**Network Traffic Analysis Report: Detecting Malicious Activity**

**Date**: September 2, 2024  
**Analyst**: [George Gamal]

**1. Introduction**  
This report details the analysis of network traffic to identify potential security threats, specifically focusing on detecting malicious activity on a corporate network. The analysis was conducted using Wireshark to capture and examine network packets.

**2. Objective**  
The primary objective of this analysis is to identify suspicious activities indicative of malicious behavior and propose recommendations to mitigate the identified risks.

**3. Methodology**

**3.1. Traffic Capture**  
Network traffic was captured using Wireshark on the primary network interface. The capture session was conducted from 14:00 to 15:00 on September 2, 2024.

**3.2. Traffic Analysis**  
The captured traffic was analyzed using Wireshark’s filtering capabilities to identify unusual patterns and potential security threats.

* **Filter Applied**:
* ip.dst != 192.168.1.4 && http

This filter was used to identify HTTP traffic with a destination outside the local network.

**4. Findings**

**4.1. Unusual Data Transfers**  
A significant amount of data was observed being sent from internal IP 192.168.1.4 to external IP 38.133.127.95. This pattern is consistent with data exfiltration attempts.

**4.2. Repeated Connections**  
Multiple connections were observed from the internal IP 192.168.1.4 to the same external IP address, indicating a potential attempt to exfiltrate data.

**5. Recommendations**

Based on the analysis, the following recommendations are proposed to mitigate the identified risks:

**5.1. Implement Network Segmentation**  
Isolate sensitive data and systems from the rest of the network to limit the impact of a potential breach.

**5.2. Enhance Monitoring**  
Use Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to monitor and block suspicious activities.

**5.3. Apply Data Loss Prevention (DLP) Solutions**  
Implement DLP solutions to detect and prevent unauthorized data transfers.

**5.4. Regular Audits and Reviews**  
Conduct regular network audits and reviews to identify and address vulnerabilities.

**6. Conclusion**  
The analysis of network traffic using Wireshark successfully identified potential malicious activity targeting IP address 192.168.1.4. By implementing the recommended measures, the risk of similar incidents can be mitigated, enhancing the overall security posture of the network.