**Part 3:**

We chose to compare signature-based detection and anomaly-based detection based on four metrics:

1. **Detection Scope**: The types of attacks detected.
2. **False Positive Rate (FRP)** : The rate of false alarms (behaviors that are not considered attacks but are mistakenly identified as attacks by the system).
3. **Processing Overhead**: The processing requirements, including power consumption, memory usage, and other resource needs.
4. **Latency**: The speed of the detection process.

Starting with the first metric, **Detection Scope**, SBD tends to use a direct comparative approach, this means it only detects attacks that match those already stored in the database. On the other hand, ABD uses a learning approach, this gives it a larger detection scope which includes zero-day exploits and new techniques that do not match existing signatures.

While SBD has a limited detection scope it compensates with a significantly low rate of false positives. This brings us to the second metric, FRP. SBD generally has lower false positive rates since it strictly matches known attack signatures, making it more precise with a false positive rate of only 0.9%. In contrast, ABD tends to generate more false alarms because it flags any behavior that deviates from the normal baseline as suspicious. For instance, Avora, an ABD system, shows a much higher false positive rate of 53,6%, meaning many legitimate activities might trigger unnecessary alerts.

Looking at processing overhead, our third metric, ABD demands massive computational resources across multiple processing stages. It requires significant memory allocation for storing and maintaining the detailed behavioral profiles, with additional overhead from continuous data preprocessing, feature extraction and model training operations. Each stage has its own computational complexity: data collection and preprocessing consume resources for cleaning and normalization, feature extraction requires dedicated processing power for pattern analysis, and model maintenance demands regular computational cycles for updates and retraining. SBD, on the contrary, operates with a simpler and faster way to handle tasks, principally by allocating resources to signature database management and matching operations. Its overhead is mainly focused on the signature matching process, which scales linearly with the database size, and packet inspection routines. Both systems deal with resource allocation challenges, but ABD has more processing overhead because it involves multiple complex analytical stages that need to run at the same time while SBD's overhead is mainly focused on the single task of signature comparison and database management.

Finally, regarding latency, SBD demonstrates faster detection speeds due to its straightforward comparison process. When examining network traffic, it quickly matches patterns against known signatures and can immediately flag threats. Real-world studies have shown that network-based signature detection systems achieve an average detection latency of about 15.3 seconds. ABD, on the other hand, experiences significantly higher latency because it must perform complex statistical analyses and pattern recognition to determine if behavior deviates from the norm. Studies have measured this higher latency at approximately 1,039 seconds (17.3 minutes) for network-based dynamic analysis tools. This substantial difference in detection speed - with ABD taking about 68 times longer than SBD - demonstrates the performance trade-off between comprehensive anomaly detection and rapid response time. This additional processing time is necessary for ABD to maintain its advantage in detecting previously unknown threats, though it comes at the cost of speed.

Sources :

* Anomaly Detection — How to Tell Good Performance from Bad by Julia Bohutska ([link](https://towardsdatascience.com/anomaly-detection-how-to-tell-good-performance-from-bad-b57116d71a10))
* Performance Analysis of snort-based Intrusion Detection System DOI : 10.1109/ICACCS.2016.7586351
* Beyond the Hype : An Evaluation of Commercially Available Machine Learning–based Malware Detectors ([link](https://dl.acm.org/doi/full/10.1145/3567432?utm_source=chatgpt.com))