Southern New Hampshire University

CYB 310 4-3 Project Two Stepping Stone: Exploring IDS Best Practices

Andree Salvo
Southern New Hampshire University
CYB 310 – 13007
Instructor: Raschid Muller

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
Anomaly-Based Detection	It can detect unusual network traffic, behavior deviations, and threats.	Threat actors can perform reconnaissance, brute-force attacks, and even data exfiltration without setting off an alarm.	Confidentiality
Alert & Logging System	Alerting and Logging can generate and record alerts for suspicious events.	Attackers can freely explore any network and gain high-privileged access without being noticed or caught.	Integrity
Log Analysis	Log Analysis detects network logs, identifying patterns that deviate from normal behavior or that can match known attack signatures.	A threat actor can cover their tracks by deleting or altering evidence and exfiltrating data.	Integrity
Network Traffic Analysis	Suspicious patterns from the data flow, signs of a DDoS attack, port scanning, or data exfiltration.	An attacker can steal sensitive data, disrupt services, or set up hidden channels without being detected.	Confidentiality + Availability
Host-Based Monitoring	Network traffic analysis detects unusual patterns, protocol misuse, and indicators of activities such as scanning, data theft, or DDoS attacks.	An attacker could leak the data, map your network, or even take your Wi-Fi down without you noticing.	Confidentiality

II. Application Question

A. A small business start-up in the finance sector with one office location has identified a need for better network protection. It has identified IDS as a great low-cost solution. What IDS components would you recommend the company implement? Justify your response with at least two recommended components.

B. **Network Traffic Analysis –** A component I would have to recommend for this small business is to add a **Network Traffic Analysis**. If we add this, it provides them with visibility into all the data moving across the network, which can help identify things like scanning, unusual data transfers, or even someone attempting a DDoS attack before it causes further damage to the network.

C. **Alert & Logging System** – As for my second component, I would adopt an Alert & Logging System because this gives businesses real-time visibility to suspicious activity and can keep many records for investigations. If the company isn't adding alerts and logs, attacks can go unnoticed, and people may not be aware that threat actors have gained access to their network without being detected.