Wesley Kamotho – DCS-03-8392/2023

1. Discuss four ways AI and machine learning enhance cybersecurity defenses, and explain three new security risks they introduce.

Benefits

- Predictive analytics – AI through reliable historical data can predict potential vulnerabilities and act to prevent them.
- Threat detection – AI is able tp process large amounts of a data and detect anomalies and respond accordingly.
- Automated security processes – Processes that enforces security mechanism on a system can be automated using AI allowing human resources to focus on other tasks.
- Behavioural analytics – ML can be implemented to detect abnormal user activity and respond to prevent an attack.

Risks

- AI powered attacks – Attackers can use the AI and ML for more sophisticated attacks.
- Data privacy concerns – AI and ML require alot of data which can lead to loss of sensitive info in case of a bleach.
- Adversarial attacks – Attacks can manipulate the AI or ML model with malicious leading to incorrect decisions leaving the system susceptible to attacks.

2. Discuss three most effective security controls for personal devices, and explain how individuals can implement them to protect against emerging cyber threats.

- Timely software updates – This ensures that the device is up to date with current attacks and ready to prevent them.
- Using strong password – Through strong passwords, access to the device can be prevented by an authorized user.
- Using of antimalware software – This can prevent malicious attack on the device.

3. Explain three vulnerabilities and threats in wireless networks.

- Eavesdropping – Using specialized tools, attacks can intercept the network's traffic.
- Weak encryption protocols – Weak protocols are easy to crack which makes it easier for an attack.
- Rogue access points – Attackers can set up a fake access point through which they can intercept the network's sensitive data.