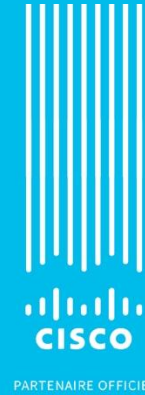
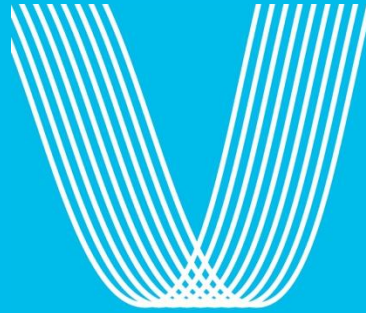




The bridge to possible



Paris 2024

Cyber Security Return of Experience

September 2024

Agenda

- Introduction
- Pourquoi Cisco ? / Prévisions et attentes avant les jeux
- Architecture
- REX du CSOC



WELCOME

Cisco x Paris 2024

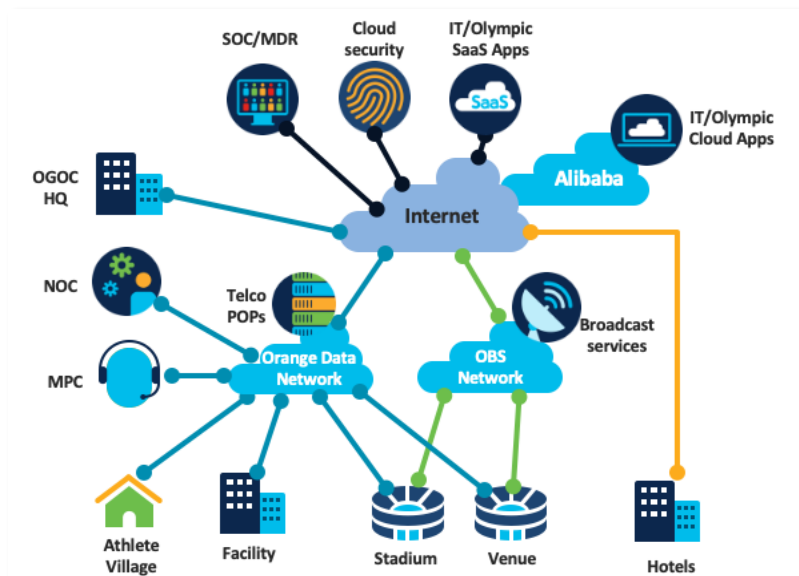


PARTENAIRE
OFFICIEL




- ✔ Official Partner for Network Infrastructure
- ✔ Official Partner of Cybersecurity Solutions
- ✔ Official Partner for Collaboration (Webex)

100 Olympic Venues
4 Major sites: TOC, IBC, MPC, Village



Cisco's Engagement in Paris 2024



Venue Network

3000+ Catalyst 9K Switches + Micro DNA Center



Network Security

80+ Firepower, ISE, Secure Network Analytics



Cloud Security

Umbrella, Duo, CES, DDOS, XDR, CII, Panoptica, VMS, Secure Cloud Analytics



Wireless Network

11000 Catalyst APs
50+ WLC




Physical Security Network

Catalyst 9K Switches
Panasonic Cameras




WAN

WAN services
Private 5G
CURWB



Compute and Storage

14 UCS C220
For Network Services



Collaboration

4k WebEx Users
50 Telepresences
1,000 IP Phones
Webex Events



Full Stack Observability


Thousand Eyes

Cisco CX



Design

Network HLD/LLD
Cyber HLD/LLD/Testing
SW recommendation & lifecycle





Governance

PMO/AMO
Event Assurance
CAP

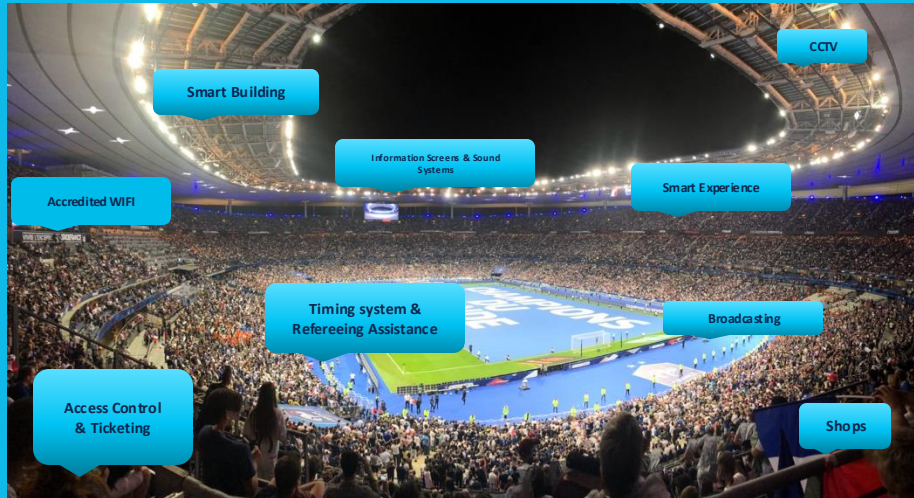


TOC/SOC Operations

TALOS TI/CIR/TH/CA
HTOM/HTTS/TAC
Smartnet/Spare Mgmt

Le contexte

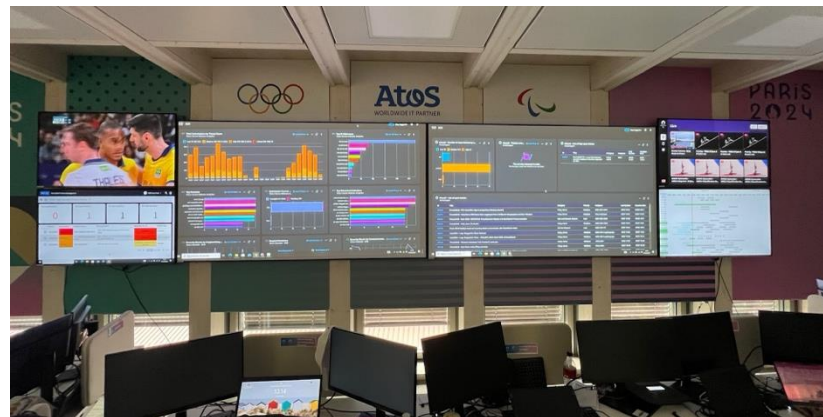
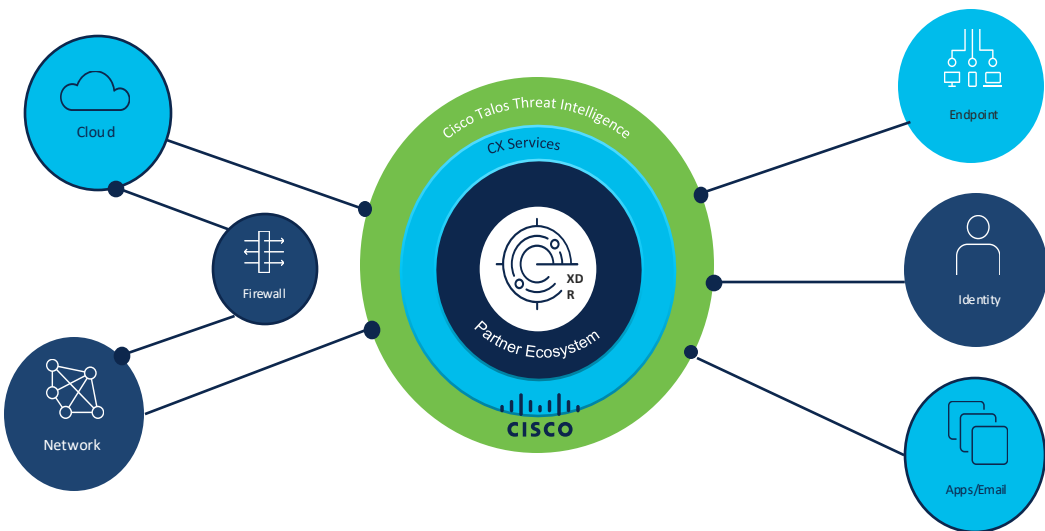


Forbes - Classements Brandvoice Bibliothèque Magazine Forbes Je m'abonne

Le succès des Jeux Olympiques et Paralympiques (JOP) repose notamment sur les moyens technologiques mis en place, c'est pourquoi la surface d'attaques s'élargit à chaque édition. Ainsi malgré des mesures de cyberdéfense extrêmement sophistiquées, le niveau de protection devient un véritable défi. Partenaire informatique mondial des Jeux depuis 2001, Atos aurait ainsi bloqué 4,4 milliards d'événements de cybersécurité pendant les Jeux de Tokyo 2020 (qui ont eu lieu en 2021). Un chiffre qui, selon les estimations, devrait connaître une augmentation notable lors des JOP de Paris ce mois-ci.

Comment les entreprises impliquées dans Paris 2024 peuvent-elles renforcer leur défense et prendre des mesures préventives pour sécuriser cet événement majeur ?

Cisco Zero Trust Architecture, 95% of portfolio



Retour de l'ANSSI



Un niveau de menace intense,
conformément aux attentes

4. Un nombre limité d'incidents cyber et sans impact sur le déroulement des JOP

Un total de 548 événements de cybersécurité affectant des entités en lien avec l'organisation des Jeux Olympiques et Paralympiques de Paris 2024 a été rapporté à l'ANSSI entre le 8 mai et le 8 septembre 2024. Ces derniers ont été portés à la connaissance de l'Agence et ont donné lieu à un traitement par les équipes opérationnelles.

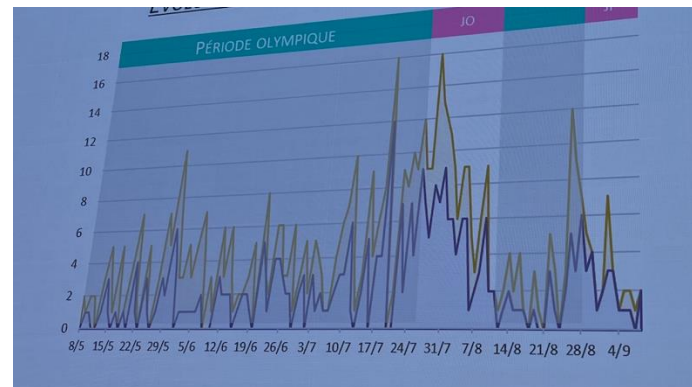
Sur les types d'événements de cybersécurité rapportés, près de la moitié des événements de cybersécurité correspondent à des indisponibilités dont un quart sont dues à des attaques par DDoS. Le reste des événements de cybersécurité correspondent à des tentatives de compromission ou des compromissions, des divulgations de données ou bien encore des signalements de vulnérabilités. Les secteurs d'activité les plus ciblés sont les entités gouvernementales, le sport, le divertissement (sites de compétitions et Paris 2024) et les télécommunications.

Ces 548 événements de cybersécurité comprennent :

- 465 signalements (événements de sécurité d'origine cyber avec un impact bas pour le système d'information de la victime, requérant une intervention minimum de l'Agence) ;
- 83 incidents (événements de sécurité pour lesquels l'ANSSI confirme qu'un acteur malveillant a conduit des actions avec succès sur le système d'information de la victime).

En conclusion, si l'ANSSI et ses partenaires nationaux ont accompagné plusieurs victimes dans la résolution d'incidents, aucun événement de cybersécurité n'a affecté les cérémonies d'ouverture, de clôture et le bon déroulement des épreuves. Tous les événements de cybersécurité survenus au cours de cette période sont globalement caractérisés par leurs faibles impacts.

<https://cyber.gouv.fr/actualites/bilan-cyber-des-jeux-olympiques-et-paralympiques-de-paris-2024>



Our Cisco view during Olympics

Source	Description	Value
ISE	Peak Endpoint	245 K
	Peak Concurrent Users	65 K
Umbrella	Total DNS Request (Accredited Users)	540 M
	Total SIG traffic (Employees)	145 TB
Router	Peak Internet Traffic	25 Gbps
Secure Network Analytics	Internet Traffic Volume	13 PB
	Internal Traffic Volume	30 PB
	Netflow Records Analyzed	9 B
Secure Cloud Analytics	Flow Record Analyzed	36 B
Cisco Email Security	Received Emails	3 M

- CrowdStrike BSOD impacting 800+ servers and 3000+ laptops
- SNCF train signaling cabling physical attack
- Many threats on Darkweb, Telegram and Social networks
- DNS abuse, selling fake tickets, streaming and merchandise while harvesting information from unknowing users
- Phishing campaigns with raffles or invoice documents attachments
- Insiders caught through honey pots
- Doxing for some delegations
- 100+ stolen laptops/phones/tablets in airports and venues

Incident Outside of P2024 responsibility

- A few DDOS towards International Olympic Committee (Switzerland) web site
- Ransomware targeting French museums



The bridge to possible