**Module 2 Technologies & Tools**

**2.1 Network Components P3**

**Network Access Control (NAC)**

* Uses set of protocols to define & implement policy that describes how to secure access to network nodes by devices upon initial access (IEEE 802.1x standard)
* Components:

1. Access Requester (AR) – device that requests access. Assessment of device self-performed/delegated to another system
2. Policy Decision Point (PDP) – system that assigns policy based on assessment. PDP determines access
3. Policy Enforcement Point (PEP) – device that enforces policy. Device can be switch, firewall or router

* Agent vs. Agentless – is agent application end-point? Yes, for corporate-devices
* Host Health Checks

1. Health of end-point
2. Is antivirus enabled?

* Dissolvable vs. permanent

**Security Information & Event Management (SIEM)**

* SIEM tools collect, correlate & display data feeds that support response activities
* Functions:

1. Log aggregation on centralised server
2. Centrally managing security events
3. Correlating & normalising events for context & alerting
4. Reporting on data gathered from various apps

* Benefits

1. Aggregation
2. Correlation
3. Automated alerting & triggers
4. Event duplication
5. Time synchronisation
6. WORM – Write-Once, Read-Many protection

**Data Loss Prevention (DLP)**

* AKA data Leakage Protection
* Prevent sensitive information from physically/logically leaving corporate systems
* Designed to detect & prevent unauthorised use & transmission of confidential information
* Network – Content-Filtering (Proxy)
* System – Application white-listing
* Hardware – USB Blocking
* Cloud data

**SSL/TLS Accelerators**

* SSL Offloading – process of shifting burden of encrypting & decrypting traffic sent via SSL from web server to another device
* Accepts SSL/TLS connections from end-point & sends connection to server unencrypted
* Associated with Load Balancers

**Gateways (Mail & Media)**

* Centralisation & routing
* Encryption
* Spam filters – Inbound & Outbound
* Proxy servers (media)

**Hardware Security Module (HSM)**

* Hardware-based encryption that manages digital keys, accelerates cryptographic processes & provides strong access authentication
* *Trusted Platform Module (TPM)* used to assist with cryptographic key generation