SECTION A

QUESTION 1

1.1 (a) Important Factors to Consider When Choosing Security Standards for the Enterprise

* **Compliance Requirements**: When choosing security standards, it’s crucial to consider legal and regulatory requirements like GDPR or HIPAA, as these can prevent fines and help avoid legal issues.
* **Flexibility and Scalability**: Standards should be flexible and scalable so they can adapt to changes within the enterprise, whether it’s new technologies, growth, or changes in the threat landscape.
* **Compatibility with Current Infrastructure**: Security standards should work well with the enterprise’s current systems and technology. This avoids issues with integration and reduces the need for costly adjustments.
* **Alignment with Risk Management Goals**: The standards should directly address the enterprise’s security risks, ensuring that all critical risks are adequately covered to reduce potential security threats.

(b) Interoperability Issues with Legacy Systems

* **Incompatibility with Newer Security Standards**: Older systems might not support modern security standards, which can create gaps in security, like the inability to use newer encryption methods.
* **Difficulty Integrating with Newer Systems**: Legacy systems might lack necessary APIs or integration features, making it hard to connect them with newer security tools, which can lead to security inconsistencies.
* **Higher Vulnerability Risks**: Legacy systems often use outdated software that may not get security updates anymore, increasing the risk of exposure to new threats.
* **Resource Constraints**: Many legacy systems don’t have the processing power or storage needed for advanced security monitoring, making it difficult to apply modern security measures.

(c) Risks of Acquiring a Smaller Competitor

* **Data Security Issues**: Integrating data from the acquired company may introduce vulnerabilities, especially if they have less robust security measures.
* **Inconsistent Security Policies**: The smaller competitor may not have security standards that align with Delware Inc., leading to gaps in protection and increased risk.
* **Cultural Differences in Security**: Different levels of security awareness and practices may exist, meaning additional training could be needed to bring everyone up to the same security standard.
* **Potential Insider Threats**: Employees from the smaller company may not fully understand or comply with Delware Inc.’s security policies, increasing the likelihood of accidental or intentional security breaches.

(d) Obstacles in Integrating IDS, IPS, and SIEM for Better Resilience

* Data Format Issues: Since the IDS, IPS, and SIEM tools come from different vendors, they may use incompatible data formats, making it challenging to standardize and analyze data across systems.
* Delays in Data Correlation: Real-time analysis could be delayed because of differing speeds or capabilities among the systems, which could reduce the effectiveness of threat detection.
* Maintenance Complexity: Managing three different security tools requires more time and resources, and the need for specialized knowledge might slow down issue resolution.
* Additional Integration Costs: Integrating the systems may require extra tools or APIs, which can increase costs and delay implementation of better threat detection practices.

1.2 (a) Advantages of Using IPv6 Over IPv4

* **Expanded Address Space**: IPv6 provides a vastly larger address space (128-bit addresses compared to IPv4’s 32-bit), which supports the growing number of internet-connected devices without needing Network Address Translation (NAT).
* **Enhanced Security**: IPv6 was designed with IPsec as a fundamental feature, allowing for better security at the network layer, including data confidentiality, integrity, and authentication.
* **Efficient Routing**: IPv6 reduces the size of routing tables, allowing for more efficient and faster routing. This is due to its simplified header format and the ability to aggregate addresses more effectively.
* **Auto-Configuration**: IPv6 supports stateless address autoconfiguration (SLAAC), which simplifies network management by allowing devices to self-configure without the need for a DHCP server.

(b) Security Issues to Consider When Implementing an 802.1x Infrastructure

* **EAP Method Vulnerabilities**: The Extensible Authentication Protocol (EAP) used in 802.1x can have vulnerabilities depending on the chosen method, potentially exposing the network to risks like man-in-the-middle attacks if not properly secured.
* **Certificate Management**: 802.1x often requires digital certificates for authentication. Poor certificate management practices, such as expired or compromised certificates, can reduce security and hinder access.
* **Device Spoofing Risks**: Attackers may attempt to bypass 802.1x security by spoofing authorized devices. Without proper monitoring, this could allow unauthorized access to the network.
* **Denial of Service (DoS) Attacks**: Attackers can exploit 802.1x’s authentication process to launch DoS attacks by repeatedly sending authentication requests, potentially overwhelming the network and causing disruptions.

(c) Thoughts and Concerns on Switching to a Mesh Configuration

* **Improved Redundancy**: A mesh configuration provides multiple paths for data, which can help ensure network availability and reduce the risk of downtime if a link or node fails.
* **Increased Complexity**: Mesh networks are more complex to design, deploy, and maintain. This complexity could make troubleshooting more challenging and require more skilled personnel.
* **Cost Implications**: Implementing a mesh network could require additional infrastructure investment, especially in purchasing additional devices to support the multiple connection paths, which could be costly.
* **Security Concerns**: More connection points and pathways may introduce new security risks, such as additional points of entry for attackers, making it essential to deploy strong security measures across all nodes.

(d) Security Implications of Using Software-Defined Networking (SDN)

* **Centralized Control Risks**: SDN’s reliance on a central controller for managing network traffic creates a single point of failure, which could be exploited by attackers to compromise the entire network.
* **Increased Attack Surface**: Since SDN controllers communicate frequently with switches and routers, attackers could intercept or manipulate this traffic, gaining unauthorized access or disrupting network functions.
* **Authentication and Authorization Challenges**: Managing access to the SDN controller is critical. Without strict authentication and authorization controls, unauthorized users could access and manipulate network configurations.
* **Potential for Malicious Configuration**: An attacker who gains access to the SDN controller could deploy malicious configurations or policies that disrupt network traffic, potentially leading to data breaches or service outages.

SECTION B











