Optimizing and Automating Event Management to Support Incident Management

White Paper by

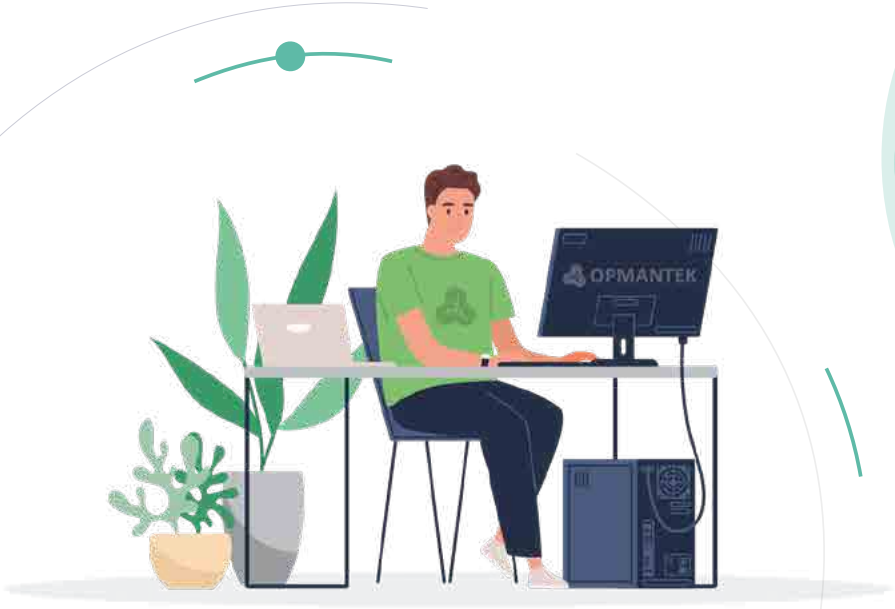
Rob Pavone

Network Operations Expert

OPMANTEK

Optimizing and Automating Event Management to Support Incident Management

Opie has just arrived in the office and sat down to check his email. "Holy moly!" He yells out. He is looking at a massive influx of email messages in his Inbox from the Event Management tool, which was just configured to send out the alert notifications via email. "There's no way the operations team will be able to respond to all those notifications in an efficient and timely manner. There has to be a better way to handle and address network events."



> **There's no way the operations team will be able to respond to all those notifications in an efficient and timely manner. There has to be a better way to handle and address network events.**

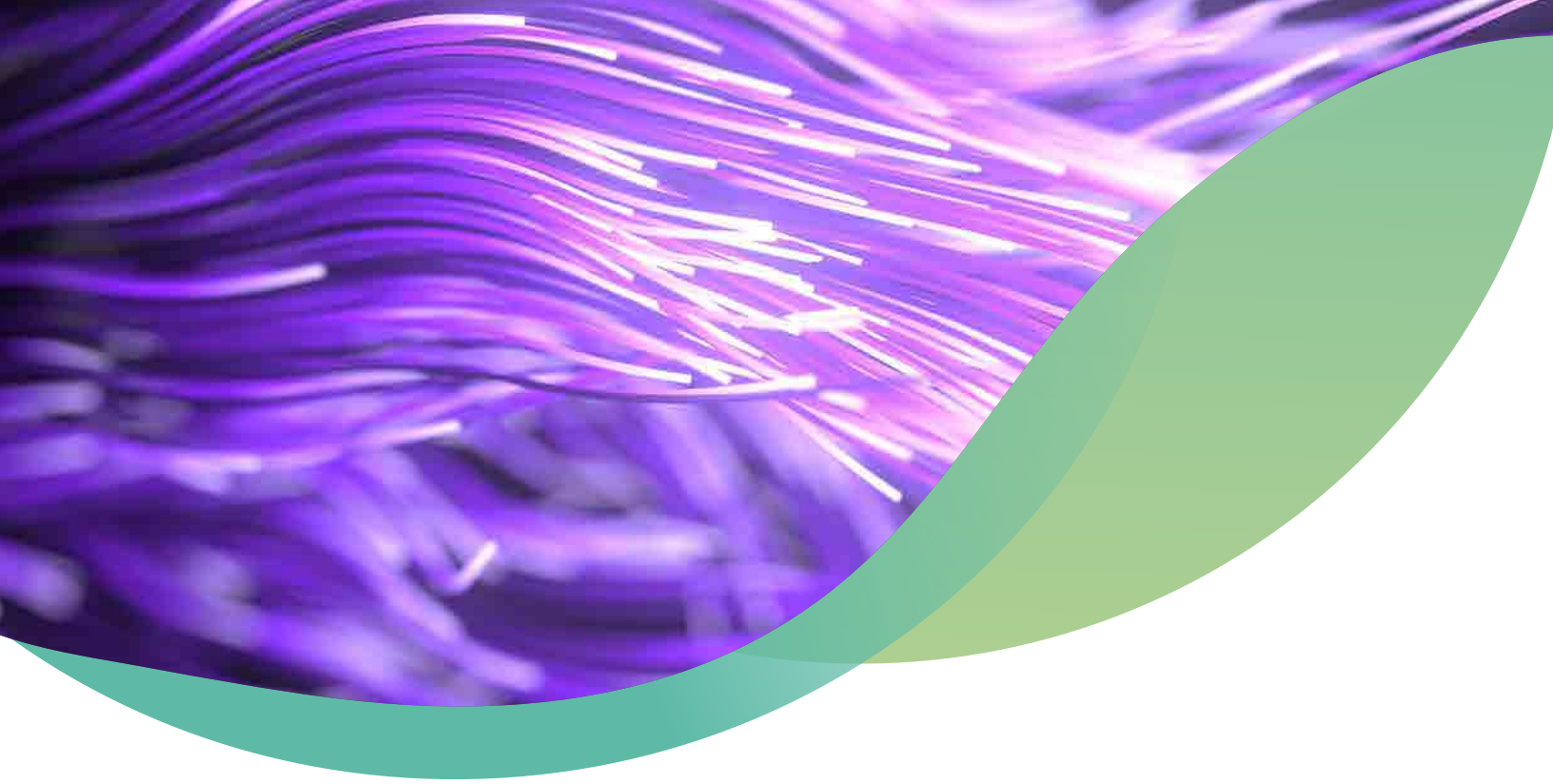


Table of Contents

01

Opie's Challenge To Resolve...

Opie's challenged with finding a better way to filter out and optimize the amount and type of events showing up in the operations team's Inbox, while providing the team with the necessary information needed to troubleshoot and resolve incidents taking place on the network, ideally before the customers and the business sees the issue. He needs to reduce the organization's mean time to resolution (MTTR).

Opie has established the following criteria to help eliminate the unnecessary "noise" seen from the event notifications:

1. **Only report events that require some kind of action**
2. **Suppress underlying events due to a broader related event**
3. **Provide more context around what the event "really" is telling us**
4. **Determine what events are proactive versus reactive, so the operations team can detect them before a customer does**
5. **Have the team track and record the events along with the actions taken through the company's incident ticketing tool**

02

Difference Between Events and Incidents

Before we help Opie identify a solution, we first need to differentiate an Event from an Incident.

- An incident is an unplanned interruption or a sudden reduction in the performance of an IT service. If an incident occurs, it means that something is already wrong.
- An event is a slight change in the state of the system or service in the IT infrastructure. If an event occurs, it is an indication of a possible system failure occurring in the future.
- All incidents are events, but not all events are incidents.
- Events are classified by criticality e.g. Information, Warnings, or Exceptions. For Incidents that require actions, we will primarily care about more critical events.

> All Incidents are Events, **But NOT all Events are Incidents.**

03

Proposed Solution To Address Opie's Challenges

Events and alerts coming in from the network can overwhelm a NOC and operations team to the point of not paying attention to the alerts anymore and throwing them into the “bit bucket", thus missing the pertinent and critical events requiring some kind of action and resolve. Ideally, you want to get your operations team to be more proactive in identifying actionable events before customers and end-users encounter an incident. Leveraging your Network Management tool and “fine tuning” it to notify appropriately will not only help out operations but also reduce the “noise” on the network.

The solutions presented in this whitepaper will help you establish an event management optimization strategy. It will focus on network management capabilities like correlation, automation and integration that will decrease the mean time to resolution of incidents, increase the effectiveness of operations and improve the end-user experience. This new event management strategy will also support your organization's incident and problem management process more efficiently.

We will look at four main capabilities available to you through Opmantek's tool suite to help resolve Opie's challenges:

1. **Filtering, Correlation, and Suppression of Event Notifications.**
2. **Proactive Automated detection, diagnosis and action on events**
3. **Enriching Event Information to support incident management**
4. **Integration with outside IT Service Management tools and processes, like incident ticketing**

Filter, Correlate and Suppress Event and Alarm Notifications

The first thing Opie needs to think about and address is the number of events coming from the network via the network management system(s). These events are comprised of SNMP polled "threshold" breaches, SNMP traps, and or Syslog messages triggering excessive email notifications.

Several tasks can take place to minimize the number of events the operations team needs to focus on:is the following:

1. Filter out only events that require some kind of action by the operations team or through automated tasks. This task may be "painful" at first because you may not know what kind of events to filter out, so your team will have to identify the critical events that warrant acknowledgement, action and initial human intervention. **Utilize the opEvents summary reports for identifying events statistics, metrics and impacts on the network. Start by focusing on the following types of events at a minimum:**

- Events from devices deemed as critical to the business based on role, function or location – Ex. Data centers, core, manufacturing, etc.
- Node down
- Interface down – especially single points of failure links
- Route peers down (ex. BGP neighbor)
- Reboots
- Warning and Critical level Syslog messages
- Threshold breaches based on your Network Management tool settings you defined or defaulted within the tool, or SNMP trap settings (ex. Environmental, CPU, Memory, excessive bandwidth usage if configured)

If an event comes through that is filtered out and not initially identified and an incident results from it, then add that event back into the notification criteria. Over time, accurate, actionable events will be captured and reported.

Filter, Correlate & Suppress Event & Alarm Notifications Cont.

2. Correlate (use Downstream device dependency) and correlate and suppress events based on events relating to the same groupings or locations or services as well as complementary related events (ex. Interface down because of the neighbor device down). This can be an arduous task for a human to do, so relying on the intelligence of a network management system (NMS) capability is recommended. There is no need to notify or alert on events that are a result of a residual event from a broader event or incident (the "parent-child" relationship for dependencies), however, understanding the relationship is important as the event can still be saved with the "parent" event. We will discuss specifics around this capability using Opmantek's tools in the next section: "How Opmantek's Tools specifically supports the Solution".
using Opmantek's tools in the next section: "How Opmantek's Tools specifically supports the Solution".

3. If email or sms (text) notifications are required, only send out alerts that require actions. Over time, as the operations team matures, these email notifications may be minimized if not eliminated. Actionable events can then be integrated with and monitored through your incident ticketing system.

Proactive Automation to Detect, Diagnose & Act upon Event & Fault Alerts

To get a handle on actionable events coming from the network, either via human intervention or through automation, Opie and the operations team needs to "get ahead" of the incidents and become proactive. Find the incidents before end-users and the customers see the issues.

You can minimize the reactive responsiveness by setting up and doing the following tasks within your network management tool:

1. Set exception thresholds for SNMP polled objects like CPU utilization, Memory utilization, bandwidth utilization, and dropped packets and start alerting on those threshold breaches as they occur. You can also rely on SNMP traps or Syslog messages for warning and critical events built into the vendor product as well, like environmental information from routers (ex. CPU, Temperature).

2. Based on recurring or consistent breaches from devices, auto-open PROACTIVE incident tickets (see "Integrate with your Incident Management Process and Incident Tracking Tools" section in this document) and have the operations team work those "tickets" to resolution.

3. Provide the operations team with necessary and timely information from the network in support of an incident. Using automation, collect and insert valuable diagnostic information into the PROACTIVE incident tickets related to the event, like "Show" command CLI output from the device having the issue along with appropriate Configuration Item (CI) information about the device. Group data that can be automatically collected, like the "show" command information, and include it in the incident tickets.

4. Leveraging the automated collection of diagnostic information, provide the operations team with a common interface (besides the CLI) they can work from to acknowledge and troubleshoot incidents in a consistent timely manner having everything at their fingertips. The troubleshooting information can then be synced with your IT Service Management incident ticketing system for reporting and tracking.

Event Enrichment

Complementing the automated collection of diagnostic information from the network, it would be ideal to "enrich" that collected information with other pertinent information that is related to the event and helpful to Opie and the team for resolving incidents, minimizing MTTR. This enriched information can be imported in from outside sources (outside from what your NMS collects and stores) or parsed from information in event sources, like the logs, CMDB, CRM, or ERP systems. **Examples of this kind of information could be location, business service, customer name, circuit ID, location, or contact information.**

Integrate with your Incident Management Process & Incident

Again, not all events are incidents, but when incidents occur and require actions, your operations team should track those incidents for the business. A lot of network operation organizations say their team is always "fighting fires," "interrupt driven," and "don't have time to be proactive." It is VERY important for Opie's management to track, record and report to senior leadership what their team is working on, especially if it is reactive in nature. This proof is how the operations team can justify the need for more resources and support as well as show the business where vulnerabilities and issues reside in the network.

Leveraging the capabilities already addressed previously in this document, supporting your incident management process is critical. In order to accomplish this, the following tasks and capabilities can be enabled and set up in Opmantek's tool suite:

1. Auto-open incident tickets based on actionable events seen on the network from Opmantek's NMIS. Start with only one or two events (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 operations team becomes more proficient with handling these kinds of incident tickets, look to add more events that auto-open the tickets.

2. As mentioned earlier, collect and insert valuable diagnostic information into the incident tickets related to the event, like "Show" command CLI output from the device having the issue and appropriate Configuration Item (CI) information from the CMDB about the device.

04

How Opmantek's Tools Specifically Support The Solution

There are several capabilities and features within Opmantek's tool suite that can be used to address the different parts of the solution identified. We will discuss each one.

Use NMIS & opEvents to Filter, Correlate, Detect & Suppress Related and Dependent EventsTracking Tools

There are several places within Opmantek's tools to filter out events: NMIS and opEvents. NMIS is the source of the events coming in from the network, and you can do an early discard of events you know you don't care about by using **Event Configuration.** If you opt to forward events to opEvents, you can establish **whitelists and blacklists** of the events, or **Configure Event Actions and Escalations** to deprioritize certain events.

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

Use NMIS & opEvents to Filter, Correlate, Detect & Suppress Related & Dependent EventsTracking Tools Cont.

Leverage the Top-N Events **Summary reports** in opEvents to help identify the majority of the events seen on the network so you can make a decision on which ones to initially focus on. **opEvents** can be used and configured to do automatic **event correlation**, **deduplication and suppression.**

Once you have identified actionable events (aka incidents), you can then **set up email notifications** and **customize the email template** if you like. ***Note: If you are auto-opening incident tickets based on the majority of the actionable events, then sending out email notifications when the event occurs may not be necessary except early on in determining what events are important.***

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

Managing Events in NMIS

opEvents Input Sources – White and blacklisting

Summary Report Views in opEvents

Configuring Event Actions & Escalations in opEvents

Configuring opEvents Event Correlation

Configuring Deduplication & Storm control in opEvents

Setting up Email notifications

Creating Email templates for Event Notifications

Use automation in opEvents and opConfig to Proactively Diagnose, Troubleshoot, and Act on an Event

In support of your Incident management process, Opmantek's **opEvents** tool can be used to **perform automated actions** based on events, like SSHing into a router and collecting "show" commands which can then be collected and populated into incident tickets.

A common process for larger Network Operation Centers (NOC) who have well developed but inefficient processes is to simply take the most commonly used 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.

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 operations team to respond and acknowledge events.

To see how to automate and manage events more efficiently, refer to the following links in the Opmantek Community to configure and perform these tasks:

Webinar on Automation Event response

opEvents Technical Service Desk

Configuring opEvents Triggers
opConfig to Collect Targeted Diagnostic Data

Setup Thresholds in NMIS for Managing Events

To become more proactive in managing incidents before end-users and customers see an incident, Opmantek's **NMIS** can be configured with threshold settings for different metrics and KPIs. These thresholds result in alert notifications which NMIS can send out when it sees a threshold breached.

The alert notifications can then auto-open proactive incident tickets for the operations team to research further (see "Use REST API to Auto-open and Populate Incident Tickets with Necessary Information").

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

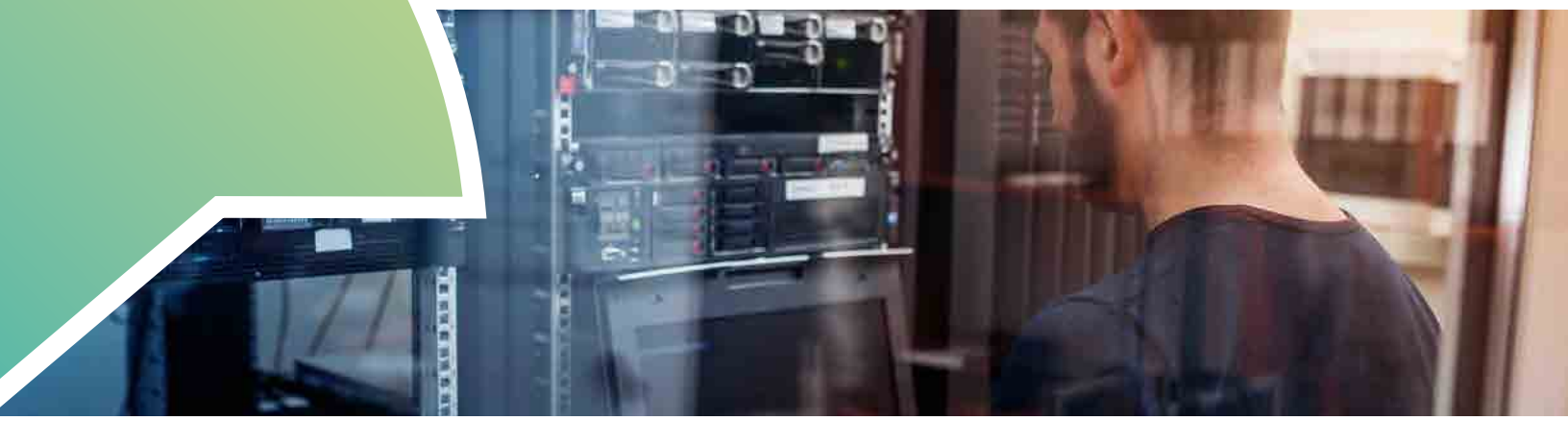
Refer to the following links in the Opmantek Community on how to configure and perform these tasks:

Understanding NMIS Threshold Configuration

Configuring Basic and Advanced Thresholds in NMIS8

Use plugin Capabilities in opEvents to Enrich events with External Information

While monitoring events on the network via NMIS, some of those actionable events reported may seem a bit "cryptic". Thus you're not sure how your operations team should handle the Event. Building some intelligence into what the events REALLY mean, will require accessing external resources like CMDBs or CRMs to provide pertinent information related to an event. Importing that data into opEvents will contain more enriched information for the support staff to have direct access to at their fingertips.



Leveraging Opmantek's **plugin capabilities in opEvents**, enriched data (ex. Circuit IDs, BGP neighbor IP address) can be added to the Event and can be visually displayed in opEvents and opCharts. **Example of enriched data based on a BGP neighbor down event:**

```
'wan-router1--192.168.1.249' => {
   'BGP_Neighbor' => '192.168.1.249',
   'CE_Address' => '192.168.1.254',
   'Circuit_Role' => 'circuit-primary',
   'Management_IP' => '192.168.1.254',
   'WIN_Name' => 'WG123',
   'country' => 'Australia',
   'location' => 'Graceville',
   'location_id' => '888',
   'node' => 'wan-router1',
        'original_node'  =>  'wg123_ankydmw-1-r0-
usipn__peer_10.140.218.78'
```

This enriched data, along with the Event and any results from automated diagnostics, can then be sent to your IT Service Management system for incident ticketing via API integration from opEvents, which leads us to the next capability.

opEvents: External Enrichment of Events

opEvents: Event Enrichment using Parser Plugins

Use REST API in opEvents to Auto-open & Populate Incident Tickets with Information

In support of your Incident management process, integrating Opmantek's Tools with ITSM tools, like your incident ticketing system, is a way to become more efficient at responding to critical events taking place on the network and require some kind of action.

No need to have a support engineer watch the alarm console so much anymore. Use Opmantek's API through opEvents to auto-open incident tickets based on commonalities, repetitiveness in action and resolve, and higher priority events.

Start with just a subset of those higher priorities more common events that happens infrequently, so you don't overburden the ITSM system. Auto-open tickets on more events as Operations becomes more mature in the incident handling workflow process. As you trend the success of the auto-opened tickets' resolutions, Opmantek tools can then be used to auto-resolve and auto-close out the incident tickets using automation for verified and proven resolution

Make use of backlinks from the incident 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.**

Configuring opEvents REST API

Benefits of Optimizing your Event Management Process

Events from your NMS is your window into how well your network is performing and operating. Without that view, it is difficult to understand what is normal, what is wrong, and what could be going wrong. Being able to optimize, automate, and understand the events on your network will:

1. **Reduce operations team intervention and effort from false positive alarms and wasted troubleshooting.**

2. **Foster quicker response times from the operations team and from your NMS tool for real incidents thus reducing MTTR.**

3. **Increase the operations team's effectiveness by being more proactive in taking actions on events not yet seen by the end-user**

4. **Supports and matures your incident and problem management process through richer information being captured for the operations team before the first response or first "touch."**

5. **Improves the end-user experience, increasing overall customer satisfaction.**

05 Conclusion

Opie and his operations team were overwhelmed with the number of notifications coming from his network management system. Thus critical events requiring some kind of action were probably getting lost with all the “noise.” Opie tackled this issue by defining what he knew his team needed to see and how his team and the NMS tool needed to respond. He leveraged several capabilities available within Opmantek's tool suite to solve this problem:

- **Correlation**
- **Dependency mapping**
- **Event Actions (automation)**
- **Integration**

His event management process is more streamlined and useful for his team to act on.

If you have more questions about the different solutions presented here, please reach out to **Opmantek's Support.**

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.

OPMANTEK

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 Opmantek engineer.

REQUEST A DEMO

FOR MORE INFORMATION CONTACT YOUR NEAREST REGIONAL OFFICE OR VISIT OPMANTEK.COM

OPMANTEK USA
(USA & CANADA HEAD OFFICE)
315 Montgomery Street, 10th Floor
San Francisco, California 94104
United States of America
PH: +1 512 430 4450
E: usa@opmantek.com

OPMANTEK MEXICO
(LATAM OFFICE)
Mexico City Paseo de la Reforma 342
Floor 26 Col. Juarez, C.P. 06600 Mexico, D.F.
PH: +525 584 213 294
E: latam@opmantek.com

OPMANTEK AUSTRALIA
(ASIA PACIFIC OFFICE)
50 Cavill Avenue
Surfers Paradise, Gold Coast
Queensland 4218 Australia
PH: +617 3102 3042
E: apac@opmantek.com

OPMANTEK UK
(EUROPE OFFICE)
7200 The Quorum
Oxford Business Park North,
Garsington Rd
Oxford OX4 2JZ, United Kingdom
PH: +441 865 522 032
E: europe@opmantek.com