## Phase 3 – Detection and Comparison

Phase 3 focuses on comparing baseline network traffic observed in Phase 1with the simulated HTTP activity from Phase 2. The goal of this phase is to identify observable differences and determine which characteristics could be used as indicators for detection in a SOC environment.

## Traffic Comparison Overview

When comparing the baseline traffic to the simulated HTTP activity, several key differences become apparent. Baseline traffic primarily consisted of encrypted HTTPS communication and standard DNS resolution patterns associated with normal user behavior.
In contrast, the simulated traffic showed repeated clear-text HTTP requests to a single internal destination, creating a consistent and predictable communication pattern.

## Potential Detection Indicators

Based on the comparison between baseline and simulated traffic, several characteristics could be used as potential detection indicators in a SO environment.
• Repetitive HTTP requests to the same destination at regular intervals
• Use of unencrypted HTTP instead of HTTPS for consistent communication
• Communication with a single host without variation in request patterns
• Predictable request frequency that differs from normal user behavior

## Limitations

This analysis is limited to network-level observations and does not include host-based telemetry or correlation with endpoint logs. In addition, the simulated traffic was generated in a controlled lab environment and does not account for external network variability or user-driven behavior.

### Final Project Conclusion

This project demonstrated a structured approach to network traffic analysis by establishing a baseline of normal activity, simulating controlled HTTP communication, and comparing both scenarios to identify potential detection indicators.

Through this process, the importance of context, pattern recognition, and baseline comparison was reinforced, reflecting core skills required in a SOC environment. Understanding when traffic is normal, suspicious, or benign is essential for effective incident detection and response.