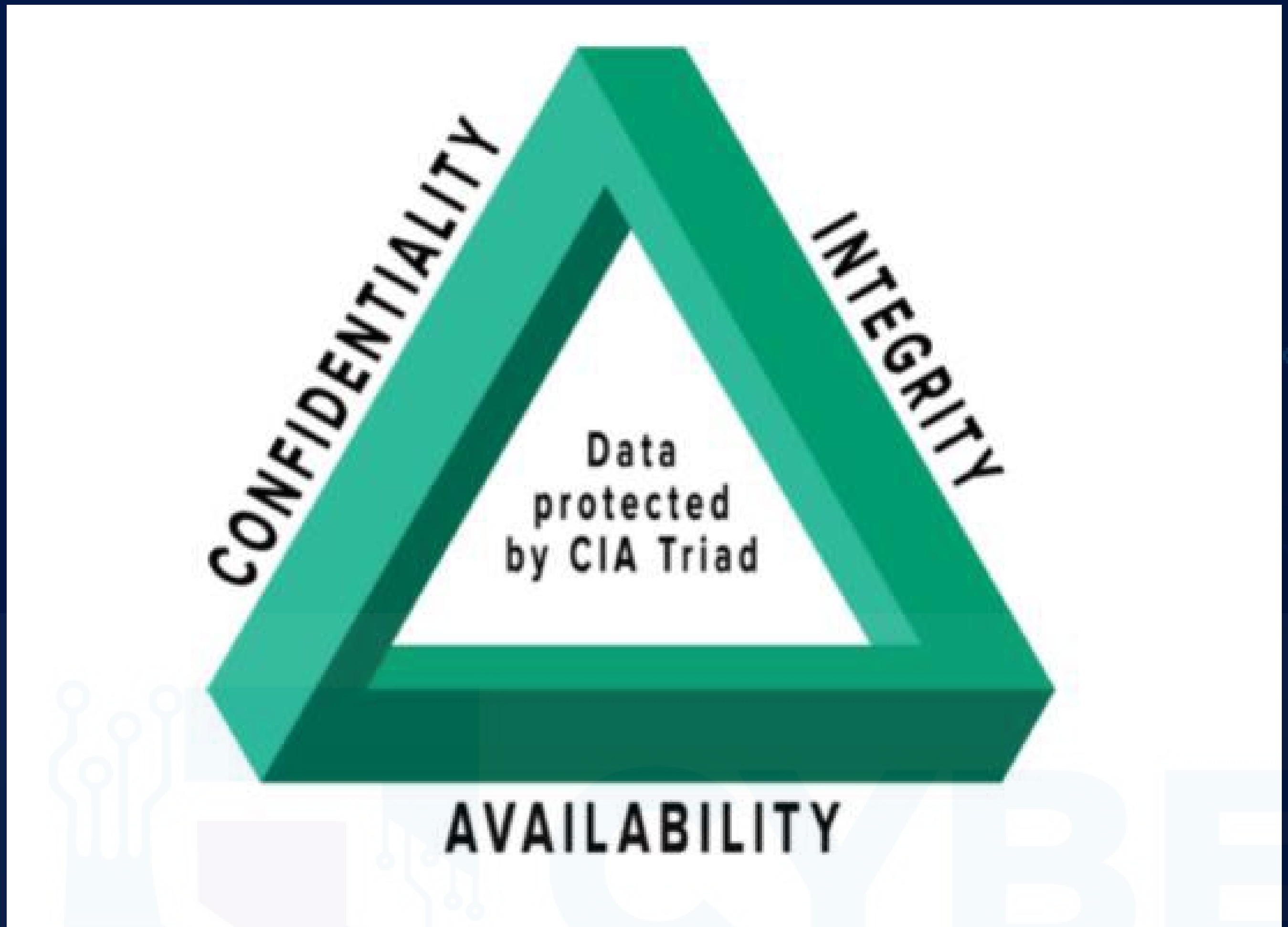
CyberlyUSA

SECURITY OPERATIONS CENTER ANALYST TRAINING

Free PDF

Oct 2024

CIA Triad



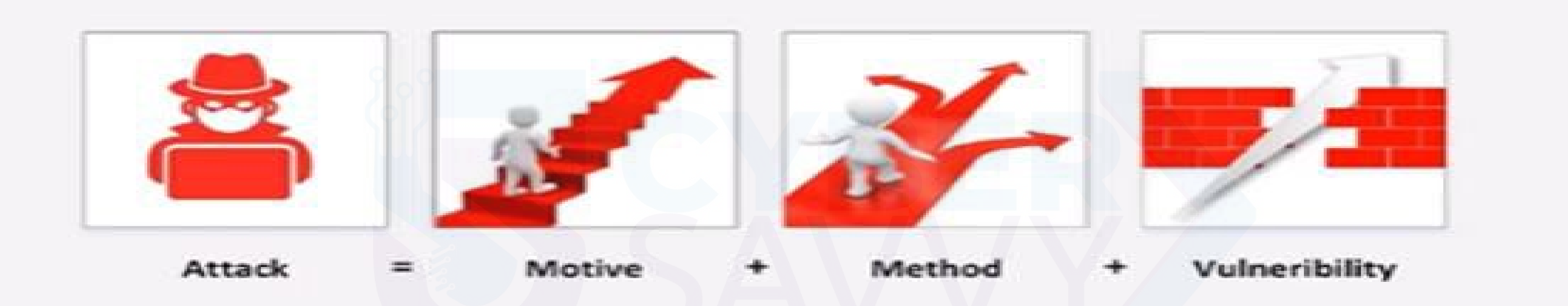
Confidentiality
Confidentiality refers to an efforts to keep data private or secret. Typically, this involves ensuring those who are authorized have access to specific assets/information.

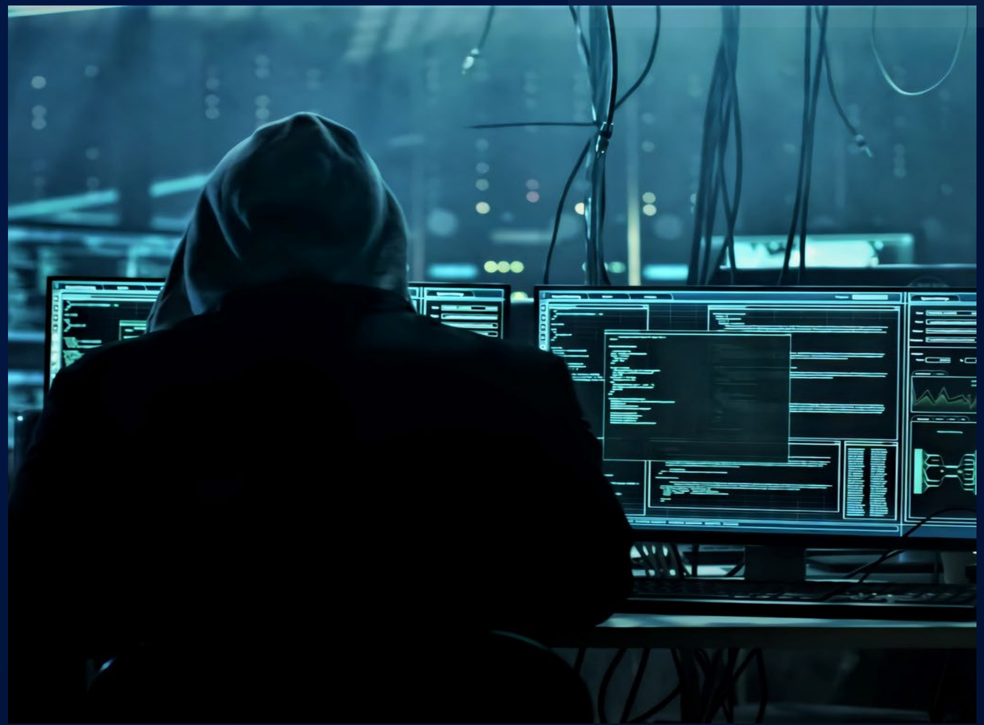
Integrity
Integrity is about ensuring that data has not been tempered with and therefore, can be trusted. It is correct, authentic and reliable.

Availability
Availability means that networks, systems and applications are up and running. It ensures that authorized users have timely, reliable access to resources when they are needed.

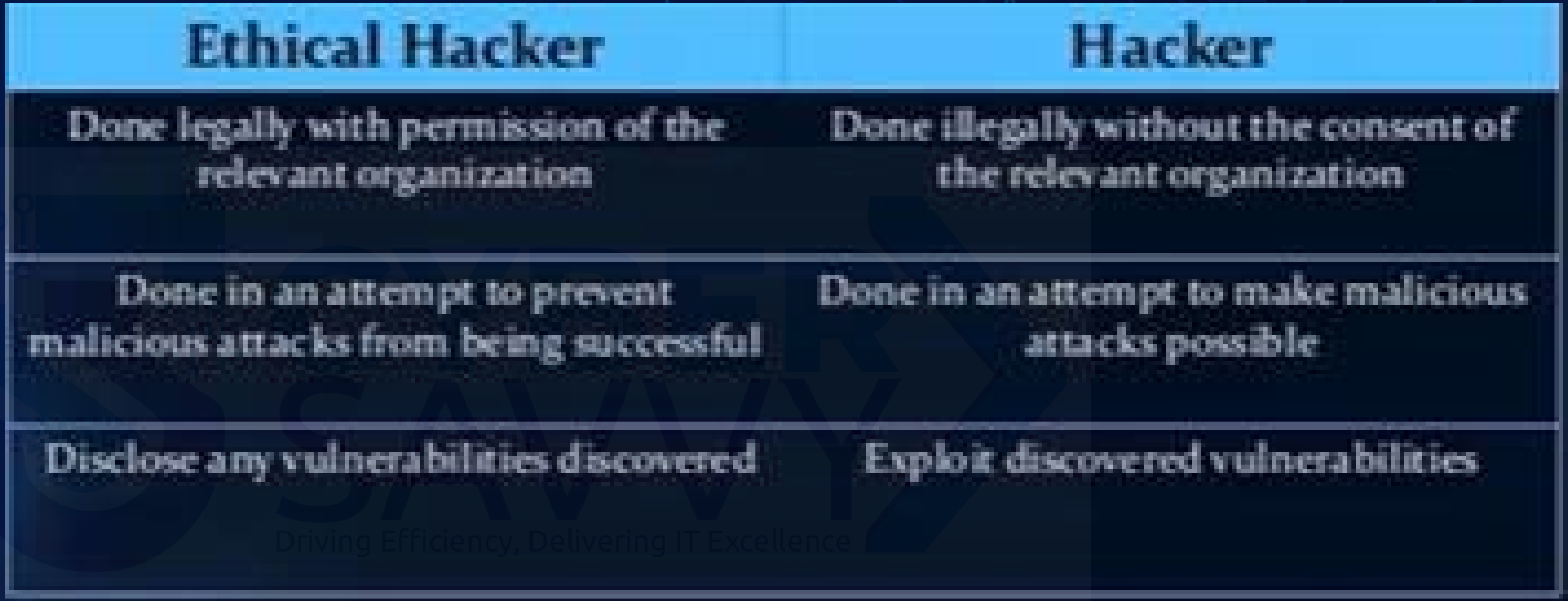
ATTACKER

Malicious actor who seeks to exploit computer systems with the intent to change, destroy, steal or disable their information, and then exploit the outcome.



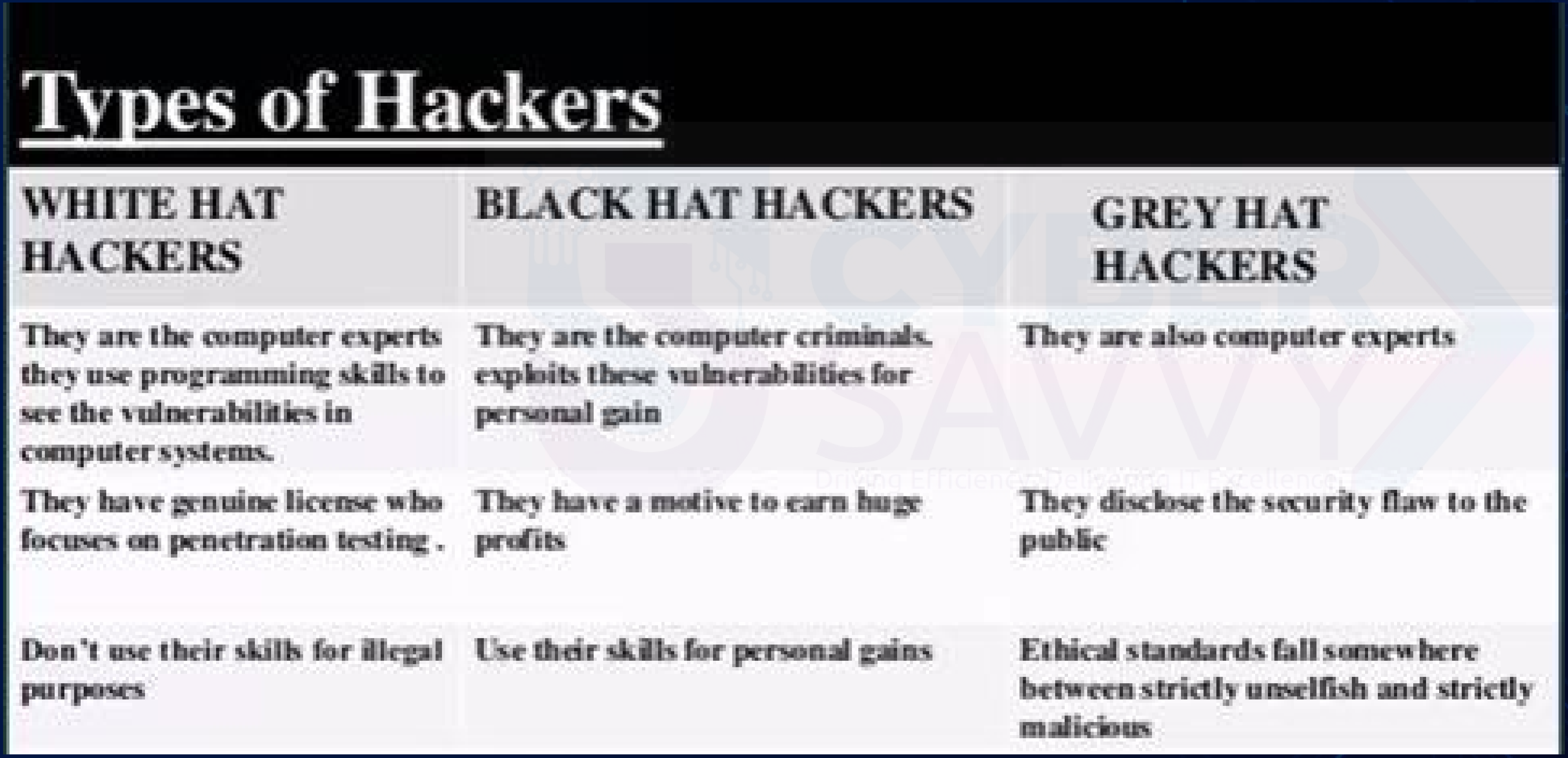


Ethical Hacker Vs. Hacker



Ethical Hacker	Hacker
Done legally with permission of the relevant organization	Done illegally without the consent of the relevant organization
Done in an attempt to prevent malicious attacks from being successful	Done in an attempt to make malicious attacks possible
Disclose any vulnerabilities discovered	Exploit discovered vulnerabilities

Types of Hackers



Types of Hackers

WHITE HAT HACKERS	BLACK HAT HACKERS	GREY HAT HACKERS
They are the computer experts they use programming skills to see the vulnerabilities in computer systems.	They are the computer criminals. exploits these vulnerabilities for personal gain	They are also computer experts
They have genuine license who focuses on penetration testing .	They have a motive to earn huge profits	They disclose the security flaw to the public
Don't use their skills for illegal purposes	Use their skills for personal gains	Ethical standards fall somewhere between strictly unselfish and strictly malicious

Reconnaissance

Reconnaissance
It is practice of covertly discovering and collecting information about target system.

How Reconnaissance Works?

Reconnaissance generally follows seven steps:

1. Collect initial information
2. Determine the network range
3. Identify active machines
4. Find access point and open ports
5. Fingerprint the operating system
6. Uncover services on ports
7. Map the network

Using these steps, an attacker will aim to gain following information about a network

File permissions
Running network services
OS Platforms
User account information

One of the most common techniques involved with reconnaissance is port scanning

Types Of Reconnaissance

Active Reconnaissance & Passive Reconnaissance

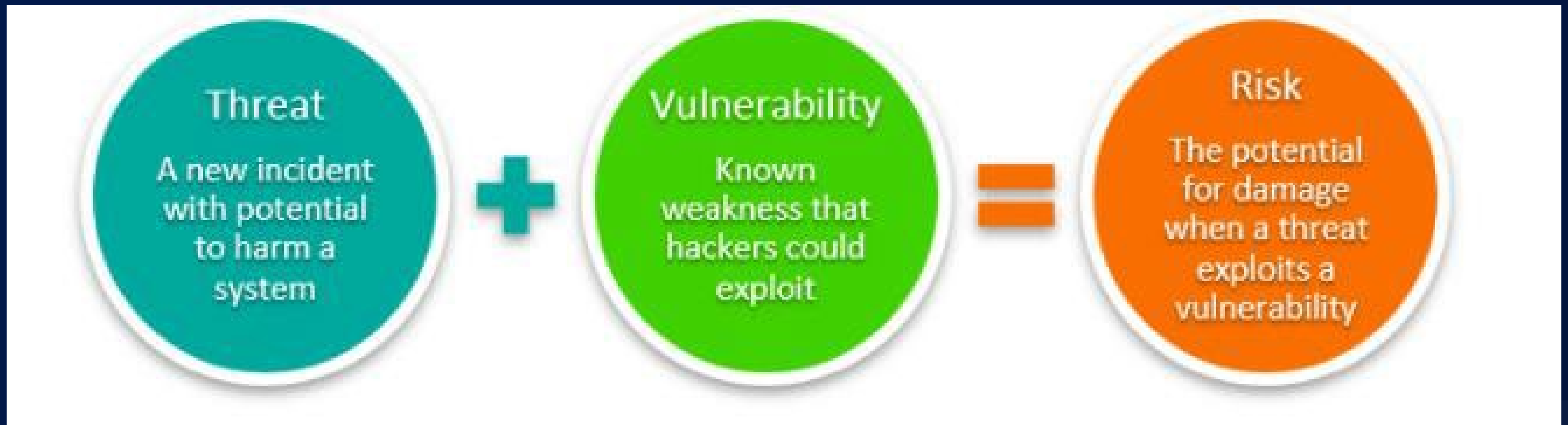
Active Reconnaissance
With active reconnaissance, hacker interacts directly with computer system and attempt to obtain information through techniques like automated scanning or manual testing and tools like ping and netcat.

Passive Reconnaissance
Passive reconnaissance gathers information without directly interacting with target system.

How to Prevent Reconnaissance
Organizations can use penetration testing to determine what their network would reveal in the event of a reconnaissance attack. During testing, organizations can deploy port scanning tools (which scan large networks and determine which hosts are up) and vulnerability scanners (which find known vulnerabilities in the network).

SIEM solutions can also detect source IPs that are running a port scanning tool in your network.

Difference Between Threat, Risk & Vulnerability.



Threat

A new incident with potential to harm a system

+

Vulnerability

Known weakness that hackers could exploit

=

Risk

The potential for damage when a threat exploits a vulnerability

Asset
People, property, and information. People may include employees and customers along with other invited persons such as contractors or guests. Property assets consist of both tangible and intangible items that can be assigned a value. Intangible assets include reputation and proprietary information. Information may include databases, software code, critical company records, and many other intangible items.

In simple words, An **asset** is what we’re trying to protect.

Threat
Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.

In Simple words,
A **threat** is what we’re trying to protect against.

Vulnerability
Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset.

In simple words, a **vulnerability** is a weakness or gap in our protection efforts.

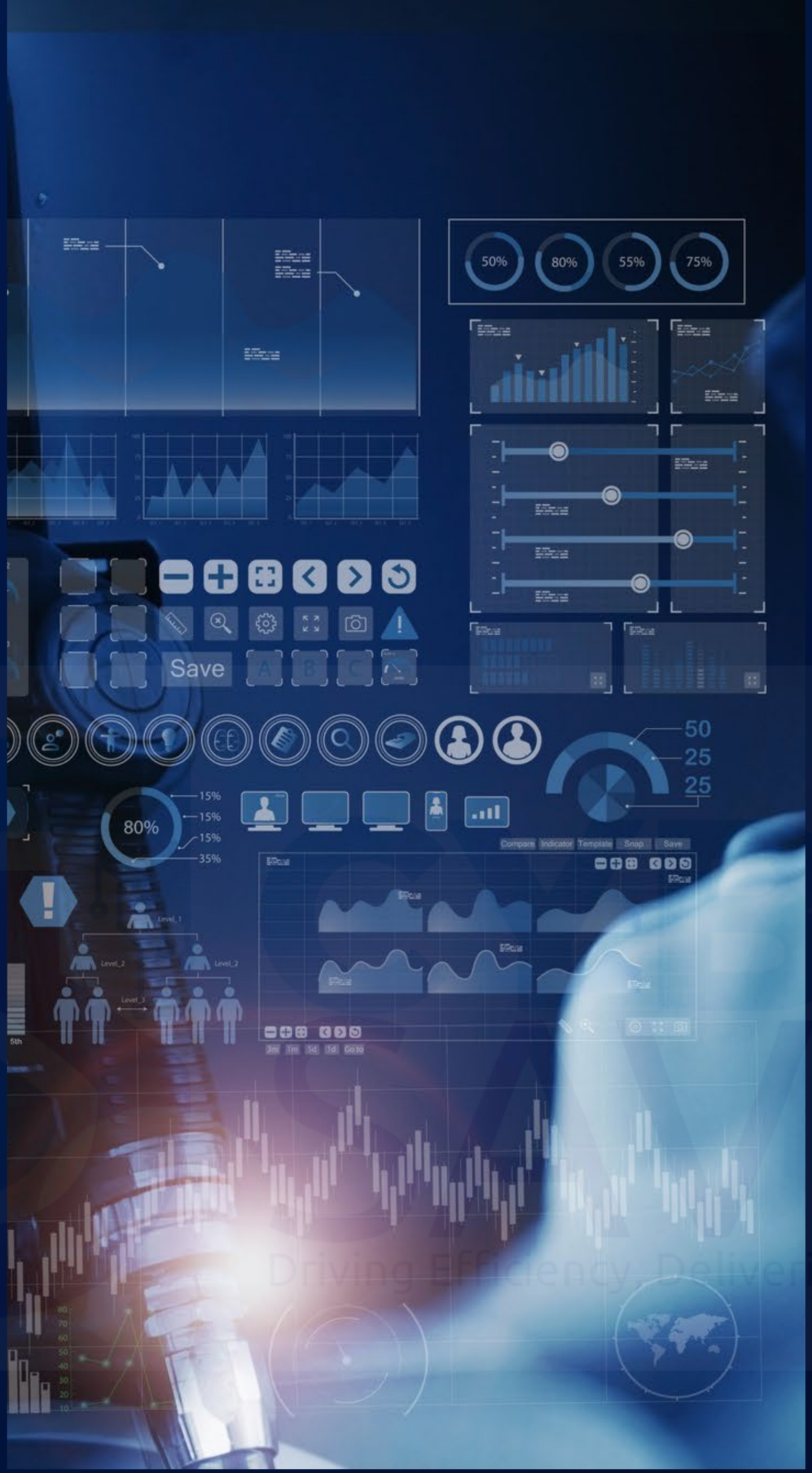
Risk
The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.

In simple words, **Risk** is the intersection of assets, threats, and vulnerabilities

Relation Between Asset, Threat, Vulnerability & Risk
A + T + V = R

That is

Asset + Threat + Vulnerability = Risk



Thank You !!

☎ +1-240-422-8488

THANK YOU

https:/cyberlyusa.com/