**QUIZ 1 – WHAT COLOR IS MY HAT? (WHITE / GREY / BLACK)**

**QUESTION 1**

While carrying out some research, this attacker stumbled across a security vulnerability on an organization’s network that they are authorized to access

**ANSWER – WHITE HAT**

**QUESTION 2**

This attacker used malware to compromise a company’s system and steal credit card information that was then sold to the highest bidder

**ANSWER – BLACK HAT**

**QUESTION 3**

This attacker ‘s job is to identify weaknesses in a company’s computer system

**ANSWER – WHITE HAT**

**QUESTION** **4**

Tis attacker transferred $10 million into their bank account using customer account and PIN credentials gathered from recordings

**ANSWER – BLACK HAT**

**QUESTION 5**

After hacking into ATM systems remotely using a laptop, this attacker worked with the ATM manufacturers to resolve the identified security vulnerabilities.

**ANSWER – GREY HAT**

**QUIZ 2**

What level of cyber protection does each of the following factors require?

1. Your Identity? (Government / Personal / Organizational)

**ANSWER – PERSONAL**

1. A customers Database? (Government / Personal / Organizational)

**ANSWER – ORGANIZATIONAL**

1. Economic stability? (Government / Personal / Organizational)

**ANSWER – GOVERNMENT**

1. An individual user profile on a social network site is an example of an (online / offline) identity? \_\_\_\_\_\_\_

**ANSWER – ONLINE**

1. Which of the following pieces of information would be classified as personal data? (NIN / Driver license number / Date and place of birth / Job title / IP address)

**ANSWER – NIN / DRIVER LICENSE NUMBER / DATE AND PLACE OF BIRTH**

1. Your neighbor tells you that they don't have an online identity. They have no social media accounts and only use the Internet to browse. Is your neighbor, right? (Yes / No)?

**ANSWER - NO**

1. What are the 3 foundational principles for protecting information systems as outlined in the McCumber Cube? (Access / Integrity / Scalability / Availability / Confidentiality / Intervention)?

**ANSWER – CONFIDENTIALITY / INTERGRITY / AVAILABILTY**

1. What is a key motivation of a white hat attacker?

**ANSWER - A primary motivation of a white hat attacker is to enhance cybersecurity. Ethical hackers, or white hat attackers, leverage their expertise to pinpoint vulnerabilities within systems, networks, and applications. Their primary objective is to aid organizations in bolstering their security defences by pre-emptively identifying and rectifying potential security weaknesses prior to malicious exploitation. White hat attackers typically operate within legal and ethical frameworks, collaborating with organizations under mutual consent to strengthen their security measures.**

1. Why might internal security threats cause greater damage to an organization than external security threats?

**ANSWER – Internal security threats have the potential to cause greater damage to an organization than external security threats due to several factors:**

**1. Insider Knowledge: Internal threats often come from employees or individuals with intimate knowledge of the organization's systems, processes, and sensitive information. This insider knowledge enables them to exploit vulnerabilities more effectively and navigate security measures with greater ease.**

**2. Access to Critical Systems: Internal actors typically have legitimate access to the organization's critical systems, databases, and networks as part of their job roles. This level of access allows them to inflict significant damage, steal sensitive data, or disrupt operations without the need to bypass external security measures.**

**3. Trust and Privilege: Internal threats operate within an environment of trust and privilege, which can make their malicious activities harder to detect. They may abuse their positions of authority or misuse their access privileges to carry out attacks without raising suspicion.**

**4. Lack of External Monitoring: External security measures such as firewalls, intrusion detection systems, and perimeter defences are often designed to detect and mitigate external threats. However, these measures may be less effective against internal threats that originate from within the organization's trusted network, making them harder to detect and mitigate.**

**5. Potential for Insider Threats: Internal threats may be motivated by a variety of factors such as financial gain, revenge, or ideology. This makes them more unpredictable and potentially more dangerous than external threats, which are often driven by more predictable motives such as financial gain or espionage.**

1. Describe cybersecurity in your own way?

**ANSWER – To me, Cybersecurity is like having a lock on your digital stuff. It's all about keeping your online information safe from bad guys who try to break in and mess things up. Just like you lock your door to keep your home safe, cybersecurity helps keep your computer, phone, and all your online accounts secure from hackers and other troublemakers.**