Dataminr®

2026 World Cup Security Checklist

Use this actionable checklist to safeguard stadiums, fan zones, and city-wide areas during the 2026 World Cup—covering risk assessment, security operations, tech tools, and post-event review.

The 2026 World Cup—hosted across 16 stadiums and three countries—will kick off in Estadio Azteca, Mexico City in June 2026. With expected attendance around 6.5 million spectators, plus staff, teams, vendors, executives, and others, security planning remains a top priority. Ensuring the safety of millions of people and security facilities and venues requires intense planning and cross-agency cooperation.

Security experts can use this checklist to effectively plan and secure your stadium and surrounding areas for the 2026 World Cup.

Preparation

Conduct a Comprehensive Risk Assessment

A comprehensive risk assessment is a foundational piece of any effective security planning. This critical planning step forms the base for operational plans, policies, and procedures as well as contingency and emergency plans. Security teams should begin here to highlight and review all past incidents and potential risk areas, including buildings, fan areas, indoor and outdoor facilities, or any physical assets.

- [ ] Identify threats/hazards, vulnerabilities, and potential risks at stadiums, fan zones, transit hubs, and city-wide event areas.
- [ ] Evaluate past security incidents from similar large-scale events for insights.
- [ ] Collaborate with local law enforcement, emergency services, and private security partners.

Dataminr®

Establish a Security Operations Plan

A security operations plan focuses on mitigation, deterrents, and responses for any security threat, whether cyber or physical. Utilize the risk assessment (e.g., the risks, vulnerabilities, and threats) to clearly establish roles, responsibilities, plans, compliance, and other security needs.

- [ ] Document roles and responsibilities for all security personnel and partners.
- [ ] Design clear incident response protocols and communication workflows.
- [ ] Create or validate contingency plans for mitigation of incidents with the stadium's safety and security teams. (e.g., bad weather, fan disruption).
- [ ] Create emergency plans involving any necessary emergency services in the event of a major incident (e.g., fire, terrorist attack, bomb threat).
- [ ] Ensure compliance with local and international regulations.

Implement Real-Time Event, Threat & Risk Intelligence Tools

When it comes to event security, accurate real-time information on threats and incidents reduce response and mitigation times. Quality risk, threat, and event detection enables security teams to better protect people, secure events and facilities, and eliminate potential blind spots.

- [ ] Deploy AI-powered event, threat and risk detection tools, like Dataminr, for 24/7 threat intelligence across public information sources. These systems help spot public safety incidents and anomalies in real time, reducing the burden on security teams and enabling faster response times.
- [ ] Configure alerts for hyper-local threats such as protests, severe weather, or public disturbances. For events happening across multiple jurisdictions and geographies, develop communication plans that keep everyone on the same page.
- [ ] Utilize the insights these tools provide with their updates for better, more effective responses or threat mitigation.
- [ ] Incorporate archived historical data on safety incidents at certain locations into planning and response playbooks.

Test Compatibility with Existing Systems

Ensure full integration of these tools within existing physical security, communication apps, or other solutions to realize the most value. The key is to invest in a real-time event, threat and risk intelligence tools that improve established protocols and offer additional insights and seamless workflow solutions.

- [ ] Incorporate real-time monitoring tools with CCTV, access control, and other on-site security platforms (e.g. Genetec).
- [ ] Utilize biometric security and smart ticketing to enhance safety and operational efficiency.
- [ ] Integrate real-time AI platforms with security and crisis management solutions (e.g., Esri), collaboration tools (e.g. Microsoft Teams), or custom solutions and third-party applications.
- [ ] Invest in a tool that enables communication with employees at the event for real-time updates and safety checkins.
- [ ] Conduct functionality tests to ensure seamless operations.

On-the-Ground Security Measures: Secure Stadium Perimeter and Entry Points

Physical security measures, in combination with technical and operational elements, remain a key piece of ensuring a safe event. These should be proactive, layered security measures that are adaptable to new and emerging security threats.

- [ ] Establish a plan to control and monitor all entry and exit points at all times via cameras, access control cards, biometric scanners, or other security measures.
- [ ] Layer physical barriers (e.g., fences, walls, landscaping, terrain, blast or ballistic protection elements), technology-based deterrents (e.g., cameras utilizing AI), and other security measures (e.g., K-9s for explosive detection) as appropriate for the specific venue, building, or fan areas.
- [ ] Set up bag checks, body scanners, and walk-through metal detectors at all access points.
- [ ] Use physical barriers or bollards to address hostile vehicle-based threats.

Establish Crowd Control Systems

Crowd control breaks down into two distinct, but intertwined areas: Crowd safety and crowd security.

Crowd safety ensures the “physical safety and well-being of individuals within a crowd” by focusing on preventing overcrowding, inspecting physical areas for safety concerns or hazards, ensuring access to emergency services, and a focus on general crowd control.

- [ ] Use digital signage to communicate crowd control measures in real-time.
- [ ] Ensure easy access to emergency exits and trained personnel to assist with evacuations.
- [ ] Coordinate with key teams to ensure medical personnel and emergency services are accessible and ready.
- [ ] Inspect all areas of the venue to address potential dangers or areas of concern.
- [ ] Plan dedicated fan zones to reduce congestion around the stadium.
- [ ] Position trained security staff and volunteers at high-traffic zones and exits.

Crowd security focuses on “measures taken to protect the crowd” from threats by focusing on internal or external threats with potential criminal or malicious intents.

- [ ] Utilize surveillance technology to watch for potential problems or threats.
- [ ] Deploy trained crowd security personnel in coordination with local, state, and federal law enforcement.
- [ ] Utilize AI-powered risk detection tools, like Dataminr, for better awareness and reduced mitigation or response time.

Dataminr®

Communication & Coordination

Train and Prepare Security Teams

The way in which the security team interacts with attendees in a crowded space can have "significant impact on crowd behavior." A well-trained security team will diffuse situations, reduce response times, and effectively handle a variety of security threats and actors.

- [ ] Provide scenario-based training for threat detection, evacuation, and medical emergencies, including conflict resolution, de-escalation techniques, and communication skills.
- [ ] Host regular briefing sessions for all stakeholders, including federal and city officials and emergency services.

Establish A Unified Command Center

Effective crowd safety risk management often hinges on a broad group of individual teams being proactive about threat identification and recognition, clearly communicating across a potentially complex web of public and private sector organizations, and being able to react effectively with each unit clearly understanding its role.

- [ ] Set up a central operations hub to coordinate incident responses in real time.
- [ ] Use multi-channel communication tools to link all teams and stakeholders seamlessly.
- [ ] Ensure security personnel are communicating clearly and effectively with attendees

Dataminr®

Proactive Emergency Management

Develop and Share Emergency Response Plans

Emergency response plans require a proactive, well-documented, oft-tested (and retested) set of clear guidelines for each member of the response team.

- [ ] Create predefined plans for evacuations, medical incidents, fires, and active threats.
- [ ] Communicate these plans to staff, volunteers, and first responders.
- [ ] Document clear communication protocols for all potential scenarios.

Conduct Pre-Event Drills

Outdated or untested plans can be a catastrophic point of failure during an emergency event. Make sure the team is testing various pieces of the emergency plans and under a variety of scenarios.

- [ ] Test contingency plans with live simulations for critical scenarios and document gaps and flaws for review.
- [ ] Test, retest, and test one more time. Make sure each test folds in any changes or improvements from the previous test.
- [ ] Ensure staff knows emergency exits, medical stations, and key contacts. The better the training, the more effective staff will be during a true emergency or problem.

Event Day Execution

Respond to events, threats and risk in real time

Engage deeply with any real-time threat identification technology to stay ahead of any potential problems or react quickly on the day of the event. These platforms pick up events happening faster than the mainstream media through fan social media or other public forums. The faster security teams are notified, the more quickly they can respond and the more effective the mitigation or action.

- [ ] Keep security teams updated with live alerts from monitoring tools.
- [ ] Respond quickly to emerging risks and communicate actions to the command center.
- [ ] Follow practiced and established response playbooks and plans.

Provide Visible Security Presence

A visible, well-trained security presence will serve as both a visual deterrent to potential attackers or incidents and create a sense of safety for attendees.

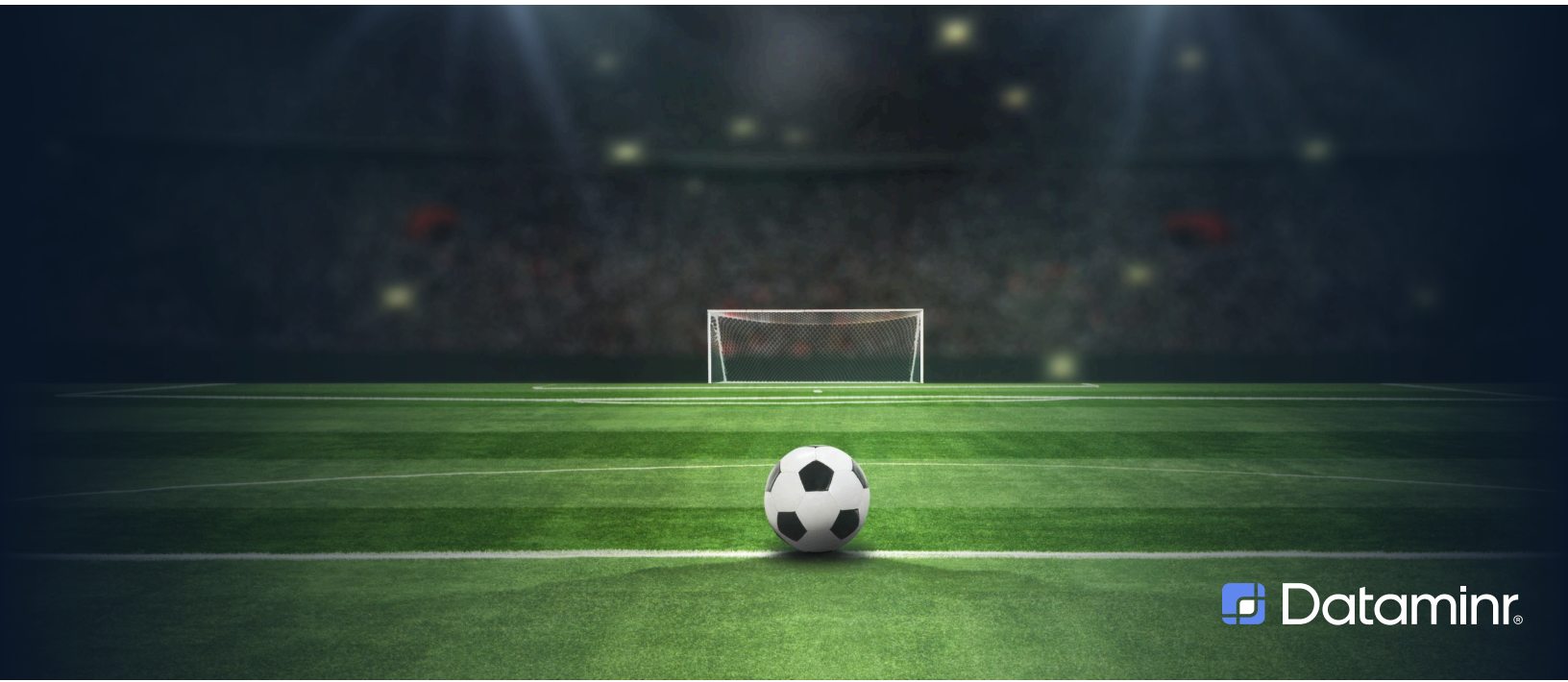
- [ ] Deploy some highly visible (e.g. wearing high-visibility vests or venue-branded uniforms) security teams to deter potential security threats.
- [ ] Ensure the public knows how to report suspicious activity and ensure that information is prominently displayed through digital signage, apps, and in other public areas.
- [ ] Station security at all entrances and high-traffic areas to monitor potential hot-spots.

Dataminr®

Post-Event Assessment

Once the World Cup has concluded, security teams should meet for a post-mortem discussion on the event. This is crucial to improve the safety and the approach for future events. Due to the number of World Cup events, this content could also be valuable to other stadium hosts, in addition to local authorities and anyone in charge of future events at the venue.

- [ ] Assess security effectiveness, including response times, detected risks, and handled incidents.
- [ ] Collect feedback from staff, vendors, and attendees for improvement.
- [ ] Create a detailed report highlighting successes and challenges for future events. Include quantitative metrics in the post-mortem report (e.g., average time to respond after detection, congestion data, incident numbers.)
- [ ] Ensure all discussions are "blameless" – meaning they don't focus on who was at fault – with constructive feedback to ensure people are comfortable sharing information and insights.
- [ ] Host a cross-agency briefing to share and capture insights across law enforcement, emergency services, contractors and vendors, and any other involved parties.



Learn More

See how Dataminr empowers your organization to ensure a safe and successful large-scale event.

REQUEST DEMO

Dataminr®