Assessment Description

Word count: 4000

Scenario:

Incident Report: Unauthorized Access to Engineering Workstation

Location: Petrochemical Facility, Urban Area Adjacent to City

Incident Summary:

A site engineer has reported a significant concern regarding the modification of critical project documentation. An immediate investigation was launched, revealing the following key findings:

- Remote Access Identified: It has been confirmed, with a high degree of certainty, that the engineering workstation was accessed remotely without authorization.

- Unauthorized Modifications: Several parameters within the project file were altered during this unauthorized access.

Details:

- Affected System: Engineering Workstation

- Nature of Modification: Unauthorized changes to critical project parameters

Investigation Outcomes:

- Source of Access: The investigation has traced the remote access to [insert findings if available], confirming the breach of the engineering workstation.

- Extent of Changes: A thorough review has identified the specific parameters thatwere modified, and their potential impact on the project is currently being assessed.

Tasks:

You have been hired as a security engineer to ensure the security of the IT and OT systemsand instructed to perform an essay that thoroughly addresses the following tasks:

Task Instructions

1. Network Setup and Configuration:

- Network Deployment: Set up the network infrastructure as per the provided network topology diagram.
- Endpoint Configuration: Download the provided virtual machines (VMs) from the designated folder and configure each endpoint according to the specifications outlined in the network topology.

2. Security Assessment:

- OT Network Analysis: Conduct a comprehensive security assessment of the Operational Technology (OT) network.

- Threat Identification: Identify and document potential security threats and vulnerabilities within the OT network.

3. Firewall Rule Recommendations:

- Rule Development: Suggest firewall rules to mitigate the identified security threats. These rules should be designed to control traffic, restrict unauthorized access, and protect critical assets within the OT network.

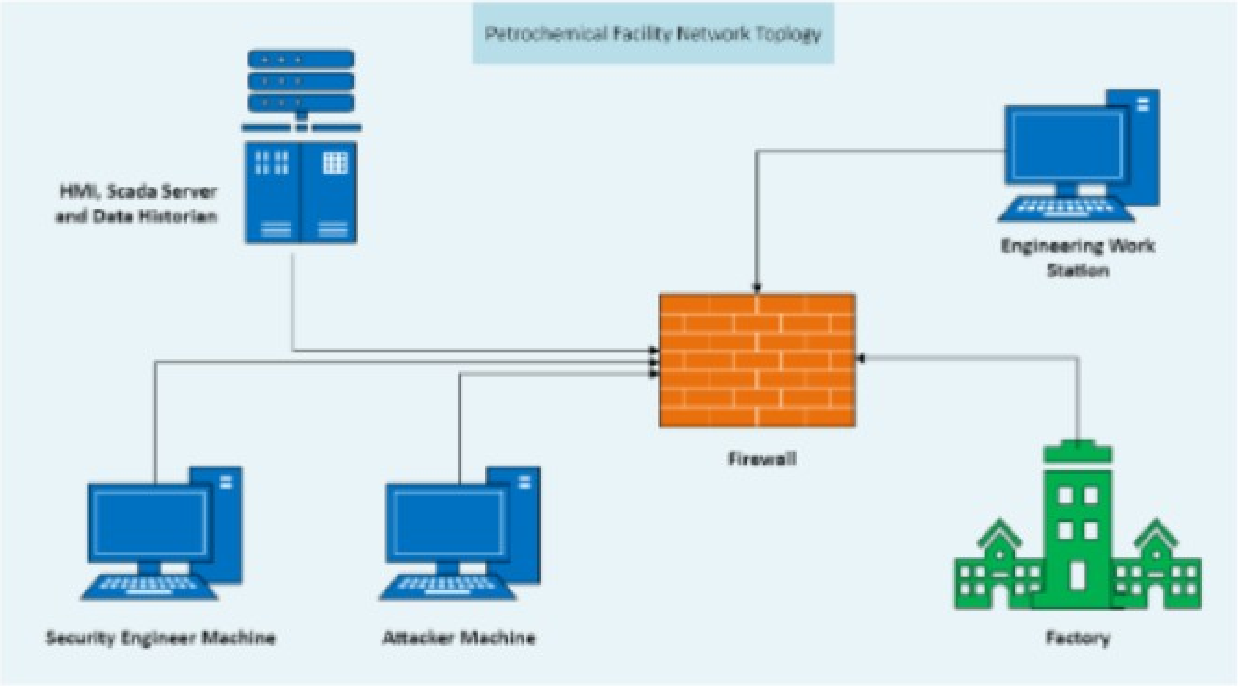
4. Preventative Measures:

- Security Protocol Enhancement: Propose recommendations to enhance existing security protocols.

- Incident Prevention: Develop and implement strategies to prevent future security incidents, ensuring the long-term protection of the OT network.

5. Incident Simulation:

- Attack Simulation: Utilize the attacker machine to replicate the incident in a controlled environment. This will involve simulating the steps taken by the attacker, including gaining unauthorized access, manipulating the engineering workstation, and altering the project file parameters, this to understand the tactics, techniques, and procedures (TTPs) used by the attacker.


Petrochemical Facility Network Toplogy
HMI, Scada Server and Data Historian
Engineering Work Station
Firewall
Security Engineer Machine
Attacker Machine
Factory

Marking Scheme	**Marks Available**
1. Network Setup and Configuration: • Network Deployment: Set up the network infrastructure as per the provided network topology diagram. • Endpoint Configuration: Download the provided virtual machines (Vms) from the designated folder and configure each endpoint according to the specifications outlined in the network topology	**20**
2. Security Assessment: • OT Network Analysis: Conduct a comprehensive security assessment of the Operational Technology (OT) network. • Threat Identification: Identify and document potential security threats and vulnerabilities within the OT network.	**20**
3. Firewall Rule Recommendations: • Rule Development: Suggest firewall rules to mitigate the identified security threats. These rules should be designed to control traffic, restrict unauthorized access, and protect critical assets within the OT network.	**10**

4. Preventative Measures: • Security Protocol Enhancement: Propose recommendations to enhance existing security protocols. • Incident Prevention: Develop and implement strategies to prevent future security incidents, ensuring the long-term protection of the OT network	**20**
5. Incident Simulation: • Attack Simulation: Utilize the attacker machine to replicate the incident in a controlled environment. This will involve simulating the steps taken by the attacker, including gaining unauthorized access, manipulating the engineering workstation, and altering the project file parameters, this to understand the tactics, techniques, and procedures (TTPs) used by the attacker.	**20**
6. Report structure, spelling, grammar and referencing.	**10**
Total	**100**