Network Traffic Monitoring SOP:

Purpose:
This SOP outlines procedures for managing critical network alerts and guiding the Network Operations team in identifying, analyzing, and resolving issues. It also emphasizes documenting incidents and solutions for future reference.

Scope:
This procedure applies to the Network Operations team, covering the identification, analysis, and resolution of critical network alerts.

Responsibilities:
The team member overseeing network operations is accountable for implementing, following, reviewing, maintaining, and updating this policy. The IT manager is responsible for regularly checking the Event Viewer and Performance Monitor, which are configured to notify of critical events.

Prerequisites:
- Access to the alert monitoring system.
- Familiarity with network monitoring tools, including Wireshark.

Procedure:
1. Alert Identification:
    a. Continuously monitor the alert dashboard for critical network alerts.
    b. Prioritize alerts based on severity and potential impact on network performance.
2. Root Cause Analysis:
    a. Investigate identified alerts to determine the underlying cause.
    b. Utilize network monitoring tools, such as Wireshark, to capture and analyze relevant network traffic.
    c. If a real-time networking issue is identified through Event Viewer or Performance Monitor alerts, further investigate with Wireshark.
    d. Examine packet-level details to gain insights into the nature of the issue.
3. Corrective Actions:
    a. Implement corrective actions based on the root cause analysis.
    b. Take necessary steps to promptly resolve the identified network issue.
4. Incident Documentation:
    a. Document incident details, including alert information and root cause analysis.
    b. Include findings from Wireshark analysis in the incident report:
        i. Incident Report - [Date and Time]
            1. Alert Information: [Provide details on the triggered alert.]
            2. Root Cause Analysis: [Describe the findings from the analysis.]
            3. Implemented Solutions: [Specify the actions taken to resolve the issue.]

4. Wireshark Findings: [Include relevant insights gained from Wireshark analysis.]

References:

- Microsoft User Guide: https://learn.microsoft.com/en-us/windows-server/
- Wireshark User Guide: https://www.wireshark.org/docs/wsug_html_chunked/
- Code Fellows Github: https://github.com/codefellows/seattle-ops-301d14/blob/main/class-15/SOP-example-template.md

Definitions:

- Policy: Provides broad, overarching guidance on the "why" of this procedure.
- SOP: Specifies "what, when, why," and there could be multiple SOPs to support a specific policy.
- Work Instructions: Offer in-depth, step-by-step directions for a particular task.

Revision History:

- Version 1.0 (12-18-2023): Initial document creation by Dominique Bruso