



AFG

LePointsur



Cybersécurité :

Quel est le niveau de maturité des SGP en matière de cybersécurité ?

Jeudi 28 novembre 2024

9h30-11h00

AVERTISSEMENT

L'intervention des intervenants est proposée à titre d'information ou d'exemple pour présenter aux participants une pratique du marché applicable, une innovation en matière de technologie ou d'organisation. Cette présentation n'est pas une incitation pour les participants à utiliser les services des intervenants ou des sociétés pour lesquels ils travaillent, ni une offre commerciale.

L'AFG ne garantit pas la conformité réglementaire de cette proposition.

Aussi il appartient à chaque participant :

- de vérifier cette conformité au regard de sa situation propre
- de s'assurer que les propositions présentées sont adaptées à sa situation en vérifiant notamment si sur le marché d'autres offres sont plus pertinentes au regard de sa situation.

Cybersécurité : Niveau de maturité des SGP



AFG

LePointsur

Introduction



Laure Delahousse
Directrice générale de l'AFG



AFG



LePointsur

Cybersécurité : Niveau de maturité des SGP

**N'hésitez pas à poser vos questions
aux orateurs sur la plateforme**

Posez vos questions ici



Bienvenue à
"Point sur" CYBERSECURITE



Questionnaire Cybersécurité : Restitution de l'enquête 2024



Wilfried Lauber

Président du GT Cybersécurité
de l'AFG et RSSI adjoint, Amundi



Olivier PALLANY

Group CISO et Data Protection
Officer, Sienna Investment
Managers



Walif EL HITTI

RSSI, Comgest

QUESTIONNAIRE CYBER SÉCURITÉ 2024

- 🏢 Collecte auprès de toutes les SGP adhérentes de l'AFG réalisée entre juin et septembre 2024
- 🏢 L'échantillon est composé de 74 SGP ou groupe* de gestion qui représentent plus de 84 SGP. Parmi celles-ci 33 SGP sont filiales d'un groupe financier et 41 SGP sont entrepreneuriales
- 🏢 Selon le montant des encours gérés, l'échantillon est composé, de :
 - ▶ 10 SGP gérant plus de 50 mds €
 - ▶ 10 SGP gérant entre 15 et 50 mds €
 - ▶ 20 SGP gérant entre 1 et 15 mds €
 - ▶ 34 SGP gérant moins de 1 md €
- 🏢 Ensemble les 74 SGP de l'échantillon gèrent des encours de 3 880 mds €, soit 74% des encours en France, (3 050 Mds € en 2022) et emploient des effectifs de 13 815 ETP dont 151 ETP internes dédiés à la définition et à la mise en œuvre de la sécurité de l'information.

LE RISQUE CYBER – UNE PRIORITÉ 2024

90% des SGP

placent le **risque cyber**
dans le TOP 3
des risques les plus redoutés

Une vraie prise de conscience (+19%)



Top 6 risques pour les experts et le public

	EXPERTS	GRAND PUBLIC
	1 Changement climatique	1 Changement climatique
	2 Instabilité géopolitique	2 Nouvelles menaces sécuritaires et terrorisme (+4)
	3 Risques de cybersécurité	3 Risques de cybersécurité (+1)
(Nouveau risque)	4 Risques liés à l'intelligence artificielle et au big data	4 Tensions et mouvements sociaux (+3)
(+1)	5 Tensions et mouvements sociaux	5 Pandémies et maladies infectieuses (-3)
(+1)	6 Biodiversité et ressources naturelles	6 Instabilité géopolitique (-3)

<https://www.axa.com/fr/actualites/2024-future-risks-report>

MOYENS MIS EN ŒUVRE 2024

Budget stable ou en croissance pour 95% des SGP

comme en 2022

☰ Budget **sécurité récurrent**

versus IT

- ▶ **6.3%** SGP gérant **plus de 15 Mds**
- ▶ **10.7%** SGP gérant **moins de 15 Mds**

Ces chiffres sont des % du budget IT

☰ **sécurité projets** versus IT

- ▶ **5.1%** SGP gérant **plus de 15 Mds**
- ▶ **7.3%** SGP gérant **moins de 15 Mds**

En 2024, **dans la finance**
la moyenne s'élève à **7,8% (+2%)**

- Wavestone cyber benchmark 2022 : 6,1% en moyenne et 5,8% pour la finance
- Wavestone cyber benchmark 2024: 7.8% pour la finance



☰ En 2022, c'était

- ▶ **5.3%** SGP +15Mds
- ▶ **12.9%** SGP -15Mds

Baisse de l'écart entre SGP

MOYENS MIS EN ŒUVRE 2024

Effectifs internes dédiés à la définition et à la mise en œuvre de la sécurité de l'information (en % de l'ensemble des effectifs) :

- ▶ SGP gérant entre 1 et +15 mds € : moyenne : entre 1 et 2%
- ▶ SGP gérant moins de 1 md € : entre 2% et 17% - moyenne à 6,3%

Il ne faut pas sous-estimer l'implication de la cyber pour une SGP gérant moins de 1 Mds





Un RSSI nommé pour 68% des SGP

Stable depuis 2020

Deux tendances

- ☑ **Pour les SGP gérant plus de 10 mds – 100%** ont un RSSI (+14%)

Il dédié dans 84% (+1%) des cas

- ☑ **Pour les SGP gérant moins de 10 mds - 56%** ont un RSSI (-6%)

et dédié dans 22% (+9%) des cas

Son rattachement reste principalement « hors DSI » pour 73% (+6%) des cas

Le reporting cyber et résilience à la direction est clé



⚠ 13% ne reporte pas à la direction – DORA l'exige

- ☑ 59% (+6%) des SGP déclarent avoir un tableau de bord. Il faudrait tendre vers le 100%
- ☑ La fréquence de la déclaration est semestrielle dans +72% des cas. C'est une bonne chose.
- ☑ 95% des SGP déclarent que leur niveau de maturité sur la cybersécurité augmente. Très positif !

Le RSSI est une fonction clé dans l'organisation, indépendante et proche de l'IT.

Il peut être responsable DORA.

RISQUE ET MOYENS MIS EN ŒUVRE 2024

Relatif au ransomware

Top Risque

- 1 – Indisponibilité de système d'information
- 2 – Ransomware
- 3 – Intrusion (+3) ↗
- 4 – Phishing (-2) ↘
- 5 - Défaut de conformité réglementaire (+2) ↗
- 8- Espionnage (-5) ↘

Top Projets

- 1 – DORA (83%)
- 2 – DLP (-1) ↘
- 3 - Détection des menaces (+2) ↗
- 4 - IAM
- 5- Sécurisation du Cloud (-2) ↘

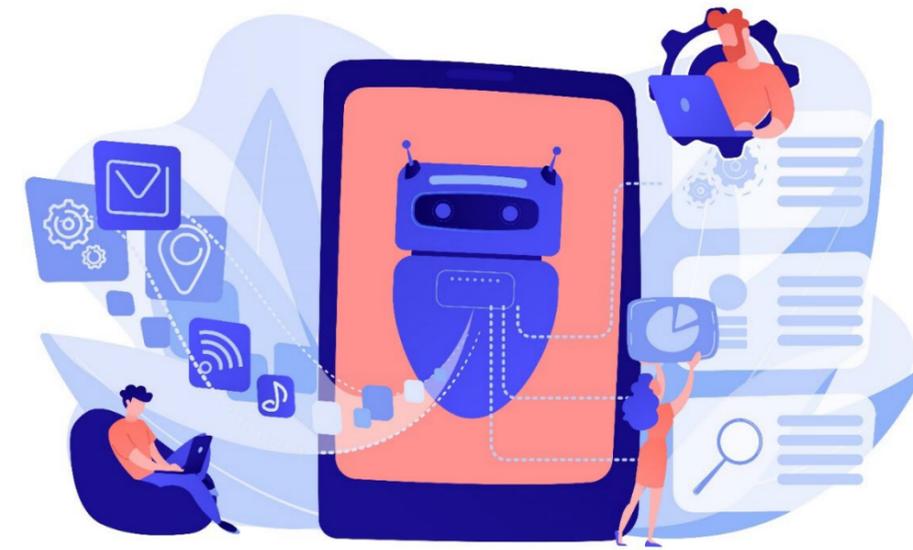
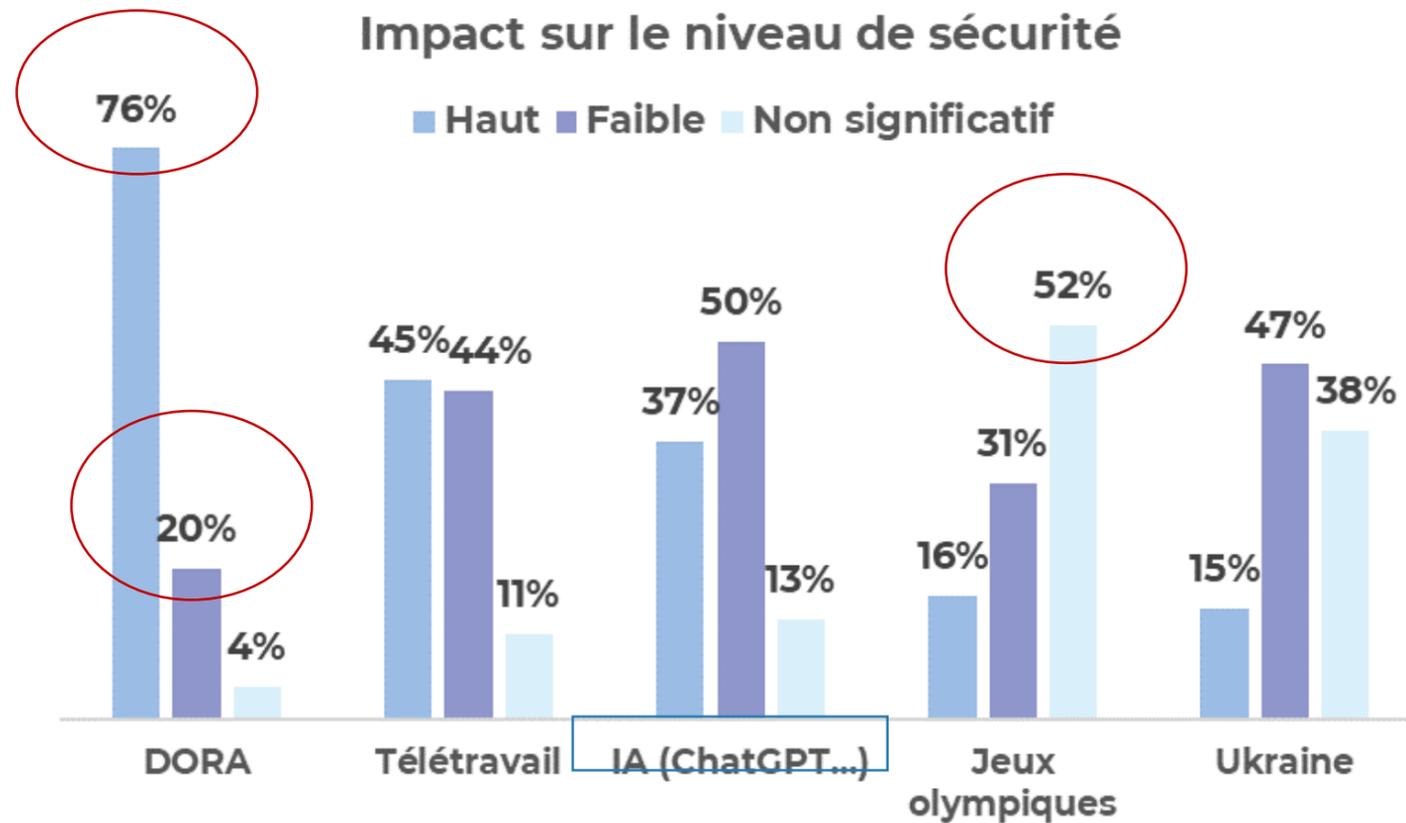


DORA en tête.

Des tendances en lien avec l'actualité.

L'espionnage fait moins peur (-5).

SUJETS IMPACTANT L'ACTIVITÉ CYBER (TECHNOLOGIQUES, GÉOPOLITIQUES, ...)



- DORA est naturellement assez visible.
- Les sociétés associées à des marques/groupes connues ont été sensibles aux risques liés aux JO
- L'IA est un sujet

Politiques et chartes de sécurité

- 84% des SGP ont des politiques de sécurité (PSSI) et 68% ont des RSSI
- 88% déclarent disposer d'une charte d'utilisation des moyens informatiques



Utilisez les [guides cyber AFG](#)

Certifications

- Certification reçue par la société de gestion:
 - ISAE3402 : 14%
 - ISO27001 : 11%
 - SOC2 : 5%

Intérêt des certifications	
Être Aligné	Être Certifié
Est une bonne cible à atteindre en termes de maturité	Permet de répondre à des attentes clients

CARTOGRAPHIE DES APPLICATIONS 2024

80% des SGP sont en cours ou ont cartographié leurs applications suivant les 4 critères DICP*.

54% l'ont fait et 26% sont en cours



DORA nécessite une cartographie complète



100% (+3%) des SGP inclus la sécurité dans leur projet.

Très bon point !



Définition DICP

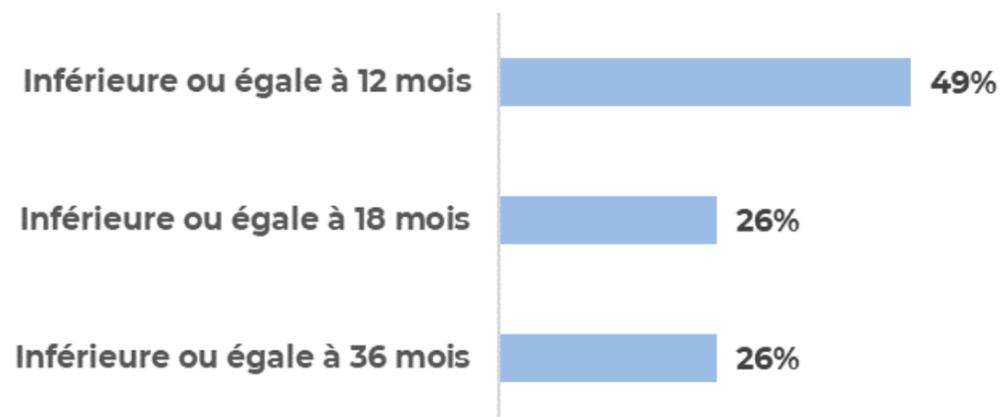
- D: Disponibilité (essentiel)
- I: Intégrité (pas forcement)
- C: Confidentialité (essentiel)
- P: Preuve (pas forcement)

Cartographie

- 92% des SGP ont ou sont en train de cartographier leur tiers
- 76% des SGP déclarent classer le niveau de criticité des tiers. *Belle progression: 52% en 2022. Mais pas suffisant.*

⚠ DORA attend un référentiel complet des tiers

Fréquence du suivi du niveau de sécurité des tiers critiques



- Cloud** : 62% des SGP ont mis en œuvre des mesures de protection spécifiques liées au service cloud.

Clauses dans les contrats

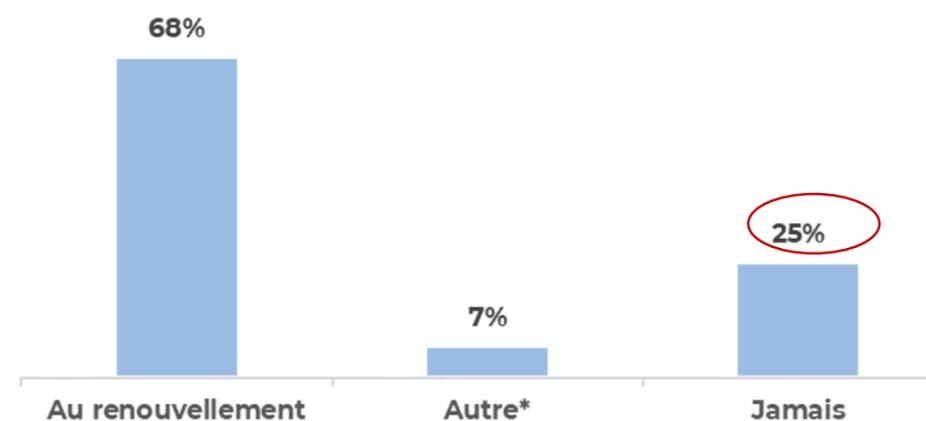
- Intégration dans les contrats avec les prestataires de clauses spécifiques liées à la sécurité de l'information (protection de données, droit d'audit technique, notification d'incidents, etc.)

- Toujours (45%) ; Souvent (38%) ; **Jamais (17%)**



DORA définit des exigences en termes de clauses qu'il faut proposer à vos prestataires

Fréquence de la revue des mesures contractuelles de protection (Plusieurs réponses possibles)

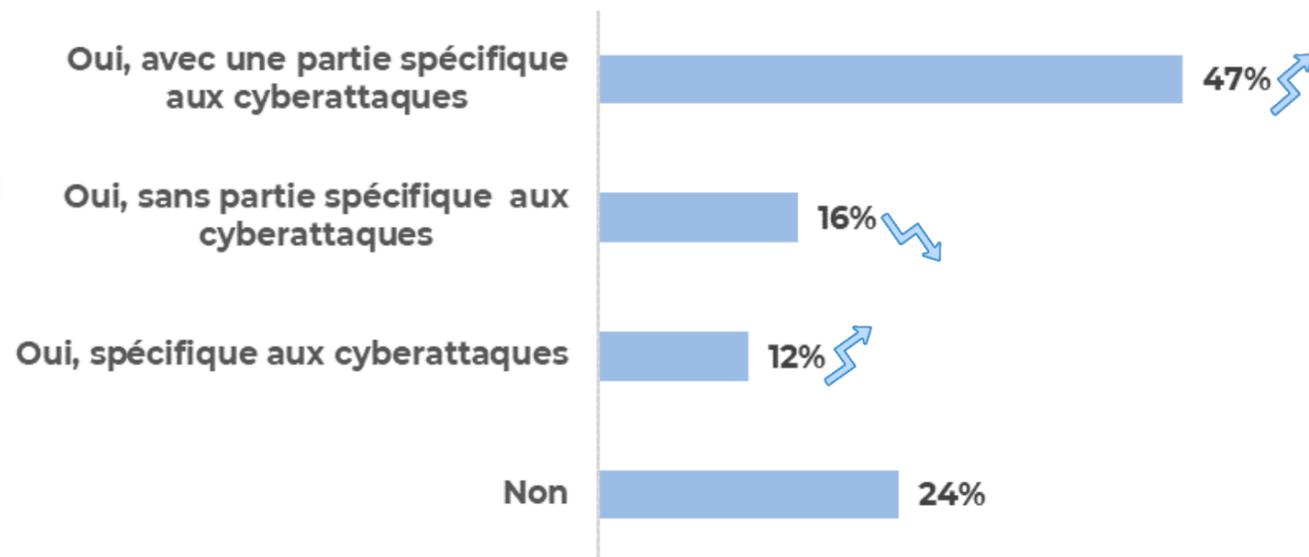


RÉPONSE À INCIDENT EN 2024

Incidents de Sécurité

- 1% des SGP déclarent avoir subi des incidents critiques avec un impact matériel (financier, réputationnel, ...) relatifs à la cybersécurité sur les 12 derniers mois
- 53% des SGP déclarent disposer d'un SIEM* (42% en 2022) en lien avec le nombre de SGP ayant un SOC* (50%). Approche proportionnée, en adéquation avec le besoin de la SGP.

Formalisation d'un plan de réponse à incident

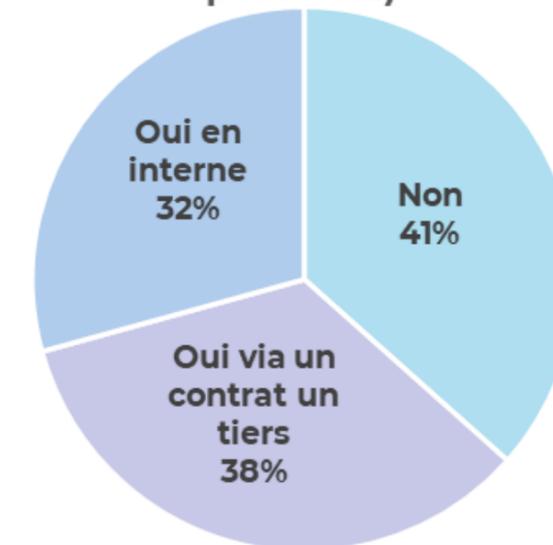


SIEM: Security Information and Event Management Outil qui permet de collecter, détecter et signaler des comportements inhabituels pour protéger l'entreprise.
SOC: Security Operation Center. Equipe (interne/externe/hybride) assurant une surveillance des événements de sécurité.

Gestion de crise

- 57% des SGP ont souscrit une assurance. Nette progression entre 2020 et 2024 (+22%) et stagnation depuis 2022.
- 59% dispose d'un service d'intervention spécialisée en cas d'incident cyber. Notre recommandation.

Sécurisation de l'intervention d'équipe en cas d'incidents cyber (plusieurs réponses possibles)



CONTINUITÉ D'ACTIVITÉ

Réalisation de sauvegardes

- 100% des SGP font des sauvegardes
 - 81% avec tests
 - 19% sans tests

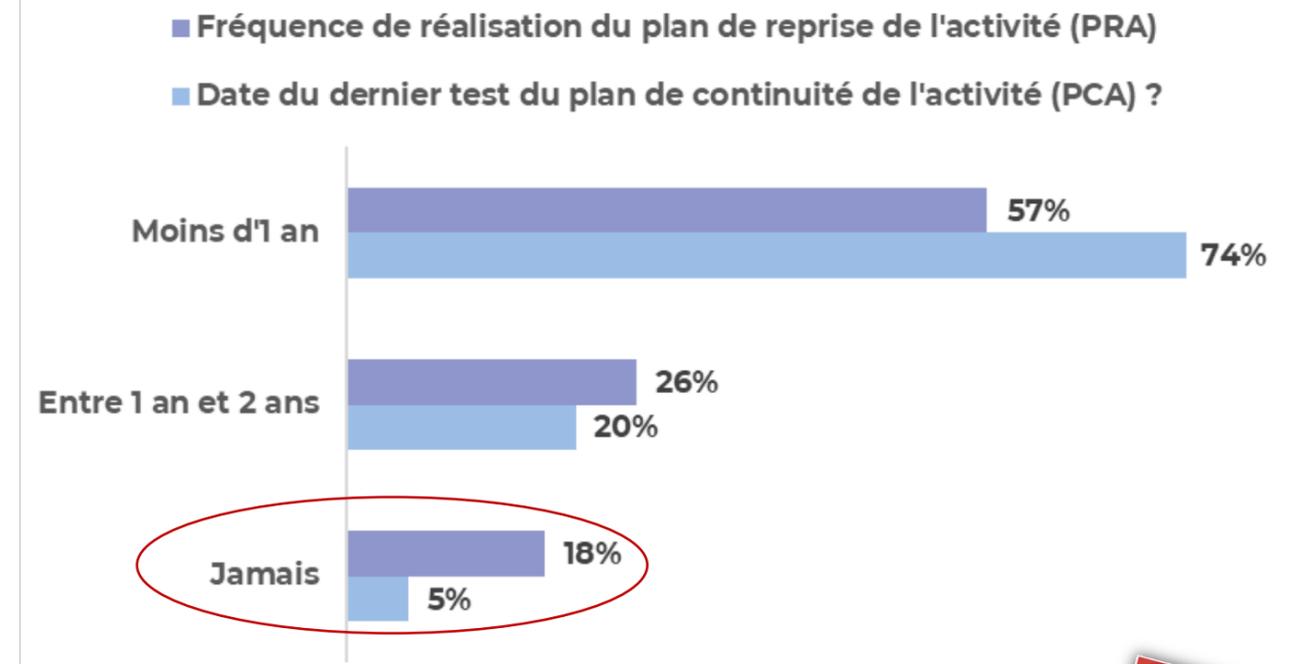
DORA attend 100% de tests sur les périmètres liés aux fonctions critiques ou importantes

- En complément:
 - 62% des SGP déclarent disposer de sauvegarde à froid / déconnectée / offline
 - **72% disposent de sauvegardes pouvant répondre à des attaques type ransomware.**
- C'est une préconisation forte de l'AFG (100% attendu)**



Plan de continuité d'activité

Les PCA doivent avoir lieu tous les ans pour vos services critiques



Votre plan de continuité d'activité proportionné

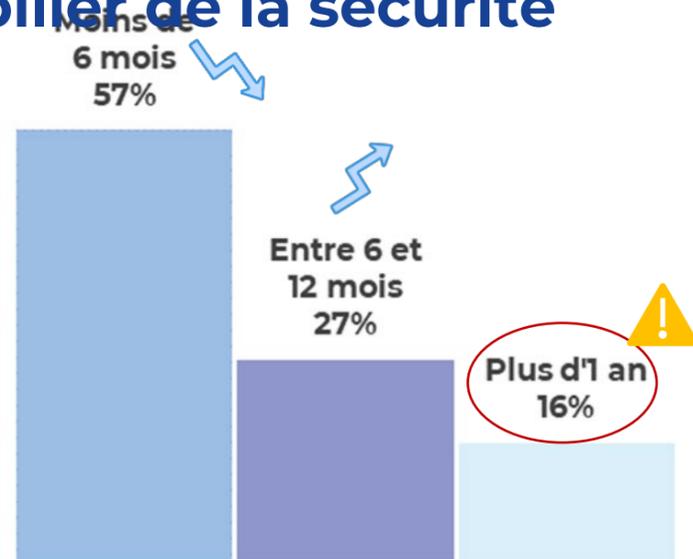
notamment sur vos fonctions critiques ou importantes avec des tests annuels.
C'est une **exigence DORA !**



LA SÉCURITÉ AU SEIN DE L'ENTREPRISE 2024

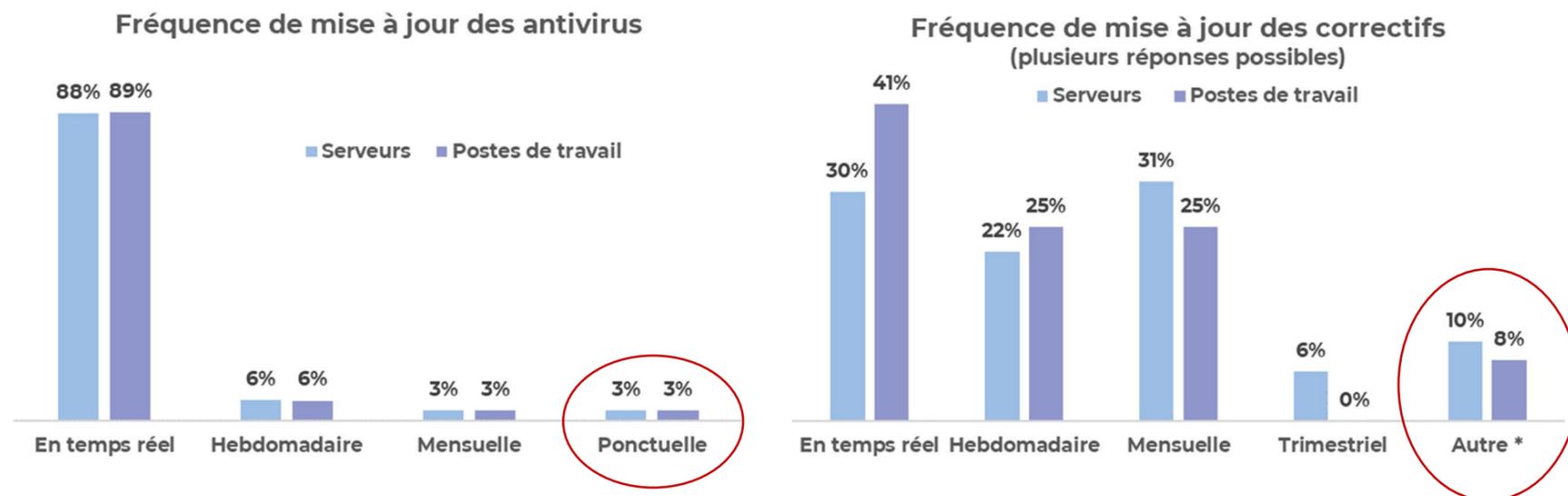
Revue des comptes à privilèges

Un pilier de la sécurité



Patch et mises à jour

Le deuxième pilier de la



La certification régulière des comptes à privilèges est une action essentielle à mener.
Pas d'amélioration globale, un changement de tendance.

Les patches et les mises à jour de vos antivirus font partie des basiques de l'hygiène cyber sécurité à ne pas négliger.
Ils sont globalement bien mis en œuvre.

CONTRÔLES

Dispositif de contrôles

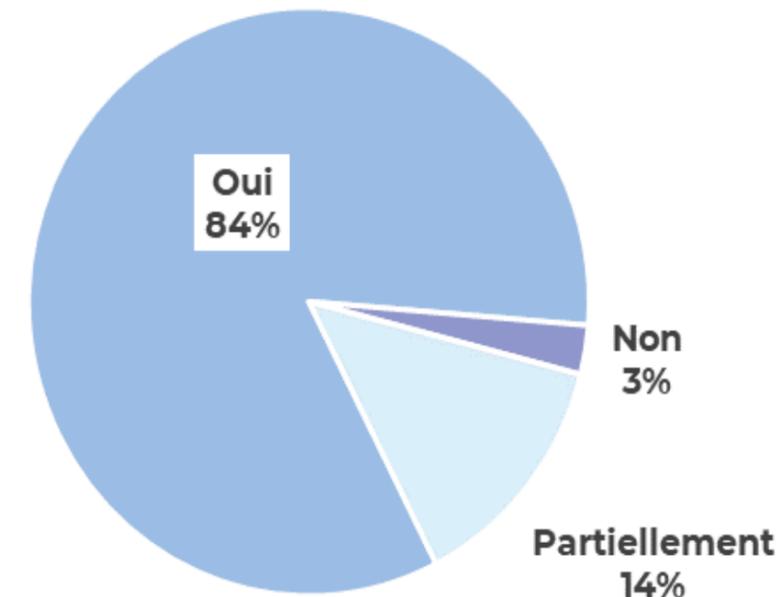
- ☑ **91%** des SGP déclarent que leur programme de contrôles intègre des contrôles de sécurité de l'information
- ☑ Dans le **Top 3** des techniques de contrôles de sécurité:
 - Audit de sécurité techniques équipe externe
 - Scan de vulnérabilité
 - Test d'intrusion/Red team



Protection des accès à distance

La protection des accès distants par une solution **d'authentification à double facteur** est obligatoire.

- ☑ Pas d'augmentation
- ☑ **100% est obligatoire !**



MESURE DE PROTECTION 2024

EDR*

Outil de détection et de remédiation

Mis en place pour 68% des SGP (56% en 2022)
en cours pour 11%

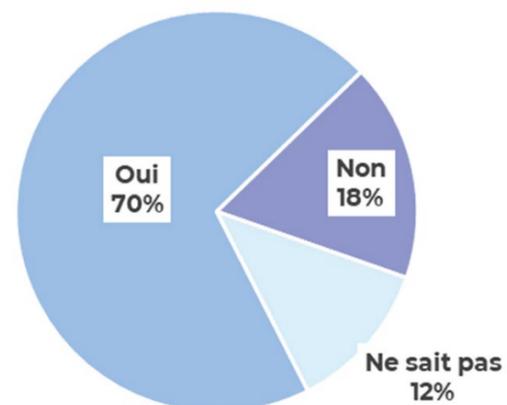
Un EDR est un outil clé pour votre sécurité
La supervision des évènements aussi !

Un proxy Internet est aussi intéressant

Dispositif permettant de filtrer

- des sites frauduleux/inappropriés
- réaliser des analyses antivirales en plus du poste de travail

L'accès internet passe par un proxy



EDR: Endpoint Detection & response. Logiciel permettant de détecter/bloquer des activités suspectes/malicieuses sur les serveurs ou postes de travail avec une capacité d'intervention.



TOP 5

des mesures de durcissement implémentées
pour sécuriser les postes de travail

- Reduction des droits d'administration - 93%
- Limitation des accès réseaux - 90%
- Limitation de l'installation d'application tierce - 78%.
- Le chiffrement – 74%.
Bitlocker est votre ami !
- Le blocage des ports USB – 67%.
contrôles SPOT AMF



SENSIBILISATION 2024

Le collaborateur est la première ligne de défense

100% des SGP ont formés 100% des collaborateurs sur les 3 dernières années.

90% des SGP sensibilisent les dirigeants à la cyber.
Attention, ce doit être une sensibilisation spécifique à leur responsabilité.

S'entraîner à lutter contre le phishing, c'est bien. Mais cela ne suffit pas pour sensibiliser.



92% (+2% versus 2022, +32% versus 2018)
des SGP ont des programmes de sensibilisation en place via :

- ☒ Des campagnes de phishing en majorité (81% ↗)
- ☒ Des e-learning (66% ↗)
- ☒ L'utilisation du « mail simple » (54% ↘)
(une diminution positive)
- ☒ Des conférences (24%)
- ☒ Des *serious games* (9%)
- ☒ Des écrans de veille (4%)



Cybersécurité : Niveau de maturité des SGP

Présentation de la fiche DORA pour les SGP « Microentreprise »

FICHE THÉMATIQUE NOVEMBRE 2024
AFG CYBERSÉCURITÉ : SGP MICROENTREPRISES & DORA

En plus du principe général de proportionnalité mentionné à l'article 4 de DORA, ce règlement européen précise que certaines exigences sont allégées pour les SGP classées comme microentreprises.

❗ QU'EST-CE QU'UNE MICROENTREPRISE ?
Une entité qui emploie moins de 10 personnes et dont le chiffre d'affaires annuel et/ou le total du bilan annuel n'excède pas 2 millions d'euros.

❗ PAR OÙ COMMENCER ?
• Cartographiez votre système d'information, identifier et répertorier les processus informatiques de votre SGP et les fonctions utilitaires.
Cette première étape vous permettra de détecter les sources de risques spécifiques à votre SGP.

❗ ENSUITE ?
• Consultez le Guide pratique DORA élaboré par le Groupe de travail Cybersécurité de l'AFG, ce guide vous apporte des indications concrètes sur les attentes en termes de conformité et de bonnes pratiques.
• Pour les SGP microentreprises, le guide met en évidence les points essentiels du Règlement DORA pour vous aider à anticiper son entrée en vigueur le 17 janvier 2025.
• Vous y trouverez un contact de proportionnalité et des exigences adaptées à votre taille facilitant la mise en œuvre progressive des dispositions réglementaires.

❗ QUELLES SONT LES EXIGENCES MINORÉES ?
1. Gestion des risques de sécurité informatique
• Gouvernance, organisation et cadre de gestion
Pour les SGP microentreprises, les exigences en matière de gouvernance et d'organisation des risques liés aux Technologies de l'Information et de la Communication (TIC), peuvent être simplifiées grâce au principe de proportionnalité. Elles ne sont pas obligées de mettre en place des dispositifs plus complexes.
Les stratégies, procédures et outils de gestion des risques TIC doivent être adaptés à la taille et à la portée de leurs activités.
Une revue périodique du cadre de gestion des risques TIC est nécessaire. Toutefois, une revue annuelle n'est pas obligatoire sauf en cas d'incident majeur lié aux TIC.
• Plan de réponse et rétablissement
Si toutes les SGP doivent avoir des plans de continuité d'activité pour les TIC et des plans de réponse et de rétablissement régulièrement revus, certaines modalités sont allégées pour les microentreprises (article 11).
• Politiques, procédures de sauvegarde, restauration et examen post-incident
Les politiques et procédures de sauvegarde et de restauration et les examens post-incident s'appliquent à toutes les entités financières. Toutefois, les SGP microentreprises doivent évaluer, en fonction de leur profil de risque, s'il est nécessaire de maintenir des capacités redondantes en matière de TIC redondantes.



Valentine Bonnet
Directrice Gouvernement
d'entreprise et Conformité,
en charge du GT cybersécurité
de l'AFG



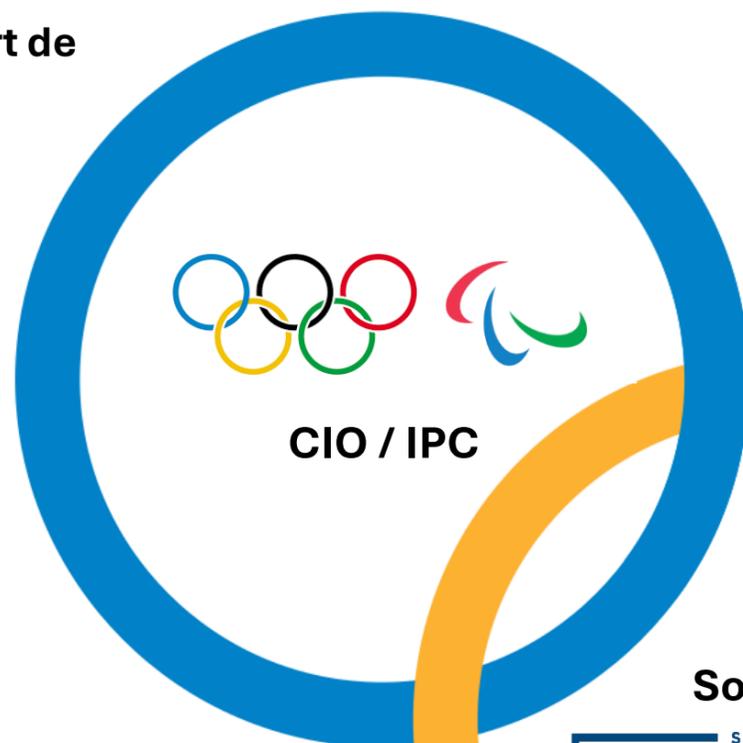
Cybersécurité : Niveau de maturité des SGP

Bilan « cyber » des JO 2024



Franz REGUL
directeur cybersécurité du
Comité d'organisation des
Jeux olympiques de Paris 2024

**Attribution des Jeux, promotion
et financement du mouvement
olympique et transfert de
connaissances**



CIO / IPC

**Conception, livraison,
opération & financement des
compétitions & célébrations**



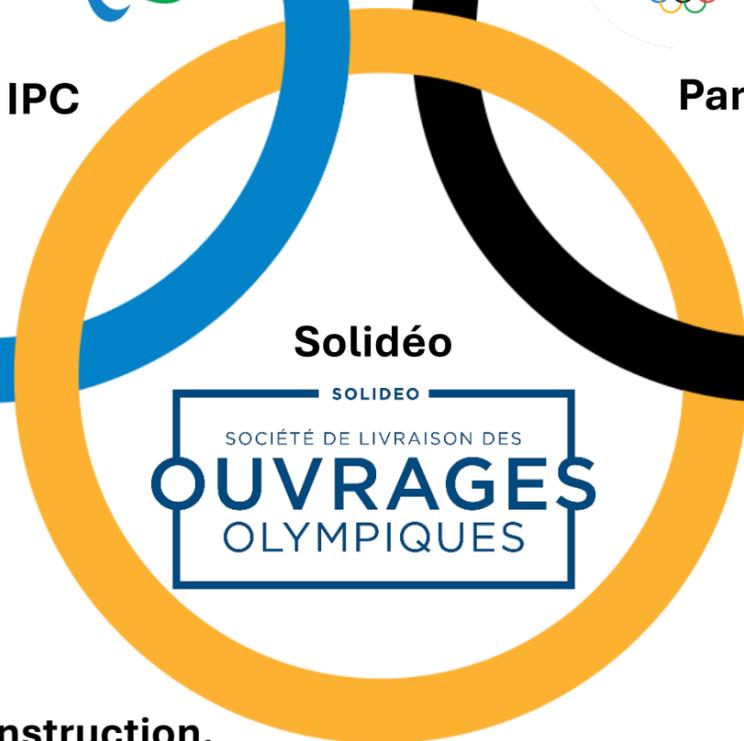
Paris 2024

**Signature du contrat de ville
hôte, supervision du COJOP et
support opérationnel**



Ville de Paris

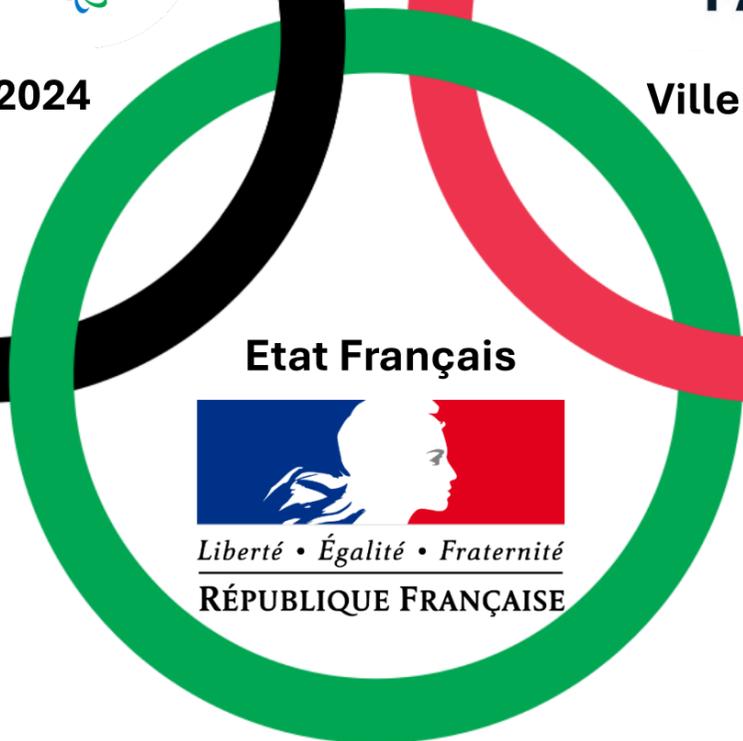
**Conception, construction,
livraison & restitution des
ouvrages olympiques (village,
centre aquatique...)**



Solidéo

SOLIDEO
SOCIÉTÉ DE LIVRAISON DES
OUVRAGES
OLYMPIQUES

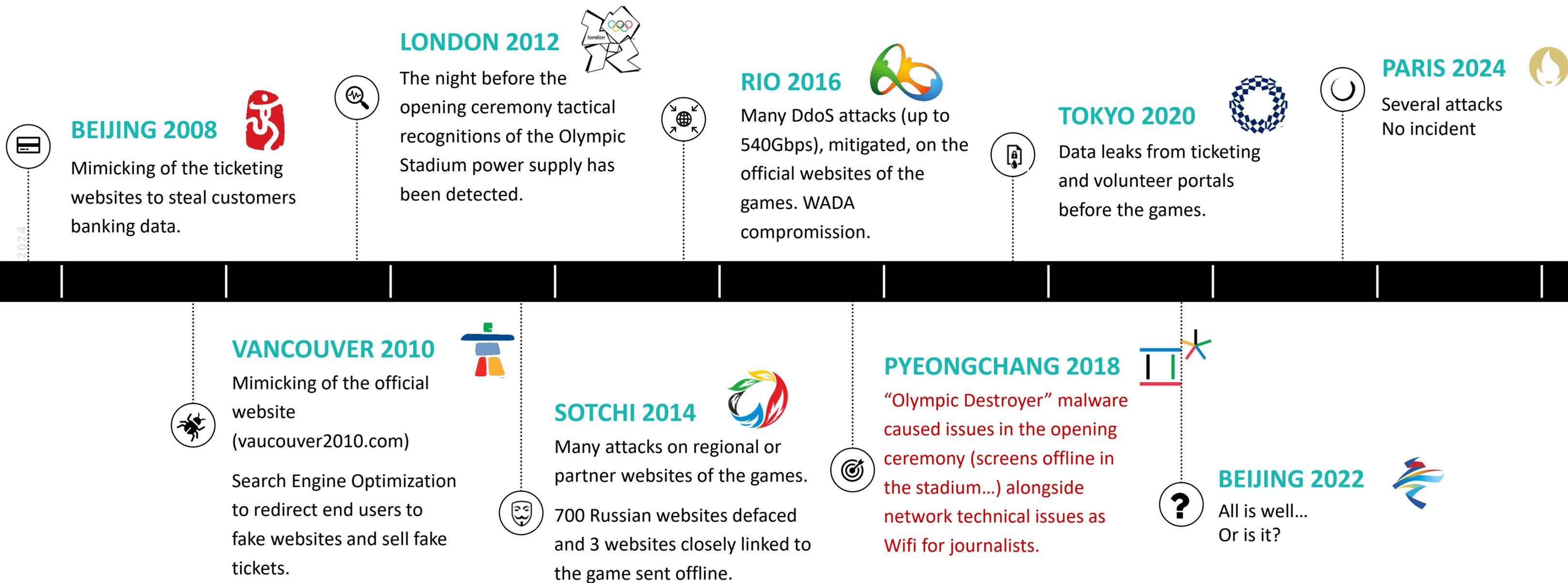
Etat Français



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

**Garantie du financement et de la sécurité des Jeux
Maintien de l'ordre et continuité des services publics**

LA MENACE CYBER SUR LES JEUX



MOTIVATIONS DES ATTAQUANTS

	Fun / Défi	Idéologie / Médiatisation	Espionnage	Profit	Revanche / Malveillance
Attaquants opportunistes	☠	☠		☠	☠
Hacktivistes		☠	☠		☠
Cyber mafias				☠	
Collaborateurs malveillants		☠			☠
Acteurs étatiques			☠		☠



LES ENJEUX DE CYBERSÉCURITÉ POUR PARIS 2024

Compétitions &
célébrations

Services

Technologies

Cybersécurité

- Broadcast
- Chronométrage & arbitrage
- Logistique
- Services aux délégations
- Services aux médias
- Télécommunications
- ...

- PC & mobiles
- Serveurs
- Réseaux
- Applications Web & mobile
- Services Cloud
- Objets connectés
- ...

- Atteinte à la sécurité des personnes
- Sabotage des opérations
- Atteinte à l'image et aux revenus

390.000+
Km de fibre optique

10.000+
PC

7.000+
Points d'accès réseau

200+
Applications

10.500 + 4.350

Athlètes

206

Nations représentées

350.000+

Heures de diffusion TV et plateformes

4 milliards

Télespectateurs

13,5 millions

Spectateurs

15 millions

Spectateurs du Relais de la Flamme Olympique

26.000+

Représentants accrédités des médias

100+

Experts, analystes, chefs de projet...

5%

Du budget TEC

2

Partenaires officiels

10+

Contributeurs majeurs

LES ENJEUX DE CYBERSÉCURITÉ POUR PARIS 2024

Atteinte à la sécurité des personnes

- PA : messages pirates
- Contrôle d'accès : intrusions sur les sites
- ...

Sabotage des opérations

- Connectivité : interruption des retransmissions ou de la couverture médiatique
- T&S : perturbation de l'arbitrage
- Logistique : reports ou annulations d'épreuves
- Anti-doping : triche
- Bureautique : ransomware sur les PC
- ...

Atteinte à l'image et aux revenus

- Connectivité : interruption des retransmissions
- Billetterie : fraude
- Réseaux sociaux : retrait de partenaire
- ...



LES ENJEUX DE CYBERSÉCURITÉ POUR PARIS 2024

Systemes Paris 2024

Atteinte à la sécurité des personnes

- PA : messages pirates
- Contrôle d'accès : intrusions sur les sites
- ...

Sabotage des opérations

- Connectivité : interruption des retransmissions ou de la couverture médiatique
- T&S : perturbation de l'arbitrage
- Logistique : reports ou annulations d'épreuves
- Anti-doping : triche
- Bureautique : ransomware sur les PC
- ...

Atteinte à l'image et aux revenus

- Connectivité : interruption des retransmissions
- Billetterie : fraude
- Réseaux sociaux : retrait de partenaire
- ...

Ecosystème des Jeux/Team France



CYBERSÉCURITÉ : LES CHIFFRES CLÉS

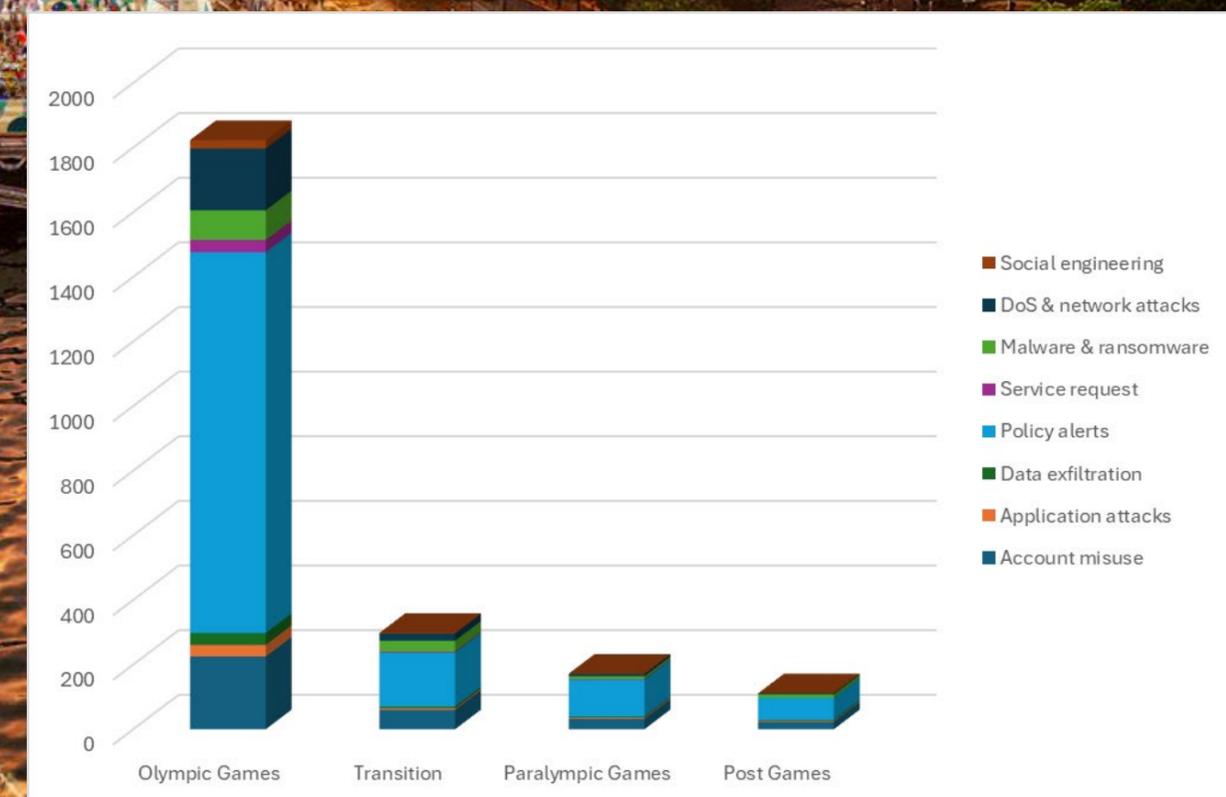
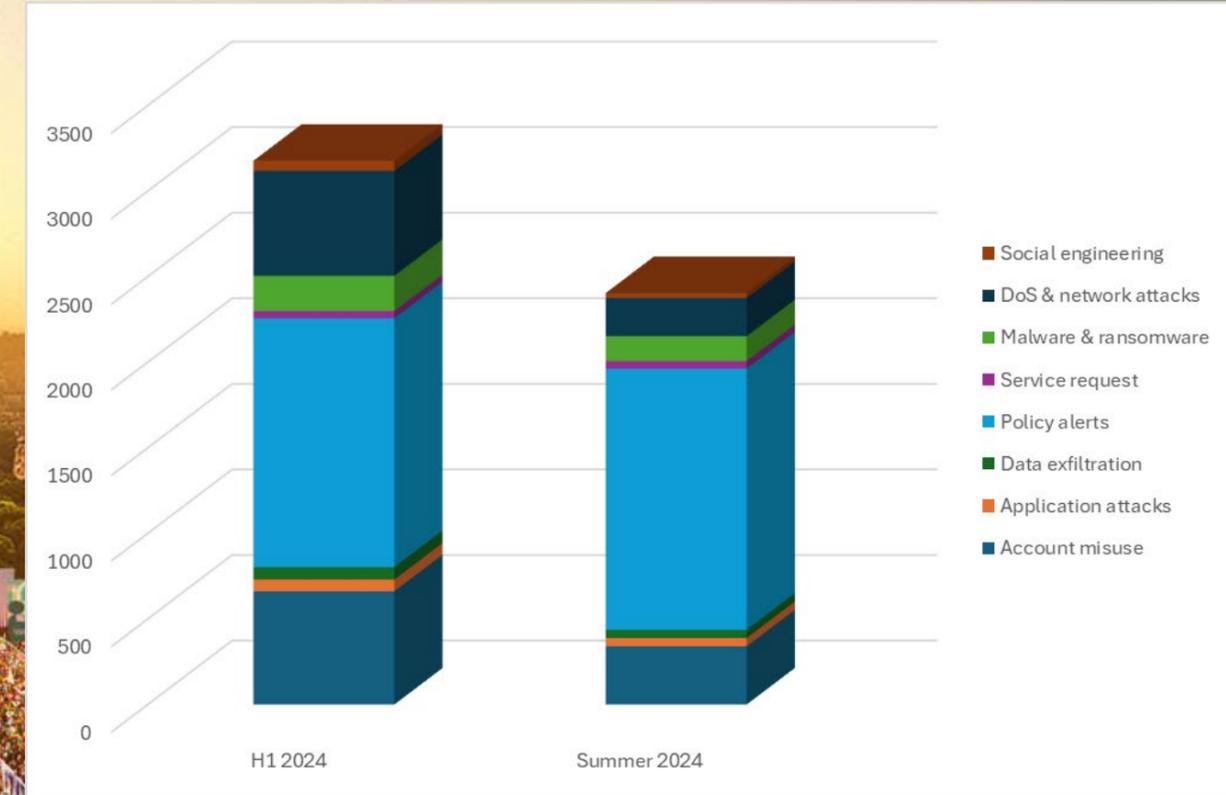
55 Milliards
Evènements de
cybersécurité (logs)

71 k
Alertes et
remédiations
automatisées

2200
Tickets
nécessitant
un traitement
humain

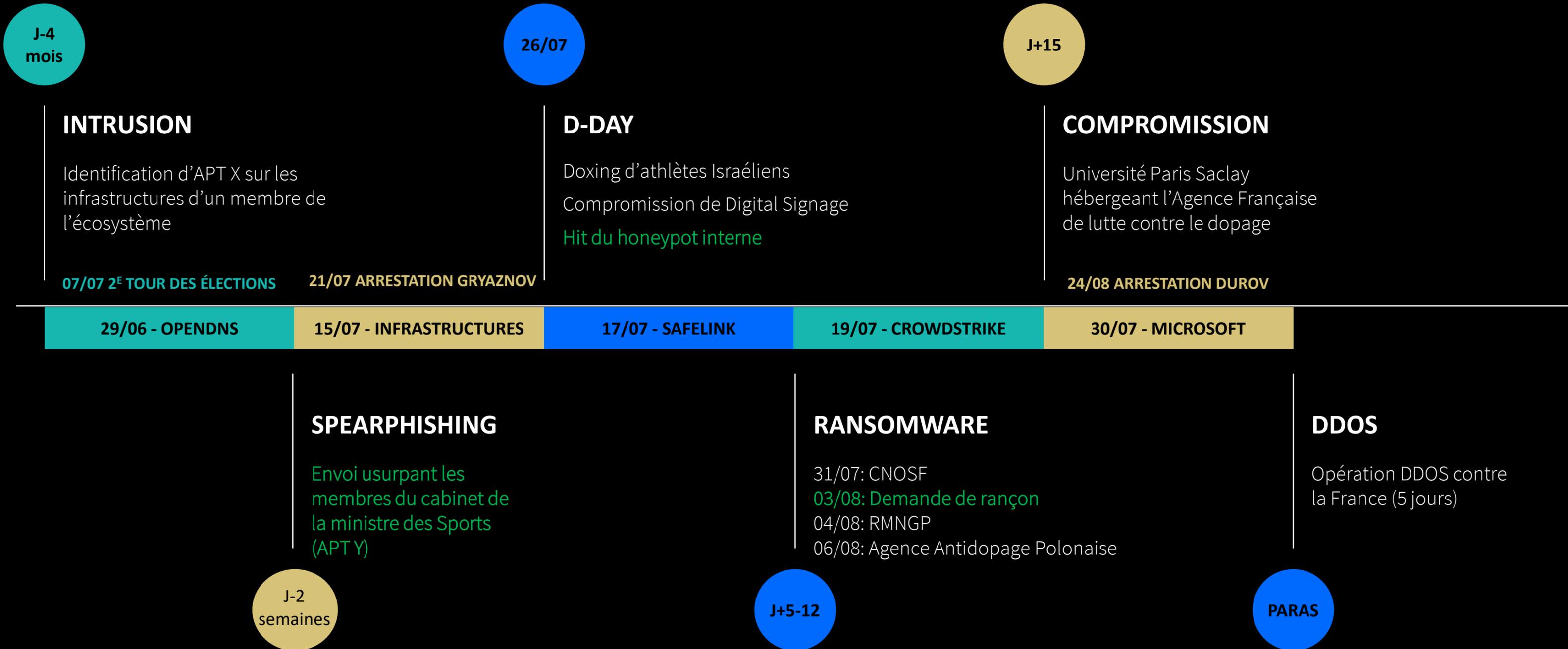
0
Incidents
affectant
les
opérations

Information	Volume
Number of technologies integrated into SIEM	46
Number of assets monitored by EDR	10 725
•Crowdstrike	4 832
•MS Defender for Endpoint	5 893
Number of monitored user accounts (MS Entra ID)	31 979
Average daily logins with user accounts (MS Entra ID)	167 337
Number of monitored user accounts (SAP Gigya)	8 747 364
Cisco XDR executed workflows	7 400
•Contain Asset (EDR)	97
•Reset user password	57
•Lost & Stolen device	35



DERRIÈRE LES CHIFFRES

PARIS2024





Evolution de la menace

1

Menaces cyber-physiques & opérations d'influence

2

Ingénierie sociale enrichie à l'IA

3

Attaques contre l'écosystème et la chaîne d'approvisionnement

Evolution de la défense

1

Mise en réseau du renseignement cyber

2

Remettre l'humain au cœur de la cyberdéfense

3

Défendre les TPE/PME

MERCI À TOUTE L'ÉQUIPE POUR CES JEUX SÛRS

- Marie-Dominique A.
- Romain A.
- Jessica B.
- Adèle B.
- Bahija B.
- Elio B.
- Filip B.
- Wojciech B.
- Paweł B.
- Marie-Caroline B.
- Nicolas B.
- Basile B.
- Olaf B.
- Przemyslaw B.
- Gabriel Daniel B.
- Jean-Thierry C.
- Charles C.
- Laurent C.
- Shailesh C.
- Zhen C.
- Krzysztof C.
- Katarzyna C.
- Hélène C.
- Jérémy C.
- Matei C.
- Rachel D.
- Geoffroy D.
- Michal D.
- Alice D.
- Nicolas D.
- Benoit D.
- Sébastien D.
- François D.
- Velizar D.
- Laure D.
- John Patrick E.
- Hamid E.
- Wenqing F.
- Joshua F.
- Maciej G.
- Wes G.
- Kinga G.
- Alexandre G.
- Damien G.
- Marcin G.
- Eric G.
- Julian G.
- Karolina G.
- Mehdi H.
- Jamie H.
- Kamila H.
- Esther H.
- Patrick H.
- Nicolas H.
- Yannick H.
- Steve H.
- Patrick H.
- Mark H.
- David H.
- Alexandre H.
- Antoan H.
- Tian H.
- Paul-Henri H.
- Ionut Cristian I.
- Amit J.
- Agnieszka J.
- Piotr J.
- Maciej J.
- Magdalena J.
- Patryk J.
- Tomica K.
- Gergana K.
- William K.
- Waldemar K.
- Magdalena K.
- Yuri K.
- Janusz K.
- Joanna K.
- Emeric L.
- Julien L.
- Bartosz L.
- Yang L.
- Marcin L.
- In-Ming L.
- Lukasz L.
- Xiaoxiao L.
- Ryan M.
- Nam M.
- Rik M.
- Julien M.
- Oscar M.
- Victor M.
- Julien M.
- Murtaza M.
- Bartosz M.
- Franek M.
- Willy M.
- Adrien M.
- Sergi M.
- Krzysztof N.
- Artur N.
- Audrey O.
- Jaroslaw O.
- Jean-François O.
- Soufiane O.
- Zakaria O.
- Manuela Roxana P.
- Szymon P.
- Daria P.
- Aleksander P.
- Sebastian P.
- Stephanie P.
- Dawid P.
- Joan Marc P.
- Patryk P.
- Julien P.
- Stéphane P.
- Franz R.
- Krzysztof R.
- Albert R.
- Emma R.
- Perla R.
- Francisco R.
- Michail S.
- Darryl S.
- Carly S.
- Jeanne S.
- Chamandeep S.
- Radoslaw S.
- Bartosz S.
- Krzysztof S.
- Alexander S.
- Octavian S.
- Vincent S.
- Arkadiusz S.
- Ewa S.
- Giorgi S.
- Hemant S.
- Justyna S.
- Pawel S.
- Marcin S.
- Marion T.
- Jean-Philippe T.
- Adrian T.
- Djamila T.
- Nigel T.
- Dimitri T.
- Giannis T.
- Stanislas V.
- Vara V.
- Piradi V.
- Juan Miguel V.
- Iza W.
- Bo W.
- Patryk W.
- Bartosz W.
- Krzysztof W.
- Matt W.
- Mateusz W.
- Arnaud W.
- Lyu X.
- Yi X.
- Shuren X.
- Dominique Y.
- Jingyi Y.
- Maciej Z.
- Mateusz Z.



AFG

LePointsur

Cybersécurité : Niveau de maturité des SGP

Questions-Réponses



Valentine Bonnet

Directrice Gouvernement
d'entreprise et Conformité,
en charge du GT cybersécurité
de l'AFG



Wilfried Lauber

Président du GT Cybersécurité
de l'AFG et RSSI adjoint
d'Amundi

Publications du GT cybersécurité AFG

disponibles sur le site AFG



PUBLICATION 2024

Fiche DORA pour les
SGP Microentreprise



AFG



LePointsur

Cybersécurité : Niveau de maturité des SGP

Rappel :



La vidéo de cette conférence, les slides et les documents cités seront disponibles prochainement sur le site de l'AFG



Ensemble,
s'investir pour demain

Merci !

