ONSOLVE
By CRISIS24

EBOOK

The Risk and Resilience Professional's Guide to Responsible AI

How to Identify the Right AI for Critical Event Management

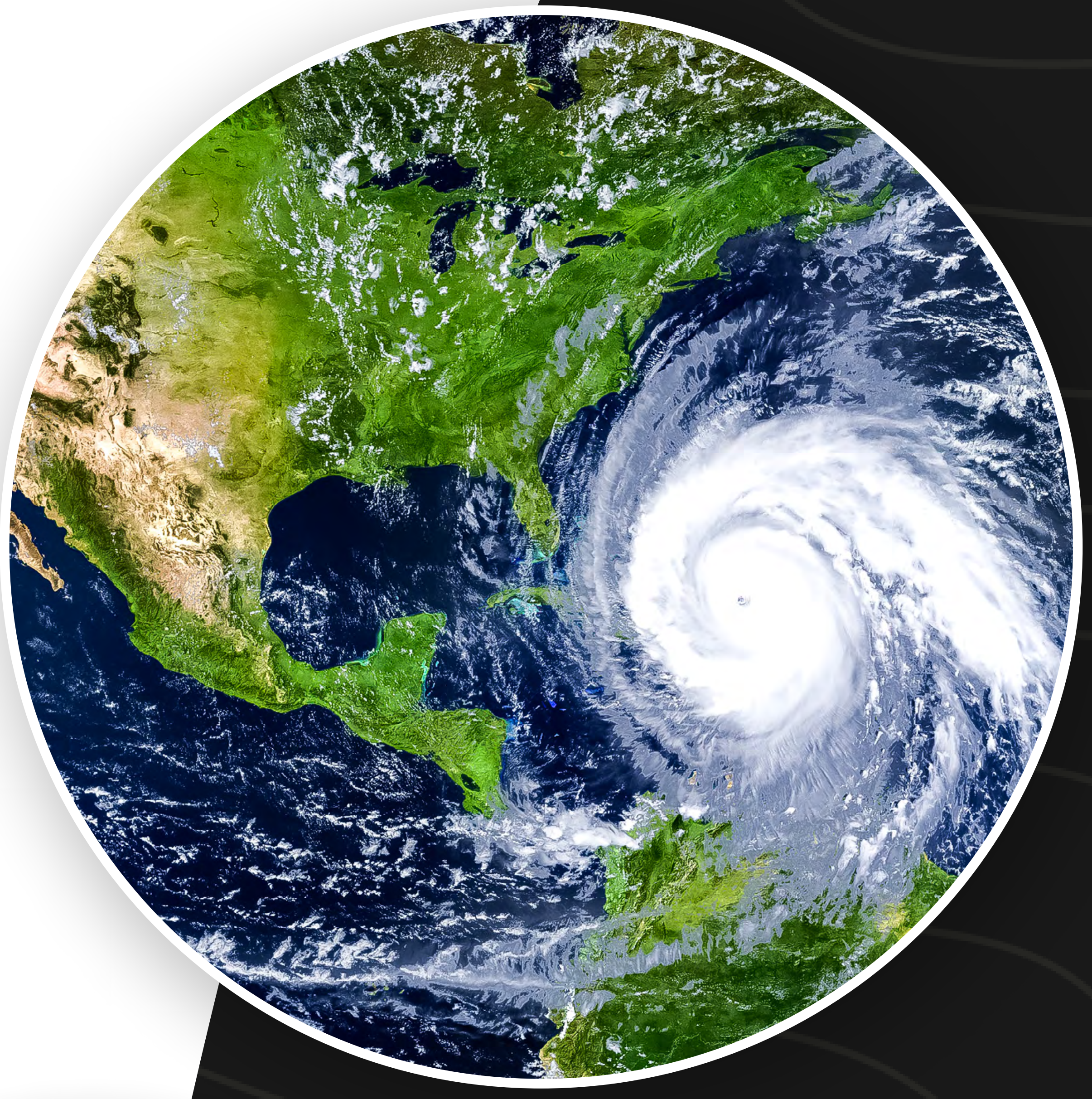
The dynamic risk landscape is harder to manage. AI can help.

There's a hurricane barreling toward the Gulf of Mexico. Public tensions over an upcoming election threaten to boil over into protests. Crime is popping near one of your key production facilities.

The size and complexity — not to mention the cascading impacts — of each threat mean risk and security teams must evaluate millions of data points to determine what's relevant.

Artificial intelligence (AI) has emerged as a solution to support fast, accurate decision-making in the face of data overload.

But while evolving technologies like generative AI show potential for critical event management (CEM), risk and resilience professionals are left questioning how it can and should be used before, during and after a crisis.



The volume of the world's data is projected to grow to **more than 180 zettabytes** by 2025.

— Statista

99%

of executives and

100%

of U.S. government leaders said their organization or agency experienced a physical threat in the last 24 months.

— 2024 OnSolve Global Risk Impact Report

Every organization is likely to face a physical threat in this dynamic risk landscape — and they'll need to be prepared to mitigate the impact.

Protecting people and operations requires around-the-clock monitoring and the ability to quickly make sense of an extraordinarily large volume of data.

That's why risk and security professionals are considering the role of AI to improve the:

SPEED
of threat detection

RELEVANCE
of information received

ABILITY
to act quickly

But what kind of AI works best for critical event management? It's important to understand:

Not all AI is **created equal.**

We encounter AI every day.

AI covers a range of evolving technologies, each with different use cases.

Consumers engage with AI regularly. The technology powers tasks such as personalized recommendations on Netflix, automatic corrections to our photographs and predictive text in our writing applications.

More recently, many people — from students to businesspeople across industries and regions — are finding applications for generative AI (such as ChatGPT).

For organizations and executives, it offers a powerful promise to drive efficiencies and boost productivity across the enterprise, ultimately delivering a competitive edge.

Artificial Intelligence (AI):

Anything that mimics intelligence.

37%

of C-suite executives and

40%

of senior managers say they regularly use generative AI at work, outside of work or both.

42%

of C-suite executives and senior managers have used it at least once.

— McKinsey

Right now, the field of AI is growing rapidly with new subsets and types.

To better evaluate AI for critical event management, risk professionals should begin with a clear understanding of a few core capabilities:

1 **Natural Language Processing (NLP)** uses machine learning to help computers understand human language. It's extremely important for critical event management because many reports are written using natural language.

2 **Machine Learning (ML)** enables machines to learn without being explicitly programmed. If it sees language like "high winds" or "rotation," it learns to mark the event as a weather event.

3 **Generative AI** is trained on an extremely large, public dataset and is capable of understanding and generating language. The size of training data makes it more flexible.

Risk managers and security professionals might be wondering:

Which types of AI can help me identify risk sooner, make decisions quickly and act faster?

How is AI used for critical event management?

AI can help improve the **speed of threat detection**, the **relevance of information that's received** and the **ability of risk professionals to act quickly**.

Yet, generic AI solutions aren't a good fit for risk management because they aren't designed for specific risk intelligence and communications tasks.

The same AI that powers a warehouse robot can't answer customer questions about an order. A chatbot trained on retail customer support can't identify an incoming hurricane — or if it will impact the warehouse or the customer.

The right AI will be specifically designed and used to meet the purpose of a task.

We call this **responsible AI.**

Remember:

Risk and security professional need AI that's fit for the purpose of critical event management. Solely relying on public large language models (LLMs), like ChatGPT, is insufficient. Not all LLMs can understand linguistic, cultural, and historical nuances when identifying and contextualizing critical event information.

AI alone does not deliver actionable intelligence.

Effective critical event management requires actionable intelligence. Actionable intelligence is achieved by leveraging human discernment in combination with the data obtained by the AI. In these examples, responsible AI provides actionable intelligence so risk leaders can act quickly.

Active Assailant Example

The risk management team receives a report of an active shooter at a nearby high school.

AI processes a large volume of primary and secondary sources — such as police reports, local news coverage and social media — at very high speeds. It surfaces important details quickly and connects them across many different reports.

With responsible AI, the team knows they're reviewing sources vetted by analysts with domain expertise. In addition, because it's the right model for this purpose, it's evaluating information within the right context.

Without sifting through all the individual reports, the team is confident they're being alerted to an event that may impact them.

Severe Weather Example

A tornado is detected in proximity to a manufacturing plant along a main supply route.

AI triangulates warning signals and notifies decision-makers. Leaders gain the time they need to shift operations and reroute shipments in advance, so employees are kept safe and business disruptions are minimized.

AI doesn't make the decisions for the leaders, and it doesn't compose the emergency alerts. It provides the information necessary to take proactive steps and deliver the right messages to the right audience.

There are many ways technologies such as AI can be misused. How can risk and resilience professionals identify responsible AI for critical event management?

Use these four criteria:

Application

"Should we?" rather than "Can we?"

For CEM, extractive AI is best.

For example, when analyzing a report related to a critical event, this type of AI looks for specific information already referenced within the report and answers questions such as "Is this risk ongoing?" instead of "Is it safe?"

Pro Tip: Look for extractive AI. It doesn't make judgment calls or perform tasks outside of the area of training.

Selection

Purpose Built

Most AI models perform best when optimized for a specific task. For instance, the AI model used in a delivery robot won't be good at identifying a wildfire that could threaten your operations.

A task such as creating an event report could contain many AI models — from ingesting and cleaning data to identifying severity and clustering.

Pro Tip: Break down larger tasks so the appropriate AI model can be optimized for performance.

Fine Tuning

Garbage in = Garbage out

The source of data can range from traditional media to social media, government, analysts and more.

Social media content, for example, is often much shorter than traditional media content. This may introduce abbreviations in communication that have a different meaning within the context of event reports.

Pro Tip: Train the AI models with appropriate data for each task for better accuracy.

Quality Assurance

Process and Bias

Bias in this context means ensuring the model isn't behaving differently than its intended design.

Quality assurance (QA) for responsible AI should include:

- Monitoring for accuracy at every stage
- Incorporating feedback in the QA process
- Including continuous iteration in your process

Pro Tip: Put processes in place to validate performance and detect bias.

Responsible AI: A checklist

Responsible AI for critical event management delivers data that's specific and relevant — and actionable. It looks for particular information and filters out extraneous data to identify events that could impact your people and operations.

A critical event management platform that uses AI responsibly should:

☑ **Focus on the physical threat landscape,** versus a generic solution like ChatGPT. It's essential to have accurate data on the dynamic risk landscape, not just a singular event based on limited data.

☑ **Leverage established domain expertise in risk management**, including AI and language processing.

☑ **Be fit-to-purpose for CEM and your industry**, based on solid research into models and technology tailored to specific industry needs.

☑ **Use a tested process** that includes authentication, correlation and analysis to ensure the data is relevant to your organization and specific to events likely to impact your people and operations.

☑ **Assign context-driven severity levels** and update them as new factors come into play so leaders can assess the big picture and stay on top of fluid situations.

☑ **Put a high priority on data quality** and leverage data scientists with expertise in machine learning to vet sources.

☑ Be provided by a vendor with deep e**xperience in AI and the critical event management domain.**

Responsible AI = Speed, relevance, usability

When AI is used responsibly within a CEM platform, risk and security professionals can mitigate risk and strengthen resilience thanks to:

SPEED

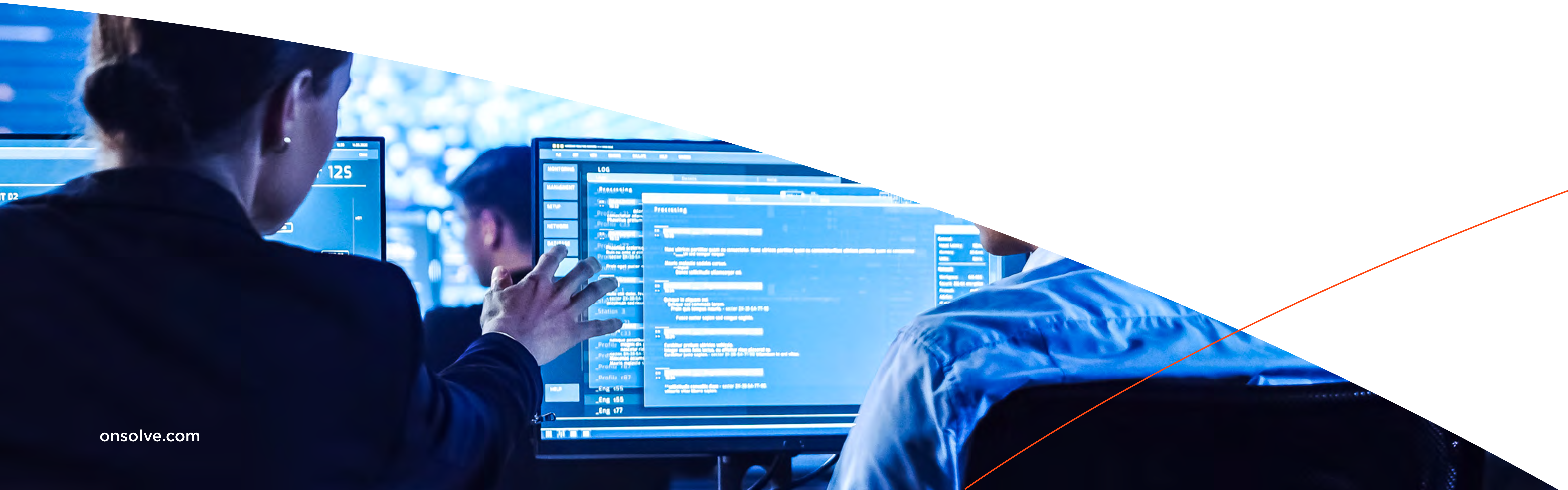
Effective response starts with awareness. AI drives both increased coverage and detection of critical events and decreases overall time to detect these events through automation. This expands your overall situational awareness.

RELEVANCE

AI surfaces key details on critical events that pose a threat to your people and operations. You can focus on making fast, informed decisions rather than wasting time gathering information.

USABILITY

When you're responding to critical events, time is precious. AI can be used to surface insights that allow you to optimize how your team uses the CEM platform, driving even better outcomes in the future.



Why OnSolve for responsible AI?

As an industry leader with a high level of comfort and understanding of the role AI can and should play in CEM, OnSolve leverages AI responsibly.

- Our AI-powered Risk Intelligence has unmatched speed, detecting more than 50 million reports of risk events from 2020 – 2023 for our customers.
- Our data scientists enforce stringent criteria for data quality and integrity.
- Our Intelligence Services team continuously monitors AI output, conducting quality control and validating event feeds.
- Our mass notification technology leverages AI to auto-populate key information in alerts, saving time during an emergency.

Learn more about how OnSolve uses responsible AI for critical event management.

Watch our on-demand webinar

WATCH NOW

About OnSolve

OnSolve® is the leading provider of AI-powered critical event management technology that enables organizations to proactively mitigate risk and remain agile when a crisis strikes. With powerful and reliable risk intelligence, mass notification and incident management technology, the unified OnSolve Platform allows enterprises, organizations and government agencies to prepare, detect, activate and recover from physical threats. Named a leader in the Forrester Wave™: Critical Event Management Platforms, Q4 2023, OnSolve received the highest possible scores across 12 criteria, including Physical Threat Intelligence, Employee Mass Communication and more. For more information, please visit www.onsolve.com.

ONSOLVE®
By CRISIS24