# CYB 310 Project Two Stepping Stone Template

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

1. 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** |
| --- | --- | --- | --- |
| Sensors | Collect raw data from network traffic, logs, or host activity | Threat actors could infiltrate systems undetected, bypassing initial visibility | Confidentiality |
| Detection Engine | Analyzes data using signature-based, anomaly-based, or heuristic methods | Attackers could exploit known vulnerabilities or zero-days without triggering alerts | Integrity |
| Response System | Triggers alerts, logs events, or initiates automated actions (e.g., blocking IPs) | Malicious activity could persist without containment, leading to prolonged compromise | Availability |
| Management Console | Interface for configuring IDS, reviewing alerts, and managing policies | Attackers could alter IDS settings, disable alerts, or hide their tracks | Confidentiality |
| Database & Storage | Stores logs, signatures, and historical data for analysis and correlation | Adversaries could tamper with logs, erase evidence, or poison detection models | Integrity |

1. Application Question
   1. For a small finance-sector startup with one office location, I recommend implementing network-based sensors and a hybrid detection engine as part of their IDS setup. Network-based sensors are essential because they monitor traffic at critical points in the network, such as between the internal systems and the internet. This allows the business to detect suspicious activity like unauthorized access attempts, phishing payloads, or data exfiltration. Given the sensitivity of financial data, having visibility into network traffic is crucial for early threat detection. The second component, a detection engine that combines both signature-based and anomaly-based methods, offers a balanced approach to identifying threats. Signature-based detection quickly flags known attacks, while anomaly-based detection helps uncover unusual behavior that could indicate zero-day exploits or insider threats. This hybrid approach is especially valuable for small teams without dedicated security analysts, as it automates much of the threat identification process. Together, these components provide a cost-effective, scalable foundation for network protection, helping the startup safeguard client data and meet regulatory requirements without overwhelming their resources.