How to Monitor the Organization Network in Real Time.

By: Ulises Servellon

Department of Computer Technology, **Bowie State University**

CTEC402.001

Dr. Haydar

Spring 2024

I. **Abstract**.

Network monitoring in real-time is a feature all companies must have implemented not only because they are able to oversee the incoming and outgoing traffic but also because it is in real-time, that cybersecurity specialists can act upon faster. A healthy network maintains traffic being monitored all the time because it is part of the security of a company, this allows performance to be at its peak and users are aware of how reliable and trustful the network is. The purpose of this paper is to show the reader multiple methods companies use to monitor their networks in real-time and how this can help prevent breaches. The methodologies used for this paper involve real-time monitoring software, network data collection, and anomaly detection algorithms.

Some of the key features written in this paper include real-time monitoring which can help IT personnel to be aware of possible anomalies on the network and act based on the occurrence. It is important to include all traffic in the monitoring system, no blind spots can be undetected. This will increase the network security of the company. Usually, computer hackers look for weak spots to infiltrate a network. Anomaly detection algorithms or software is another important aspect of securing a network, it is important to understand the traffic moving along the network. Combining these technologies, the IT personnel will be able to identify and clearly visualize network traffic.

Keywords: real-time, network monitoring, network security, network traffic.

II. **Research Approach**.

My approach to addressing the challenges of real-time network monitoring focuses on implementing a robust and scalable solution capable of continuously monitoring and analyzing network traffic, system performance metrics, and security events in real time. To achieve this, I created a comprehensive network framework that focuses on key components that include data collection, analysis, and visualization.

For data collection, I included monitoring software used by companies. The software captures network traffic from different devices including routers, switches, firewalls, and intrusion detection systems. For the data analysis, researched machine learning methods that cyber security specialists use to manage the data collected better, this involves organizing the data to improve its readability. Lastly, in order to visualize the data, I provided graphs and charts, which give the reader a clear path to understanding what the anomalies in the network are.

Overall, my approach combines state-of-the-art technologies, methodologies, and best practices to develop a real-time network monitoring solution that enhances the security, performance, and reliability of the organization's network infrastructure.

III. **Results**.

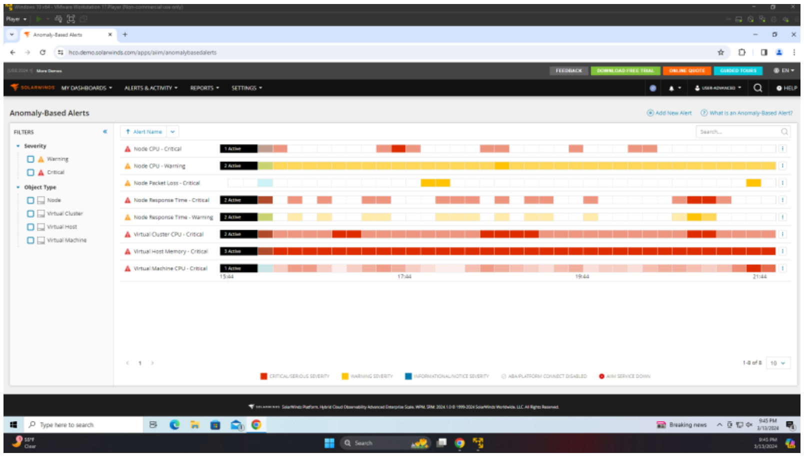
1. SolarWinds.

SolarWinds monitoring tool is a comprehensive software solution for organizations to monitor, manage, and optimize their network infrastructure. The tool captures crucial metrics such as bandwidth usage, latency, packet loss, and uptime. It deploys software agents or sensors across the network infrastructure to collect data from various network devices and services, which are then aggregated and analyzed in real-time.

Through a centralized dashboard, IT professionals can access a wealth of network monitoring data, configure alerts and notifications, and seamlessly perform troubleshooting tasks. The software's ability to automate configuration management tasks ensures that network devices are correctly and securely configured, enhancing overall network efficiency and reliability.

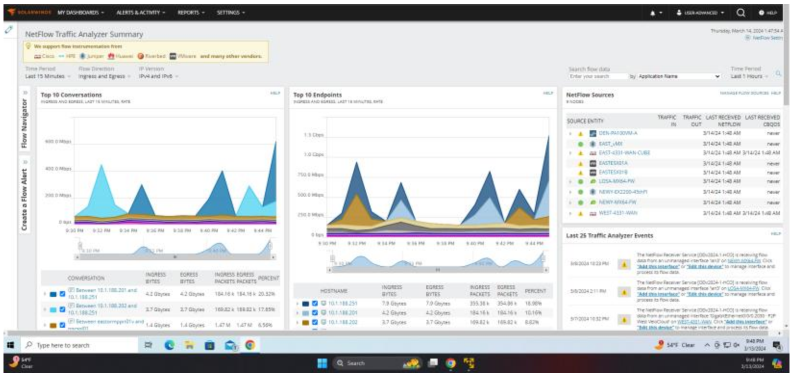
SolarWinds network monitoring empowers IT teams to proactively identify and address network issues before they escalate, enhancing operational efficiency, boosting productivity, and customer satisfaction. Moreover, it facilitates compliance with regulatory requirements by offering features for security auditing and compliance monitoring.

Overall, SolarWinds network monitoring is a vital tool for organizations seeking to maintain a robust and resilient network infrastructure in today's digital landscape.



Anomaly-Based Alerts

Alert Name	
Node CPU - Critical	1 Active
Node CPU - Warning	2 Active
Node Packet Loss - Critical	
Node Response Time - Critical	2 Active
Node Response Time - Warning	2 Active
Virtual Cluster CPU - Critical	2 Active
Virtual Host Memory - Critical	3 Active
Virtual Machine CPU - Critical	1 Active



NetFlow Traffic Analyzer Summary

Thursday, March 14, 2024 1:47:54 A

CONVERSATION	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
Between 10.1.188.201 and 10.1.188.251	4.2 Gbytes	4.2 Gbytes	184.16 k	184.16 k	20.32%
Between 10.1.188.202 and 10.1.188.251	3.7 Gbytes	3.7 Gbytes	169.82 k	169.82 k	17.85%
Between eastormppri01v and [illegible]	1.4 Gbytes	1.4 Gbytes	1.47 M	1.47 M	6.56%

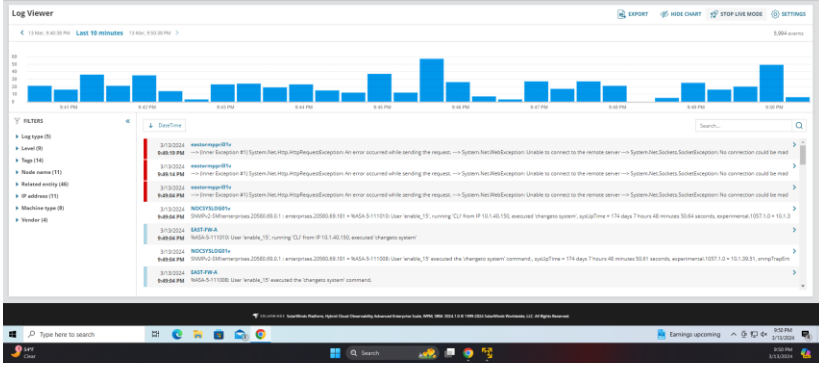
HOSTNAME	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
10.1.188.251	7.9 Gbytes	7.9 Gbytes	355.38 k	354.86 k	18.98%
10.1.188.201	4.2 Gbytes	4.2 Gbytes	184.16 k	184.16 k	10.16%
10.1.188.202	3.7 Gbytes	3.7 Gbytes	169.82 k	169.82 k	8.82%

NetFlow Sources

SOURCE ENTITY	TRAFFIC IN	TRAFFIC OUT	LAST RECEIVED NETFLOW	LAST RECEIVED CBQOS
DEN-PA100VM-A			3/14/24 1:48 AM	never
EAST_vMX			3/14/24 1:48 AM	never
EAST-4331-WAN-CUBE			3/14/24 1:48 AM	3/14/24 1:48 AM
EASTESX01A			3/14/24 1:48 AM	never
EASTESX01B			3/14/24 1:48 AM	never
LOSA-MX64-FW			3/14/24 1:48 AM	never
NEWY-EX2200-4[illegible]			3/14/24 1:48 AM	never
NEWY-MX64-FW			3/14/24 1:48 AM	never
WEST-4331-WAN			3/14/24 1:48 AM	3/14/24 1:48 AM

Last 25 Traffic Analyzer Events

3/8/2024 10:23 PM	The NetFlow Receiver Service [[illegible]] is receiving flow data from an unmanaged interface 'isn3' on NEWY-MX64-FW. Click "Add this interface" or "Edit this device" to manage interface and process its flow data.
3/8/2024 2:11 PM	The NetFlow Receiver Service [[illegible]] is receiving flow data from an unmanaged interface 'isn3' on LOSA-MX64-FW. Click "Add this interface" or "Edit this device" to manage interface and process its flow data.
3/7/2024 10:32 PM	The NetFlow Receiver Service [[illegible]] is receiving flow data from an unmanaged interface 'GigabitEthernet0/0/0.2030 · P2P West VeloCloud' on WEST-4331-WAN. Click "Add this interface" or [illegible]



Log Viewer

13 Mar, 9:50:38 PM · 5,994 events

```
3/13/2024 9:49:19 PM  eastormppri01v
--> (Inner Exception #1) System.Net.Http.HttpRequestException: An error occurred while sending the request. ---> System.Net.WebException: Unable to connect to the remote server ---> System.Net.Sockets.SocketException: No connection could be mad
3/13/2024 9:49:14 PM  eastormppri01v
--> (Inner Exception #1) System.Net.Http.HttpRequestException: An error occurred while sending the request. ---> System.Net.WebException: Unable to connect to the remote server ---> System.Net.Sockets.SocketException: No connection could be mad
3/13/2024 9:49:04 PM  eastormppri01v
--> (Inner Exception #1) System.Net.Http.HttpRequestException: An error occurred while sending the request. ---> System.Net.WebException: Unable to connect to the remote server ---> System.Net.Sockets.SocketException: No connection could be mad
3/13/2024 9:49:04 PM  NOCSYSLOG01v
SNMPv2-SMI::enterprises.20580.69.0.1 : enterprises.20580.69.181 = %ASA-5-111010: User 'enable_15', running 'CLI' from IP 10.1.40.150, executed 'changeto system', sysUpTime = 174 days 7 hours 48 minutes 50.64 seconds, experimental.1057.1.0 = 10.1.3
3/13/2024 9:49:04 PM  EAST-FW-A
%ASA-5-111010: User 'enable_15', running 'CLI' from IP 10.1.40.150, executed 'changeto system'
3/13/2024 9:49:04 PM  NOCSYSLOG01v
SNMPv2-SMI::enterprises.20580.69.0.1 : enterprises.20580.69.181 = %ASA-5-111008: User 'enable_15' executed the 'changeto system' command., sysUpTime = 174 days 7 hours 48 minutes 50.61 seconds, experimental.1057.1.0 = 10.1.39.51, snmpTrapEnt
3/13/2024 9:49:04 PM  EAST-FW-A
%ASA-5-111008: User 'enable_15' executed the 'changeto system' command.
```

2. SIEM

Security Information and Event Management (SIEM) is a comprehensive security implementation that is more reliable and complete than other security solutions. SIEM involves the implementation of not only software but also sensors, collectors, and management consoles. By using this additional hardware, you can collect data from different devices, even if they are located far away from the main location.

SIEM is not the name of a software, but it is a security solution that comes in several varieties, such as McAfee Enterprise Security Manager, IBM QRadar, and Elastic NV. While the SIEM software can differ depending on the vendor, they all serve the same purpose. SIEM is a combination of Security Information Management (SIM) and Security Event Management (SEM). SIM collects and analyzes traffic data and logs data from firewalls, IDS, or antivirus software. On the other hand, SEM focuses on real-time monitoring and analysis of security events. This allows SEM to alert the user for immediate response to security threats as they occur.

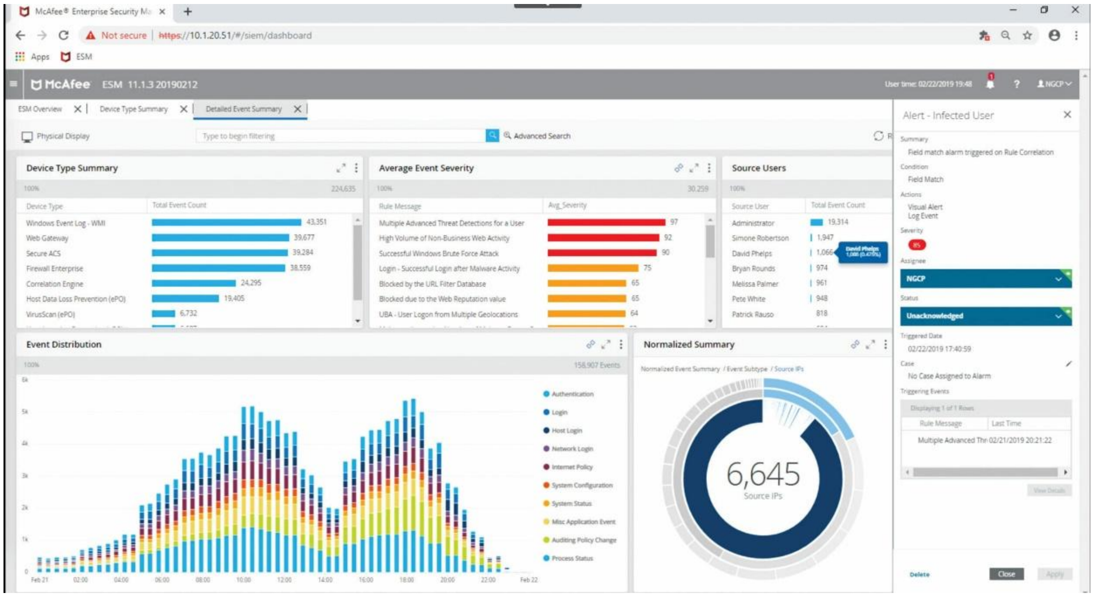
Overall, SIEM technology is critical in enhancing an organization's security. Its ability to provide real-time visibility into security events facilitates threat detection and incident response, which makes it a more robust and reliable security solution.

A proposed method called The Hierarchical Managers Architecture extends the traditional SIEM model by introducing intermediary SIEM servers called "Child Managers." In this setup, the central SIEM server communicates with Child Managers instead of directly with Log sources. Each Child Manager collects, normalizes, and forwards data to the central SIEM server for aggregation and correlation while retaining raw even data locally for forensic purposes.

This approach offers benefits such as distributing data management load among multiple engines, reducing network overhead by passing only relevant data to the central server, and facilitating easier storage, backup, and processing with smaller data sets. Child Managers handle alerting, filtering, and policy enforcement, while the Parent Manager collects correlated events from all regional instances for global correlation.

The proposal recommends having separate Security Operation Centers (SOC) for regional SIEM implementations and a global SOC for the Parent SIEM. Analysts access the SIEM Manager through global or regional monitoring layers as needed [Anastasov & Davcev].

In addition to reinstating what was mentioned before, fundamentally, all SIEMs have the ability to collect, store, and correlate events generated by a managed infrastructure. The difference between SIEM systems reflects their positions in the market. According to the article, the evolution of SIEM solutions from 2010 to 2020 is presented, highlighting key vendors such as RSA, IBM, NetIQ/Microfocus/ArcSight, McAfee/Intel, and LogRhythm. Some capabilities listed on the article are threat intelligence detection, compliance, and log management [Gonzales-Granadillo, Gonzalez-Zarzosa, & Diaz].



Device Type Summary

100% 224,635

Device Type	Total Event Count
Windows Event Log - WMI	43,351
Web Gateway	39,677
Secure ACS	39,284
Firewall Enterprise	38,559
Correlation Engine	24,295
Host Data Loss Prevention (ePO)	19,405
VirusScan (ePO)	6,732

Average Event Severity

100% 30,259

Rule Message	Avg_Severity
Multiple Advanced Threat Detections for a User	97
High Volume of Non-Business Web Activity	92
Successful Windows Brute Force Attack	90
Login - Successful Login after Malware Activity	75
Blocked by the URL Filter Database	65
Blocked due to the Web Reputation value	65
UBA - User Logon from Multiple Geolocations	64

Source Users

100%

Source User	Total Event Count
Administrator	19,314
Simone Robertson	1,947
David Phelps	1,066
Bryan Rounds	974
Melissa Palmer	961
Pete White	948
Patrick Rauso	818

Alert - Infected User

Summary
Field match alarm triggered on Rule Correlation
Condition
Field Match
Actions
Visual Alert
Log Event
Severity
85
Assignee
NGCP
Status
Unacknowledged
Triggered Date
02/22/2019 17:40:59
Case
No Case Assigned to Alarm
Triggering Events

Displaying 1 of 1 Rows

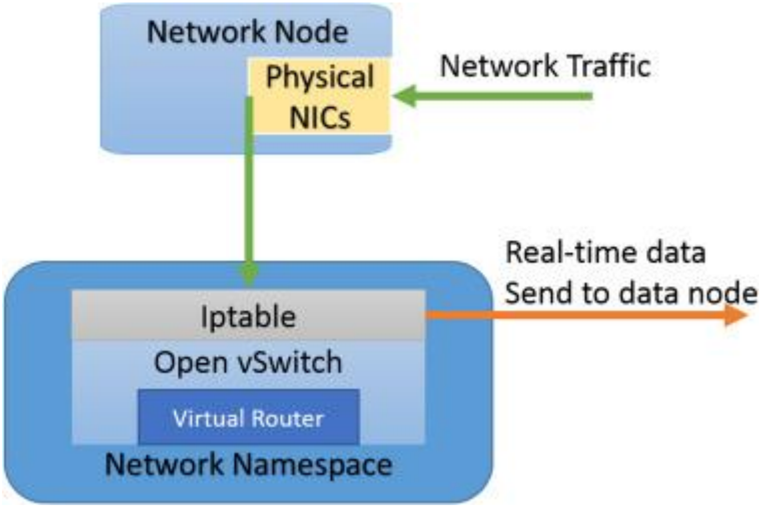
Rule Message	Last Time
Multiple Advanced Thr	02/21/2019 20:21:22

3. OpenFlow in a Virtual Environment.

Another method to monitor real-time traffic in a company's network is by using OpenFlow in a virtual environment. To implement real-time traffic monitoring using OpenFlow, the network namespace can be utilized. This involves creating a network namespace using the "ip netns" command, which inherits configuration from the host. By setting up specific rules in the iptables filter with the namespace, incoming traffic can be monitored. When traffic matches these rules, data is collected and periodically sent to a data node for analysis.

The workflow of the filter table calculation mechanism involves creating rules in the iptables filter within the network namespace. When traffic enters the namespace, it is subjected to these rules. If the source IP of incoming traffic matches the rules, the corresponding data is collected for analysis. This allows network administrators to monitor traffic in real time and gather relevant data for analysis.

Additionally, statistical data analysis can be implemented similarly to real-time traffic monitoring. By using the "ip netns" command to create network namespaces and virtual routers, Open vSwitch can support the NetFlow protocol to collect packet information. This information is translated into NetFlow data and sent to a data node for periodic collection. This approach enables the monitoring of network traffic and the collection of statistical data for further analysis by administrators [Yang, et al.].



IV. Lessons Learned and Future Work.

From the research, I was able to learn new information on network traffic monitoring. I learned that there are many software and many security solutions to implement a real-time network traffic monitor. I learned that even though SIEM is not software per se, it is a security solution that can be powerful by adding additional hardware to its implementation. This hardware allows the user to monitor even more devices, which can become helpful especially when you have to manage devices outside your workplace.

In the future, I plan on investing and learning more about real-time network monitoring because it is important to know what kinds of anomalies can go through a network and it is important to get ahead of any malicious infiltration that could harm not only the systems but entire the network. For IT students/professionals, it is necessary to keep learning and completely understand emerging threats and technologies to be better equipped to address potential security challenges and protect network systems effectively.

V. Summary and Conclusion.

This paper went over some real-time network monitoring technologies that are used by other IT specialists and that can be implemented at the corporate level. These technologies include SolarWinds monitoring, which is software that can be installed in a centralized environment and then can be used to monitor traffic and manage devices. Another technology reviewed was SIEM, which is a combination of SIM and SEM and for that reason, it is a robust network solution. It is used to monitor, store, and analyze traffic. Lastly, I went over the user of OpenFlow in a virtual environment. This involves using commands to create a namespace that inherits its configuration from the host. The network administrator can create rules using the iptables filters and because the namespace inherits its configuration from the host, the traffic entering the namespace will be under the set of rules.

In conclusion, because technology continues evolving and with its network threats, it is important to continue studying and creating security solutions that can not only address those threats on companies' networks but also home networks. If threat actors don’t rest when researching malicious ways to cause harm to computer systems, why would we? There is still a lot of room for improvement and because of this, we must keep creating and testing new technologies to make networks safer.

VI. References.

Anastasov, I., & Davcev, D. (2014 January 17). SIEM Implementation for Global and Distributed Environments. IEEE Xplore. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6916651

Gonzalez-Granadillo, G., Gonzalez-Zarzosa, S., Diaz, R. (2021, June 3). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructure. MDPI. https://www.mdpi.com/1424-8220/21/14/4759

SolarWinds. (n.d.). Network monitoring software. SolarWinds. https://www.solarwinds.com/network-performance-monitor/use-cases/network-monitoring-software

Yang, C., Chen, S., Liu, J., Yang, Y., Mitra, K., Ranjan, R. (2019, April). Implementation of a real-time network traffic monitoring service with network functions virtualization. Science Direct. https://www.sciencedirect.com/science/article/pii/S0167739X1830311X?casa_token=1Gz4WmAejqIAAAAA:aoWX24oNHmXVX-aqxeBN8D4zQwUAt9j0YVDqjtLPpLAeOREzQtKxkqGccKkLCyXMwj-R8SiFiLo