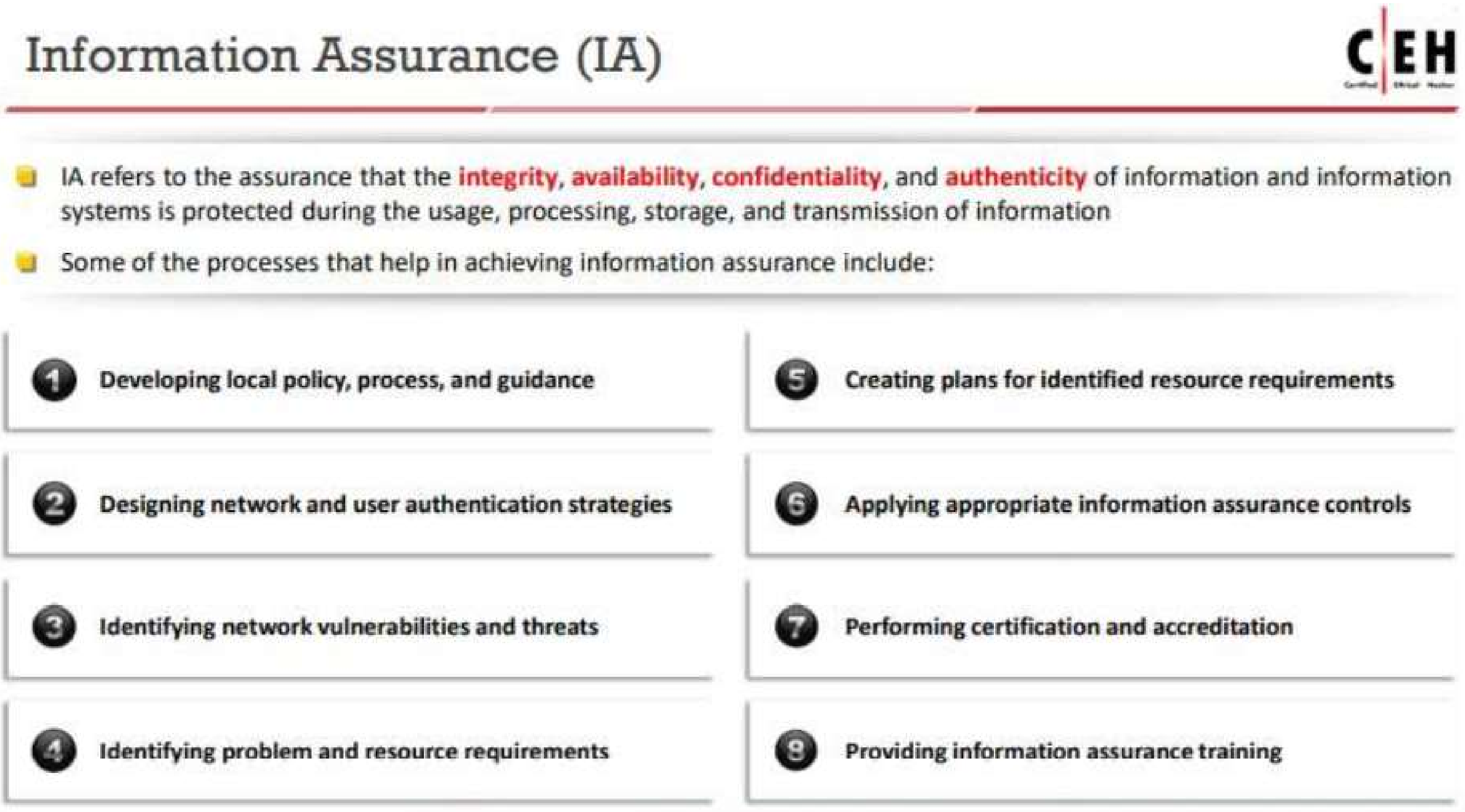
Again we will discuss

by 5.45pm

Module Flow



1. Information Security Overview
2. Cyber Kill Chain Concepts
3. Hacking Concepts
4. Ethical Hacking Concepts
5. Information Security Controls
6. Information Security Laws and Standards



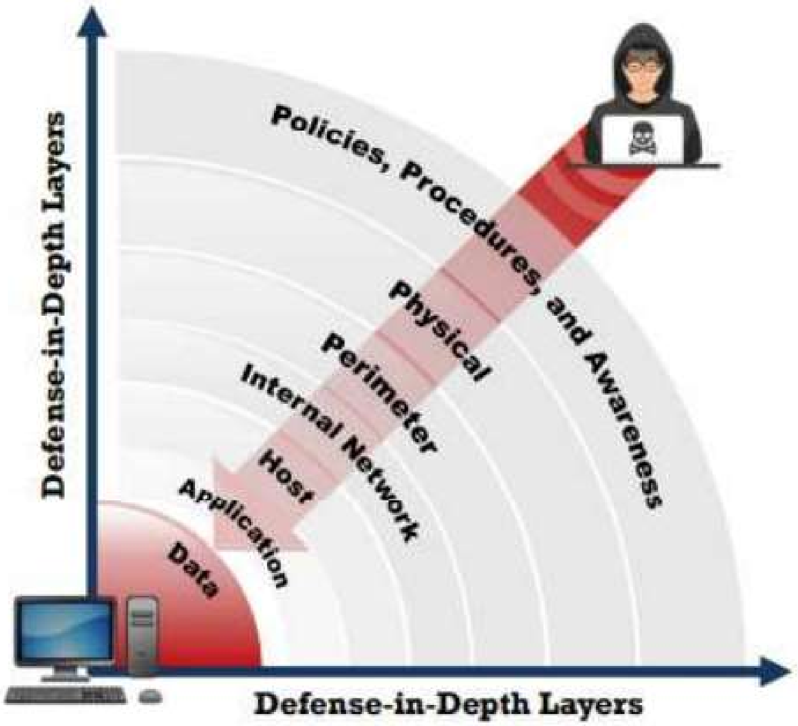
Information Assurance (IA)

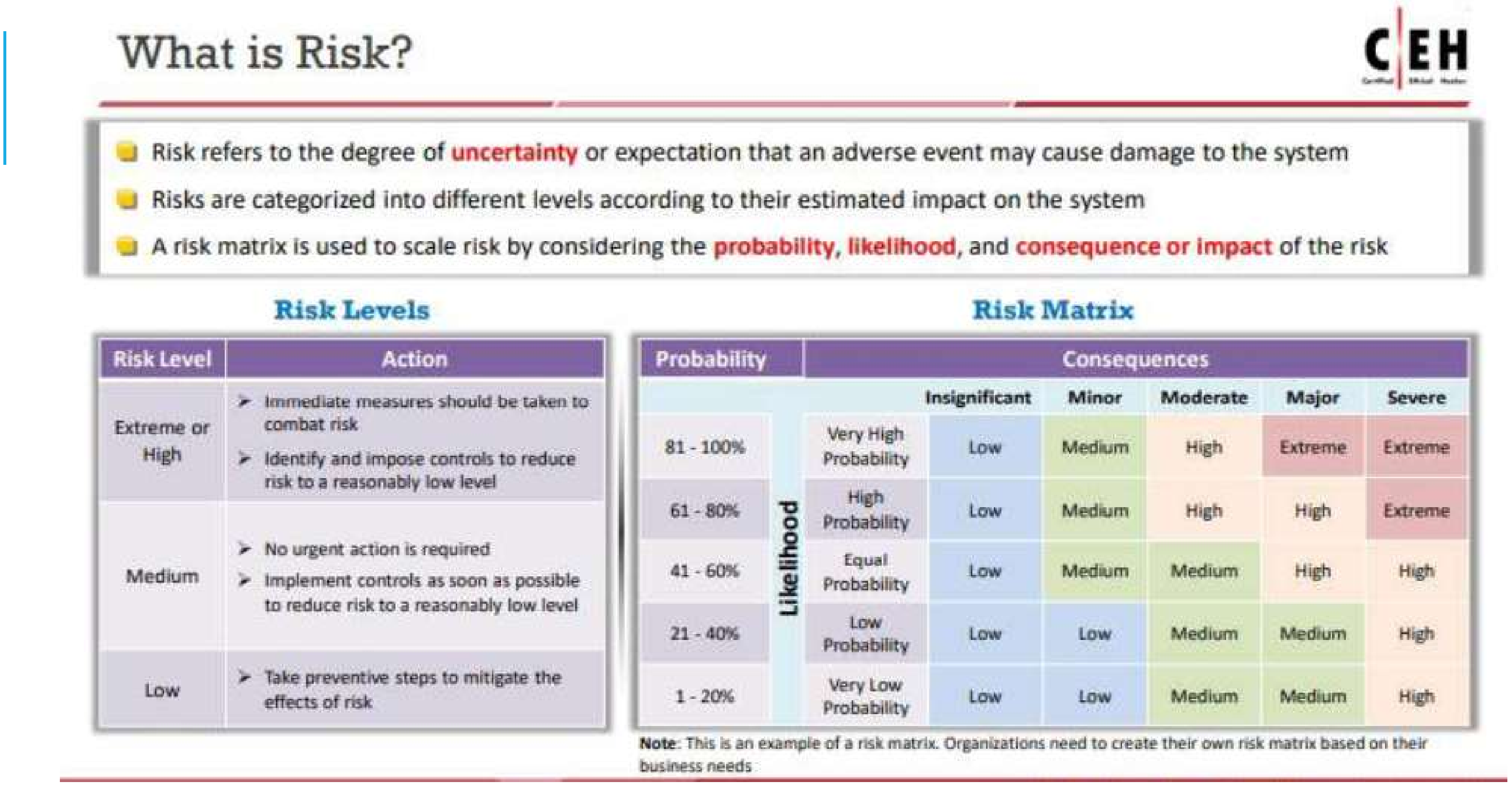
- IA refers to the assurance that the **integrity**, **availability**, **confidentiality**, and **authenticity** of information and information systems is protected during the usage, processing, storage, and transmission of information
- Some of the processes that help in achieving information assurance include:

1. **Developing local policy, process, and guidance**
2. **Designing network and user authentication strategies**
3. **Identifying network vulnerabilities and threats**
4. **Identifying problem and resource requirements**
5. **Creating plans for identified resource requirements**
6. **Applying appropriate information assurance controls**
7. **Performing certification and accreditation**
8. **Providing information assurance training**

Defense-in-Depth

- Defense-in-depth is a security strategy in which **several protection layers** 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 the attacker to the next layer





What is Risk?

- Risk refers to the degree of **uncertainty** or expectation that an adverse event may cause damage to the system
- Risks are categorized into different levels according to their estimated impact on the system
- A risk matrix is used to scale risk by considering the **probability**, **likelihood**, and **consequence or impact** of the risk

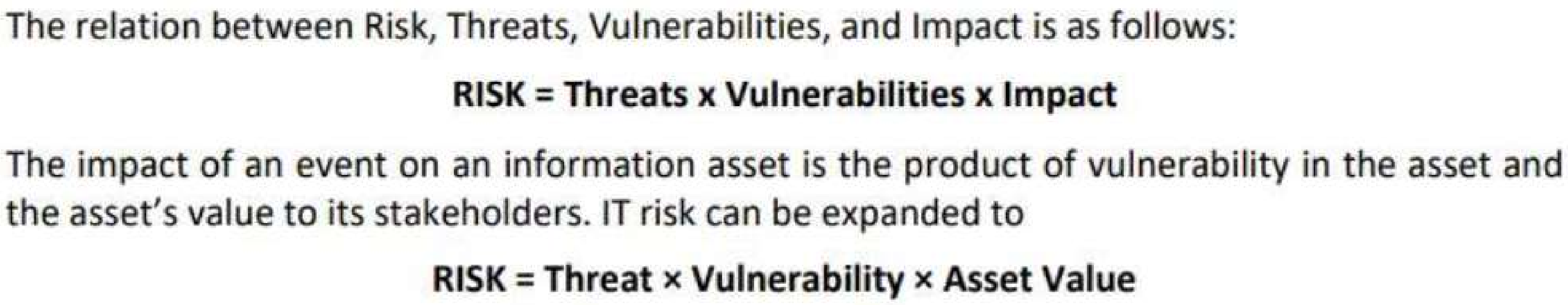
Risk Levels

Risk Level	Action
Extreme or High	➢ Immediate measures should be taken to combat risk ➢ Identify and impose controls to reduce risk to a reasonably low level
Medium	➢ No urgent action is required ➢ Implement controls as soon as possible to reduce risk to a reasonably low level
Low	➢ Take preventive steps to mitigate the effects of risk

Risk Matrix

Probability			Consequences				
			Insignificant	Minor	Moderate	Major	Severe
81 - 100%	Likelihood	Very High Probability	Low	Medium	High	Extreme	Extreme
61 - 80%		High Probability	Low	Medium	High	High	Extreme
41 - 60%		Equal Probability	Low	Medium	Medium	High	High
21 - 40%		Low Probability	Low	Low	Medium	Medium	High
1 - 20%		Very Low Probability	Low	Low	Medium	Medium	High

Note: This is an example of a risk matrix. Organizations need to create their own risk matrix based on their business needs

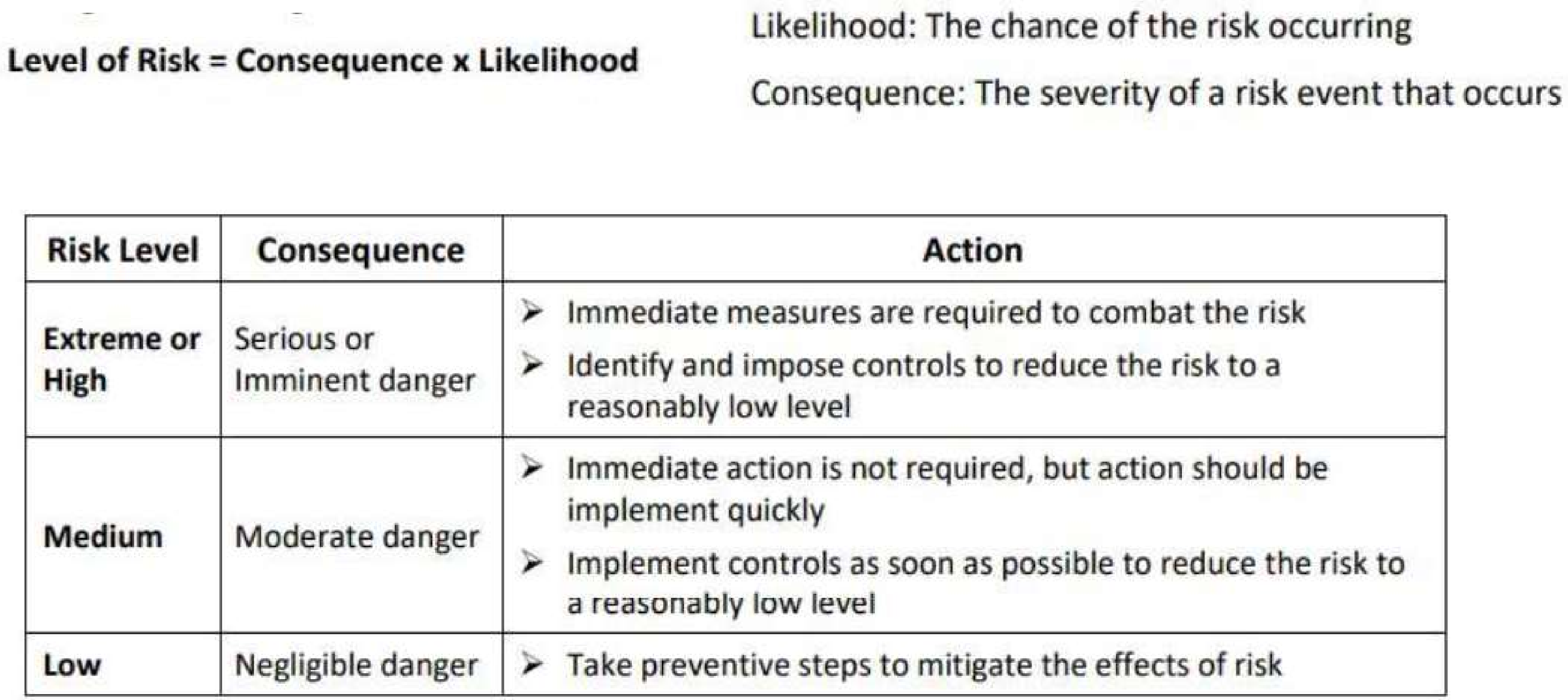


The relation between Risk, Threats, Vulnerabilities, and Impact is as follows:

RISK = Threats x Vulnerabilities x Impact

The impact of an event on an information asset is the product of vulnerability in the asset and the asset's value to its stakeholders. IT risk can be expanded to

RISK = Threat × Vulnerability × Asset Value

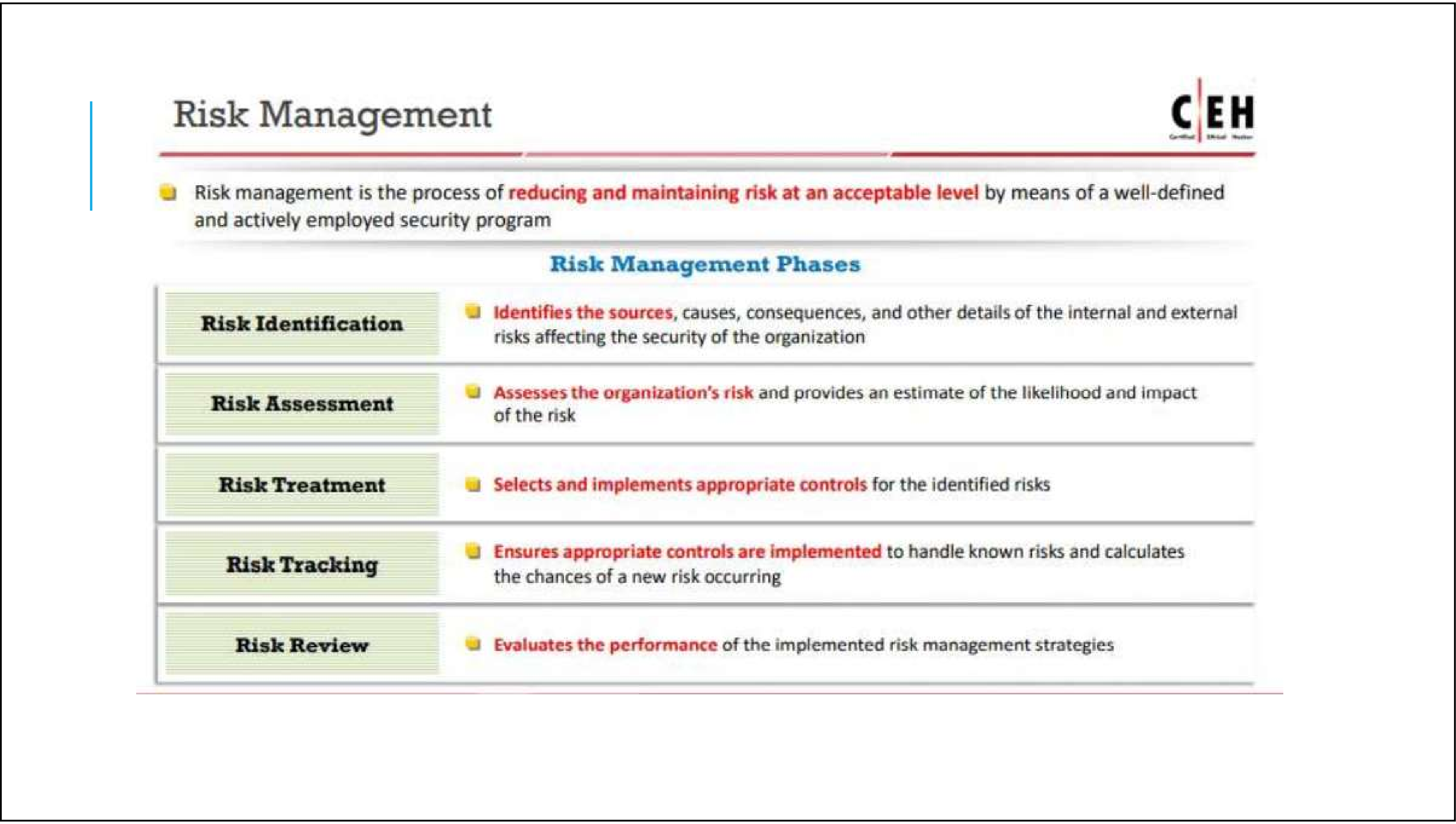


Level of Risk = Consequence x Likelihood

Likelihood: The chance of the risk occurring

Consequence: The severity of a risk event that occurs

Risk Level	Consequence	Action
Extreme or High	Serious or Imminent danger	➢ Immediate measures are required to combat the risk ➢ Identify and impose controls to reduce the risk to a reasonably low level
Medium	Moderate danger	➢ Immediate action is not required, but action should be implement quickly ➢ Implement controls as soon as possible to reduce the risk to a reasonably low level
Low	Negligible danger	➢ Take preventive steps to mitigate the effects of risk

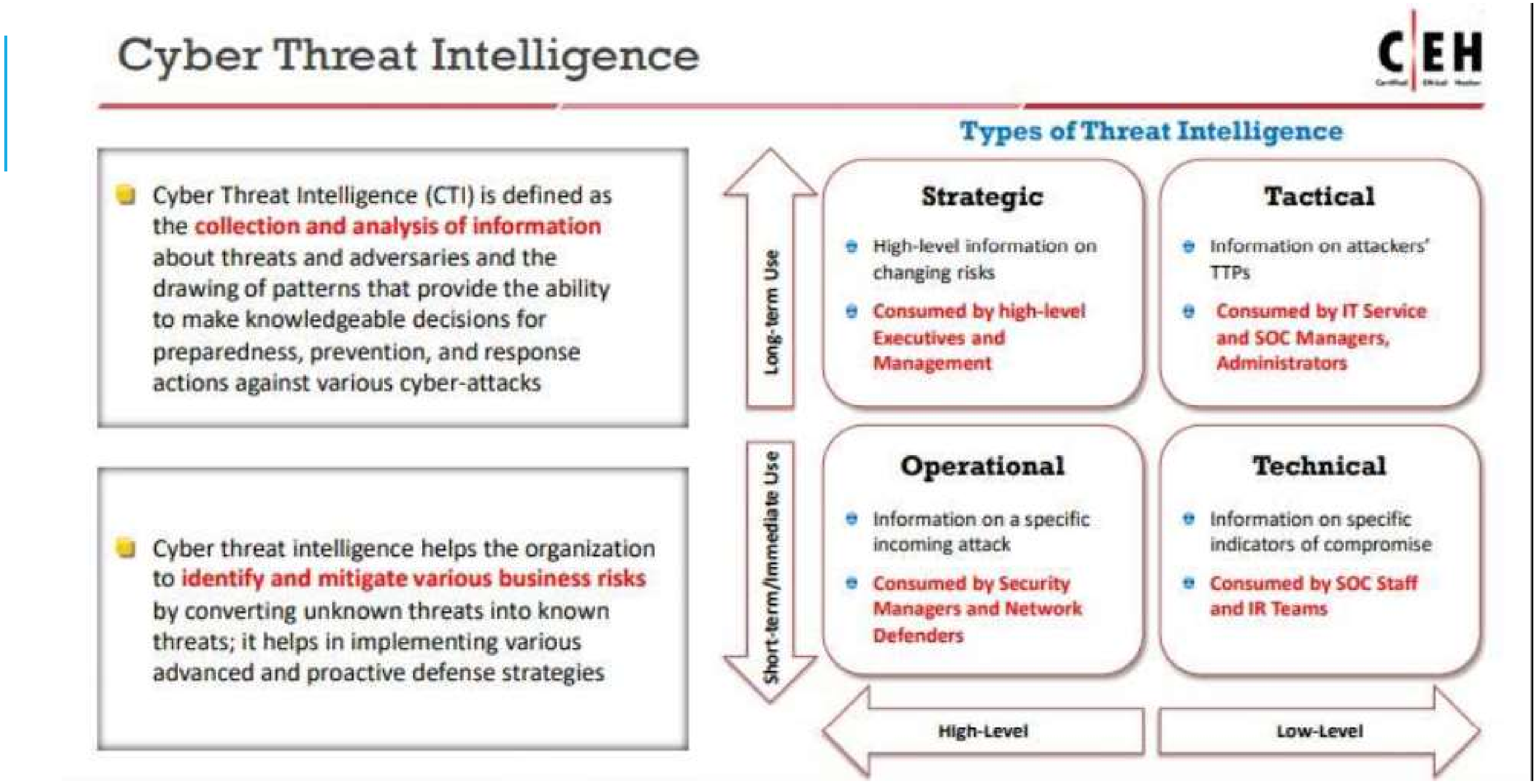


Risk Management

- Risk management is the process of **reducing and maintaining risk at an acceptable level** by means of a well-defined and actively employed security program

Risk Management Phases

Risk Identification	**Identifies the sources**, causes, consequences, and other details of the internal and external risks affecting the security of the organization
Risk Assessment	**Assesses the organization's risk** and provides an estimate of the likelihood and impact of the risk
Risk Treatment	**Selects and implements appropriate controls** for the identified risks
Risk Tracking	**Ensures appropriate controls are implemented** to handle known risks and calculates the chances of a new risk occurring
Risk Review	**Evaluates the performance** of the implemented risk management strategies



Cyber Threat Intelligence

C|EH

- Cyber Threat Intelligence (CTI) is defined as the **collection and analysis of information** about threats and adversaries and the drawing of patterns that provide the ability to make knowledgeable decisions for preparedness, prevention, and response actions against various cyber-attacks

- Cyber threat intelligence helps the organization to **identify and mitigate various business risks** by converting unknown threats into known threats; it helps in implementing various advanced and proactive defense strategies

Types of Threat Intelligence

Strategic

- High-level information on changing risks
- **Consumed by high-level Executives and Management**

Tactical

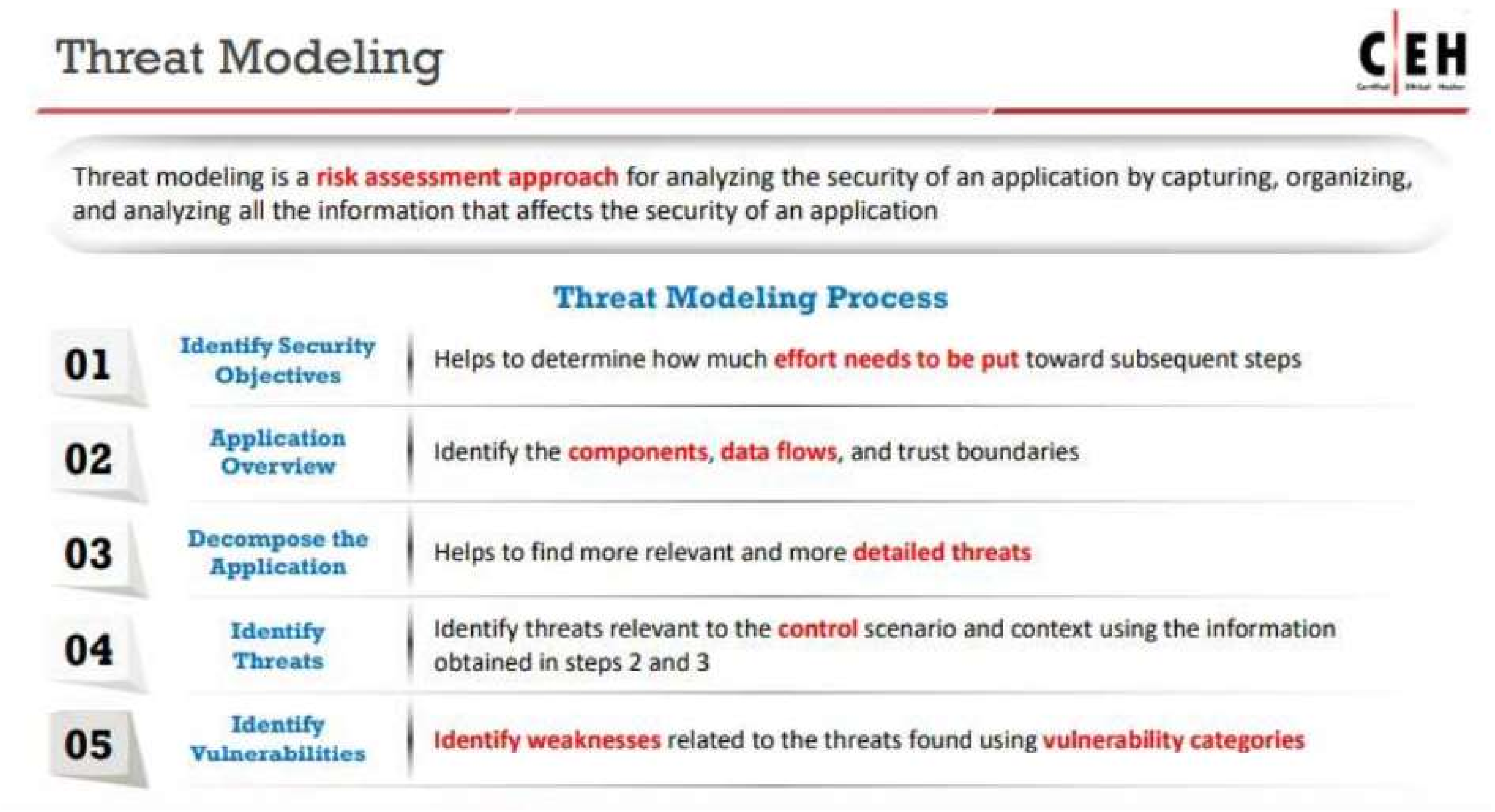
- Information on attackers' TTPs
- **Consumed by IT Service and SOC Managers, Administrators**

Operational

- Information on a specific incoming attack
- **Consumed by Security Managers and Network Defenders**

Technical

- Information on specific indicators of compromise
- **Consumed by SOC Staff and IR Teams**

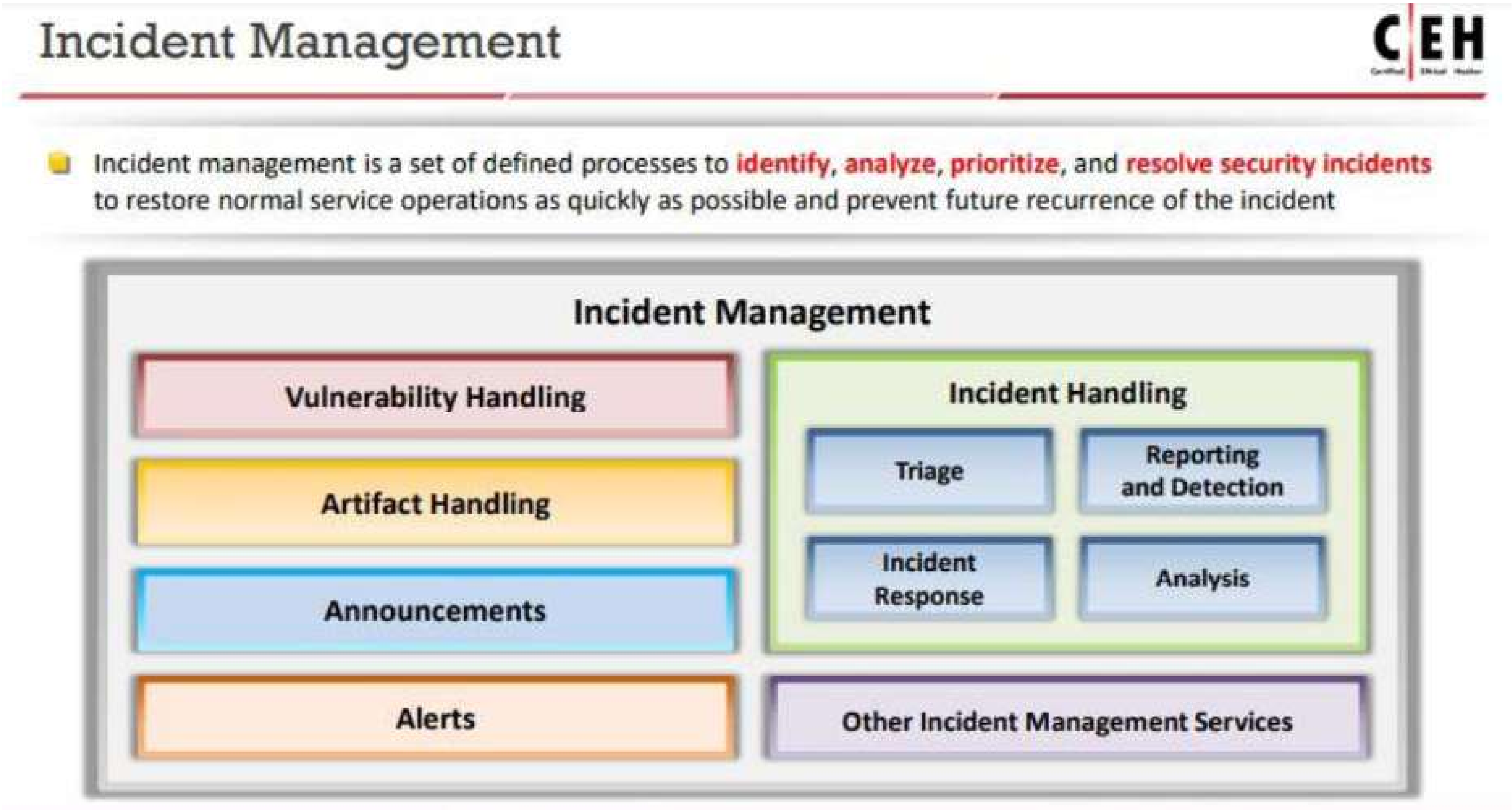


Threat Modeling

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**



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

Artifact Handling

Announcements

Alerts

Incident Handling

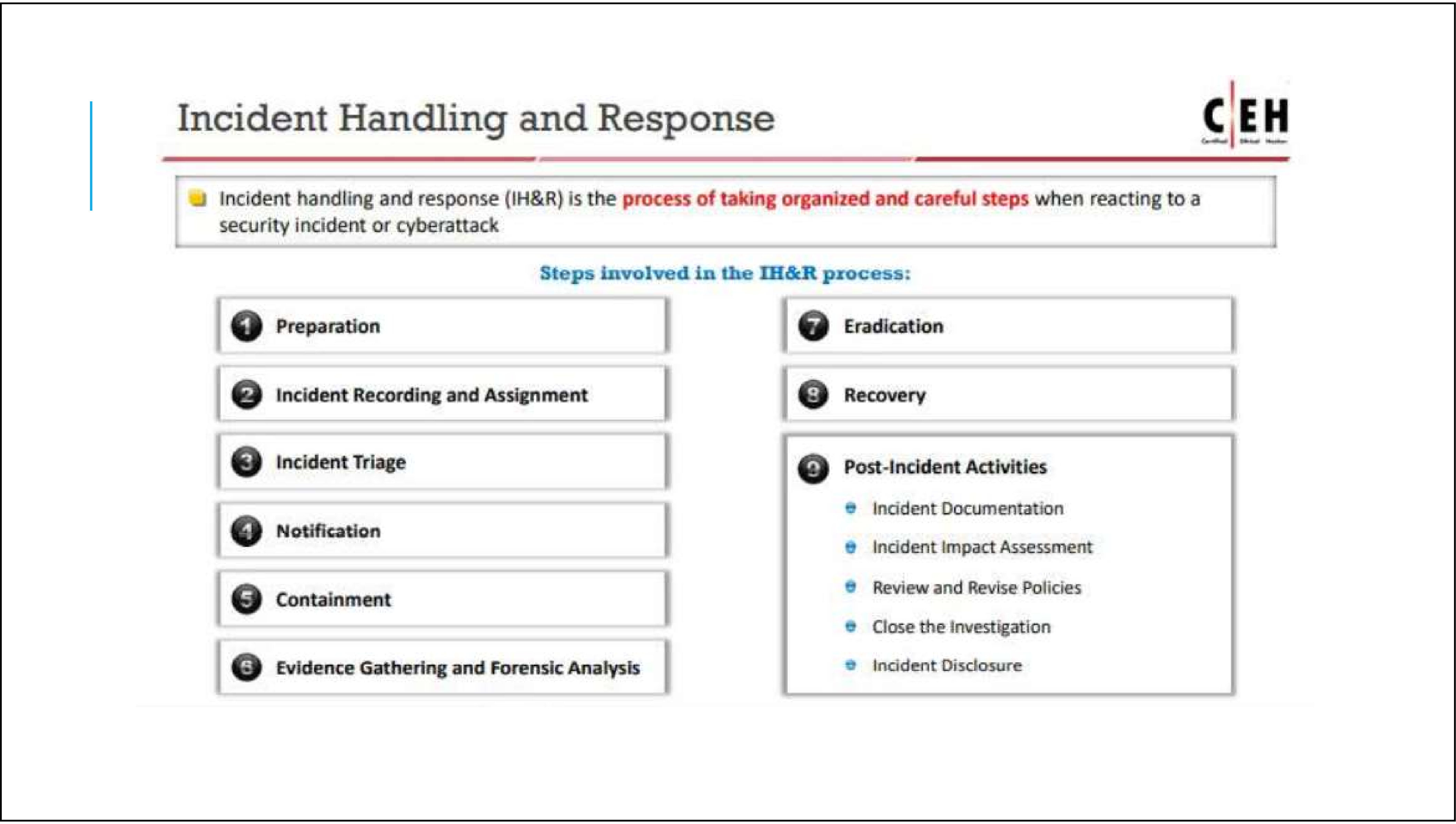
Triage

Reporting and Detection

Incident Response

Analysis

Other Incident Management Services

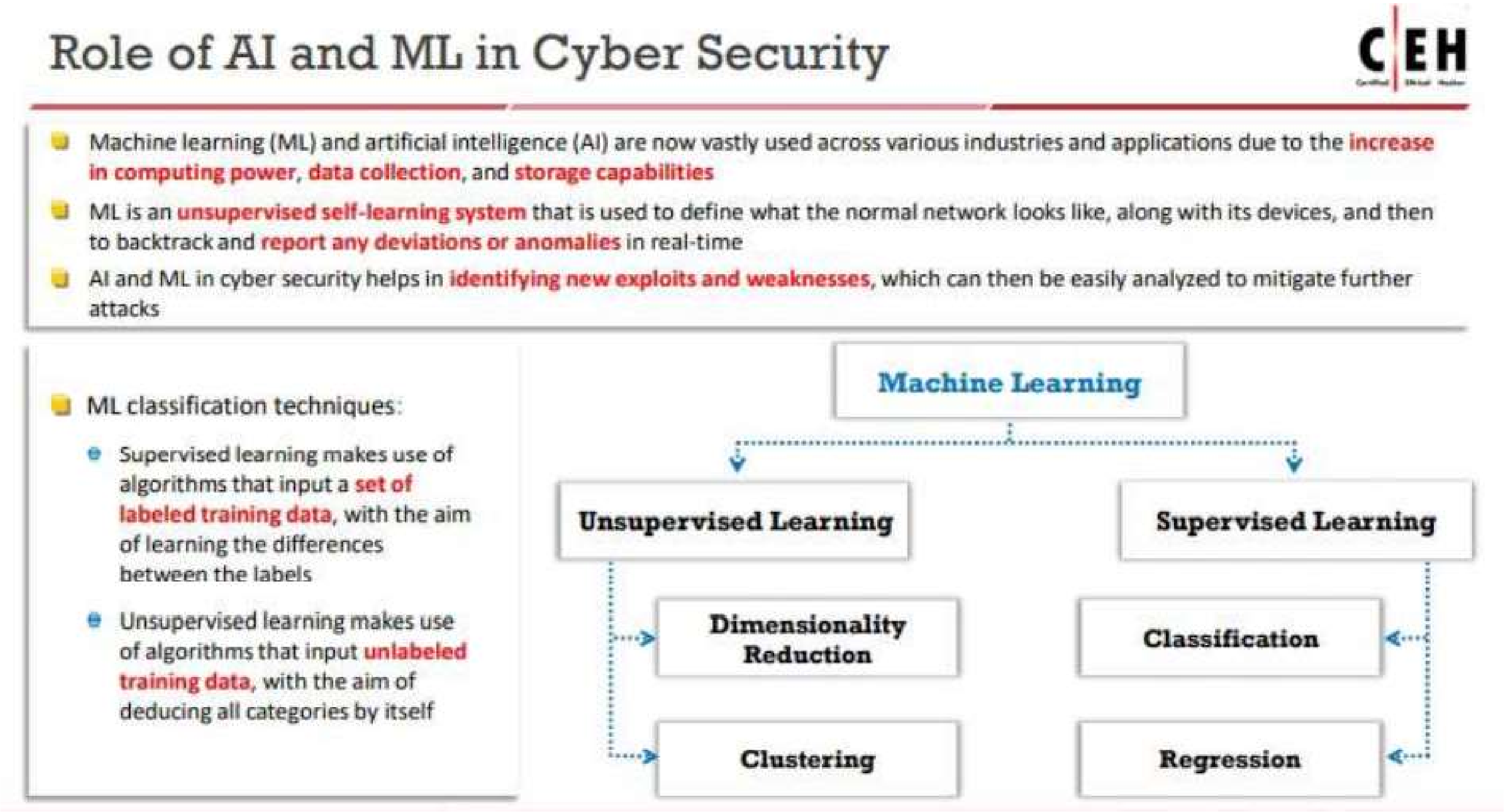


Incident Handling and Response

- 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**
2. **Incident Recording and Assignment**
3. **Incident Triage**
4. **Notification**
5. **Containment**
6. **Evidence Gathering and Forensic Analysis**
7. **Eradication**
8. **Recovery**
9. **Post-Incident Activities**
   - Incident Documentation
   - Incident Impact Assessment
   - Review and Revise Policies
   - Close the Investigation
   - Incident Disclosure



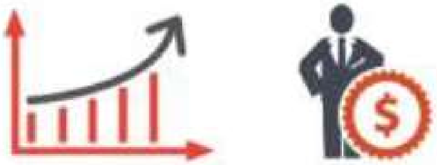
Role of AI and ML in Cyber Security

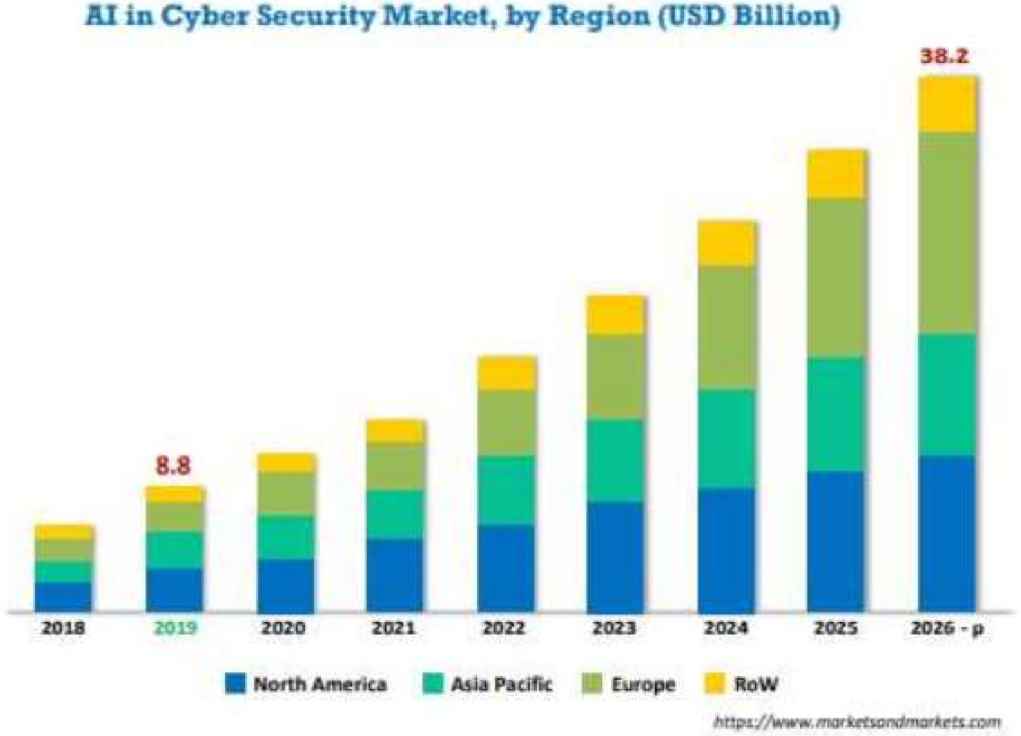
- Machine learning (ML) and artificial intelligence (AI) are now vastly used across various industries and applications due to the **increase in computing power**, **data collection**, and **storage capabilities**
- ML is an **unsupervised self-learning system** that is used to define what the normal 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

Role of AI and ML in Cyber Security (Cont'd)

- The cyber security market is set to exceed $300 billion by 2024, and the AI-related cyber security market is predicted to reach a value of $38.2 billion by 2026



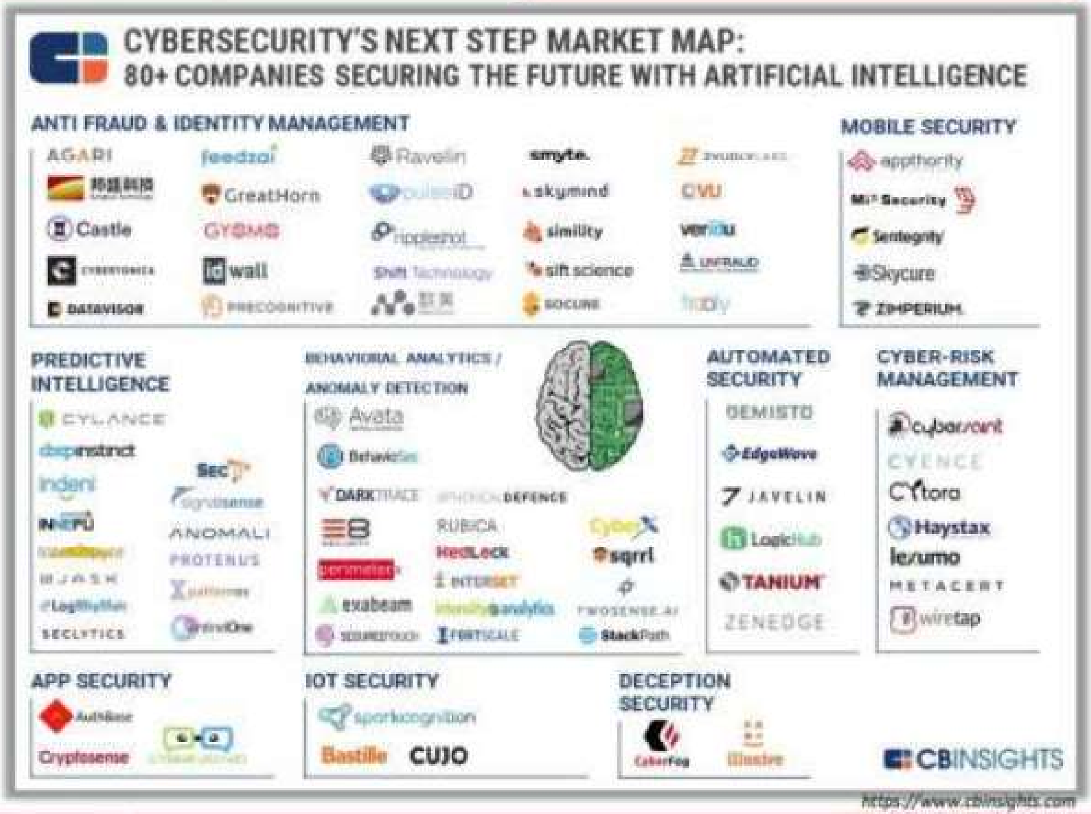


https://www.marketsandmarkets.com

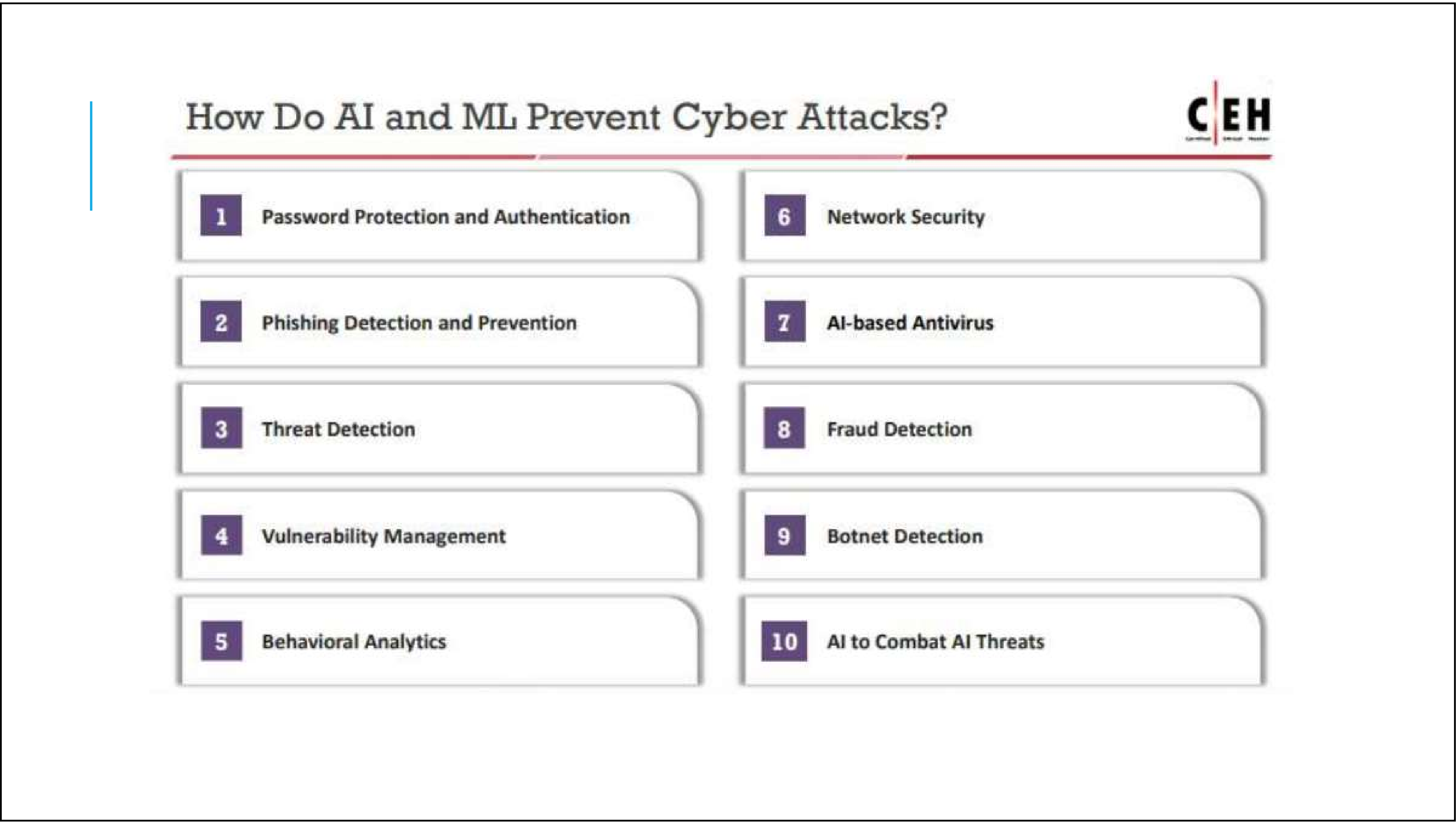
Role of AI and ML in Cyber Security (Cont'd)

According to CB Insights, alongside overall rising investment activity, many cybersecurity companies are emerging to **offer novel solutions to cyber threats by leveraging the advantages of AI**

Cybersecurity is the fourth most active industry that deals with companies applying AI



https://www.cbinsights.com



How Do AI and ML Prevent Cyber Attacks?

1 Password Protection and Authentication

2 Phishing Detection and Prevention

3 Threat Detection

4 Vulnerability Management

5 Behavioral Analytics

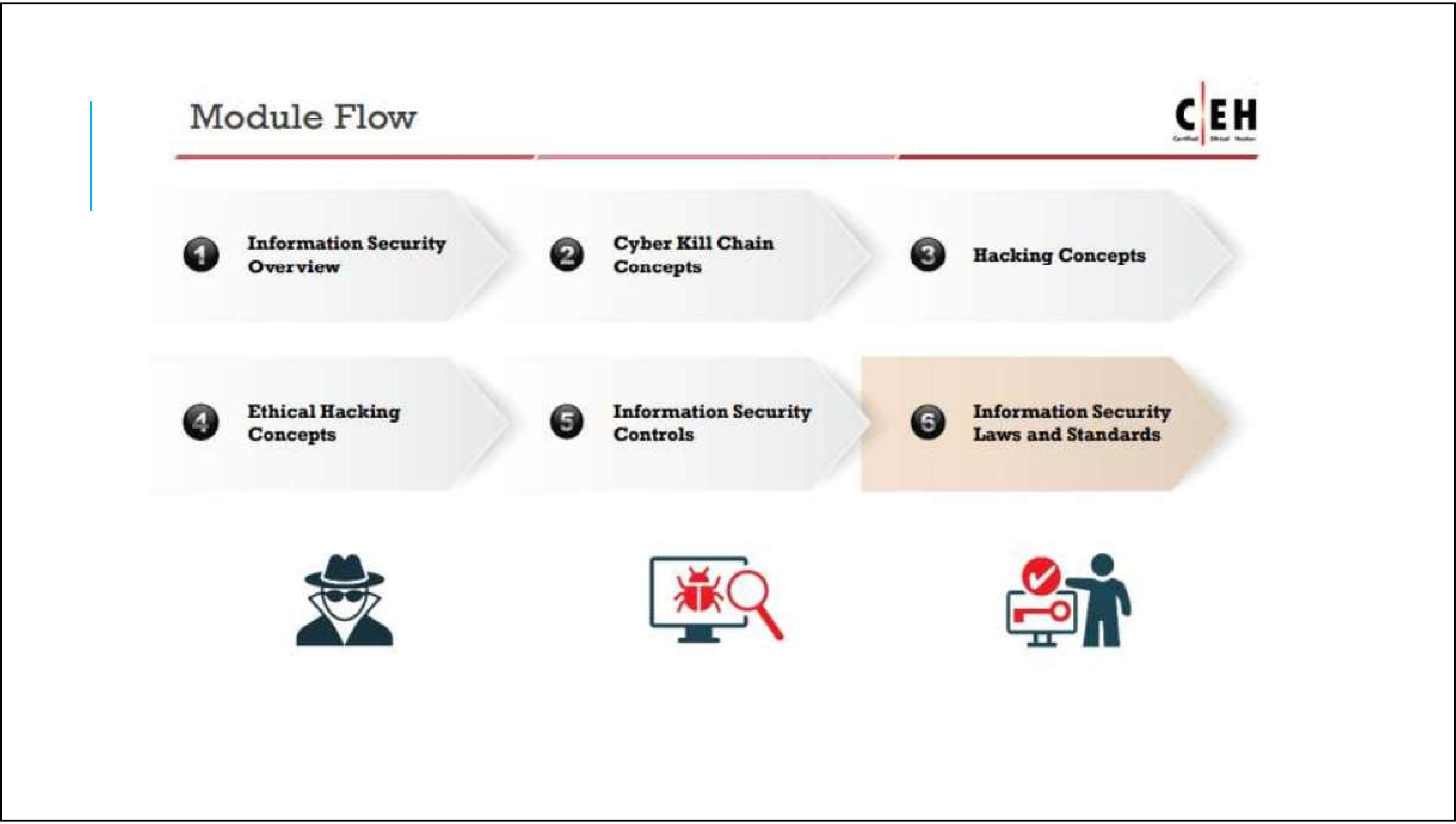
6 Network Security

7 AI-based Antivirus

8 Fraud Detection

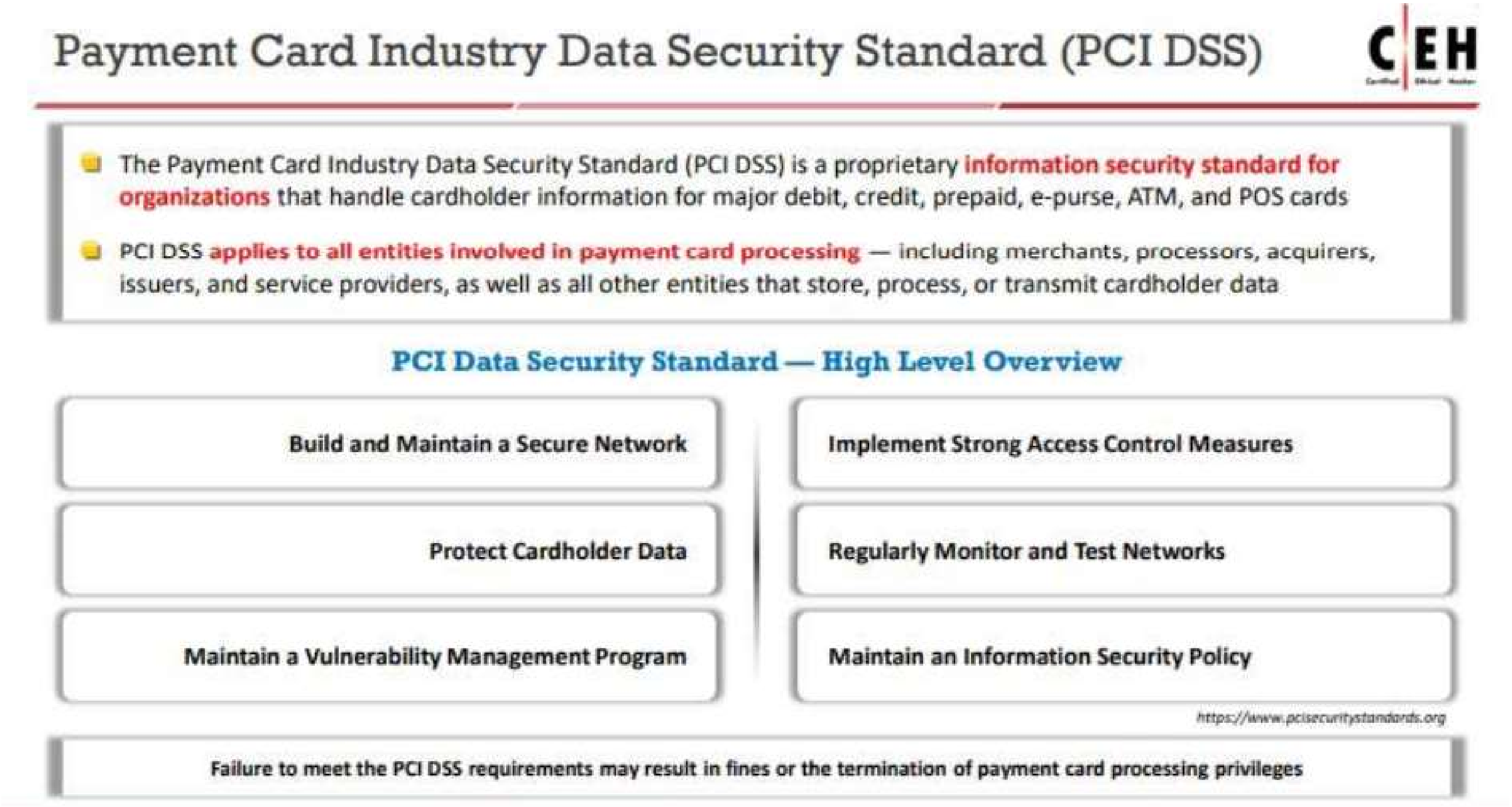
9 Botnet Detection

10 AI to Combat AI Threats



Module Flow

1. Information Security Overview
2. Cyber Kill Chain Concepts
3. Hacking Concepts
4. Ethical Hacking Concepts
5. Information Security Controls
6. Information Security Laws and Standards



Payment Card Industry Data Security Standard (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

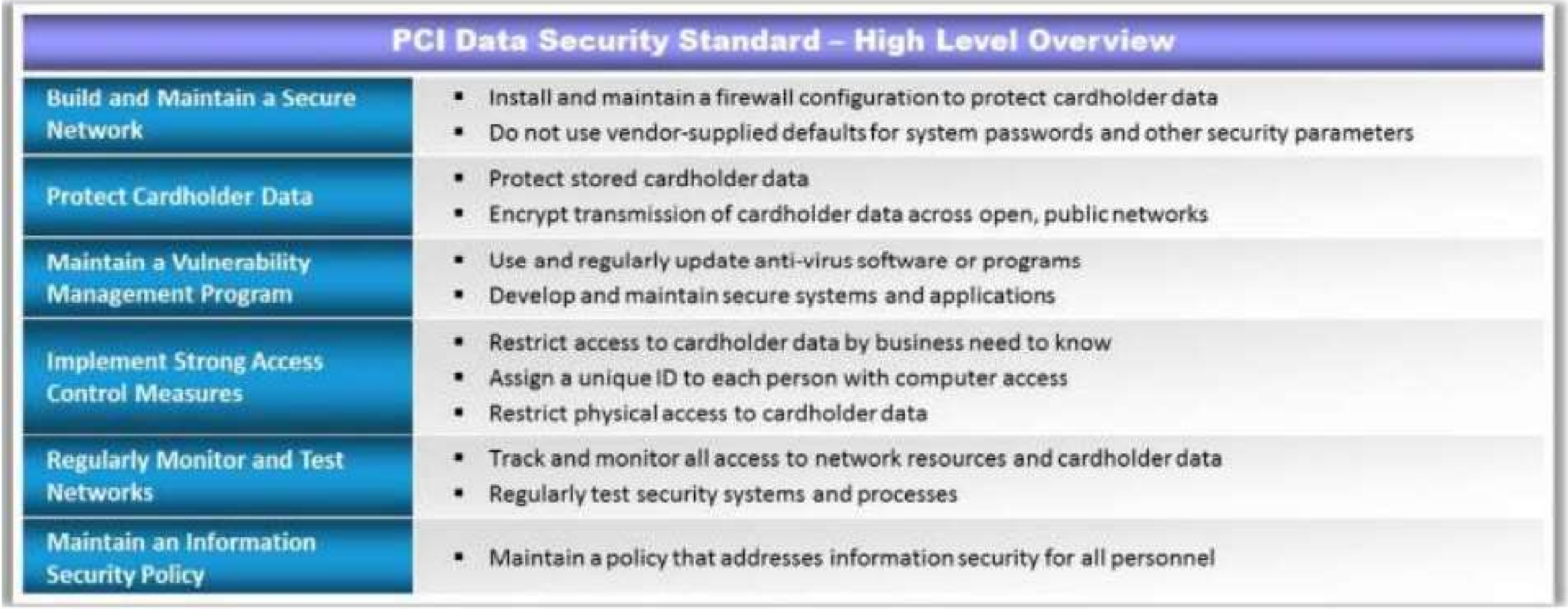
Regularly Monitor and Test Networks

Maintain a Vulnerability Management Program

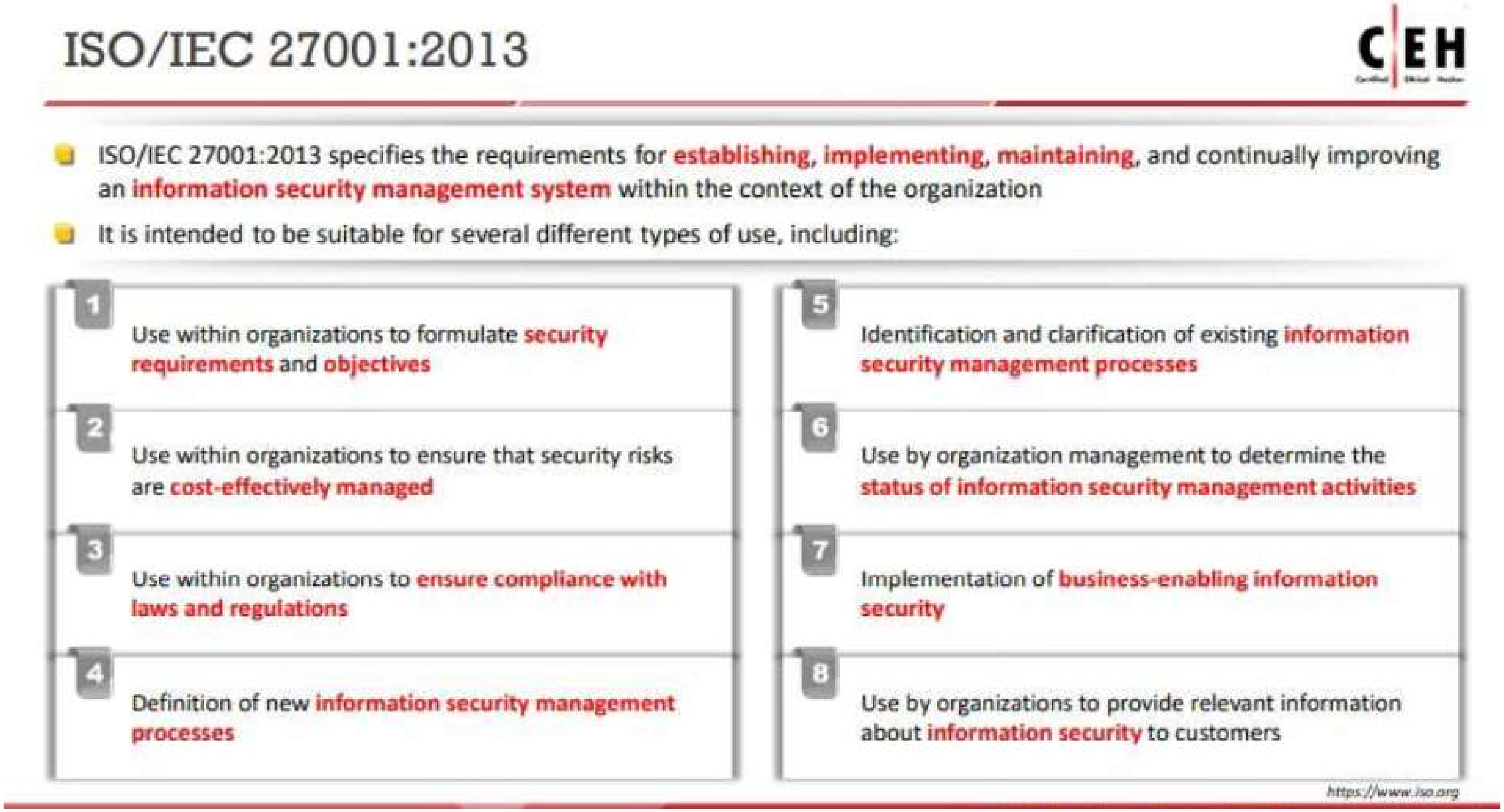
Maintain an Information Security Policy

https://www.pcisecuritystandards.org

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



PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network	▪ 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	▪ Protect stored cardholder data ▪ Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	▪ Use and regularly update anti-virus software or programs ▪ Develop and maintain secure systems and applications
Implement Strong Access Control Measures	▪ 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	▪ Track and monitor all access to network resources and cardholder data ▪ Regularly test security systems and processes
Maintain an Information Security Policy	▪ Maintain a policy that addresses information security for all personnel

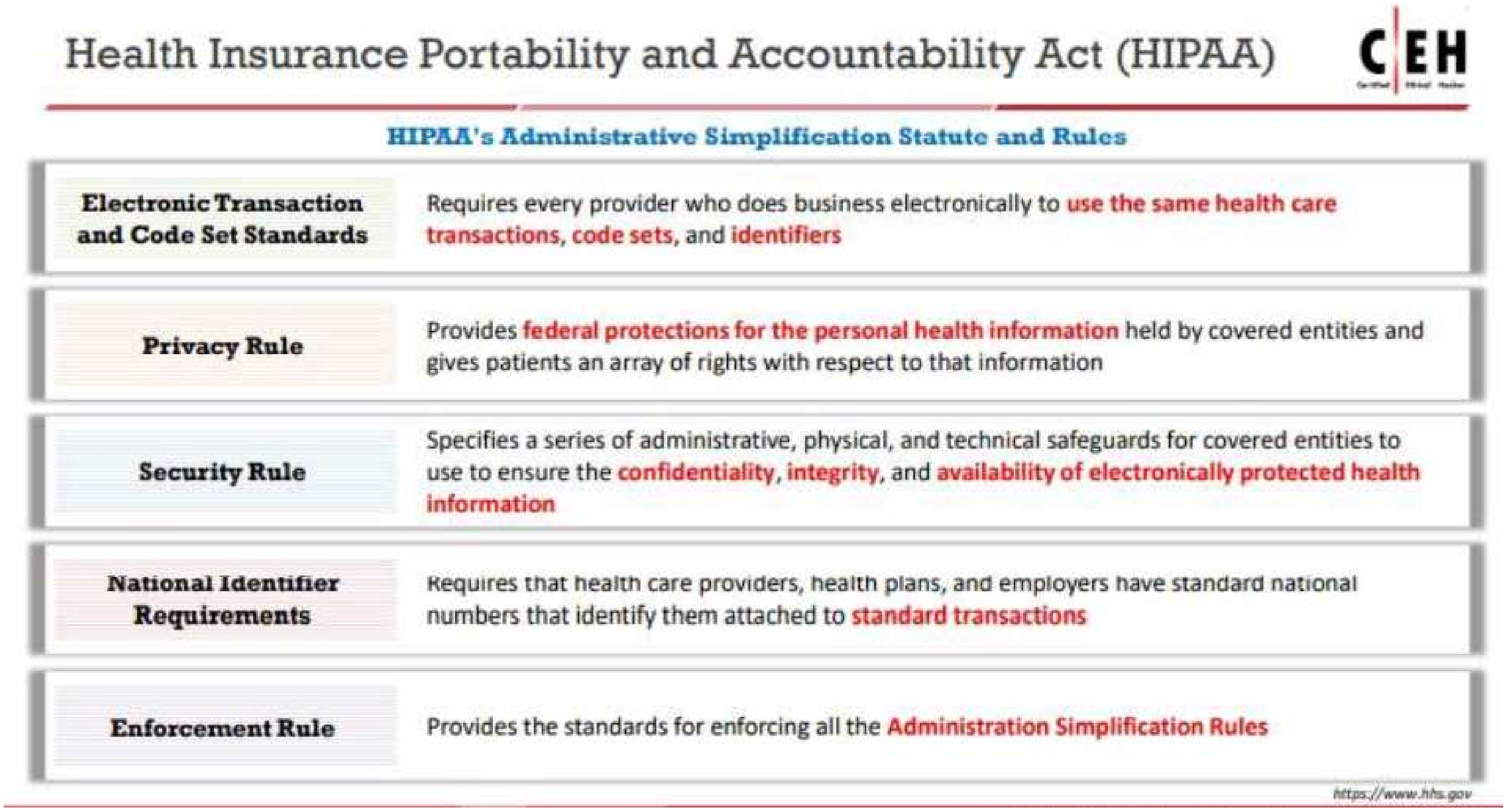


ISO/IEC 27001:2013

- 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:

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**
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

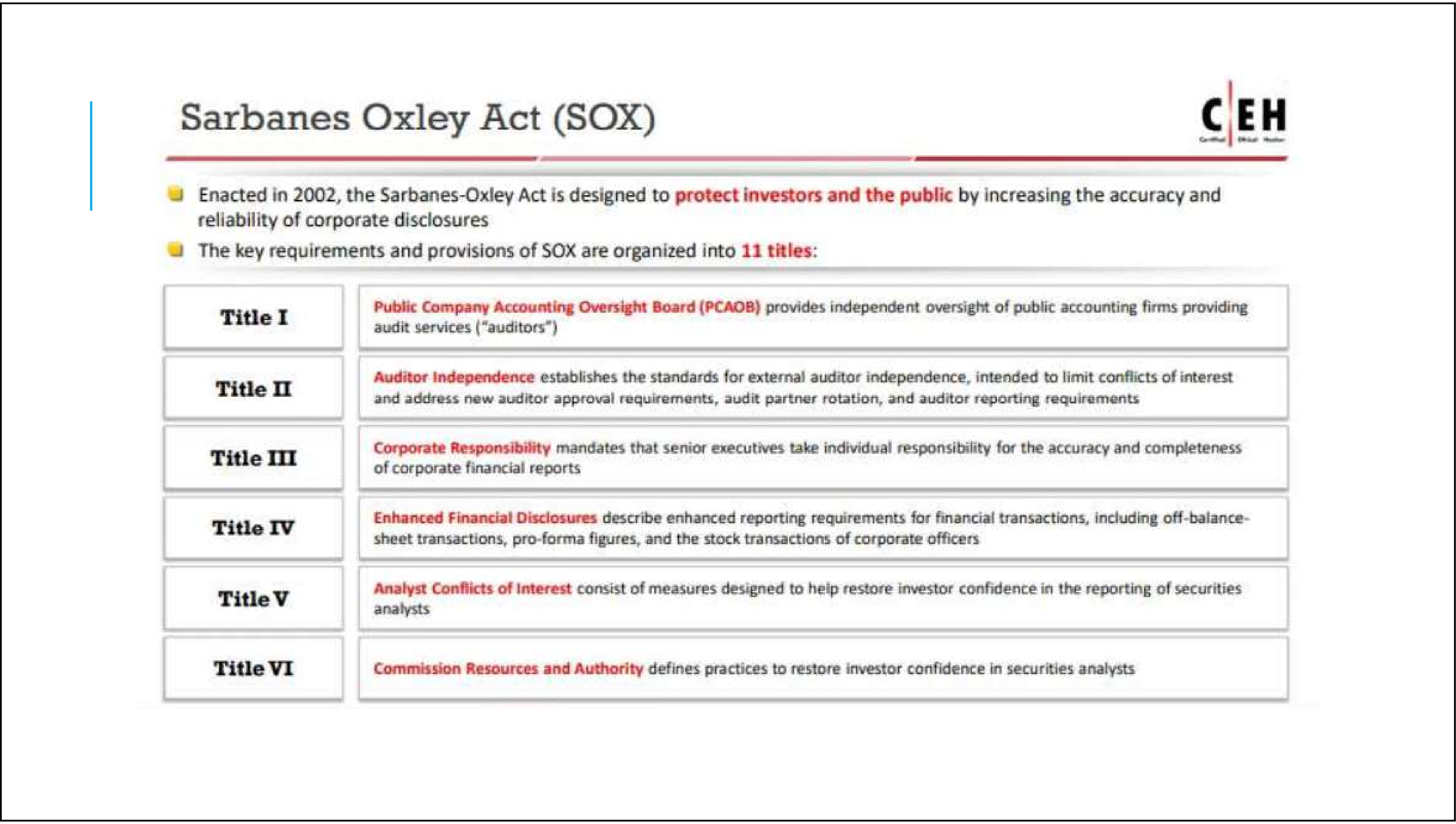


Health Insurance Portability and Accountability Act (HIPAA)

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**

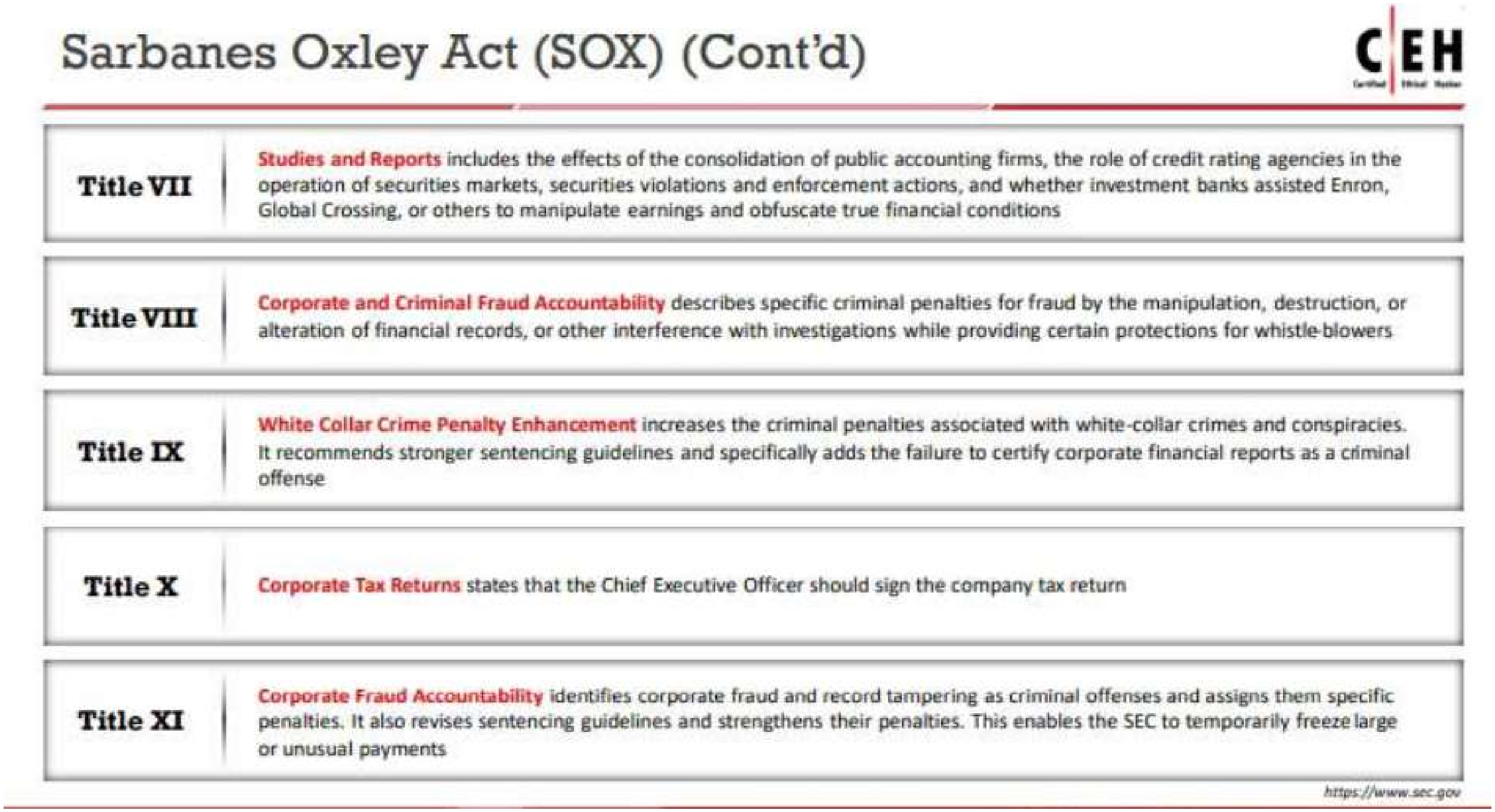
https://www.hhs.gov



Sarbanes Oxley Act (SOX)

- Enacted in 2002, the Sarbanes-Oxley Act is designed to **protect investors and the public** by increasing the accuracy and reliability of corporate disclosures
- The key requirements and provisions of SOX are organized into **11 titles**:

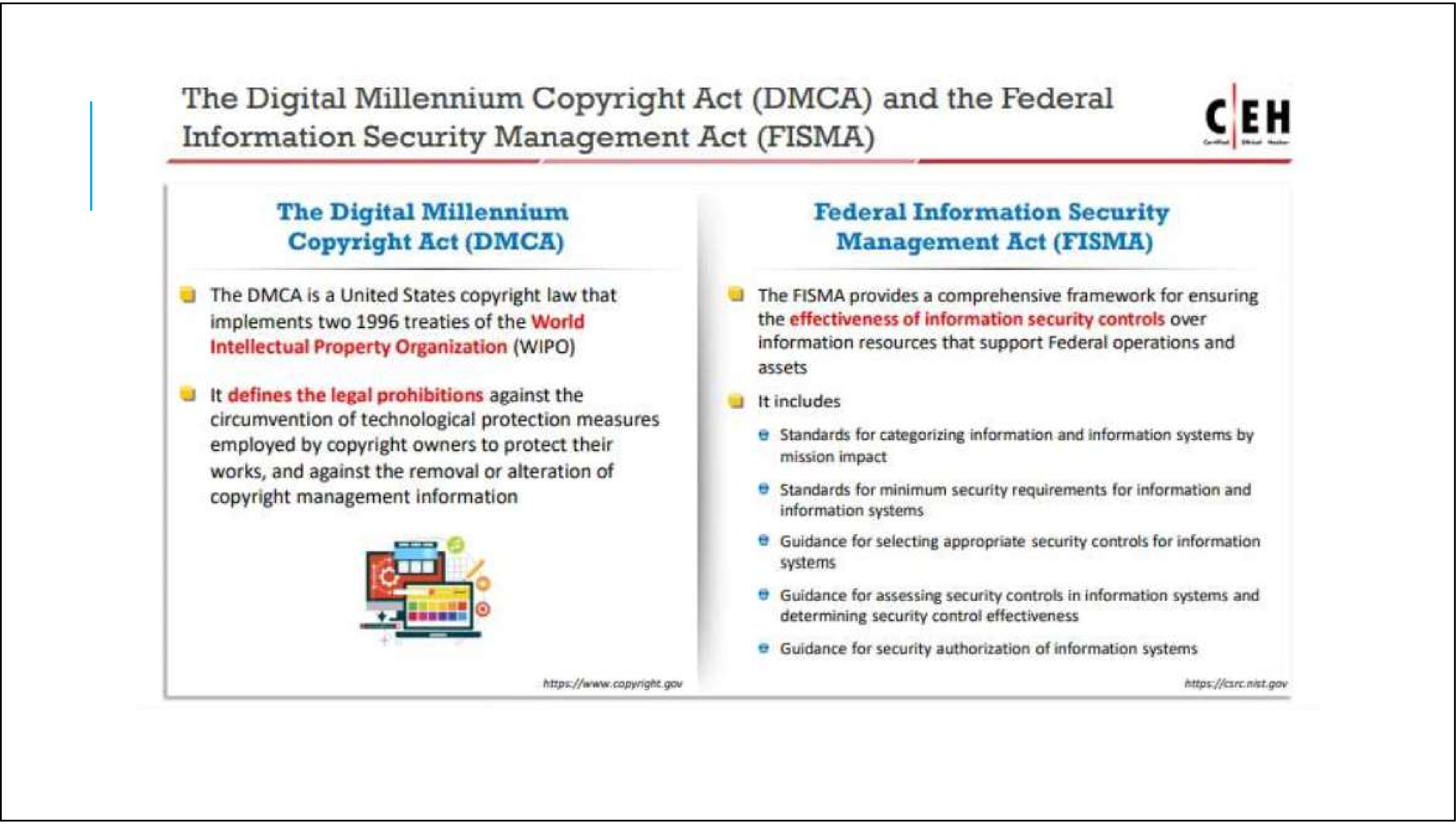
Title I	**Public Company Accounting Oversight Board (PCAOB)** provides independent oversight of public accounting firms providing audit services ("auditors")
Title II	**Auditor Independence** establishes the standards for external auditor independence, intended to limit conflicts of interest and address new auditor approval requirements, audit partner rotation, and auditor reporting requirements
Title III	**Corporate Responsibility** mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports
Title IV	**Enhanced Financial Disclosures** describe enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures, and the stock transactions of corporate officers
Title V	**Analyst Conflicts of Interest** consist of measures designed to help restore investor confidence in the reporting of securities analysts
Title VI	**Commission Resources and Authority** defines practices to restore investor confidence in securities analysts



Sarbanes Oxley Act (SOX) (Cont'd)

Title VII	**Studies and Reports** includes the effects of the consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations and enforcement actions, and whether investment banks assisted Enron, Global Crossing, or others to manipulate earnings and obfuscate true financial conditions
Title VIII	**Corporate and Criminal Fraud Accountability** describes specific criminal penalties for fraud by the manipulation, destruction, or alteration of financial records, or other interference with investigations while providing certain protections for whistle-blowers
Title IX	**White Collar Crime Penalty Enhancement** increases the criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds the failure to certify corporate financial reports as a criminal offense
Title X	**Corporate Tax Returns** states that the Chief Executive Officer should sign the company tax return
Title XI	**Corporate Fraud Accountability** identifies corporate fraud and record tampering as criminal offenses and assigns them specific penalties. It also revises sentencing guidelines and strengthens their penalties. This enables the SEC to temporarily freeze large or unusual payments

https://www.sec.gov



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

C|EH

The Digital Millennium Copyright Act (DMCA)

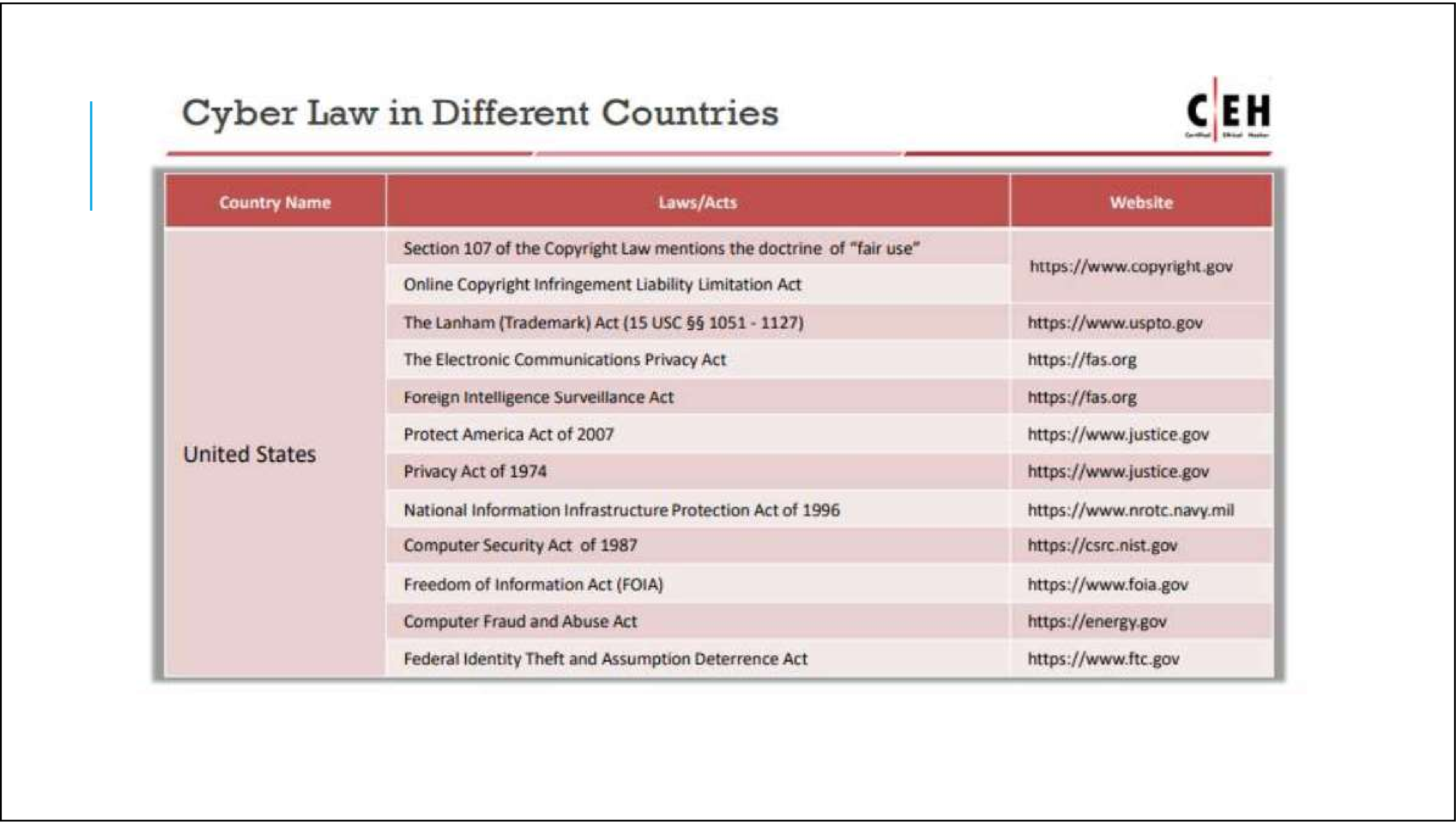
- The DMCA is a United States copyright law that implements two 1996 treaties of the **World Intellectual Property Organization** (WIPO)
- It **defines the legal prohibitions** against the circumvention of technological protection measures employed by copyright owners to protect their works, and against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

https://www.copyright.gov

Federal Information Security Management Act (FISMA)

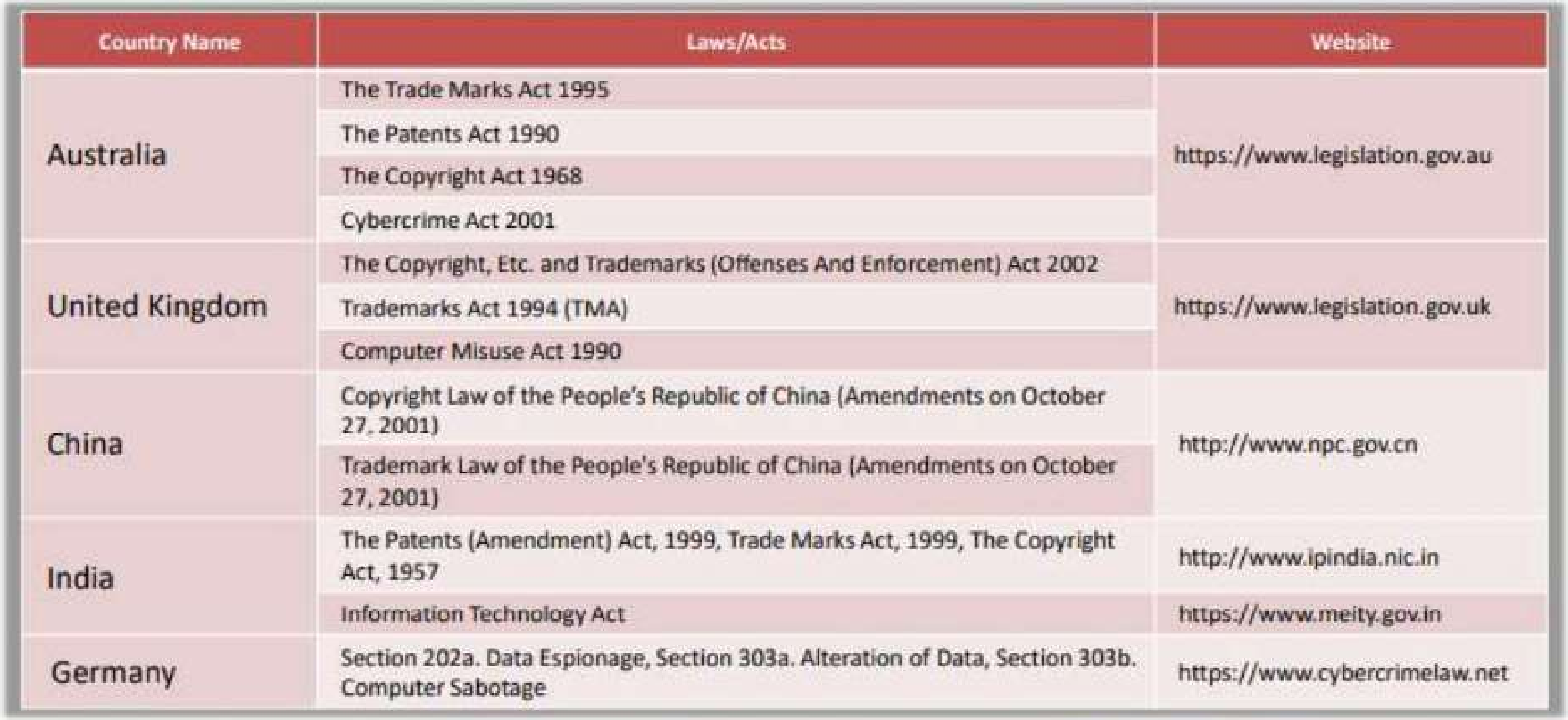
- The FISMA provides a comprehensive framework for ensuring the **effectiveness of information security controls** over information resources that support Federal operations and assets
- It includes
  - Standards for categorizing information and information systems by mission impact
  - Standards for 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

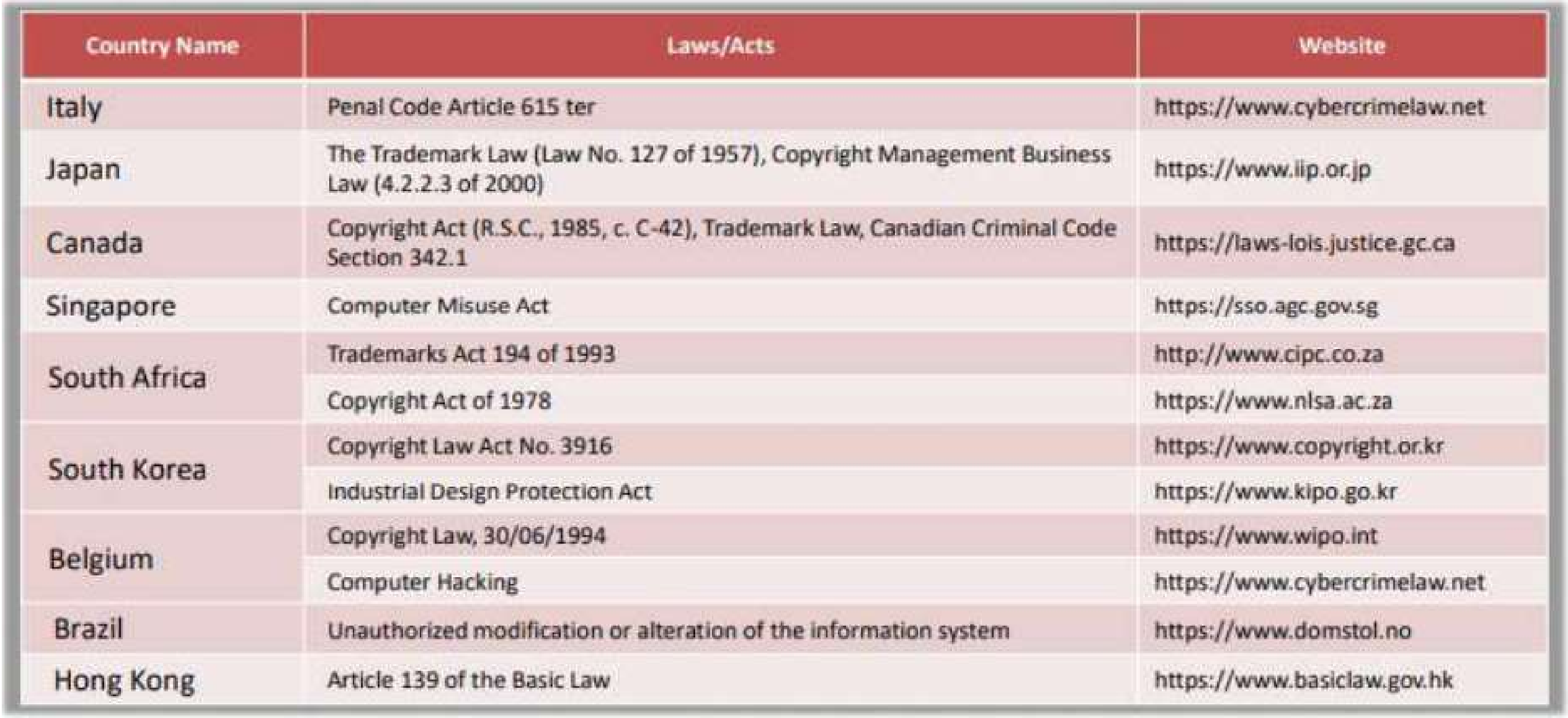


Cyber Law in Different Countries

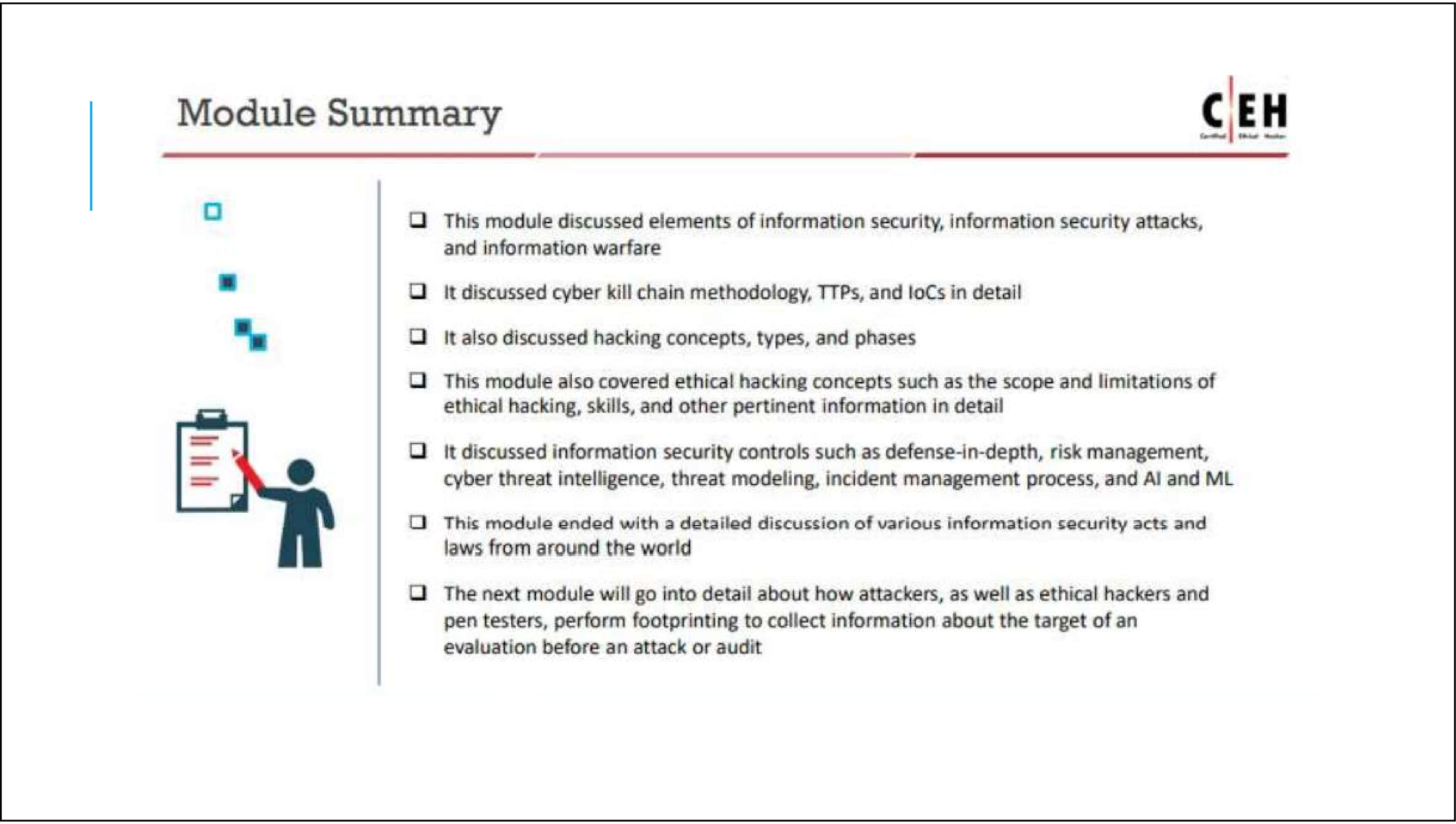
Country Name	Laws/Acts	Website
United States	Section 107 of the Copyright Law mentions the doctrine of "fair use"	https://www.copyright.gov
	Online Copyright Infringement Liability Limitation Act	
	The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)	https://www.uspto.gov
	The Electronic Communications Privacy Act	https://fas.org
	Foreign Intelligence Surveillance Act	https://fas.org
	Protect America Act of 2007	https://www.justice.gov
	Privacy Act of 1974	https://www.justice.gov
	National Information Infrastructure Protection Act of 1996	https://www.nrotc.navy.mil
	Computer Security Act of 1987	https://csrc.nist.gov
	Freedom of Information Act (FOIA)	https://www.foia.gov
	Computer Fraud and Abuse Act	https://energy.gov
	Federal Identity Theft and Assumption Deterrence Act	https://www.ftc.gov



Country Name	Laws/Acts	Website
Australia	The Trade Marks Act 1995	https://www.legislation.gov.au
	The Patents Act 1990	
	The Copyright Act 1968	
	Cybercrime Act 2001	
United Kingdom	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	https://www.legislation.gov.uk
	Trademarks Act 1994 (TMA)	
	Computer Misuse Act 1990	
China	Copyright Law of the People's Republic of China (Amendments on October 27, 2001)	http://www.npc.gov.cn
	Trademark Law of the People's Republic of China (Amendments on October 27, 2001)	
India	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957	http://www.ipindia.nic.in
	Information Technology Act	https://www.meity.gov.in
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	https://www.cybercrimelaw.net



Country Name	Laws/Acts	Website
Italy	Penal Code Article 615 ter	https://www.cybercrimelaw.net
Japan	The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000)	https://www.iip.or.jp
Canada	Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1	https://laws-lois.justice.gc.ca
Singapore	Computer Misuse Act	https://sso.agc.gov.sg
South Africa	Trademarks Act 194 of 1993	http://www.cipc.co.za
	Copyright Act of 1978	https://www.nlsa.ac.za
South Korea	Copyright Law Act No. 3916	https://www.copyright.or.kr
	Industrial Design Protection Act	https://www.kipo.go.kr
Belgium	Copyright Law, 30/06/1994	https://www.wipo.int
	Computer Hacking	https://www.cybercrimelaw.net
Brazil	Unauthorized modification or alteration of the information system	https://www.domstol.no
Hong Kong	Article 139 of the Basic Law	https://www.basiclaw.gov.hk



Module Summary

CEH

□ This module discussed elements of information security, information security attacks, and information warfare

□ It discussed cyber kill chain methodology, TTPs, and IoCs in detail

□ It also discussed hacking concepts, types, and phases

□ This module also covered ethical hacking concepts such as the scope and limitations of ethical hacking, skills, and other pertinent information in detail

□ It discussed information security controls such as defense-in-depth, risk management, cyber threat intelligence, threat modeling, incident management process, and AI and ML

□ This module ended with a detailed discussion of various information security acts and laws from around the world

□ The next module will go into detail about how attackers, as well as ethical hackers and pen testers, perform footprinting to collect information about the target of an evaluation before an attack or audit