Dataminr®

3 Best Practices

to Ensure Public Safety at Large-scale Events

Large-scale events, whether concerts, corporate conferences or sporting events, bring thousands of people together—sometimes much more—for celebration and connection. Take for example the Olympic Games and FIFA World Cup, high-stakes global summits like the UN General Assembly, or convention-style gatherings like the annual Consumer Electronics Show.

Now more than ever, risks associated with these high-profile events are manifold and complex—ranging from physical safety concerns to cyber attacks. Both public and private organizations must effectively prepare for these threats to protect all attendees, including spectators, conference registrants, heads of state, athletes, media etc., as well as the infrastructure and personnel that facilitate them.

Here we share three best practices organizations should adopt to ensure a smooth and safe event.

Formalize Communications Between the Public and Private Sectors

Public safety concerns at large-scale events are unique and require expert coordination across public and private organizations. Often, multiple government agencies—at the national, state and local level—as well as private security teams manage different aspects of an event's safety strategy. Bridging communication gaps between these entities is crucial.

While this allows for broader coverage, the intersection of multiple agencies requires a clear communications framework—which is often lacking and can lead to poor public safety outcomes. The key is to develop an official line of communication supported by a structured process and informed by the best available information. This coordination and communication work best when each party has a designated point of contact. Together, these enable:

- Proactive planning for the tools and data sources needed to ensure information symmetry between agencies and organizations, reducing time spent comparing data
- Balanced and streamlined flows of information that prevent lags and delays in critical responses times
- Coordination across departments, organizations and sectors to eliminate duplicative efforts
- More transparency in critical, high-stakes moments that enables faster response times

Top security challenges at large-scale events

1. Ineffective crowd management
2. Terror threats and/or violence
3. Severe weather
4. Cyber attacks
5. Medical emergencies
6. Lack of coordination between public and private organization

©Dataminr 2025

Dataminr®

As public safety challenges often emerge beyond the physical borders of large-scale events, it's imperative that organizations' communication and coordination are informed by relevant and accurate real-time alerts. They need to know what's happening in and around the event venue, and they need to know as soon as a risk arises.

This is especially true for large sporting events as they tend to be convergence points for macro issues like human trafficking, disease outbreaks and other high-stakes incidents. They require fast and coordinated responses, which can be actioned in real time when organizations have an early line of sight into emerging incidents.

Take, for instance, the 2025 U.S. Super Bowl. In preparation for the event, held in New Orleans, Louisiana, nearly 200 private and public sector organizations met to discuss security strategies for protecting those in and outside the stadium.

One strategy included leveraging Dataminr's real-time information to maintain situational awareness of relevant incidents and threats—both leading up to and during the event. Dataminr delivers the information via its real-time alerts, allowing these organizations to proactively determine what, if any, actions are needed to safeguard the area and attendees.

Using ReGenAI to safeguard large-scale events

With Dataminr's ReGenAI a new form of generative AI, public and private sector organizations can gain a rapid understanding of evolving risks via live information briefs that are automatically updated with a summary of an event as it unfolds in real time. Organizations can then quickly determine the impacts on public safety and operations, thus being better able to protect event attendees, infrastructure and surrounding communities.

For example, when a truck drove into a crowd of people in the French Quarter of New Orleans on New Year's Day 2025, killing 14 people and injuring at least 35. Dataminr's ReGenAI kept customers informed of the situation in real time, via its event briefs, which continuously updated and regenerated as the situation unfolded.

©Dataminr 2025

Dataminr®

Establish a Core Planning Group

Proper preparation is critical to a successful public safety plan. Before taking on the responsibility of safeguarding any large-scale events, the various entities involved should begin the preparation process in the months, even years, prior. For example, the 2028 Olympics host city of Los Angeles already started the process in 2024.

Let's consider those who were charged with protecting the safety of attendees at the 2024 Summer Olympics in Paris, France. Security experts from dozens of countries, led by France's government agencies, came together to formulate a strategic public safety plan. Coordination began years before the actual event and included different groups from within specific countries.

For instance, U.S. representation included governmental and non-governmental organizations:

- U.S. Diplomatic Security Service, responsible for protecting its embassies and citizens traveling outside of its borders
- Overseas Security Advisory Council, a voluntary organization of U.S. companies and entities that operate overseas, some of which were involved in the games
- U.S. National Olympic Committee and its security team
- U.S. National Counterterrorism Center
- U.S. National Geospatial Intelligence Agency

A good first step is to identify a core planning group—organized around a common public safety goal and resourced with key decision makers from each of the participating stakeholder groups and planning agencies. Each member of the planning group should have decision-making power within their respective organization—both in the lead-up to the event, but also in case of an emergency on the day of.

Building on the first best practice, this core planning group should include representatives from both public and private sectors, establishing a single point of contact at each agency or organization to manage information flows, emergency management plans and cybersecurity protocols. This collaboration ensures a unified approach to protecting physical, digital and human assets while mitigating harm to individuals and damage to infrastructure—both tangible and virtual.

©Dataminr 2025

Access to relevant, real-time information is essential for the planning group to stay ahead of emerging incidents. Tailoring information to the event's size, scale and geography ensures the most relevant data is available, enabling faster and more effective responses to both safety and cybersecurity challenges.

Real-time information and cross-sector collaboration allow emergency response plans to be executed more effectively. Public and private organizations can mobilize resources quickly, maintain visibility into physical incidents and cyber threats as they unfold, and safeguard attendee safety and critical infrastructure.

Stress Test Response Plans

Once all stakeholders have been assembled into a core planning group and communications symmetry begins to materialize, the planning group should develop and test an array of response plans that cover a wide range of safety incidents—both physical and cyber.

It's vital that these plans are scalable and adaptable to handle everything from small disturbances to large-scale emergencies. Cybersecurity strategies should include responses to phishing attempts, malware attacks, and denial-of-service (DoS) attacks that might target event systems, disrupt communications, or compromise personal data.

While planning for worst-case scenarios is essential, many events face multiple smaller challenges that can still have a major impact when mismanaged. Because of this, response plans must be flexible enough to handle simultaneous threats. For example, an extreme weather event might coincide with a cyber attack on the event's communication systems, requiring a coordinated response that mitigates both disruptions.

Cyber criminals targeting major events

- The 2024 Paris Olympics suffered from over 140 cyber attacks.
- With digital ticketing and event apps becoming increasingly common, malicious actors have a new battleground. In May 2024, hackers stole personal information of more than 500 million Ticketmaster customers worldwide.

©Dataminr 2025

Dataminr®

Preparing for elections

Elections are another type of large-scale event with significant risks to the public and organizations. The work needed to secure them begins well in advance of election day and extends far beyond it.

Security teams should discuss possible scenarios and track key risk indicators leading up to election day and after it has been completed. They need to ensure they and their teams are prepared to respond to incidents—both physical and cyber—and stay abreast of issues as they arise.

Learn more: How to Tackle Today's Election Security Challenges

Thorough and rigorous testing of response plans is crucial. Tabletop crisis exercises are a proven means for testing the effectiveness of response plans as they help to uncover flaws and gaps in safety strategies. By simulating scenarios such as a data breach during an emergency evacuation, teams can identify weak points in their plans and strengthen their approach.

Realistic practice drills are equally important. When possible, drills should leverage event venues and the technologies that will be in use to prepare teams for high-pressure situations.

Large events will continue to face increased exposure to physical and digital risks. Public safety and private security leaders alike must adopt integrated strategies, including leveraging real-time data, to protect attendees, safeguard data and ensure operational continuity.

Learn More

See how Dataminr Pulse for Corporate Security and First Alert help private and public sector organizations secure attendees, infrastructure and communities at large-scale events.

©Dataminr 2025

Dataminr®