Dear [CISO Name],

Thank you for reaching out. Please consider the following write-up on the implementation of an IDS solution within our system.

**Suricata IDS**

The Intrusion Detection System we have implemented is Suricata. Suricata is more efficient in larger environments with large amounts of traffic passing through the firewall. This was chosen over Zeek, as Suricata is more efficient in real-time threat detection, while Zeek focuses on historical data and analysis. This was chosen over Snort as it utilizes multi-threaded architecture, while Snort uses single-threaded architecture.

**Installation Process**

Suricata was installed on the Alpine router/firewall by completing the following:

**How to Operate the IDS:**

**Successful Detection:**

Pictured below is a screenshot of the log files generated by Suricata on our system, displaying the most recent alert. Suricata has been completely configured to gather data across multiple hosts.

**Infrastructure Chart:**

**Compatibility Issues:**

We did not run into any compatibility issues causing an inability to pull information from specific hosts.

Respectfully,

Team [Number]