Southern New Hampshire University

CYB 310 Project Two Stepping Stone Template

Directions: Complete this template by replacing the bracketed text with the relevant information.

I. IDS Best Practices Table

IDS Component	What Does It Detect?	What Could a Threat Actor Accomplish if You Were Not Monitoring This Component?	Tenet of the Security (CIA) Triad Most Affected
Network Intrusion Detection System (NIDS)	Unusual traffic patterns or volume, such as large data transfers or spikes in traffic at unusual times.	A threat actor could potentially exfiltrate sensitive data undetected, leading to data breaches.	Confidentiality
Host Intrusion Detection System (HIDS)	Changes in critical system files or registry settings, unauthorized application activity.	Malware installation or rootkit placement without detection, allowing persistent access to the host.	Integrity
Signature-Based Detection	Known attack patterns and malware signatures.	Known attacks could succeed, leading to system compromise and data loss.	Integrity
Anomaly-Based Detection	Deviations from a baseline of normal activity, potentially indicating novel or zero-day exploits.	New and unknown threats could cause damage before being detected by other means.	Availability
Behavior-Based Detection	Suspicious behavior by monitoring user activities and data access patterns.	Insider threats or compromised accounts could lead to data theft or sabotage without detection.	Confidentiality

II. Application Question

For a small business startup in the finance sector, implementing strong network protection is crucial due to the sensitive nature of financial data and the high stakes in maintaining client trust and regulatory compliance. Considering this, I recommend the following IDS components:

1. Network Intrusion Detection System (NIDS)

Justification: A NIDS is critical for real-time monitoring of all network traffic, which includes incoming and outgoing data. By analyzing this traffic, the NIDS can quickly identify patterns that may signify hacking attempts, such as DDoS attacks, unauthorized data transfers, or network scanning for vulnerabilities. This is especially crucial for a finance organization since it makes it possible to identify and stop any possible incursion before any harm occurs. Furthermore, given the regulatory requirements to protect client data, a NIDS will aid in compliance by providing logs that can be reviewed during audits to demonstrate diligence in network security.

2. Behavior-Based Detection

Justification: This part is your early warning system, focusing on monitoring the behavior of users and the network to detect anomalies that deviate from established patterns of normal activity. In the finance sector, where insider threats or compromised user credentials pose a significant risk, behavior-based detection can provide early warnings of suspicious activities. This could include unusual access patterns to sensitive data or abnormal transaction volumes, which might indicate someone is attempting to exfiltrate data or commit fraud. Implementing this type of IDS component enhances security by not only catching threats from external actors but also by providing a safeguard against potential internal security breaches.