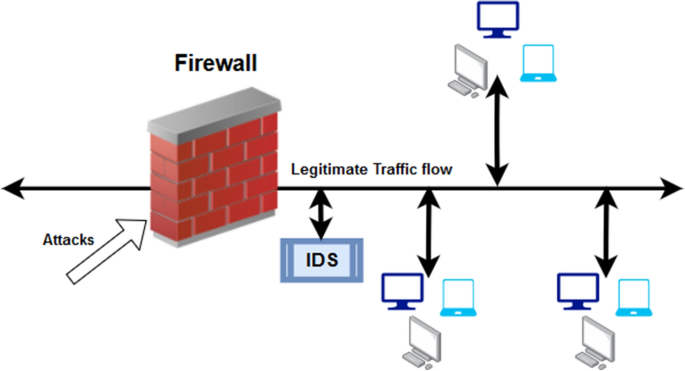
**CSCI 3250**

**Group Assignment 34**

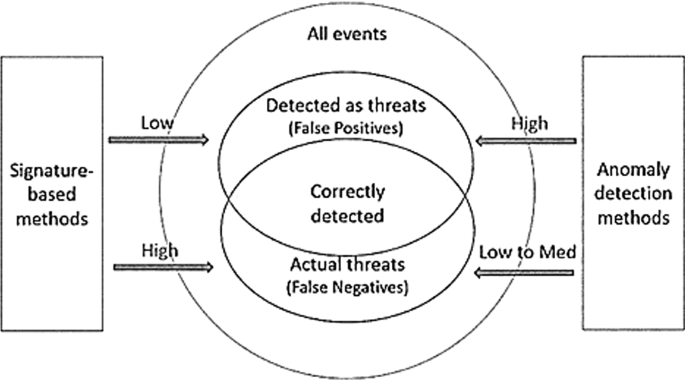
**IDS**

**Member Present: Sylas Sun, Eros Hernandez**

**Topic: IDS detection method: Statistical anomaly-based IDS**  


(fig-1: Firewall & IDS concept)

1. Definition:  
   A statistical anomaly-based IDS can be defined by the following term: A statistical anomaly-based IDS monitors system behavior for deviations from established norms (standard base-line behavior), detecting any potential threats through statistical analysis. It identifies suspicious activity by comparing real-time data to baseline patterns, enabling proactive security measures.
2. Method:  
   As the author briefly described in the definition, the core method this IDS uses to prevent intrusion include the following: this system relies on establishing baseline behavior (what is normal), continuously monitoring for deviations, and employing statistical analysis to detect anomalies indicative of intrusions. (Continue on the next page \*)

By comparing real-time data to established patterns, it identifies potential threats, enabling proactive security measures to prevent or mitigate intrusions.(Connect to previous page)  
(fig-2: Concept of Stat-based anomaly IDS)

1. Tools:  
   There are several tools that can be used such as Snort which can analyze network traffic in real-time and detect deviations from normal patterns. Another tool would be Suricata which is similar to snort, it is an open source IDS/IPS that supports both signature based and anomaly based detection. NetFlow/IPFIX, both are network telemetry protocols used to collect and analyze network traffic data.
2. Users who can benefit from this type of IDS:  
   Users who can benefit from IDS would be enterprises and businesses to protect network infrastructure, sensitive data, and intellectual property from cyber threats. Financial institutions such as banks and insurance companies can benefit because of the sensitive data they work with. It can help prevent fraudulent activities, data breaches, and other cyber attacks.
3. Threats this system can handle: The system can handle malware infections since IDS can detect the presence of malware, including viruses, worms, trojans, and ransomware. The system can also mitigate DoS attack by analyzing network traffic for abnormal patterns of traffic volume.
4. What this IDS is vulnerable to:  
   1. Baseline Drift: Over time, changes in system behavior or updates to network configurations may cause the baseline to become outdated, leading to missed detections or increased false negatives.
   2. Evasion Techniques: Sophisticated attackers may employ evasion techniques to manipulate system behavior subtly, avoiding detection by statistical anomaly-based IDS algorithms.
   3. False Positives: Statistical anomaly-based IDS may generate alerts for normal activities resembling anomalies, potentially overwhelming security teams with false alarms.

  
(fig-3: False Positive)