DATAMINR PULSE

Dataminr How-to Guide:

Use Real-time Information for Better Risk Mitigation and Protection

DATAMINR PULSE

Over the past year, 70 percent of security and risk leaders globally experienced at least two critical risk events that endangered their organization.

While the majority of a security team's time is spent on preparing for and monitoring risks, it's equally important that security teams be able to effectively act on risk information. That's why many enterprises employ sophisticated, real-time alerting tools like Dataminr Pulse for Corporate Security—an end-to-end, AI-powered solution that enables security leaders and teams to better prepare for and monitor risk exposure, initiate incident responses and notify employees of potential threats.

According to a Dataminr-commissioned Forrester study, more than half of the surveyed security and risk decision makers plan to implement or increase investment in real-time alerting solutions in the next 12 months. Seventy percent of the respondents also said an effective real-time alerting tool would have helped significantly or completely mitigated the impact of the most disruptive risk incident they encountered last year.

The majority of a security team's time* is spent **preparing** for potential risks, and then **monitoring** the world to know what is actually happening...

40% Prepare

50% Monitor

10% Respond

* Percentages are approximate

©2023 Dataminr

While many security teams are already armed with this crucial, real-time data, some find it challenging to operationalize it. Teams should keep in mind that real-time alerts are often a catalyst for their security workflow when an incident occurs, and enable them to maximize the time needed to assess risks and accelerate responses—especially in critical, time-sensitive situations.

Dataminr's Real-time Information Defined:

The alerting on risks and events in the seconds or minutes after they happen, ensuring recipients are the first to know of such occurrences—providing the context and clarity needed, as an event unfolds, to respond quickly and better mitigate risks and business disruptions.

Real-time information benefits regardless of an organization's industry and size.

It enables security and business leaders to:

- Identify the risks that are most relevant to their organization based on type, location and severity
- Swiftly assess whether a potential risk will impact their organization
- Determine the safety of employees, customers and assets
- Quickly seek the right response and course of action
- Gauge any enduring impacts on business continuity

Operationalize Real-time Information

In our experience working with numerous security leaders, functions and teams—from global, large and mid-sized corporations across myriad industries—enterprises that successfully leverage real-time information are those that think of it as their first layer of risk management and crisis response. Below we share our learnings on what a typical security workflow looks like, followed by our best practice recommendations.

The Best Defense: Prepare for the Unexpected

It's important to note that the most effective way to operationalize real-time alerts is to plan for risks and events ahead of time. Leading security teams know this to be true and, as such, make pre-planning the first step.

This includes establishing pre-planned strategies for how to handle different risk scenarios, determine who will be involved in decision making, and agree on which steps to take when an incident arises. When done right, security teams:

- Can collaborate and communicate with teams and stakeholders across the organization to plan for and manage risks and events
- Have playbooks and standard operating procedures on hand to aid decision making
- Understand and prioritize what risks or events require real-time alerts

DATAMINR PULSE

Recommendations for Operationalizing Real-time Alerts

The recommendations below provide a step-by-step look at how to use real-time alerts to better mitigate risks and protect people, assets and brands. However, it's important to remember that the process is not always linear. The order of your workflow may end up being slightly different. What's key is that you take action on the real-time information relevant to your organization.

Typical Workflow for Acting on Real-time Alerts

As enabled by Dataminr Pulse for Corporate Security

1

Discover Risk:
Use real-time alerts to identify critical events and potential threats and disruptions

2

Contextualize Real-time Information:
Leverage rich visual data to obtain the context needed to evaluate and prioritize risks and critical events

3

Collaborate to Manage Risk:
View and manage risk(s) from end-to-end, including real-time collaboration with any and all key stakeholders

4

Communicate With Employees:
Notify and confirm the safety of affected employees in real time, regardless of location

Assess risks and determine potential impact

The real-time alerts you receive are the catalyst for your security workflow. Use them to assess whether the risk is relevant to your organization and determine its potential impact. You can use alerts to help you plan for known events in the future (e.g., a major company conference), and to inform your response in the moment to unexpected critical events.

Recommendations:

- Have suitable operating procedures and playbooks—which should reflect your pre-planning—and tracking methods to ensure the right people are aware of emerging risks and are equipped to deal with them
- Know your business' critical information requirements and how to map incoming data to those requirements
- Turn information into intelligence and have a designated person responsible for the task
- Differentiate the information that goes to the doers versus the in-the-knowers
- Ensure people who need to take action are fully informed with the latest and most granular information
- Inform those who need to be aware of risks, but might not have to take action, of how to react

1

Actionable and relevant alerts

Dataminr alerts are generated from 800,000+ public data sources and are tailored to the needs of each customer, ensuring they receive only the information most relevant to them. Alerts cover global, regional and hyperlocal data translated from 100+ languages and in multiple formats.

Information vs. intelligence

To turn relevant information into actionable intelligence, you need to understand and apply the business-related context. An intelligence collection plan should be dynamic, rather than static, and supported by real-time information.

For example, if you want to have early warnings of any emerging risks to your global real estate, you'll need real-time alerts on specific and well-defined real estate criteria. You can then determine how to turn that real-time information into actionable intelligence that supports decision making.

Get additional context

Geospatial tools bring the relationship between data points to life. Use them to visualize the information contained in the real-time alerts to determine where the risks or events are occurring in relation to your personnel, facilities, assets and supply chains. With this visual context, you can better assess the full scope of potential impacts and business disruptions, and take action faster and more proactively.

Recommendations:

- Map and organize your assets by categories, such as asset type, location groups, alert types and other contextual data layers
- Set up personalized lists which will provide you with tailored views of real-time alerts that are relevant to your organization across a range of topics and geographical areas
- Zero in on and assess data from local areas of interest with geofencing tools
- Sort the alert urgency levels by color and easy-to-understand iconography to reflect your priorities—whether your security operations are global or local. This helps your team interpret the threat any alert poses to your operations at a glance

2

Prepare for and manage extreme weather events

Extreme weather events are increasing in frequency, severity and unpredictability. Organizations should tap into effective geospatial technologies to help them better understand exactly where risks lie and their potential effects. These tools can empower security teams to respond with precision and clarity to ensure:

- Duty of care
- Supply chain continuity in times of disruption
- Business continuity
- More resilience

Download eBook to learn more about how to Use Geovisualization to Prepare for Severe Weather

Kick off risk management protocols

Now that you know what the risk(s) is and its potential impact, it's time to officially initiate and manage your response. Risk management tools enable you to collaborate cross-functionally and throughout your entire organization to activate a rapid and consistent response.

Recommendations:

- Activate your security team without delay. This is especially true if the event looks like it could turn into a crisis. Get your team on standby at the earliest opportunity.
- Break out the playbook. Your playbooks should include the most optimized, pre-determined workflows with specific actionable steps users need to take if and when an event occurs. You can build or modify your response strategies for various scenarios in these playbooks by analyzing past incidents and crises.
- Follow your plan. Ensure your team follows the response plan that you created and rehearsed for similar scenarios. The goal is to not go off course or try to recreate the wheel—when possible.
- Rapidly schedule meetings. In addition, assign and prioritize tasks for team members or guest users. This streamlines teams' collaboration, communication, response protocols and critical information flows.
- Set your strategic intent. Articulate your goals and ensure alignment within the team. What does success look like? This should be formally established and communicated via your communications channel(s). Doing so helps guide decision making and prioritization.

3

Post-incident must-do:

Make sure you have an active, minute-by-minute audit trail, with clear records and analytics of your teams' actions so you can understand and identify what worked, what didn't and areas for improvement. This allows your teams to conduct post-incident evaluations, study the dos and don'ts, and tweak the playbooks accordingly to continually optimize the workflow for future events. Do this often.

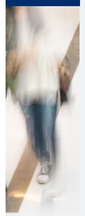
Notify affected employees

After determining who and what in the organization is at risk, notify affected employees of those risks in real time via SMS, email or voice—and confirm their safety before, during and after the risk event.

Recommendations:

- Confirm the safety of employees through multiple modes including SMS, e-mail and voice
- Disseminate key messages quickly and succinctly, but only after having first confirmed the known facts of the situation and finalized an emergency response plan
- Refine messages down to a few digestible key points to minimize stress and make sure employees are clear on what the next steps are
- Let employees know the action(s) you expect them to take. For example, you could ask if they are unsafe or need emergency assistance by requesting one or two text responses: 1=OK, 2=HELP!
- Be transparent and honest with employees about what is known and what is not

4



Pulse's two-way notification system

Our two-way notification capabilities help you keep your employees informed and safe, whether they're traveling, in the office or working remotely. Watch our video to learn more.

DATAMINR PULSE

Through years of working with leading global enterprises, we know that planning ahead, and identifying and acting on incidents as soon as they occur is paramount to mitigate risk and minimize business disruption.
But keep in mind that, as discussed earlier, the security workflow is not linear and varies by organization and/or risk type. No matter the approach, effective incident management will allow security teams to achieve their end goal: help their company build and strengthen business resilience.

Dataminr Pulse Customer Experience

Global pharmaceutical company Alnylam Pharmaceuticals has seen significant success in using Dataminr Pulse for Corporate Security and acting on its real-time alerts to safeguard its workforce and critical facilities that manufacture life-saving medicines.

In December 2022, Pulse delivered real-time alerts on advance notice of tornadoes in Texas, giving Alnylam's security team the crucial lead time needed to determine the employees and facilities that could potentially be affected. The team was then able to quickly and effectively coordinate their response strategy, including how to inform and guide employees in impacted areas and confirm their safety. Learn more.

DATAMINR PULSE

Learn More

Learn how Dataminr Pulse for Corporate Security can help. Its end-to-end solution has the real-time information and integrated tools needed to plan for and respond to risks and crises faster and more effectively.
dataminr.com/dataminr-pulse-for-corporate-security

Realize the full benefits of real-time information and how to leverage it more effectively.

Request a Demo

©2023 Dataminr All rights reserved