Microsoft

State of Play

Sporting events and venues draw cyberthreats at increasing rates

634.6 MM

Authentication attempts

Microsoft performed over 634.6 million authentications while providing cybersecurity defenses for Qatari facilities and organizations between November 10 and December 20, 2022.

Microsoft Threat Intelligence

Cyber Signals

August 2023

Introduction

Threat actors go where the targets are, capitalizing on opportunities to launch targeted or widespread, opportunistic attacks. This extends into high profile sporting events, especially those in increasingly connected environments, introducing cyber risk for organizers, regional host facilities, and attendees. The United Kingdom's National Cyber Security Centre (NCSC) found that cyberattacks against sports organizations are increasingly common, with 70 percent of those surveyed experiencing at least one attack per year, significantly higher than the average across businesses in the United Kingdom.

The pressure to deliver a smooth, safe experience on the world stage introduces new stakes for local hosts and facilities. A single misconfigured device, exposed password, or overlooked third party connection can lead to a data breach or successful intrusion.

Microsoft delivered cybersecurity support to critical infrastructure facilities during the FIFA World Cup Qatar 2022™. In this edition we offer first hand learnings about how threat actors assess and infiltrate these environments across venues, teams, and critical infrastructure around the event itself.

We are all defenders

Security Snapshot

Snapshot data represents the total number of entities and events monitored twenty-four-seven between November 10 and December 20, 2022. This includes organizations either directly involved in, or affiliated with, tournament infrastructure. Activity includes human-led proactive threat hunting to identify emerging threats and track notable campaigns.

45
Organizations protected

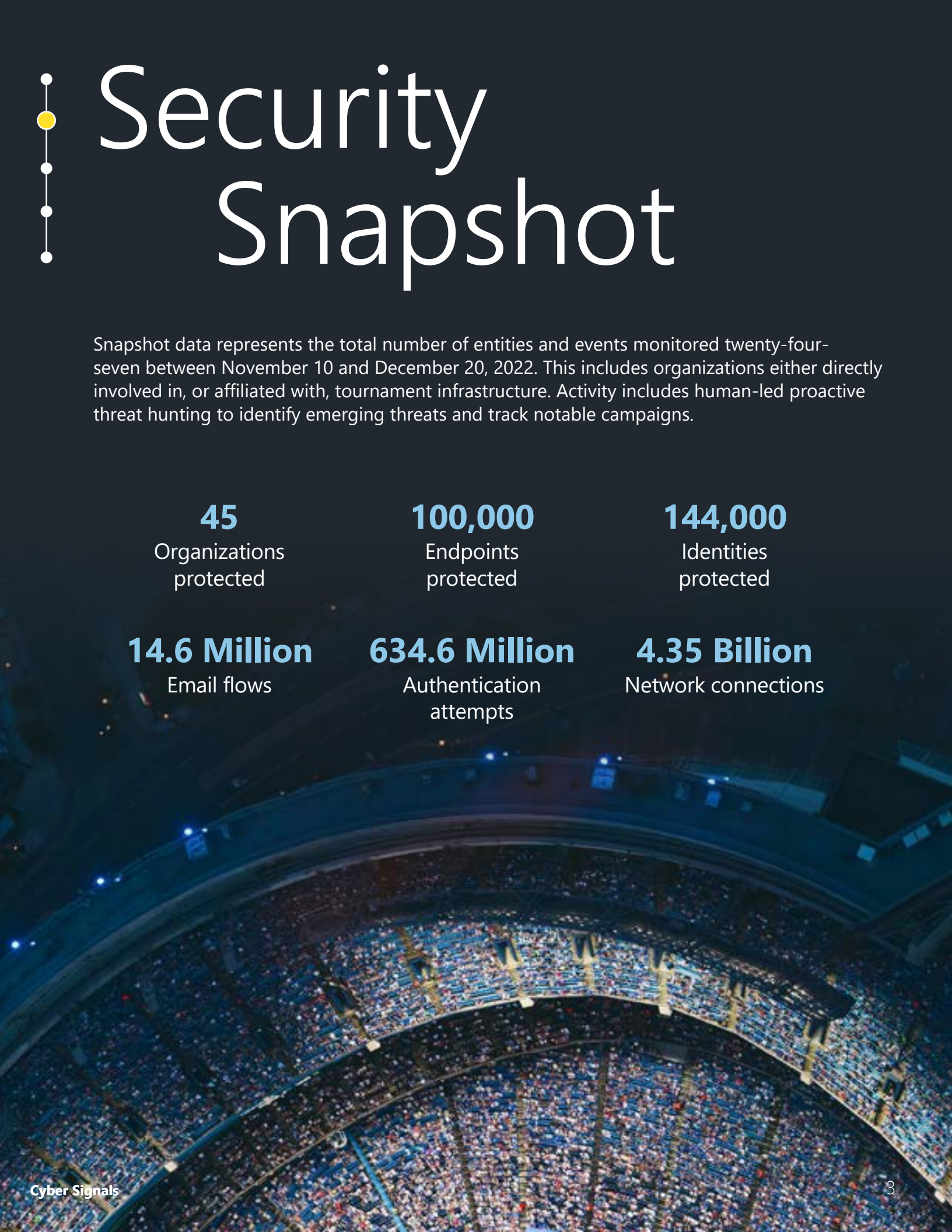
100,000
Endpoints protected

144,000
Identities protected

14.6 Million
Email flows

634.6 Million
Authentication attempts

4.35 Billion
Network connections



Threat briefing

Opportunistic threat actors exploit target-rich environment

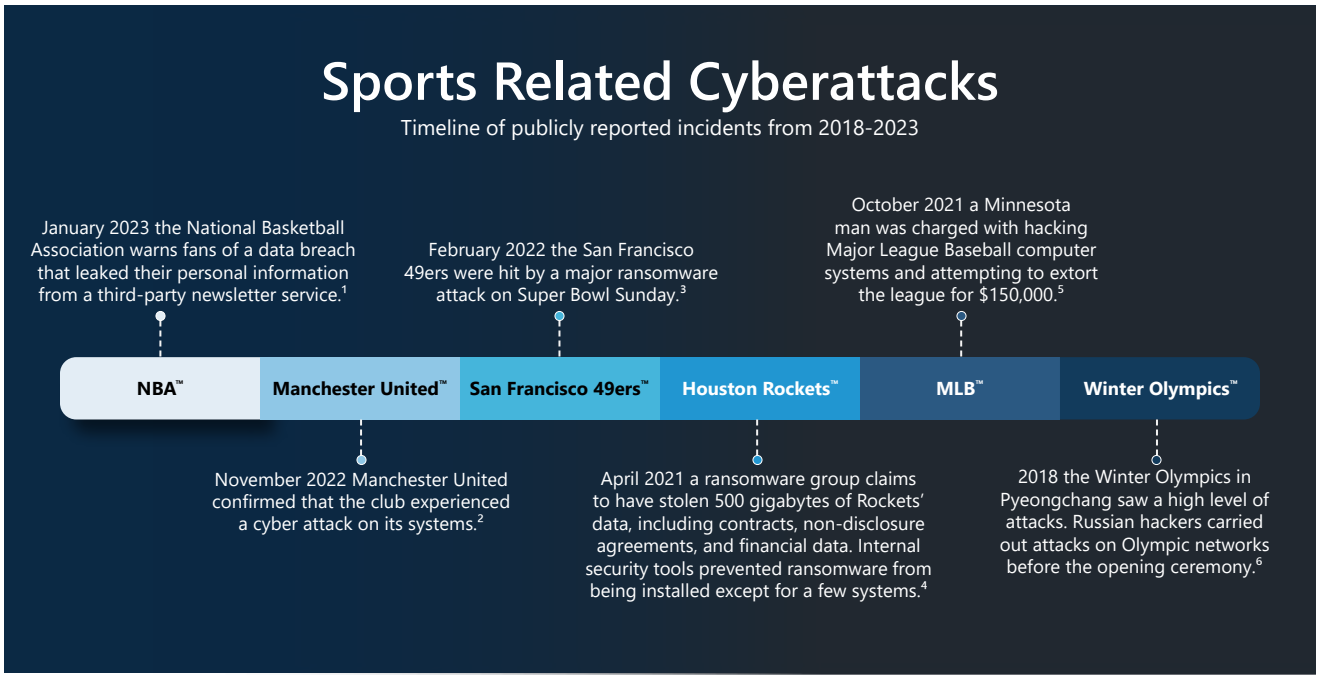
Cybersecurity threats to sporting events and venues are diverse and complex. They require constant vigilance and collaboration among stakeholders to prevent and mitigate escalation. With the global sports market valued at more than USD600 billion, the target is rich. Sports teams, major league and global sporting associations, and entertainment venues house a trove of valuable information desirable to cybercriminals.

Information on athletic performance, competitive advantage, and personal information is a lucrative target. Unfortunately, this information can be vulnerable at-scale, due to the number of connected devices and interconnected networks in these environments. Often this vulnerability spans multiple owners, including teams, corporate sponsors, municipal authorities, and third-party contractors. Coaches, athletes, and fans can also be vulnerable to data loss and extortion.

Furthermore, venues and arenas contain many known and unknown vulnerabilities that allow threats to target critical business services, such as point-of-sale devices, IT infrastructures, and visitor devices. No two high-profile sporting events have the same cyber risk profile, which varies depending on factors like location, participants, size, and composition.

To focus our efforts during the FIFA World Cup Qatar 2022™, we carried out proactive threat hunting through which we assess risk using Defender Experts for Hunting, a managed threat hunting service that proactively searches for threats across endpoints, email systems, digital identities, and cloud apps. In this instance, factors included threat actor motivation, profile development, and a response strategy. We also considered global threat intelligence on geopolitically motivated threat actors and cybercriminals.

Top-of-mind concerns included the risk of cyber disruption of event services, or local facilities. Disruptions like ransomware attacks and efforts to steal data could negatively impact the event experience and routine operations.



Threat briefing

The threat hunting team operated under a defense-in-depth philosophy to inspect and protect customer devices and networks. Another focus was monitoring the behavior of identities, logins, and file access. Coverage spanned a variety of sectors, including customers involved in transportation, telecommunications, healthcare, and other essential functions.

Overall, the total number of entities and systems monitored twenty-four-seven with human-led threat hunting and response support encompassed more than 100,000 endpoints, 144,000 identities, 14.6 million plus e-mail flows, over 634.6 million authentications, and billions of network connections.

As an example, some healthcare facilities were designated as urgent care units for the event, including hospitals delivering critical support and health services for fans and players. As healthcare facilities owning medical data, they were high-value targets. Microsoft machine- and human-powered threat hunting activity leveraged threat intelligence to scan signals, isolate infected assets, and disrupt attacks on these networks. With a combination of Microsoft Security technology, the team detected and quarantined pre-ransomware activity targeting the healthcare network. Multiple unsuccessful sign-in attempts were logged and further activity was blocked.

The urgent nature of healthcare services requires devices and systems to maintain a peak level of performance. Hospitals and healthcare facilities have a challenging task balancing service availability while maintaining a healthy cybersecurity posture. A successful attack, in the near term, could have immobilized medical facilities from a data to IT perspective, leaving medical providers relegated to pen and paper when updating patient data and weakening their ability to perform life-saving medical care in an emergency or mass triage situation.

Long term, malicious code planted to provide visibility across a network could have been leveraged for a broader ransomware event aimed at further disruption. Such a case could have opened the door to data theft and extortion.

As large global events continue to be desirable targets for threat actors, there are a variety of motivations from nation-states which seem to be willing to absorb collateral damage from attacks if it supports broader geopolitical interests. Furthermore, cybercriminal groups looking to leverage the vast financial opportunities that exist in sporting and venue-related IT environments will continue to see these as desirable targets.

Recommendations:

Augment the SOC team: Have an additional set of eyes monitoring the event around the clock to proactively detect threats and send notifications. This helps correlate more hunting data and discover early signs of intrusion. It should include threats beyond endpoint, like identity compromise or device to cloud pivot.

Conduct a focused cyber risk assessment: Identify potential threats specific to the event, venue, or nation where the event occurs. This assessment should include vendors, team and venue IT professionals, sponsors, and key event stakeholders.

Consider least privileged access a best practice: Grant access to systems and services only to those who need it and train staff to understand access layers.

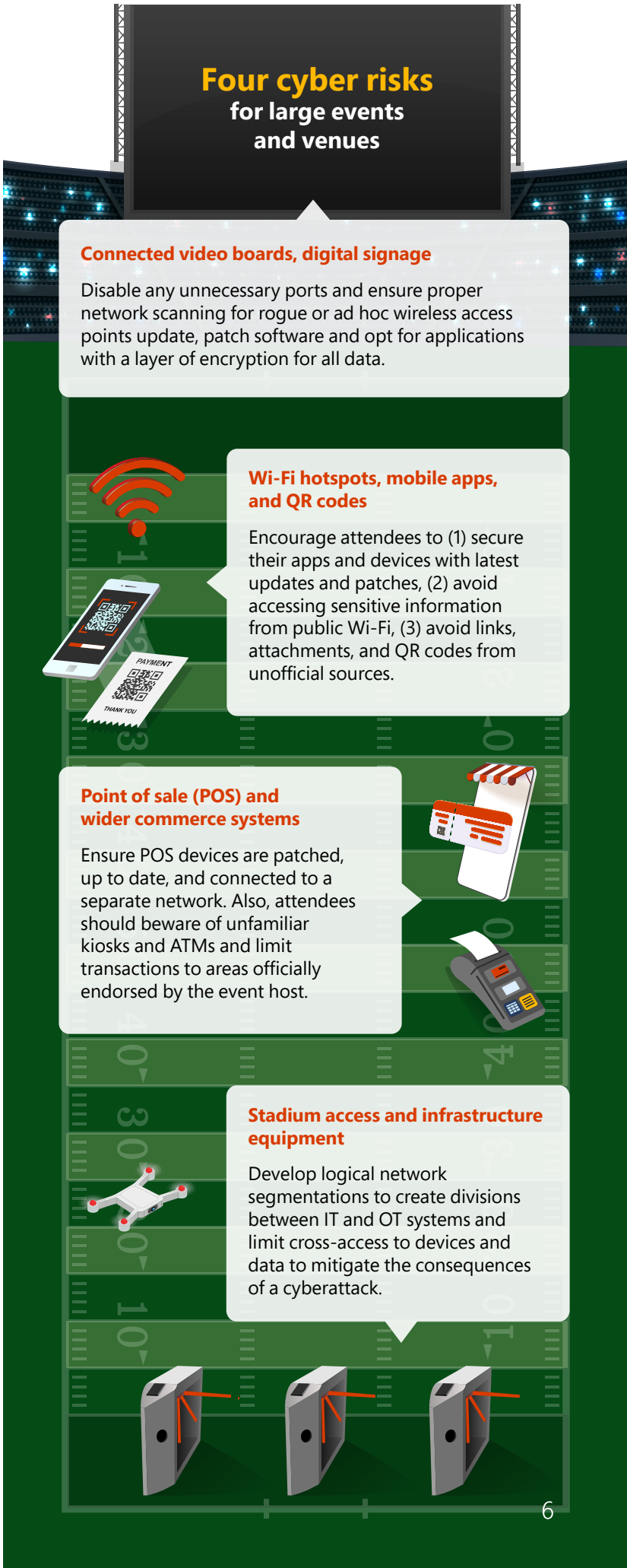
Defending against attacks

Vast attack surfaces require additional planning and oversight

With events like the FIFA World Cup Qatar 2022™, the Winter Olympics™, and sporting events in general, known cyber risks surface in unique ways, often less perceptibly than in other enterprise environments. These events can come together quickly, with new partners and vendors acquiring access to enterprise and shared networks for a specific period of time. The pop-up nature of connectivity with some events can make it hard to develop visibility and control of devices and data flows. It also fosters a false sense of security that "temporary" connections are lower risk.

Event systems can include the team or venue web and social media presence, registration or ticketing platforms, game timing and scoring systems, logistics, medical management and patient tracking, incident tracking, mass notification systems, and electronic signage.

Sports organizations, sponsors, hosts, and venues must collaborate on these systems and develop cyber smart fan experiences. Further, the huge swell of attendees and staff that bring data and information with them through their own devices increases the attack surface.



Defending against attacks

Providing security teams with information they need upfront—including critical services that must remain operable during the event—will better inform response plans. This is essential in IT and OT environments that support venue infrastructure, and to maintain the physical safety of attendees. Ideally, organizations and security teams could configure their systems before the event to complete testing, snapshot the system and devices, and make them readily available to IT teams to rapidly redeploy when needed. These efforts go a long way in deterring adversaries from taking advantage of poorly configured, ad hoc networks within the highly desirable, target-rich environments of large sporting events.

Additionally, somebody in the room should consider privacy risk and whether configurations add new risks or vulnerabilities for attendees' personal information or teams' proprietary data. This person can implement simple cyber smart practices for fans, directing them, for example, to scan only QR codes with an official logo, to be critical of SMS or text solicitation they didn't sign up for, and to avoid using free public Wi-Fi.

These policies and others can help the public better understand the cyber risk at large events, specifically, and their exposure to data harvesting and theft. Knowing safe practices can help fans and attendees sidestep becoming victims of social engineering attacks, which cybercriminals can wage after gaining a foothold into exploited venue and event networks.

In addition to the recommendations below, the National Center for Spectator Sports Safety and Security offers these considerations for connected devices and integrated security for large venues.

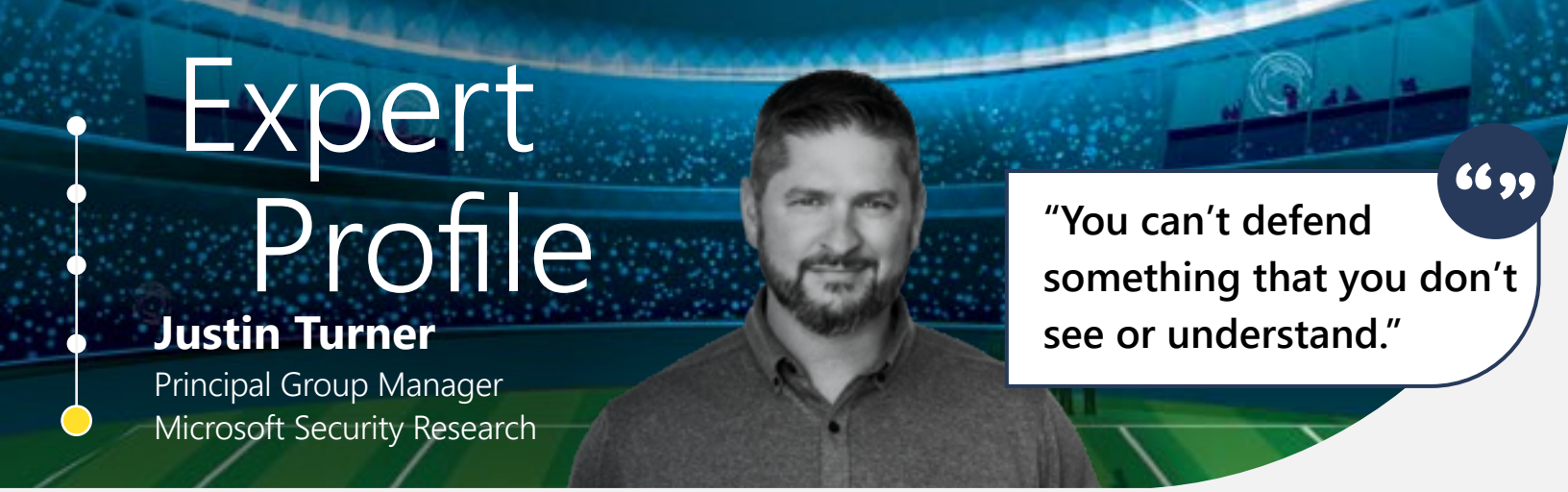
Recommendations:

Prioritize the implementation of a comprehensive and multi-layered security framework: This includes deploying firewalls, intrusion detection and prevention systems, and strong encryption protocols to fortify the network against unauthorized access and data breaches.

User awareness and training programs: Educate employees and stakeholders about cybersecurity best practices, such as recognizing phishing emails, using multi-factor authentication or passwordless protection, and avoiding suspicious links or downloads.

Partner with reputable cybersecurity firms: Continuously monitor network traffic, detect potential threats in real-time, and respond swiftly to any security incidents. Conduct regular security audits and vulnerability assessments to identify and address any weaknesses within the network infrastructure.

Expert Profile



Justin Turner
Principal Group Manager
Microsoft Security Research

> **"You can't defend something that you don't see or understand."**

Justin Turner began his career building and breaking communications networks for the United States Army. This allowed him to travel the world and work in places like Iraq, Bahrain, and Kuwait. When his active-duty adventure ended, Justin transitioned to civilian life in Florida in 2006. The job was similar—building, hacking, and breaking things—but this time, he was with the MITRE Corporation.

In 2011, he got a call from a former Army commander about a role at SecureWorks exclusively focused on the commercial side of cybersecurity.

His initial role was in threat intelligence production, looking across customer data sets and responding to questions on malicious files or malware. That included doing analysis and investigating active threat campaigns.

"At the time, banking Trojans were prevalent. Some might remember the Zeus banking Trojan. A lot of remote access tools really came to bear around that time. A couple years after that, I was asked to help develop a threat hunting practice for the company. This was before threat hunting existed in the market as a service like it does now."

When Microsoft decided to launch Defender Experts for Hunting, Justin received another call from a former colleague and friend. He said, "we're launching a new service for Microsoft Security, I can't think of anybody better for this role."

Justin says the three challenges that persist across his 20 years of experience in cybersecurity are configuration management, patching, and device visibility.

"Across the board, misconfigurations are a monumental challenge. Our network environment has dramatically changed, we went from server mainframe environments, which had thin client edges, to everyone owning a personal computer. Fast forward to today, there are countless network connected devices from smart homes to manufacturing environments to personal devices. Maintaining a secure baseline across that is a challenge, sustaining patch levels adds another layer of the problem."

As the complexity and size of the networks grow, so does the number of vulnerabilities, Justin explains.

"Our customers with expanding blended environments try to keep up with patching. It's easy for us to say, 'just patch' but it's a massively challenging problem that takes a lot of time and continued investment."

The third challenge is visibility. Justin says many of the customer conversations he has center around a problem that occurred because the customer didn't know that a vulnerable system exposed to the Internet was operating in their network.

"Recently, for a conference, I took an intrusion from decades ago then looked at an intrusion from a week ago. I put the two side-by-side and asked, 'Which one of these happened in 1986 and which one of these happened last week?'

No one could tell because the two looked so similar. The attack was a software vulnerability that nobody knew existed. It was a misconfiguration of the server, poor auditing and logging, with little to no patch management. The technical details of the problems are different now, but the fundamentals are the same. As a defender, you can't defend something that you don't see or understand."

Methodology: For snapshot data, Microsoft platforms and services, including Microsoft Extended Detections and Response, Microsoft Defender, Defender Experts for Hunting, and Microsoft Entra ID, provided anonymized data on threat activity, such as malicious email accounts, phishing emails, and attacker movement within networks. Additional insights are from the 65 trillion daily security signals gained across Microsoft, including the cloud, endpoints, the intelligent edge, and our Compromise Security Recovery Practice and Detection and Response Teams. Cover art does not depict an actual soccer game, tournament, or individual sport. All sports organizations referenced are individually owned trademarks.

1: https://www.bleepingcomputer.com/news/security/nba-alerts-fans-of-a-data-breach-exposing-personal-information/

2: https://www.independent.co.uk/sport/football/premier-league/manchester-united/manchester-united-cyber-attack-organised-criminals-data-b1759472.html

3: https://www.espn.com/nfl/story/_/id/33283115/san-francisco-49ers-network-hit-gang-ransomware-attack-team-notifies-law-enforcement

4: https://rocketswire.usatoday.com/2021/04/15/rockets-working-with-fbi-to-investigate-cyberattack-on-team-systems/

5: https://www.cnn.com/2021/10/29/tech/mlb-hack/index.html

6: https://www.nytimes.com/2018/02/12/technology/winter-olympic-games-hack.html