Company Login Contact us

TANIUM Platform Solutions Customers Partners Resources SEE A DEMO

IT OPERATIONS RISK & SECURITY THREAT INTELLIGENCE BUSINESS TRANSFORMATION LEARN TANIUM NEWSROOM

Cyber Triumph: 6 Skills the Paris Olympics Got Right

Paris has a lot to be proud of. The Olympics went off (for the most part) without a cybersecurity hitch. Best of all – and you don't get to say this very often about the Olympics –anyone can do what they did (with just a few tweaks to fit your budget).

SEPTEMBER 5, 2024

(This article was updated on September 16, 2024.)

Last month's Paris Olympics – and the Paralympic Games, which wrap up this week – were widely considered a triumph, not just because of the city's picture-perfect backdrop but also the complex cybersecurity efforts you didn't see.

More than 140 cyberattacks struck the games, including 119 low-impact "security events" and 22 breaches of information systems by malicious actors between July 26 and August 11, according to ANSSI, the French government's cybersecurity agency, which worked from a secret location during the Games. The attacks mainly targeted government organizations, plus sports, transport, and telecoms infrastructure. One third resulted in some limited downtime. None disrupted the competition.

Experts and analysts will be sitting down to review the Paris Olympics for months to come. What's already clear is that French officials got a lot of things right. While their efforts will surely guide cybersecurity at future global sporting events (like the Los Angeles Olympics in 2026), the lessons learned can also serve as an unofficial playbook for any enterprise.

The future of IT and security is autonomous. But most organizations don't know which manual processes are easy to eliminate. This is where you start.

Granted, most orgs can't staff up like the Olympics. The French security team included 15 members of the Paris 2024 Organizing Committee (COJOP); some 100 additional personnel supplied by corporate partners; more than 200 penetration testers, bug

Joseph V. Amodio

Joseph V. Amodio is a veteran journalist, television writer, and the Editor-in-Chief of *Focal Point*. His work has appeared in *The New York Times Magazine*, *Men's Health*, *Newsday*, *Los Angeles Times*, CNN.com, and Barrons.com, and has been syndicated in publications around the world. His docudramas have aired on Netflix, Discovery, A&E, and other outlets. He also produces Tanium's new *Let's Converge* podcast—listen **here**.

Key takeaways

- Lessons learned from the Paris Olympics can help guide any enterprise going for (cybersecurity) gold.
- Smart proactive measures include leveraging threat intel, real-time threat monitoring, and AI (with safeguards).
- Old-school strategies (updated phishing training, threat hunts) can spot new dangers (deepfakes, disinformation).

bounty hunters, and other ethical hackers employed to test the system via red teaming and tabletop exercises; tens of thousands of volunteers who provided support just before and during the event; and one (very weary, no doubt) chief information security officer.

That CISO, Franz Regul, has been on the job for the last four years, working with the International Olympic Committee (IOC) and government agencies. He met with security leaders from the Tokyo 2020 Summer Olympics and the Beijing 2022 Winter Olympics, assessed their experiences, and altered some cyber defenses to keep up with evolving technology. Rather than rely on a network primarily based on data centers – a strategy used in Tokyo – Regul opted for a cloud-based environment.

“We also chose a less centralized system, with operational infrastructure and team members scattered across France,” Regul explained just before the Games, in an interview with *Infosecurity Magazine*.

$94M

Estimated revenue increase from cybersecurity services in France this year due to cyber threats related to the Paris Olympics

Regul and his team faced “the most complex threat landscape, the largest ecosystem of threat actors, and the highest degree of ease for threat actors to execute attacks” of any Olympics, according to International Data Corporation (IDC), the renowned market intelligence firm. The attacks began months before any athletes or spectators arrived, with several distributed denial of services (DDoS) campaigns and attempts on the Games’ infrastructure and administration.

IDC estimates revenue from cybersecurity services in France will increase by $94 million in 2024 (and by $57 million elsewhere in Europe) as a result of the Olympics, adding just over two percentage points to total cybersecurity services spending.

Focal Point

Dedicated to helping business executives and IT leaders effectively use technology to connect with customers, empower employees and achieve better results.

AZBEES 2024 SILVER NATIONAL AWARD

AZBEES 2024 GOLD REGIONAL AWARD

TABBIES 2023 Award Winner

Technology & Innovation Reporting - National
Government Coverage - Pacific Region
Technology & Innovation Reporting - Pacific Region

So yes, agreed, most CISOs will never have Regul's budget or access to government resources. Still, Paris' multi-pronged approach is worth emulating, and can be, no matter the scope of your cybersecurity program.

[Read also: Global sporting and cultural events can pose a real cyber threat to your enterprise – even if you have no connection to the Olympics or, say, Taylor Swift]

Here, we tease out the key components to a medal-worthy cyberdefense, keeping in mind the French singer Yseult, who sang "My Way" at the Paris closing ceremonies. When it comes to cybersecurity, at least, making their way *your* way is not a bad idea.

1. Rely on real-time threat monitoring

During the Olympics, a highly publicized ransomware attack on the Grand Palais (an Olympics venue) and some 40 other French museums captured headlines. In a ransom note, cybercriminals claimed to have extracted consumer financial information from the gift shops and other commercial sites at these venues and threatened to expose that data within 48 hours.

> **We chose a less centralized system, with operational infrastructure and team members scattered across France.**
>
> Franz Regul, CISO, Paris 2024 Organizing Committee (COJOP)

Officials responded at lightning speed, thanks to state-of-the-art threat monitoring, which relied on real-time data. Cybersecurity teams also employed frameworks like MITRE ATT&CK to help prepare for potential cyber breaches.

As for that ransomware attack? Officials detected no data extraction at the time, reportedly paid no ransom, and the venues were open for business (and Olympic competition) that same day.

2. Stay informed with threat intel

In the months leading up to the Games, threat intelligence teams identified more than 300 fake ticket sites designed to swipe personal data from unsuspecting consumers. A specialized unit of 200 gendarmes shut down more than 50 sites and put scores more on notice.

> **Threat actors are scaling, their scope is getting bigger, they’re leveraging new tools.**
>
> Sherrod DeGrippo, director of threat intelligence strategy, Microsoft

“Threat actors are scaling, their scope is getting bigger, they’re leveraging new tools,” says Sherrod DeGrippo, director of threat intelligence strategy for Microsoft, in a recent episode of *Focal Point’s* companion podcast, *Let’s Converge*. DeGrippo outlines the best steps to building a threat intel team, the benefits of incorporating AI, and the type of intel that will impress your CISO and the board.

While the average company's threat intel team won't be as large as the French gendarme unit, it can still be enormously effective by leaning into diversity. When hiring, look for individuals with varied backgrounds, experience levels, and *preferences,*, DeGrippo advises.

[Read also: Preventing AI bias starts at the top, and requires diversity – just as these female chief AI officers]

"Trust me," she says, "if you have someone working on something that they're good at and they like, you're gonna win."

3. Leverage AI tech

Olympics officials used AI to secure sensitive data and critical information systems, and the French government enacted legislation to allow for AI-assisted video surveillance in Paris. Special cameras in real-time scanned for specific or unusual types of crowd movements, suspicious behavior, fires, and abandoned bags.

With security threats rising beyond the capacity of human analysts, AI is quickly becoming table stakes for any cybersecurity program, given its ability to process large amounts of data and make informed decisions. AI can identify baselines for normal behavior, then spot anomalies in network traffic and user behavior.

[Read also: Ultimate guide to AI cybersecurity – benefits, risks, and rewards]

But rest assured, experts insist human expertise and oversight will remain critical. The best use of generative AI starts with good governance. Case in point: Paris' extensive use of AI included guardrails – its new AI law did not allow for the processing of biometric data or the use of (controversial and unproven) facial recognition techniques.

4. Deal with disinformation

As early as last year, Russia-based hackers ginned up fabricated news websites and a feature-length documentary film, narrated with fake AI-generated audio that sounded like actor Tom Cruise, all part of a disinformation campaign designed to mar the reputation of the IOC and spread rumors of expected violence at the Olympic Games. To combat these efforts, France created a government agency, VIGINUM, a 50-person military cybersecurity team to track and expose foreign interference in the Olympics and French elections.

$94M

Estimated revenue increase from cybersecurity services in France this year due to cyber threats related to the Paris Olympics

With AI-driven deepfakes on the rise, fighting false stories about one's brand is becoming harder than ever. Enterprise leaders will need to set aside budget and personnel so marketing departments can adequately monitor online news and social media. Keep in mind, It's not just the multinationals with deep coffers that cybercriminals like to target; misinformation and disinformation campaigns strike SMBs too, leaving mom-and-pop shops scrambling to repair their damaged reputation.

The good news? Traditional cybersecurity strategies can help spot deepfake tech faster – think updated phishing training and threat hunts – helping to thwart these newfangled influence operations.

5. Incentivize your staff training

Regular and comprehensive staff training is considered an essential – and often boring – part of any organization's cybersecurity routine. Regel's team ran a series of awareness training campaigns, highlighting the dangers of social engineering and other ways hackers infiltrate networks, and sometimes incentivizing his workers with prizes and gifts.

[Read also: Workers are worried they'll be replaced by AI – but in SecOps, humans are still essential]

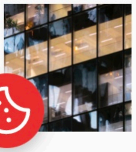
Other new approaches to training programs include immersive, Hollywood-style security-training videos that incorporate cinematic storytelling techniques and even suspense to engage workers. Some research indicates this may help employees to better retain security lessons – and to retain those lessons for longer.

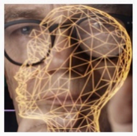
6. Keep workers and customers (clearly and easily) informed

On the Olympics.com website, a dedicated cybersecurity page for workers, athletes, and attendees provides info on how to thwart scams and respond to a suspected hack of one's official Olympics account. It also offers best practices regarding passwords, phishing, and device updates.

The same can and should be done for the workers and customers at any organization. Every website should have easy to access security pages with basic (yet vital) instructions on what to do if you suspect you've encountered a cybersecurity problem.

Related


What Return-to-Office (RTO) Means for Your Cybersecurity


I Almost Fell for This Online Scam. Why Even Tech Pros Can Be Taken

How AI Is Redefining Data Loss Prevention (DLP)

The Power of Certainty™

Tanium delivers Autonomous Endpoint Management (AEM) with the industry's only true real-time platform for AI.

SEE A DEMO →

TANIUM

CONTACT US →

About Tanium

- Careers
- Leadership
- Newsroom
- Locations
- Analyst Recognition
- Cloud Trust Center
- Security
- Sustainability

Autonomous Endpoint Management

- Tanium Platform
- Tanium Core
- Endpoint Management
- Risk & Compliance Management
- Incident Response
- Digital Employee Experience

Explore

- Focal Point Magazine
- Tanium Blog
- Let's Converge Podcast
- Downloads
- Events

Learn

- Training
- Certifications

Support

- Resource Center

Customers

- Success Stories

Partners

- Partner Finder
- Become a Partner
- Partner learning hub

Legal

- Privacy Policy
- Terms of Use
- CCPA Notice of Collection
- Do Not Sell or Share My Personal