Speed Up Your NOC With Automation

White Paper by

Rob Pavone
Network Operations Expert

FirstWave

Speed Up Your NOC... With Automation

It's just another day in the NOC for Opie and his team. Another 10-hour shift in the making. "Wonder what kind of "surprises" we will get today from the network and our customers," Opie is thinking. Seems the NOC always gets blindsided, almost daily, with outages and all the changes taking place on the network.

Opie, being the most senior NOC engineer on the team, has been tasked this day by his leadership to determine how the NOC can prevent a lot of these "blindsides" and find better more efficient ways to detect, diagnose and act upon the network "events" of the day. A more efficient method would help make the NOC a less stressful environment, especially for the junior engineers and the fact the network is continuing to grow along with new technology being introduced into the environment at a faster rate.

> **Here's how the NOC can prevent a lot of these "blindsides" and find better more efficient ways to detect, diagnose and act upon the network "events" of the day.**

Scale Up Your Solutions

CONTACT AN EXPERT

Table of Contents

01

The Problem Opie Has Been Tasked To Solve

The following information was waiting for Opie in his email Inbox this morning:

Good Morning Opie! I need you to help me and the management team with something.

We have to find a better way to operate more efficiently within the NOC. The network is growing, we have a lot of junior engineers on the team and we will probably be needing even more staff to support the growing environment, but that may be a while. I've been tracking a few of our challenges over the last few months and have jotted down some of my findings below:

We are too reactive vs pro-active for incident

• A lot of the incidents occurring on the network, we are notified either through customers calling in to our help desk and opening a ticket or via an alert we see through our monitoring tool FirstWave's NMIS when the event occurs. We are too reactive and it takes a long time for us to respond and start tracking down the root cause and troubleshoot the issue. There are lots of common incidents that should be resolved with the same process! We have to shorten our MTTR!

• There's a 6-8 week lag time for us to procure more bandwidth on our WAN links. We don't seem to see the capacity need until it is too late, when services slow down or stop working, customers start complaining, and the WAN links are overly congested. We have to find a way to get ahead of this capacity planning curve for congested WAN links and put in bandwidth increase requests before our customers see the impact first.

We are too reactive vs pro-active for incidents

I pulled a few device configurations down from the network and looked at them. There is a lot of variability in our device configurations out there on the network. We are not consistent. It looks like people are making their own changes to the configs and at times it has caused outage situations. We need to get better control of our device configurations.

Let me know what you are able to figure out. I know we can't automate "chaos", so let's try to get a handle on the information we have available to us and find a solution.

Thanks! The NOC Boss

> **...effective automated solutions made his NOC team more efficient, aligning the right capabilities to the right operational processes**

02 Proposed Solution To Help The NOC

In the "NOC Boss's" email to Opie, they bring up challenges with some process-oriented tasks that NOCs are typically responsible for supporting. When putting together an automation and tools-based solution for these challenges, it is important to align the tools with the IT service management processes, NOT the other way around. What needs to be optimized and improved in the processes and how can tools/automation help SUPPORT the processes?

From the challenges identified by the NOC Boss there are 5 IT Service Management process areas that need to be addressed in the solution:

- ***Incident Management***
- ***Problem Management***
- ***Change Management***
- ***Performance and Capacity Management***
- ***Asset and Configuration Management***

While we won't go into depth into each of these process areas specifically here, we will look at how automation can support each of these process areas to build efficiencies into the process workflow and assist NOC personnel with their roles and responsibilities.

We need to provide solutions that can Detect, Diagnose and Act intelligently upon the information available from the network.

Automation support for
Incident Management

Let's first look at incident management, one of the primary processes NOC teams support and are responsible for, and how automation can help build efficiencies into the process workflow.

The challenge Opie has been presented with is the following:

- "A lot of the incidents occurring on the network, we are notified either through customers calling in to our help desk and opening a ticket or via an alert we see through our monitoring tool FirstWave's NMIS when the event occurs."
- "We are too reactive and it takes a long time for us to respond… and troubleshoot the issue."
- "We have to shorten our MTTR!"

These challenges are all too common in NOCs, reactive, slow to respond, long time to troubleshoot, long Mean Time Resolve or MTTR. So how can a NOC be more proactive, quicker to respond and troubleshoot, and lower MTTR for incidents?

1. Auto-open incident tickets based on events and alerts seen on the network from FirstWave's NMIS. Start with only one or two alerts (so the incident ticketing system is not flooded with tickets the team cannot handle) that are more critical in nature and have proven documented resolution actions for verified service outages. As the NOC becomes more proficient with handling these kind of incident tickets, look to add more alerts that auto-open the tickets.

2. Insert valuable diagnostic information in the incident tickets related to the event or alert, like "Show" command output from the device having the issue and appropriate Configuration Item (CI) information about the device.

3. As automation is introduced more into the environment for handling incidents, some incident tickets could even be automatically closed after being resolved from automated tasks.

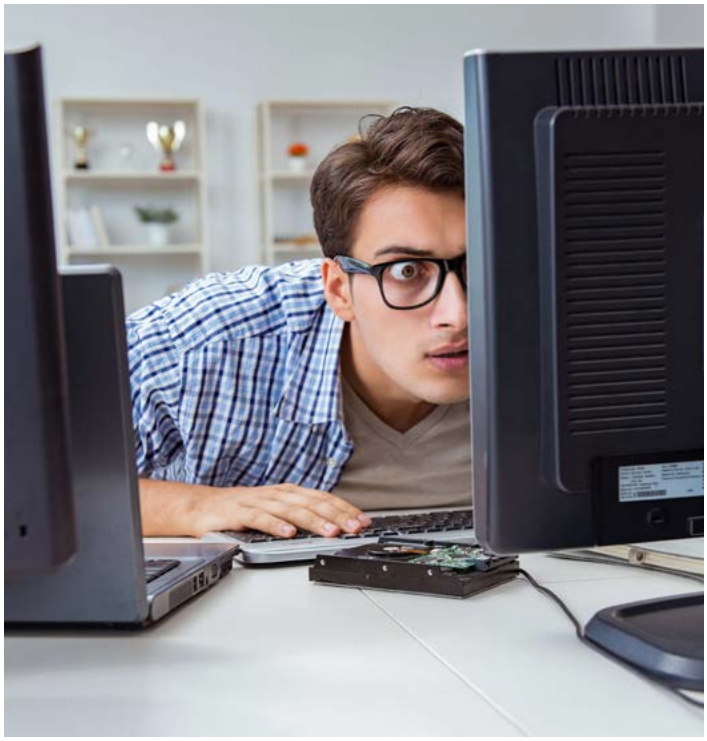
4. Provide alarm suppression and correlation on "downstream" events to prevent unnecessary work from the NOC for potentially false positives providing more time to work on the actual event. information about the device.

Automation support for
Problem Management

Similar to incident management but with a little bit more responsibility after an incident is resolved, is where problem management "kicks in." Its responsibility is to identify and document root cause of incidents and to minimize and address recurring incidents or "known errors".

- **"Track down the root cause."**
- **"There are lots of common incidents that should be resolved with the same process."**

Problem management in support organizations is sometimes an after-thought because it is not reactive in nature, where teams spend most of their time generally. Problem management workflows seem to kick in after a major incident and leadership wants to understand the root cause of why the incident occurred. So how can automation help support the problem management process?



1. Provide the necessary and timely information from the network in support of incident resolution. Group data that can be auto-collected, such as "show" command information, and report this with the incident tickets or "post-mortem" information auto-collected from the network. The information can then populate problem management tickets within IT Service Management tools and can populate and support documents that are stored in "known error databases", technical tips, or knowledge articles the NOC can reference in the future.

2. When similar incidents are reported and seen on the network, and common resolutions are performed for these incidents, automated tasks can be executed to resolve these common or "recurring" incidents instead of having NOC personnel do the same thing every time manually. Creating these automated workflows and remediation tasks should be actions that are not business impacting, established actions proven by the NOC and very routine in nature. As the NOC "matures" in their technical prowess,

Automation support for
Change Management

A lot of statistics out there state that 80% of the issues/ incidents that occur on the network are due to changes. This can be clearly experienced when a change hold is implemented, and faults are significantly reduced. NOC personnel spend a lot of their evenings and weekends executing and supporting change requests.

Opie's challenge:

"We are not consistent…It looks like people are making their own changes to the configs and at times it has caused outage situations"

So how can automation help reduce those un-authorized and inconsistent changes, alleviate some of those late nights and efficiently support the change management process?

1. Establish and automate standard changes that can take place on the network that are non-impacting, easy to implement, and routine in nature. Examples of these could be enabling and disabling switch ports for end users who move offices or changing VLANs. Leveraging an automation tool to execute these kind of changes reduces risk of manually "fat fingering" a change, ensures these changes are performed consistently and minimizes the access to the devices. More non-standard changes could also be automated but should follow the organization's normal change management process for approvals and assessing the risk.

2. Use configuration change reporting to automatically validate and report on the changes taking place on the network during change window timeframes integrate this with the Change management process and the Request For Changes opened.

3. Correlate Configuration Notifications, Configuration Management System Policy and Change detection Alerts with NMS incidents and alerts to highlight and track change related incidents. Having a report of what was changed on what devices as part of the incident means very short MTTR.

Automation support for
Performance & Capacity Management

Internal Customers, external customers, business units, VIPs. This is who the NOC supports and ensures the services are being delivered to their satisfaction. But sometimes services degrade or "seem" to degrade over time. Response times to services drop for the end users and who do they normally point the blame to as the issue, the network.

Opie has been presented with the following challenge related to the perceived "slow-downs" on the network:

- "There's a 6-8 week lag time for us to procure more bandwidth on our WAN links. We don't seem to see the capacity need until it is too late, when services slow down or stop working, customers start complaining, and the WAN links are overly congested. We have to find a way to get ahead of this capacity planning curve for congested WAN links and put in bandwidth increase requests before our customers see the impact first."

Getting a handle on how well your network is performing and understanding what "normal" is for the network can be difficult if you do not have proper visibility into the environment, not only from the network perspective but also at the services level. End-user services all "ride" over the network, and the NOC should understand how the traffic on the network is impacting those services. So how can automation be used to assist with performance and capacity management?

1. Establish an initial baseline of the network's critical devices and interfaces like primary WAN links to core sites, data centers, etc. to understand what "normal" looks like.

2. From the established baseline, set thresholds for CPU utilization, Memory utilization, bandwidth utilization, dropped packets and start alerting on those threshold breaches as they occur.

3. Based on recurring or consistent breaches from devices auto-open PROACTIVE incident tickets and provide the necessary information from the devices to perform initial triage of what's going on (see the incident management and problem management solution for automatically capturing this information). This should include the number of threshold breaches that occurred, the historical trend of the KPI/metric captured, the current state, and top-N traffic flows or top talkers for interface utilization (NetFlow will need to be enabled typically to capture this information).

4. Based on this information the NOC engineers and NOC leadership can determine the need for re-routing or offloading traffic, device upgrades, port upgrades, bandwidth upgrades and can then open up the required change request tickets to address the capacity and performance need, as most of these requests will involve funding and budgeting requests.

5. Roll all of this information into automated reporting, giving the necessary stakeholders knowledge into the status of their services.

Automation support for
Asset and Configuration Management

As mentioned earlier under the Change management section, 80% of the incidents that occur on the network are due to changes. And most of those changes are due to device configuration changes.

Look at Opie's challenge:

- I pulled a few device configurations down from the network and looked at them. There is a lot of variability in our device configurations out there on the network. We are not consistent. "
- "We need to get better control of our device configurations"

Having consistent hardware, software and device configurations on the network minimizes variability and reduces security and availability risks. Consistency helps simplify the ever growing, changing and complex network environment. While automation can't address physically replacing hardware on the network (refer to your release and deployment management process for that if you have one), it can take care of addressing software variability and device configuration inconsistencies. Let's see what can be done with automation to help ensure devices are consistently configured.

1. Asset Configuration Management

a. This is about the devices Inventory Configuration. We should check all the devices are running compliant software versions, hardware versions. This can be achieved very simply with FirstWave's Open-Audit Baselines feature or for more complex inventory with opConfig compliance engine.

2. Document and import the organization's configuration standards into a configuration tool like opConfig. Once the templates are loaded, automated tasks can be set up to do the following:

a. Schedule regular pull/backup of device configurations and use opConfig to detect and compare configuration changes. Then alert on those changes to ensure changes are correlated with events.

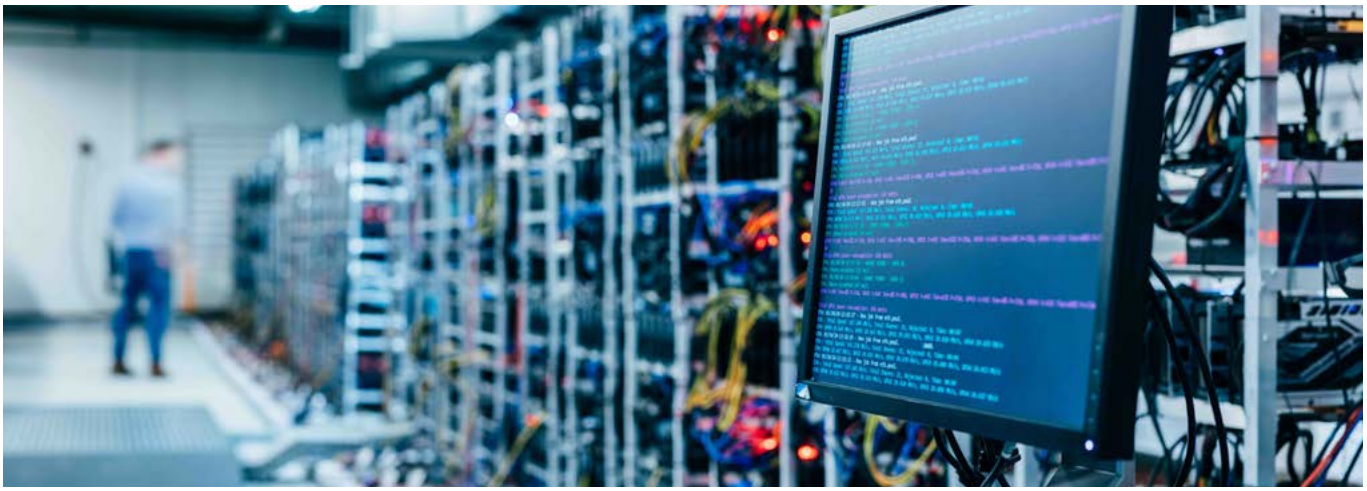
b. Schedule compliancy checks to ensure the device configurations adhere to the company policies and standards that are defined.

c. Remediate configurations based on non-compliance. Based on what is found for non-compliance the configuration management tool could be used to push out compliant configuration sections automatically to the devices as needed. Use caution with this step and use the change management process to record this kind of remediation (Refer to that 80% incident statistic mentioned earlier).

d. Push out new or changed configurations to the devices, especially if they have to be done in bulk, or to new devices just being "stood up" on the network. This saves a lot of manpower for people "ssh'ing" around the network and "screen scraping" configs or ftp'ing/ftp'ing configs from servers. Again, use the change management process to record and track configuration changes as well, even if they are standard configuration changes.

03 How FirstWave's Tools Support Automation & The Solution

Use REST API to Auto-open, Populate Incident & Problem Tickets with Necessary Information



In support of your Incident and Problem management processes, integrating FirstWave's Tools with your ITSM tools, like your incident ticketing system, is a way to become more efficient at responding to critical alerts and events taking place on the network that require some kind of action. No need to have NOC engineer watch the alarm console so much anymore. Use FirstWave's API through opEvents to auto-open incident tickets or problem tickets based on commonalities, repetitiveness in action and resolve, and higher priority alerts.

1

Start with just a subset of those higher priority more common alerts that happens infrequently, so you don't overburden the ITSM system. Auto-open tickets on more alerts as the NOC becomes more mature in the incident handling workflow process. As you trend the success of the auto-opened tickets, FirstWave tools can then be used to auto-resolve and auto-close out the incident tickets. If there is not an ITSM incident management tool available, you can use the master server of opEvents to serve as a technical service desk for your NOC personnel to respond and acknowledge alerts.

Use Event Correlation to Detect

+ Suppress Related and Dependent Events

2

Make use of backlinks from the ticket to the Event in opEvents so the engineer is led directly to the right Single Pane of Glass context for that event. This means the engineer is one click away from all correlated events, performance management graphs, configuration item change dashboards and diagnostic tools.

3

For recurring common incidents seen on the network, corresponding problem tickets can also be auto-opened, referenced and maintained. Which leads us to the next complementary capability within FirstWave's tool suite, "Using Automation to Diagnose, Troubleshoot, Collect and Report Information".

Refer to the following links in the FirstWave Community on how to configure and perform these tasks:

opEvents Input Sources – White and blacklisting

Summary Report Views in opEvents

Configuring Event Actions & Escalations in opEvents

Using Automation to Diagnose, Troubleshoot, Collect and Report Information

Complementing the auto-opening of incident and problem tickets is the need to provide timely and accurate information to support the alerts/events.

Again, supporting your Incident and Problem management processes, FirstWave's opEvents tool can be used to perform automated actions based on alerts, like SSHing into a router and collecting "show commands" which can then be collected and populated in to incident tickets, problem tickets or Knowledge articles (known error database).

A common process for larger NOCs who have well developed but inefficient processes is to simply take the most commonly use NOC Work Instructions and automate them.

Further troubleshooting tasks can also be automatically performed, captured, and even remediated using opConfig, originating from the opEvents triggers.

To see how one can automate refer to the following links in the FirstWave Community on how to configure and perform these tasks:

Webinar on Automation Event Response

Configuring opEvents Triggers opConfig to Collect Targeted

Configuring Event Actions and Escalations

Use Event Correlation to Detect

+ Suppress Related and Dependent Events

Having unnecessary alerts and events show up in an alarm display creates a lot of "noise" and "false positives" on the network that don't need to be show or acted upon. A lot of these extraneous alerts and events can be caused by upstream outages. In support of your Event and Incident management processes, FirstWave's tools can be used to correlate and suppress downstream events automatically, minimizing the alarm display and unnecessary incident tickets.

opEvents can be used and configured to do automatic event correlation, deduplication and suppression.

Refer to the following links in the FirstWave Community on how to configure and perform these tasks:

Configuring opEvents Event Correlation

Configuring Deduplication and Storm control in opEvents

Proactively Assess & Act on Performance & Capacity Needs

In support of your Performance and Capacity Management process and to become more proactive in managing capacity and responding to performance issues, FirstWave's NMIS can be configured with threshold settings for different metrics and KPIs. These thresholds result in alerts/events/notifications which NMIS can send when it sees a threshold breached.

These alerts can then auto-open proactive incident tickets for the NOC and engineering team to research further (see previous section on using the API to auto-open incident tickets).

NMIS has a set of Standard Thresholds defined but further definition and configuration of thresholds can also be set up within NMIS.

Refer to the following links in the FirstWave Community on how to configure and perform these tasks:

Understanding NMIS Threshold Configuration

Configuring Basic and Advanced Thresholds in NMIS8

Monitor & Remediate Compliance Issues & Maintain Consistency

In support of your Change Management as well as your Asset and Configuration Management processes, FirstWave's opConfig tool can be used to automatically monitor and manage device configurations ensuring compliancy and consistency.

To ensure your devices on the network adhere to your organization's configuration standards, opConfig's compliance engine can be used to monitor and report on non-compliant devices on the network.

To ensure devices maintain compliancy and are configured consistently, opConfig can automate or remediate configuration changes on the network without human intervention by pushing out the configurations, thus eliminating the configuration "fat-fingering".

Configuration change alerts can come from opConfig if a change is detected on scheduled configuration backup the resulting event can be processed and correlated in opEvents. Also, NMIS can trigger configuration change alerts based on SNMP polling whilst opEvents can interpret syslog and snmp trap events about configuration changes. Any of these events can trigger opConfig to immediately collect the latest configuration and prepare a config revision for viewing.

Refer to the following links in the FirstWave Community on how to configure and perform these tasks:

Webinar Responding to un-authorized changes

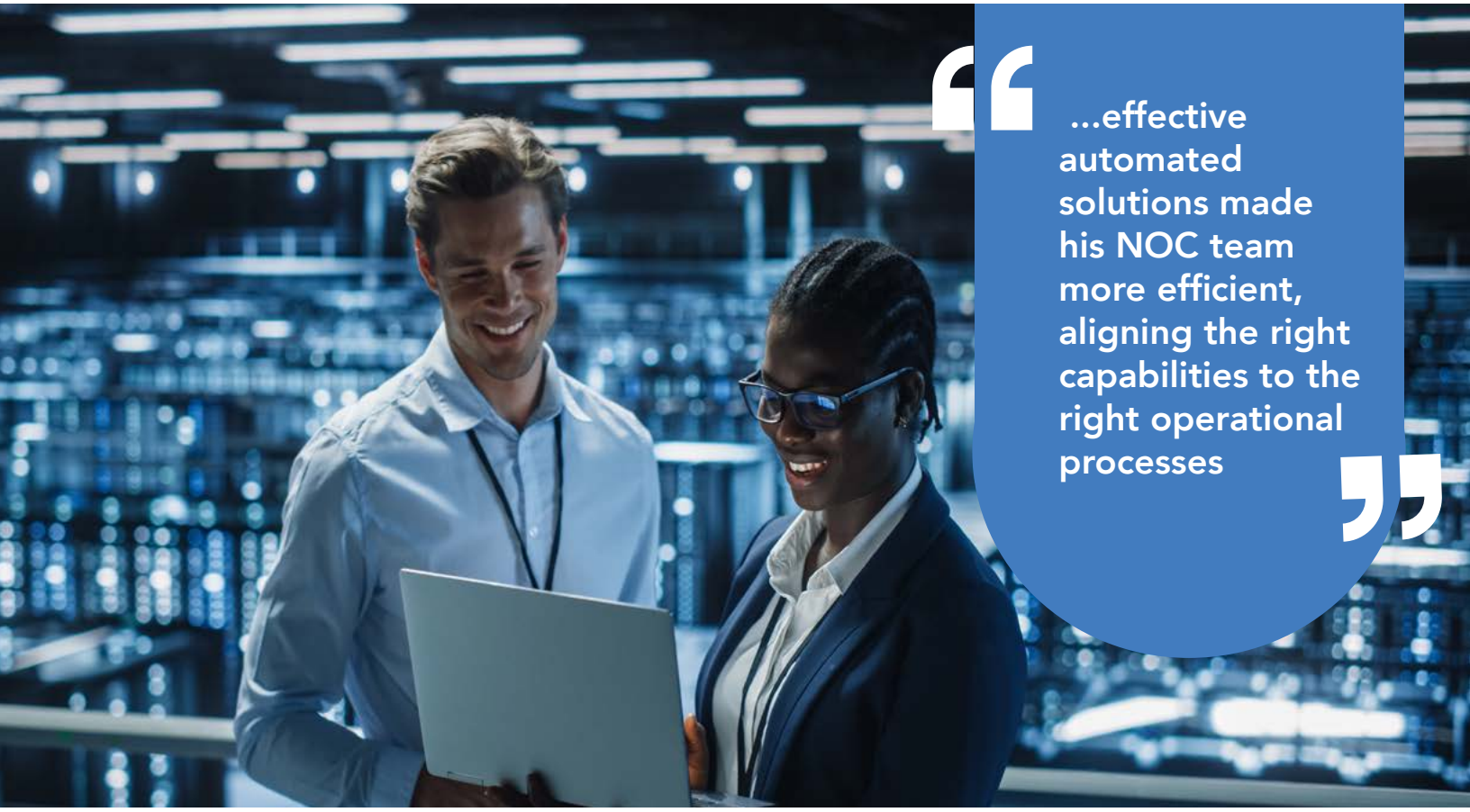
Using opConfig for Compliance Management

04 Benefits for Automating NOC tasks

With the above automated solutions provided by FirstWave's suite of tools in support of the organizations processes, NOC personnel can save manual efforts and cycles freeing them up to be more proactive and work on more important operational and engineering tasks. MTTR times will shrink, customer satisfaction will improve, and variability will be removed reducing risks in the environment.

Automation is now the crucial staple capability that augments the NOC team saving time for repetitive and menial tasks as well as driving consistency into the environment.

05 Conclusion



> ...effective automated solutions made his NOC team more efficient, aligning the right capabilities to the right operational processes

Opie was challenged with a pretty good list from his management to address and try to fix. After extensive research, through the use of FirstWave's suite of tools and the help of FirstWave support, Opie was able to come up with effective automated solutions and controls to make his NOC team more efficient, aligning the right capabilities to the right operational processes. Now Opie can only hope that the daily "surprises" in the NOC go away, or at least diminish.

About the Author

Rob Pavone

Network Operations Expert

Rob is an experienced technology Consultant spending most of his time helping organizations improve network availability, resiliency, and operational efficiency, as well as reducing Operational (OpEx) and Capital expenses (CapEx). He has been helping some of the largest enterprise organizations align business requirements with the level of service availability needed to support their business requirements. He has accomplished this through establishing operational baselines, comparing existing practices with industry identified leading practices, and providing actionable recommendations, improving the clients' processes, tools, and staffing resources. Rob has been in the IT network industry for 30 years, having spent the last 26 years at Cisco Systems in the support organizations of the Technical Assistance Center (TAC) and Advanced Services based in Research Triangle Park, NC. Rob has achieved the following notable accomplishments throughout his career: ITILv3 Expert, ITIL4 Managing Professional, CCIE, SCRUM Master.

FirstWave

Contact Our Experts

If you'd like some guidance around setup and configuration, or If there's a specific issue you're trying to solve in your network environment - click below to request a demo from an FirstWave engineer.

Book a demo

FirstWave

Our passion is to create intelligent software that our service provider partners and customers love.

Get Expert
Solutions

Book a demo

FirstWave is a publicly-listed, global technology company formed in 2004 in Sydney, Australia. FirstWave's globally unique CyberCision™ platform provides best-in-class cybersecurity technologies, enabling FirstWave's Partners, including some of the world's largest telcos and managed service providers (MSPs), to protect their customers from cyber-attacks, while rapidly growing cybersecurity services revenues at scale.

In January 2022, FirstWave acquired FirstWave Limited (FirstWave), a leading provider of enterprise-grade network management, automation and IT audit software, with 150,000 organisations using their software across 178 countries and enterprise clients including Microsoft, Telmex, Claro, NextLink and NASA.

Integrating CyberCision™ with FirstWave's flagship Network Management Information System (NMIS) and Open-AudIT product enables FirstWave to provide a comprehensive end-to-end solution for network discovery, management and cybersecurity for its Partners globally.

With over 150,000 organisations now using FirstWave technology, we are well positioned to be a leader of transformational change in the IT Operations and Cybersecurity world.

firstwave.com | connect@firstwave.com