KCA

UNIVERSITY

~ 1989 ~

**CYBER SECURITY**

**BISF 3103**

**CAT 2**

**EMMANUEL KIPKEMOI SIGEI**

**REG NO – 20/03807**

**CAMPUS: MAIN**

**FULL TIME**

**PRESENTED TO Mr. MARTIN LUTHER**

## QUESTION ONE: Ways in which Organizations can use AI to enhance Cybersecurity.

1. ***Threat Detection and Response*** - AI can be used to detect and respond to cyber threats more quickly and effectively eg through the analysis of Network Traffic for suspicious patterns by using Machine Learning algorithms.
2. ***Identifying and Fixing Vulnerabilities*** – Artificial intelligence may be used to scan systems and networks for vulnerabilities and repair them. It can be used to automate mitigation procedures like software updates.
3. ***Incident Response*** – After security incidents occur, AI can be used to assess the damage done and automatically implement remedies such as blocking malicious activities.
4. ***Behaviour Analysis*** – Based on the activities of users on the system, AI can be used to detect anomalies in the patterns of users thus detecting insider threats and user accounts on the system that might be compromised.
5. ***Intelligence Gathering*** – Artificial Intelligence can be used to collect data from security sources such as the CVE Database and use that information to come up with trends and patterns which can then be used to aid the organizations to better understand the cyber security landscape.
6. ***Asset Management*** – Artificial Intelligence can be used to continuously and automatically discover devices and users on the computer system in the organization which can then give insights for risk management and compliance levels. (Kaur, 2016)

## QUESTION TWO: The challenge of Advanced Persistent Threats (APTs) to Cyber Security Practitioners and how they can be mitigated.

APTs are sophisticated, targeted cyberattacks sponsored by organized crime groups or countries, with the primary aim of gaining unauthorized access to critical information and systems for financial gain or espionage. They are designed to remain undetected for long periods of time and are usually highly organized and are typically backed by nation-states or other sophisticated organizations.

### *Challenges that Cyber Security Practitioners face in relation to APTs.*

1. APTs are designed to be stealthy and persistent thus enabling them to avoid detection for extended periods of time thus posing a challenge to the cyber security practitioners in terms of identifying them on systems.
2. APTs are used to exfiltrate sensitive data from systems that ends up in losses and can end up causing damage to systems.
3. Due to their level of sophistication, the techniques they use such as zero-day exploits very easily outsmart security measures that have been implemented by the cyber security practitioners.
4. Based on the fact that APTs are very targeted, they are tailormade most times therefore focusing on very specific vulnerabilities in the victim's computer system.
5. Cyber Security practitioners find it hard to attribute the attacks to specific groups or individuals therefore making it hard to discover the sources of the attacks.

***Mitigation Techniques.***

These challenges can be mitigated by:

1. Identifying anomalies in Network Traffic by using threat detection systems to analyse behaviour and patterns that might be suspicious.
2. There should be awareness training and upskilling of employees to educate them on best practices for cyber security thus reducing the susceptibility levels to Social Engineering attacks.
3. Various Cyber Security tools such as Firewalls and intrusion detection systems should be used to create a layered security approach hence providing more protection for computer systems.
4. Cyber Security should stay updated on security intelligence published on platforms such as the CVE Database to enable them to stay aware of current threats in the cyber security landscape.
5. Robust and comprehensive Incident response plans should be developed and implemented to aid in quick recovery after APT Attacks.
6. User privileges on the computer system should be on a need basis, allowing users to view only information that is relevant to them