Event Management for Managed WAN/LAN

January 2024

Document ID: VZK047896

verizon✓

Content

- Introduction
- What is Event Management?
- Active Monitoring
- Alarm Creation
- Passive Monitoring
- Meraki
- From Event to Incident Ticket
- Alarm List and Thresholds
- Ticket Priority Definitions
- Alarm Correlation

Introduction

The purpose of this presentation is to provide a high level overview of the process where an event triggers the creation of a proactive incident ticket.

It is a generic overview and therefore exceptions as well as custom arrangements are not being covered.

Please refer to the appendix at the end of the presentation for an explanation of terms.

What is Event Management

Event Management Definition

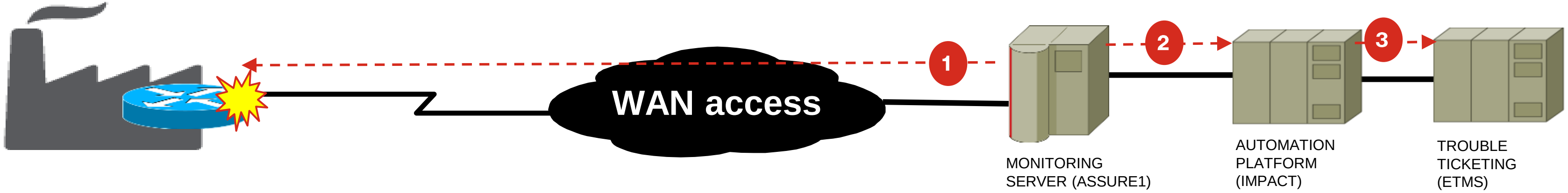
An event can be defined as any detectable occurrence that has significance for the delivery of IT services. Events are typically notifications created by an IT service, Configuration Item (CI) or monitoring tool.

Event Management by Verizon

Verizon is using Assure1 as the event monitoring tool for Managed WAN/LAN together with M3 for Meraki devices. Assure1 uses two methods to detect service interruptions:

1. **Active Monitoring:** Pollers on Assure1 are configured to poll (SNMP & ICMP walk) managed devices every 3 minutes.
2. **Passive Monitoring:** Managed devices are configured to send an alert (SNMP trap) each time a specific faults occur.

Active Monitoring



Polling: Assure1 is configured to poll the device (equipment) every 3 minutes. 1

Event sent to Automation (IMPACT): If Assure1 does not receive an answer from the second polling, Assure1 forwards the event to IMPACT. 2

IMPACT: Upon receiving an alert, IMPACT queries ESP (Managed Device Inventory Database) against the entity name to retrieve information such as: Circuit ID, Customer name, Product, Service desk, NOC, etc. This information is used to populate the alarm and to create the ticket within Verizon's Enterprise Ticket Management System (ETMS) based on set messaging policy. 3

Alarm Creation

How long does it take to create an alarm?

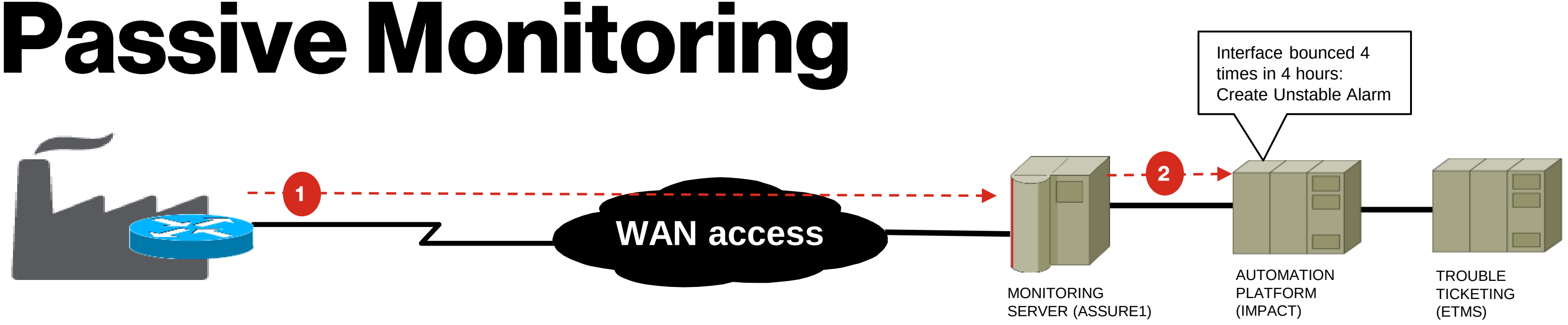
- First polling cycle detects the fault in 3 minutes
- Second cycle confirms the fault in 3 minutes
- Assure1 holds the alarm for ~1min 30sec to check if the alarm is from both datacenters
- IMPACT receives the alert and collects additional information to create the alarm in a few seconds

Total time is: 3min + 3min + ~1min 30sec + few seconds = ~ 8 minutes

Additional alarm criteria:

- The alarm creation process (from the polling mechanism) can be interrupted at any time if the device starts answering back to the polling.

Passive Monitoring


Interface bounced 4 times in 4 hours: Create Unstable Alarm
1
2
WAN access
MONITORING SERVER (ASSURE1)
AUTOMATION PLATFORM (IMPACT)
TROUBLE TICKETING (ETMS)

SNMP Traps: Traps are sent by the devices to Assure1 each time specific events occur. 1
The following default traps are configured in the customer premises devices:

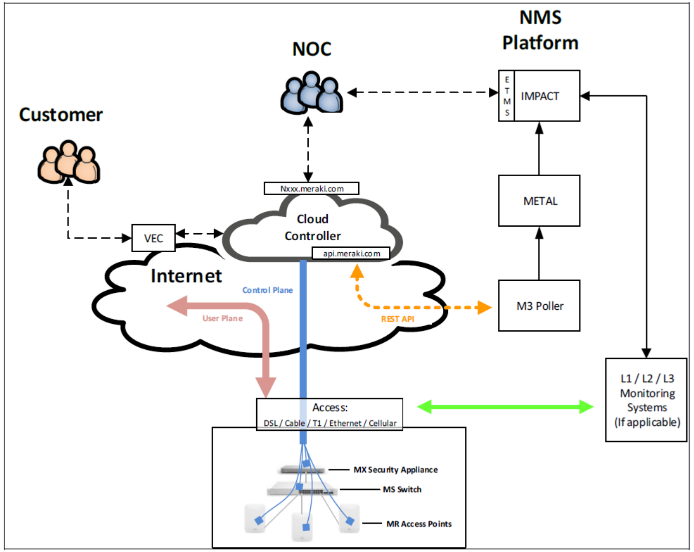
- Interface up/down (a trap is sent each time the state of an interface changes)
- Cold/Warm Start-Up (a trap is sent each time a device starts up, meaning that Assure1 knows when a device reboots (i.e. manual reset or loss of power)

IMPACT: Upon the repetitive occurrence of specific traps (for example if a device sends an interface up/down trap 4 times in 4 hours) IMPACT creates “unstable” alarms. For Interface unstable alarms it depends per management center if this also automatically will result in a proactive incident ticket. 2

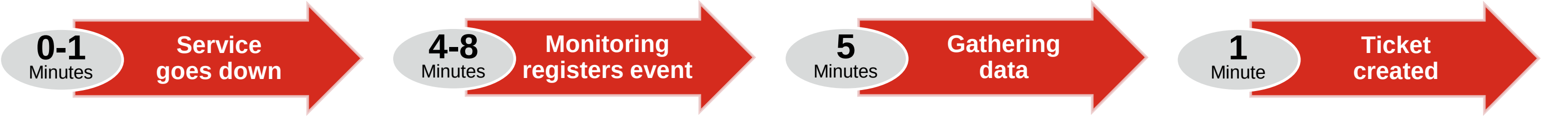
Meraki

Management of Meraki devices is not performed by Assure1 but by an Verizon internally developed monitoring system called M3. This system polls the Cloud Controller (i.e. Dashboard) at 3 minute intervals, captures availability and related data, and communicates alarm conditions to IMPACT. Meraki Cloud controller polls CPE every 5 minutes.

M3 interacts with the Meraki cloud in one of two ways – SNMP or a REST API. In the initial release of M3 the API was used for provisioning, and SNMP was used for monitoring. That approach has been replaced with one that utilizes the API exclusively and for new activations SNMP is not used.



From Event to Incident Ticket



0-1 Minutes — Service goes down

4-8 Minutes — Monitoring registers event

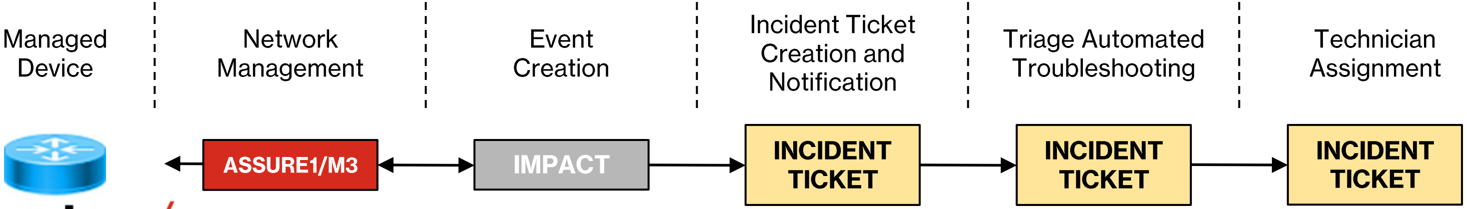
5 Minutes — Gathering data

1 Minute — Ticket created

A ticket is created in approximately 13 minutes after the initial network event.

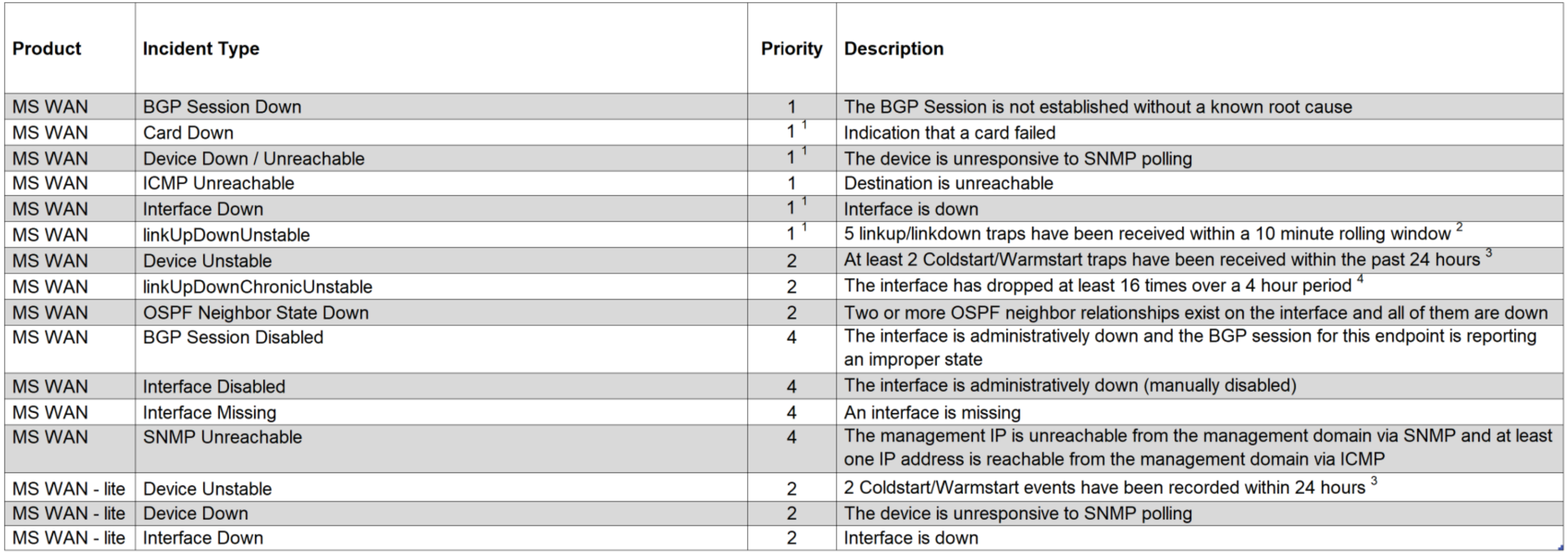
Automated troubleshooting commences immediately after the creation of the proactive incident ticket. This is the so called ‘triage‘ phase and is published on the VEC Portal and via eBonding.

Triage Automated troubleshooting enables faster resolution as ticket is automatically transferred to NOC if further diagnostics are required by technicians. The NOC technicians can also use the Triage output to diagnostic data.



Managed Device	Network Management	Event Creation	Incident Ticket Creation and Notification	Triage Automated Troubleshooting	Technician Assignment
	ASSURE1/M3	IMPACT	INCIDENT TICKET	INCIDENT TICKET	INCIDENT TICKET

Alarm List and Thresholds



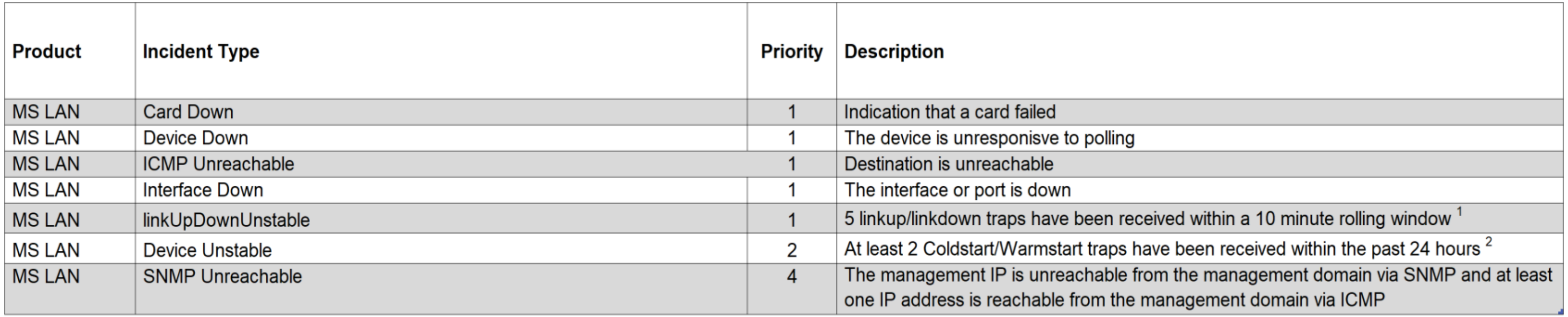
Product	Incident Type	Priority	Description
MS WAN	BGP Session Down	1	The BGP Session is not established without a known root cause
MS WAN	Card Down	1 [1]	Indication that a card failed
MS WAN	Device Down / Unreachable	1 [1]	The device is unresponsive to SNMP polling
MS WAN	ICMP Unreachable	1	Destination is unreachable
MS WAN	Interface Down	1 [1]	Interface is down
MS WAN	linkUpDownUnstable	1 [1]	5 linkup/linkdown traps have been received within a 10 minute rolling window [2]
MS WAN	Device Unstable	2	At least 2 Coldstart/Warmstart traps have been received within the past 24 hours [3]
MS WAN	linkUpDownChronicUnstable	2	The interface has dropped at least 16 times over a 4 hour period [4]
MS WAN	OSPF Neighbor State Down	2	Two or more OSPF neighbor relationships exist on the interface and all of them are down
MS WAN	BGP Session Disabled	4	The interface is administratively down and the BGP session for this endpoint is reporting an improper state
MS WAN	Interface Disabled	4	The interface is administratively down (manually disabled)
MS WAN	Interface Missing	4	An interface is missing
MS WAN	SNMP Unreachable	4	The management IP is unreachable from the management domain via SNMP and at least one IP address is reachable from the management domain via ICMP
MS WAN - lite	Device Unstable	2	2 Coldstart/Warmstart events have been recorded within 24 hours [3]
MS WAN - lite	Device Down	2	The device is unresponsive to SNMP polling
MS WAN - lite	Interface Down	2	Interface is down

Notes:

1. Depending on management center and certain criteria these might be opened as Pri 2
2. The alarm clears when 10 minutes without linkup/linkdown events
3. The alarm clears when 24 hours without Coldstart/Warmstart events
4. The alarm clears when 4 hours without linkup/linkdown traps

Each type of product has a different set of alarms, the product group is shown in the first column.

Alarm List and Thresholds (continued)

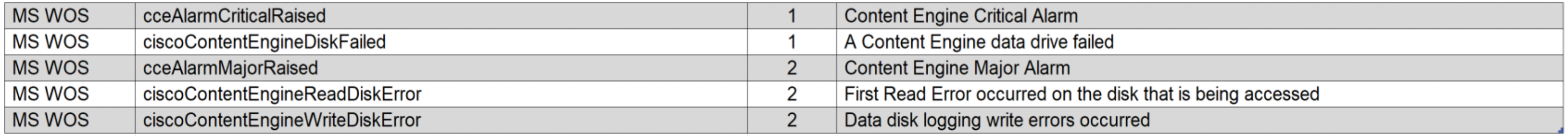


Product	Incident Type	Priority	Description
MS LAN	Card Down	1	Indication that a card failed
MS LAN	Device Down	1	The device is unresponisve to polling
MS LAN	ICMP Unreachable	1	Destination is unreachable
MS LAN	Interface Down	1	The interface or port is down
MS LAN	linkUpDownUnstable	1	5 linkup/linkdown traps have been received within a 10 minute rolling window [1]
MS LAN	Device Unstable	2	At least 2 Coldstart/Warmstart traps have been received within the past 24 hours [2]
MS LAN	SNMP Unreachable	4	The management IP is unreachable from the management domain via SNMP and at least one IP address is reachable from the management domain via ICMP

Notes:

1. The alarm clears when 10 minutes without linkup/linkdown events
2. The alarm clears when 24 hours without Coldstart/Warmstart events

Next to this each product can also have its own sets of alarms, as per below example for Managed WOS

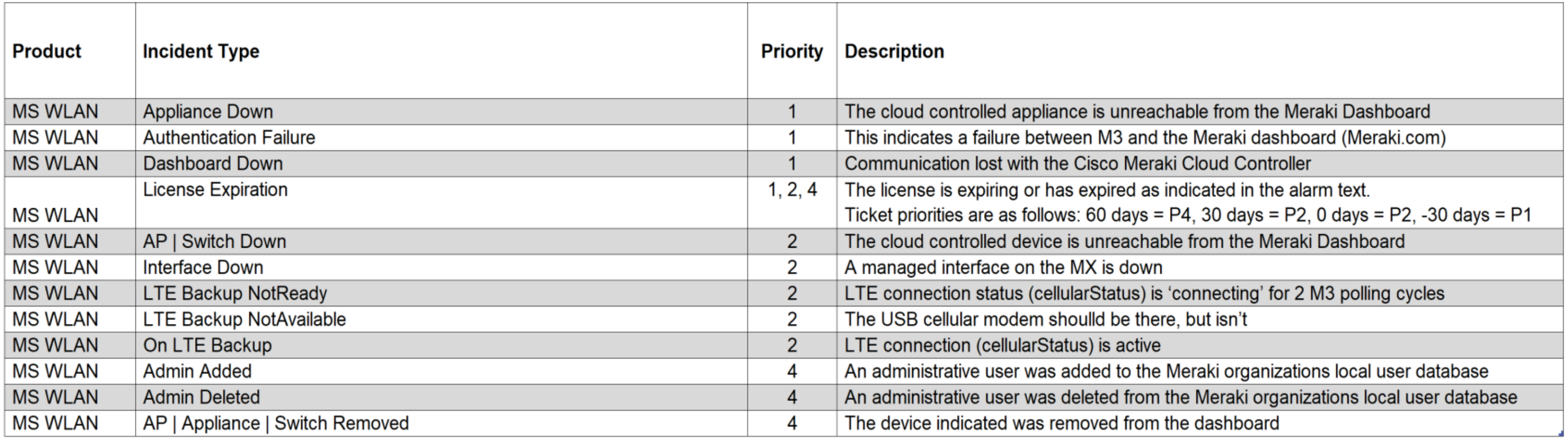


MS WOS	cceAlarmCriticalRaised	1	Content Engine Critical Alarm
MS WOS	ciscoContentEngineDiskFailed	1	A Content Engine data drive failed
MS WOS	cceAlarmMajorRaised	2	Content Engine Major Alarm
MS WOS	ciscoContentEngineReadDiskError	2	First Read Error occurred on the disk that is being accessed
MS WOS	ciscoContentEngineWriteDiskError	2	Data disk logging write errors occurred

verizon✓

Alarm List and Thresholds (continued)

Meraki Alarm List



Product	Incident Type	Priority	Description
MS WLAN	Appliance Down	1	The cloud controlled appliance is unreachable from the Meraki Dashboard
MS WLAN	Authentication Failure	1	This indicates a failure between M3 and the Meraki dashboard (Meraki.com)
MS WLAN	Dashboard Down	1	Communication lost with the Cisco Meraki Cloud Controller
MS WLAN	License Expiration	1, 2, 4	The license is expiring or has expired as indicated in the alarm text. Ticket priorities are as follows: 60 days = P4, 30 days = P2, 0 days = P2, -30 days = P1
MS WLAN	AP | Switch Down	2	The cloud controlled device is unreachable from the Meraki Dashboard
MS WLAN	Interface Down	2	A managed interface on the MX is down
MS WLAN	LTE Backup NotReady	2	LTE connection status (cellularStatus) is ‘connecting’ for 2 M3 polling cycles
MS WLAN	LTE Backup NotAvailable	2	The USB cellular modem shoulld be there, but isn’t
MS WLAN	On LTE Backup	2	LTE connection (cellularStatus) is active
MS WLAN	Admin Added	4	An administrative user was added to the Meraki organizations local user database
MS WLAN	Admin Deleted	4	An administrative user was deleted from the Meraki organizations local user database
MS WLAN	AP | Appliance | Switch Removed	4	The device indicated was removed from the dashboard

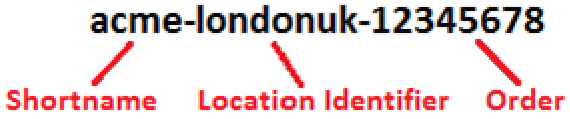
Ticket Priority Definitions

Ticket Type	Priority	Description
Outage	1	Service is unusable, complete loss of service. The service is released for testing without restriction.
Degraded	2	Service is experiencing intermittent issues or is degraded and is not released for testing without restriction.
Service Risk	3	Quality issues that threaten the performance of the service.
Assistance Request	4	Non-service impacting issues requiring investigation, resolution or other action.

These are the standard ticket priorities definitions used within Verizon.

Alarm Correlation

When alarms are presented to IMPACT, a correlation key is applied based on shortname and location identifier. Alarms with the same key will be added to the same event and ticket. This key remains active for either 15 minutes for Hub locations or for 2 hours for remote locations.



acme-londonuk-12345678

Shortname Location Identifier Order

After the timer expires new alarms will create new events, perform all of the wait-time, backend queries, etc. and then a pre-existing ticket check will move the alarm to a previous event/ticket when an open event/ticket is found against the same shortname and location identifier.

Appendix

API
Application Programming Interface, a software intermediary that allows two applications to talk to each other.

ASSURE1
Assure1 is the management platform for LAN and WAN services within Verizon and provides fault and performance alerting.

CPE
Customer Premise Equipment

ESP
This is the primary database for Managed Services Customers. All information pertaining to the management and monitoring of Managed Services devices/services is stored in ESP.

IMPACT
Integrated Management Platform for Advanced Communications Technologies is a application that provides surveillance, alarm topology augmentation, correlation, ticketing, and automation capabilities for the Verizon network.

M3
Verizon internally developed monitoring system.

NOC
Network Operation Center