

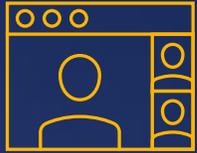
# Global Game, Global Target

Understanding and Defending  
Against the Hybrid Threat  
Landscape of FIFA 2026



OPTIV®

# Soft Target Battleground – Massive Attack Surface



Billions of viewers



Millions of devices



Tens of thousands of staff and volunteers



Thousands of vendors



Forty-eight national teams



Three host countries



Sixteen host cities



Critical infrastructure:  
transportation, energy,  
telecommunications,  
financial institutions,  
government

**= billions of potential targets**

# The Evolution of Cyber Threats at Global Events

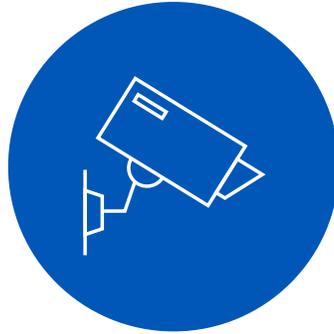
Threats targeting major sporting events have evolved from purely physical to a hybridized and more effective attack.



# Security

## Layers and

## Defence Lines



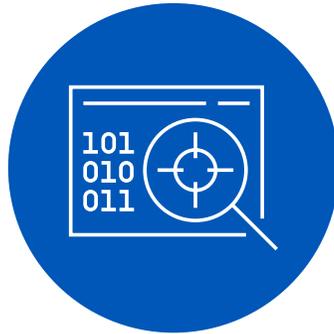
**Physical Security**



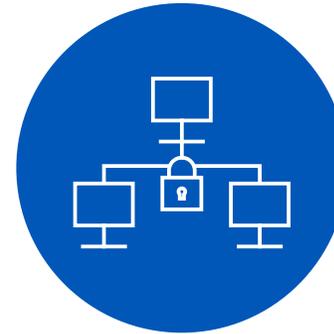
**People  
Infrastructure**



**Supply  
Chain Risks**



**Intelligence,  
National Security  
and Influence  
Operations**



**Digital  
Infrastructure and  
Interconnected  
Systems**



**Public Safety and  
Emergency  
Response  
Management**

# Physical Security Priorities

Access and  
Perimeter  
Control

Transportation  
and Mobility

Accredited-  
only  
Restricted  
Zones

Venue  
Protection  
and Public  
Spaces

Crowd  
Management

Protection of  
High-Value  
Targets

Detection  
Systems

Smart Stadiums

Biometric Gates and Passes

Digital Ticketing and Accreditation Systems

Transportation and Mobility

Operational Technology Systems

**Digital**

**Infrastructure and**

**Interconnected**

**Systems**

Communications Systems

Payments and Commercial Systems

Broadcast and Media Infrastructure

Power and Critical Utilities Infrastructure

Cybersecurity Architecture

**Supply**

**Chain Risks**

Every vendor is an entry point

## Supply chain compromise = physical disruption and risk to national credibility



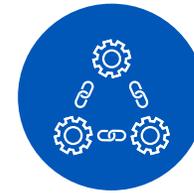
Logistics complexity and cross-border challenges



Labour and skills shortages



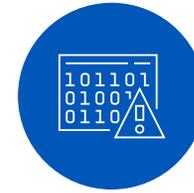
Material shortages (infrastructure, construction and materials)



Security and fraud risks in digital supply chains



Supplier compliance and governance failures



Food services and catering for athletes and security



Uniforms and equipment



Fan experience and hospitality supply chain strain

# The People Ecosystem of FIFA:

Inside the human network



**People**

- Athletes and their delegations
- Fans and spectators
- Crowd control and communication
- Staff, security personnel and volunteers
- VIPs and high-value targets
- Protecting against insider risks and human error (intentional and unintentional)

*Both our greatest defence and our weakest link*

# Paris 2024:

The human engine behind the last Olympics

How are  
we vetting?

**10% to 15%**

Selected from  
300,000 volunteer  
applications in Paris



**100,000**  
contractors



**4,500**  
Paid staff



**10,000**  
Military  
personnel



**17,000**  
Private security  
agents

Security forces;  
daily average

**30,000**  
gendarmes/day

**45,000**  
Per peak days

# Public Safety and Emergency Response Management

## Planning for worst-case scenarios

Threats of terrorism and physical threats still exist but amplified by online mobilization and disinformation

Crowd control and moving people safely in an emergency

Sabotage attacks against infrastructure  
Fire, bomb threats, natural disasters

Threat monitoring and early warning

Geopolitical and targeted delegation threats

OSINT and social media monitoring

# Intelligence, National Security and Information Operations

Protest activity and activism forecasting

Crowd behaviour and environmental awareness

Disinformation, narrative tracking and influence operations

What will this look like for FIFA 2026?

# Cyber-enabled Fraud

Fake tickets & Fraudulent ticketing platforms

Payment fraud

Phishing and social engineering at scale

Fake “official games” apps

Public Wi-Fi exploitation

Fake websites

BEC targeting vendors

Merchandise & Licensing Fraud

# The Convergence Zone

**What happens when physical,  
digital and national security collide?**

# Disinformation

Disinformation is deliberately false or misleading information shared with the intent to deceive or manipulate others. It is often used to influence opinions, create confusion or achieve a specific agenda.

# Misinformation and Disinformation

Information as a Weapon

Eroding trust and  
creating division

Disguising real-world  
actions

Dehumanization and  
incitement of violence

Inducing fear, anger,  
and uncertainty

Manipulating public  
opinion

Weakening  
adversaries

CIA bulletins about elevated terrorism threats on the metro

Ukrainian athletes competing had to wear GPS monitors

French TV channels reported mass cancellations of bookings

## Disinformation Targeting Paris 2024

IOC deleted the opening ceremony video because of widespread criticism

Seine River “Blue Dye” for the Olympics

French military flypast accidentally displays Russian flag colours

***“A lie can travel halfway around the world while the truth is still putting on its shoes.”***

## How Powerful Is Misinformation?

*“6,500 Migrant worker deaths in Qatar World Cup”*

- **6,500** deaths since Qatar was awarded the 2022 World Cup widely circulated
- This figure was tweeted over **400,000** times in multiple languages
- Became explicitly linked to deaths on **‘World Cup construction sites’**
- Became one of the most **shared English-language controversies on Twitter** regarding the 2022 World Cup

# Understanding Our Adversaries



**Nation-states**



**Geo-political  
agendas**



**Organized  
crime groups**



**Hacktivists**



**Low-level  
criminals**



# Collaboration

Taking a page out of the threat actor playbook

## Authentic collaboration can tip the scales and counter malicious threats

Are we using our expertise in the best way possible?

How do we break down silos?

Are we empowering our human firewall to be part of the security solution?

## Blueprint

## For Resilience

- ✓ Unified command models: cyber + intelligence + physical
- ✓ Cross-sector collaboration
- ✓ Continuous red-teaming and joint simulations
- ✓ Human-focused defences
- ✓ Cross-border cooperation – intelligence sharing among allies
- ✓ Public trust as an objective



**Protecting the integrity of global events like FIFA is more than protecting sport. It is an opportunity to showcase how integrating all aspects of security creates stronger, more resilient nations.**

# Thank You

Lina Dabit  
Executive Director  
Office of the CISO  
Optiv Canada  
[lina.dabit@optiv.com](mailto:lina.dabit@optiv.com)  
416.906.7609

**Secure greatness<sup>®</sup>**

