**Activity 1**

**Hamza Ghariani 4 NIDS 1**

[**Link Video**](https://www.youtube.com/watch?v=IiWFMIgKaqQ)

* **What is DiD?**

DiD stands for Defense in Depth, which is a cybersecurity strategy that involves using multiple layers of defense to protect against potential attacks or security breaches. The goal of DiD is to make it more difficult for attackers to penetrate a network by adding layers of security that must be bypassed in order to gain access to sensitive data or systems.

* **What are the 3 key layers of the defense in DiD?**

The three key layers of defense in DiD are as follows:

**Physical Security**: This layer involves controlling physical access to equipment and facilities to prevent unauthorized access or theft of hardware, such as servers or network devices.

**Perimeter Security**: This layer involves protecting the perimeter of the network using technologies such as firewalls, intrusion detection systems, and other network security devices. The goal of perimeter security is to prevent unauthorized access to the network.

**Application Security**: This layer involves securing individual applications and data by implementing secure coding practices, access controls, and other measures to protect against vulnerabilities and exploits.

* **What is the difference between a layered security and a DiD strategy?**

While both layered security and DiD involve using multiple layers of defense, the main difference between the two is their approach to security. Layered security typically involves implementing different security technologies and tools at different layers of the network, while DiD involves using a combination of technologies, policies, and procedures to create a comprehensive security strategy.

DiD emphasizes the importance of having multiple layers of defense that work together to protect against threats, while layered security focuses more on the individual components of the security system. DiD is considered a more holistic approach to security, as it involves considering all aspects of the system and how they work together.

* **What is the relation between the DiD and Regulations?**

Several regulations and compliance frameworks, such as the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), and the General Data Protection Regulation (GDPR), require organizations to implement a DiD strategy as part of their overall security program.

DiD is considered a best practice in the cybersecurity industry, and many regulations require organizations to implement a DiD strategy to protect sensitive data and systems from potential threats. By implementing a DiD strategy, organizations can help ensure that they are in compliance with applicable regulations and can avoid potential fines and legal consequences for data breaches or other security incidents.