

1. Discuss **five** impacts of AI and Machine Learning on Security.
 - a) Automated threat detection – Systems with AI integration have the capability to detect threats in real time thus preventing potential attacks.
 - b) Anomaly detection – AI and ML analyze vast amounts of data and are able to detect any patterns of anomaly and take the necessary measures.
 - c) Adversarial attacks – As AI and ML are used to secure systems, cybercriminals also adopted the capabilities of AI and ML to sophisticate their attacks.
 - d) Predictive analysis – ML can be used to predict potential threats by analysing historical data and identifying patterns before an attack.
 - e) Data quality – AI and ML models rely of the quality of data they are trained on to work effectively, thus if the quality is subpar then the effectiveness of the measures imposed by the model become ineffective leaving the system vulnerable.

2. Identify **one** Intrusion Detection/Prevention tool and describe how it works.

- a) Cisco Secure IPS

-It leverages Cisco Talos which are threat intelligence networks to provide up-to-date threat information. Also new policies and signatures are received every 2 hours to ensure the system is always equipped to handle the latest threat.

-It also monitors the network's traffic to detect and prevent malicious activities.

-Threats that come up are delt with immediately due to it's real-time response thus preventing the attack