ICS Anomaly Connection Report

# Summary

Generated on: 2024-12-18 17:27:08  
Total Conversations Analyzed: 4

# Consolidated Metrics

1. Performance Metrics:

- Total Elapsed Time: 55.23 seconds

- Average Response Rate: 12.74 words/second

2. Content Metrics:

- Total Word Count: 694

- Total Character Count: 4012

- Total Sentence Count: 72

- Average Word Length: 5.78 characters

- Average Sentence Length: 9.64 words

- Average Vocabulary Richness: 0.5984

3. Content Analysis:

- Top 5 Most Common Words: is (35), device (10), these (7), mac (6), address (6)

# Connection Conversations

## Conversation 1

172.16.50.1 is a device with manufacturer TechCorp, using MAC address 00:1A:2B:3C:4D:5E. It is communicating with 198.51.100.2, which is a device with manufacturer NetSys. The communication is happening over TCP protocol with outgoing port EPH (ephemeral port) 443 and incoming port 443. The total sum of packets exchanged between these devices is 2785.0 for the first connection and 2333.0 for the second connection. These connections are not part of the baseline/allowlist, indicating they may be anomalous. Further research is needed to determine if these connections pose a security risk. The use of ephemeral ports (EPH) for outgoing traffic is unusual and could potentially indicate malicious activity. However, without more context, it is difficult to make a definitive determination.

## Conversation 2

172.16.60.1 is a device from an ICS environment, as indicated by the use of ephemeral port EPH for outgoing traffic. The MAC address 00:1A:2B:3C:4D:5F is associated with this device. 198.51.100.2 is also a device from an ICS environment, with incoming traffic on port EPH. The MAC address 10:AB:CD:EF:12:34 is associated with this device. The communication between these two devices involves an SSH connection (TCP protocol with SRCPORT 443 and DSTPORT 443), as indicated by the use of EPH for both outgoing and incoming traffic. This is a common port used for secure remote login to UNIX-based systems. The total sum of packets exchanged between these devices is 1192.0 for outgoing traffic and 1193.0 for incoming traffic. Further research may be needed to determine the exact purpose of this communication and to assess any potential risks or vulnerabilities. For example, it would be helpful to know the specific services running on these devices and to compare their behavior with known baselines or allowlists. Additionally, it may be useful to investigate the network path between these devices to identify any potential intermediate hops or connections that could provide additional context.

## Conversation 3

172.16.50.1 (SRCIP) is a device from TechCorp, and its MAC address is 00:1A:2B:3C:4D:5E. It attempted to communicate with 203.0.113.6 (DSTIP), which is likely a device from NetSys, using ephemeral port EPH (SRCPORT) for TCP protocol. The destination MAC address is not provided, but the source MAC address is 00:1A:2B:3C:4D:5E. This connection was flagged as an anomaly due to the attempted remote access attempt. 172.16.60.1 (SRCIP) is also a device from TechCorp, with MAC address 00:1A:2B:3C:4D:5F. It communicated with 203.0.113.6 (DSTIP), which is likely a device from NetSys, using ephemeral port EPH (SRCPORT) for TCP protocol. The destination MAC address is not provided, but the source MAC address is 00:1A:2B:3C:4D:5F. This connection was likely blocked due to the potential security risk associated with the attempted communication. The total sum of packets exchanged between the devices in both connections is 2.0 CNT. Further research is needed to determine if these connections pose a significant threat to the ICS environment.

## Conversation 4

172.16.1.1 (SRCIP) is a device from the local private network, likely an industrial control system device. It is communicating with 224.0.0.1 (DSTIP), which is also on the local private network but not typically used for industrial control systems. The protocol used is IGMP (Internet Group Management Protocol), which is often used for multicast communication in ICS environments. The SRCPORT and DSTPORT are both set to NaN, indicating that no specific ports were used for outgoing and incoming traffic. The SRCMAC and DSTMAC are provided as 18:AA:BB:CC:DD:EE and 01:00:5E:AB:CD:EF respectively, which correspond to the devices involved in the communication. The SRCMFG is IndustrialTech and DSTMFG is also IndustrialTech. The CNT is set to 3334.0, indicating that a total of 3334 packets were exchanged between the devices. This conversation is noted as an anomaly and requires further research to determine if it is a potential security threat or a legitimate activity.