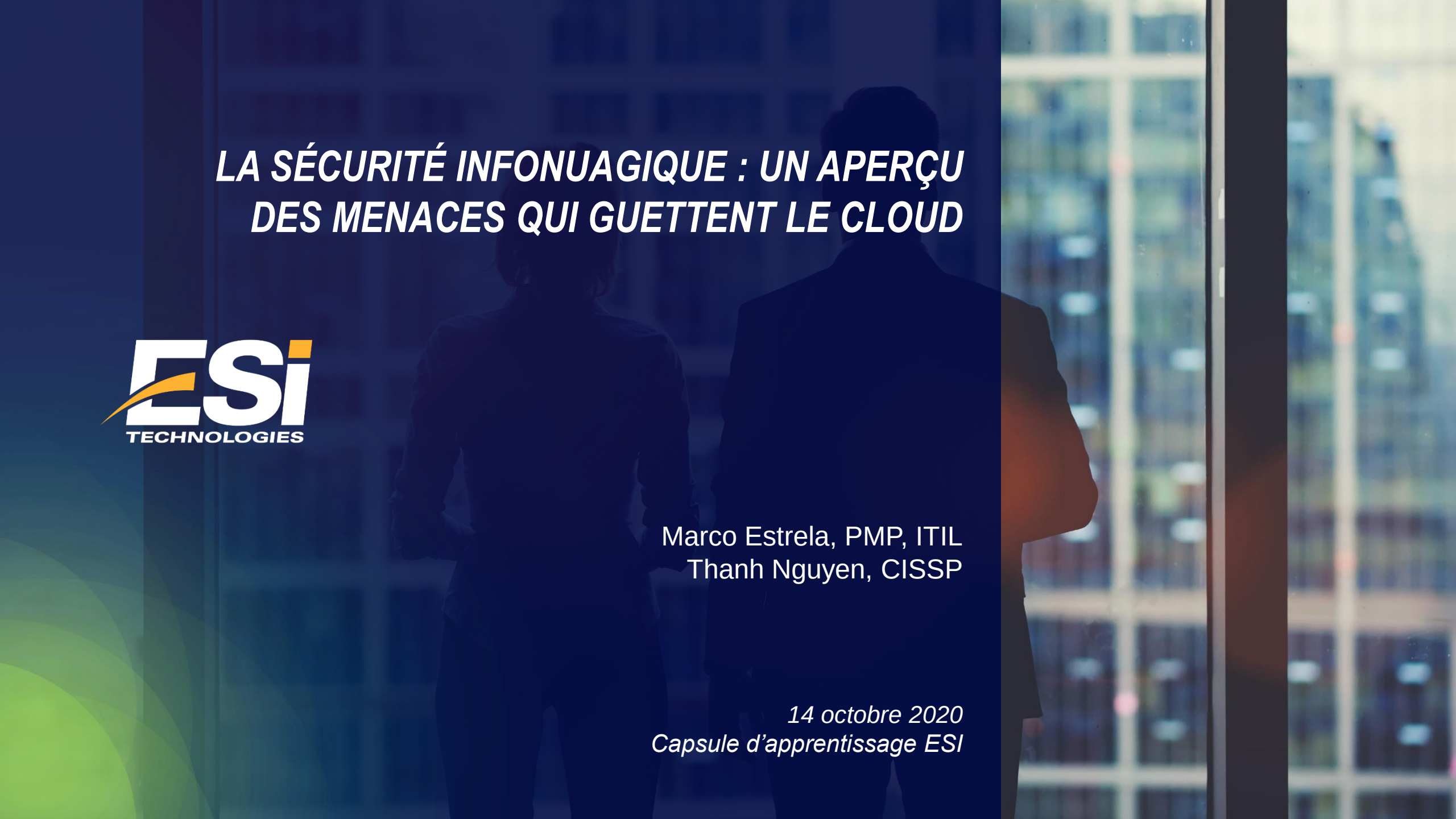
LA SÉCURITÉ INFONUAGIQUE : UN APERÇU DES MENACES QUI GUETTENT LE CLOUD



Marco Estrela, PMP, ITIL
Thanh Nguyen, CISSP

14 octobre 2020
Capsule d'apprentissage ESI

ORDRE DU JOUR

- Intro
- Coup d’œil sur le marché infonuagique
- Le cloud est-il sécuritaire?
- Comme le cloud est-il piraté?
- Démo
- Responsabilités *nuageuses*
- Solutions et pistes de réflexion

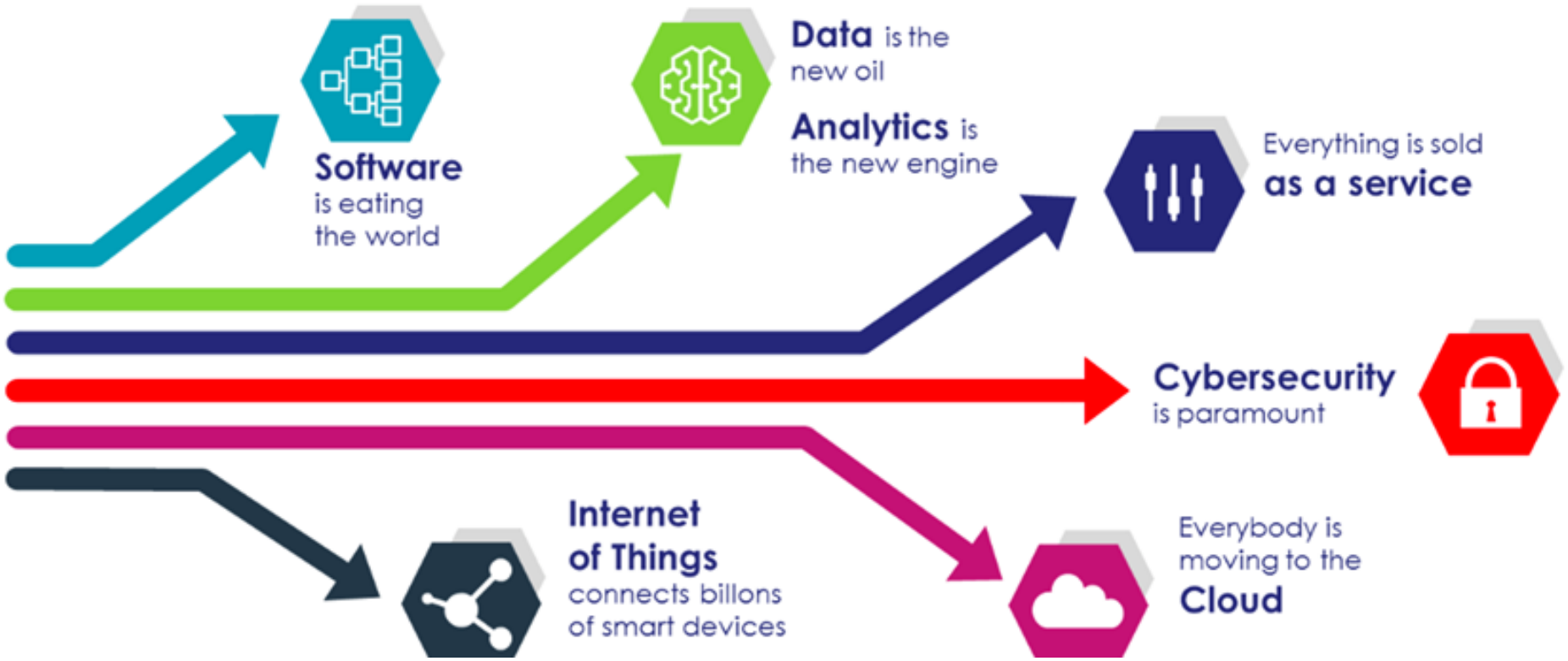
La mission d'ESI

GÉRER les données pour atteindre les objectifs d'affaires

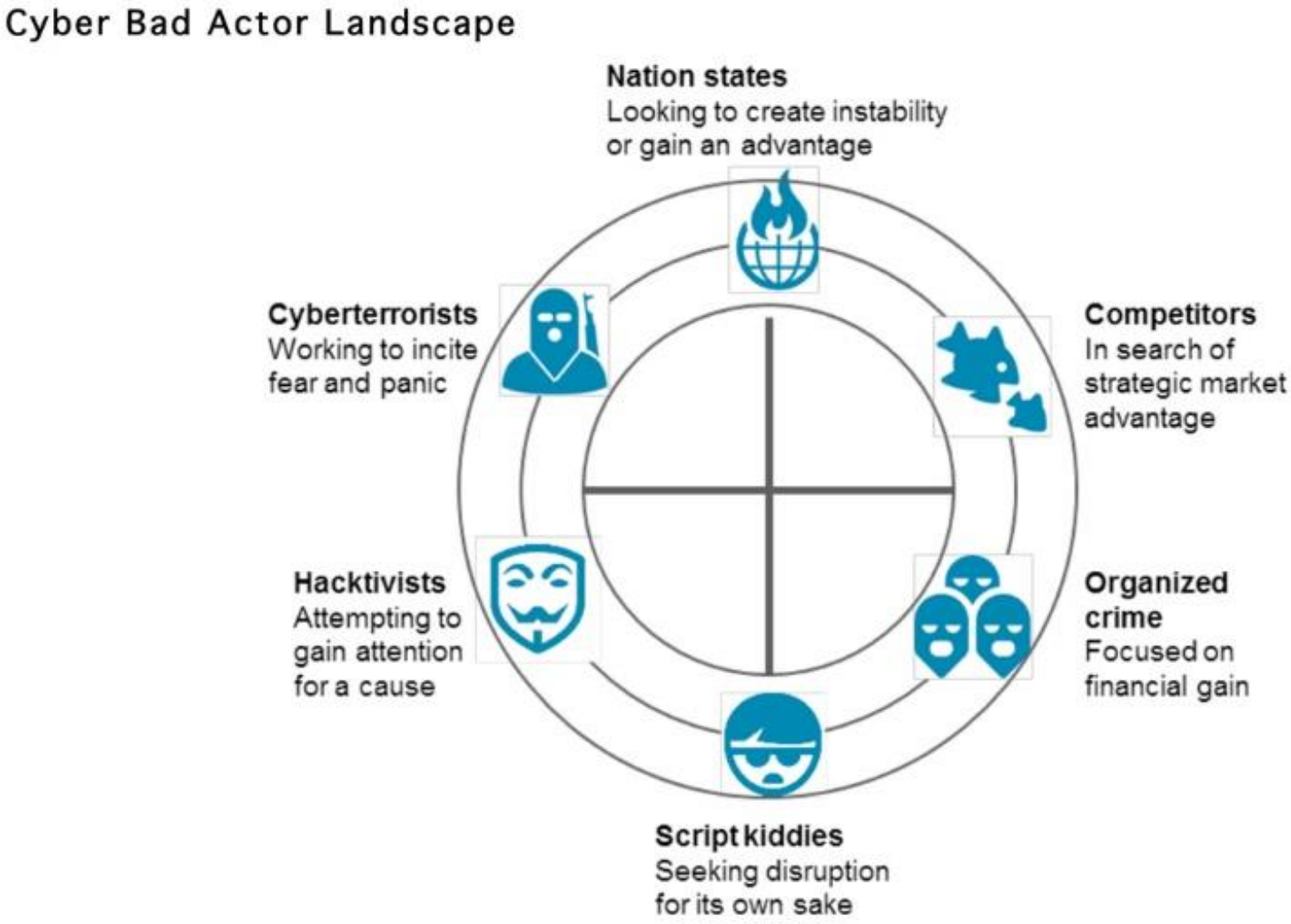
PROTÉGER les données en atténuant les risques

et **TRANSFORMER LES DONNÉES** en informations pertinentes

La cybersécurité est essentielle



Les acteurs de la cybercriminalité...



1

UN APERÇU DU MARCHÉ

LE CLOUD EST-IL GÉNÉRALEMENT ADOPTÉ?

→ Tous les joueurs majeurs investissent massivement et offre des services variés en infonuagique!

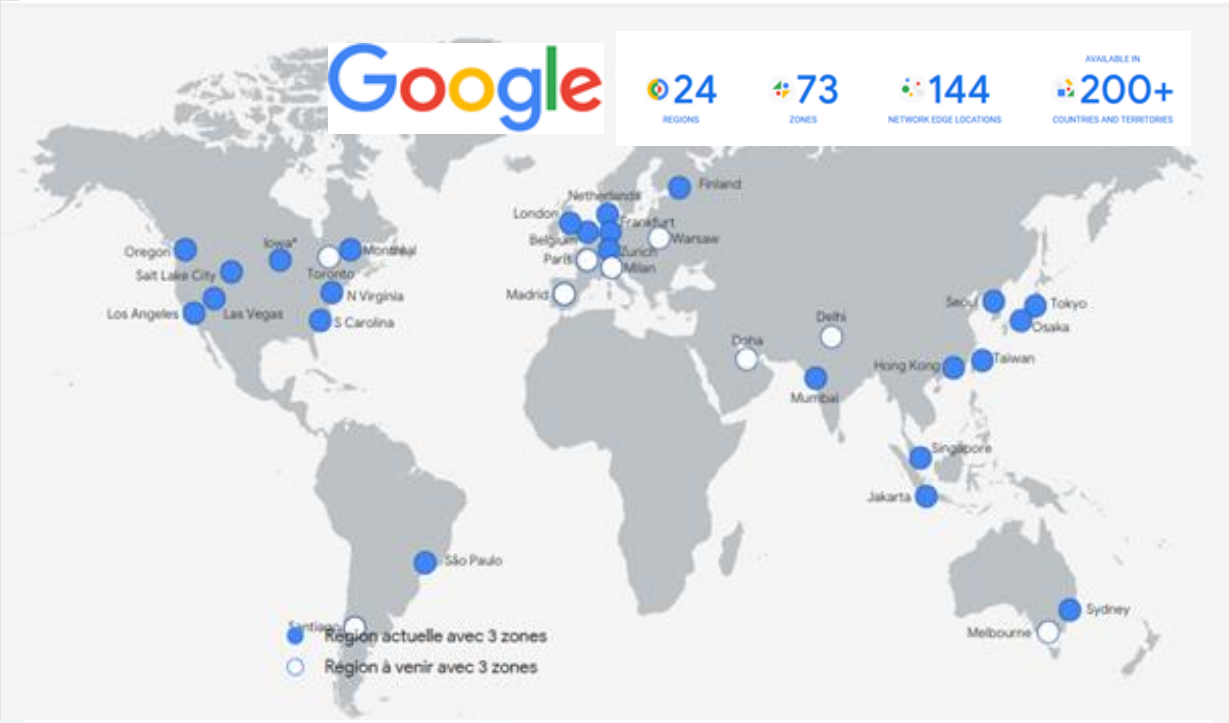
Azure

IBM Cloud

aws

Google Cloud

ESI TECHNOLOGIES



AWS now spans 77 Availability Zones within 24 geographic regions around the world

Deploy workloads in over 60 data centers and now into six regions and 18 availability zones globally.

Aujourd'hui :

191 CENTRES DE DONNÉES

Azure

Available region 30 DC

Announced region 7

Availability Zones

aws

AWS now spans 77 Availability Zones within 24 geographic regions around the world

IBM Cloud

Deploy workloads in over 60 data centers and now into six regions and 18 availability zones globally.

QU'EN PENSE GARTNER?

Figure 1. Magic Quadrant for Cloud Infrastructure and Platform Services

2

LE CLOUD EST-IL SÉCURITAIRE?

Quelques stats...

Le **gain financier** est le facteur de motivation le plus courant pour cibler les environnements cloud.

La force brute et l'exploitation d'environnements infonuagiques sont les 2 vecteurs d'infection représentant environ 45% de toutes les brèches.

Le **vol de données** – tel que l'appropriation d'informations nominatives – est l'activité préférée des cybercriminels une fois qu'ils ont pénétré un environnement infonuagique.

Les **mauvaises configurations** d'environnements cloud ont mené à plus d'un milliard de comptes compromis en 2019.

Le **rançongiciel** est le code malveillant le plus couramment déployé dans les environnements cloud compromis, représentant trois fois plus de cas que les malwares de *cryptomining* et de *botnets.*

Tirer parti des plateformes cloud pour les utiliser en tant qu'infrastructure malveillante est souvent un stratagème préféré des cybercriminels, leur permettant d'accélérer leurs opérations avec une seule compromission.

Source: Le rapport Cloud Threat Landscape d'IBM (2020)

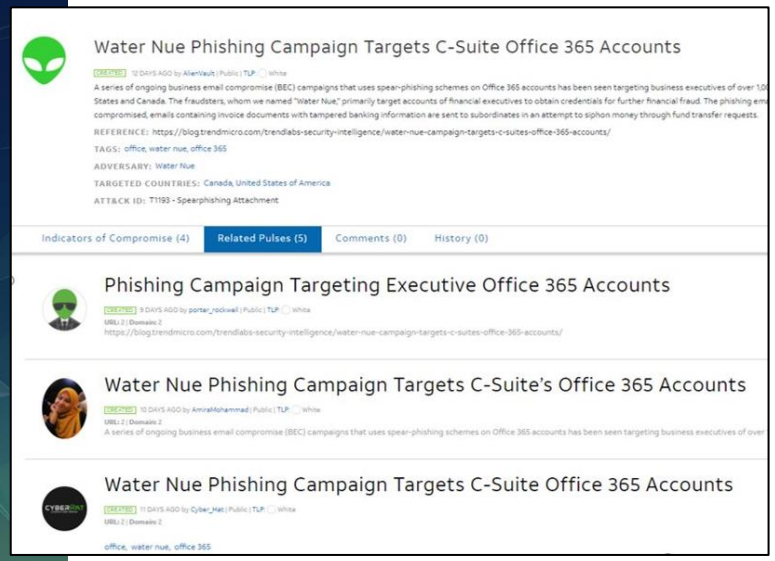
Les attaques sont quotidiennes...

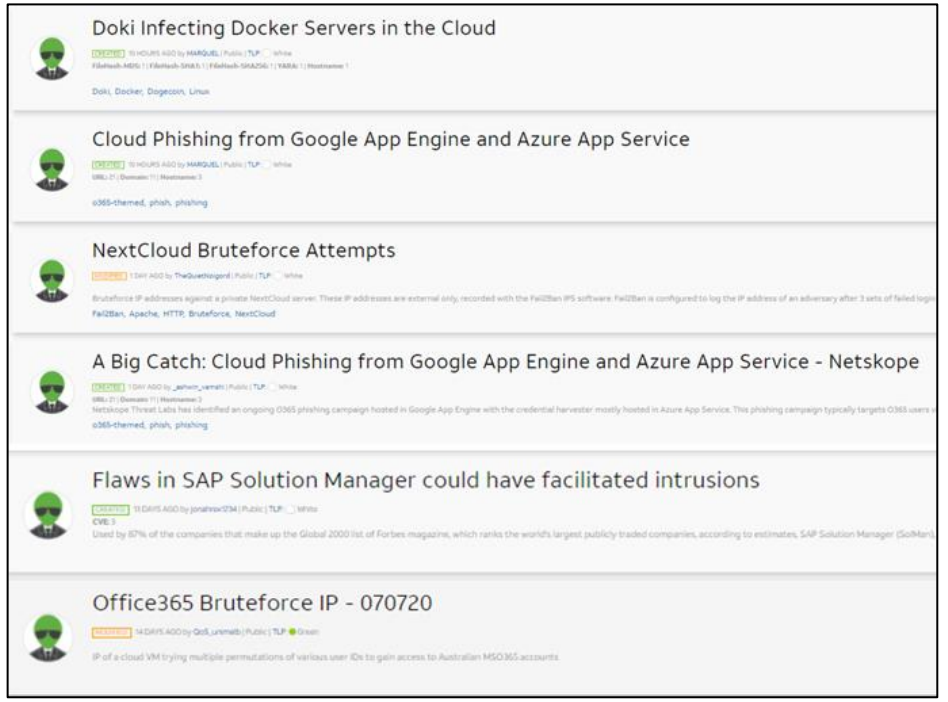
Author:
Tara Seals

September 10, 2020

A cloud misconfiguration at the gaming-gear merchant potentially exposed 100,000 customers to phishing and fraud.

An estimated 100,000 customers of Razer, a purveyor of high-end gaming gear ranging from laptops to apparel, have had their private info exposed, according to a researcher.





Les attaques ne visent pas que les grandes organisations

Figure 1: Exposure to Cloud Data Breaches

Q. Has your company experienced a cloud data breach in the past 18 months?

Percentage of respondents who answered "Yes"

INDUSTRY	Yes (%)
Manufacturing	58%
Banking	94%
Health	81%
Goverment	70%
Retail	71%

BUSINESS SIZE	Yes (%)
1,500 - 2,499	81%
2,500 - 4,999	89%
5,000 - 9,999	79%
10,000 - 19,999	71%
20,000 +	72%

Puisque les politiques d'accès doivent être fréquemment mises à jour, le potentiel d'erreur humaine augmente drastiquement. Plusieurs des brèches de sécurité cloud des dernières années ont été causées par des erreurs de configuration ou encore des permissions mal adaptées plutôt qu'en raison d'une mauvaise gestion du fournisseur (AWS/Azure etc.). Par exemple, la brèche de Capital One en 2019, où plus de 106 millions de numéros de cartes de crédit ont été compromis, a été le résultat d'une permission excessive assignée à un pare-feu d'application Web (WAF) qui a été facilement piraté pour atteindre le contenant S3 d'AWS où se trouvait l'information volée.

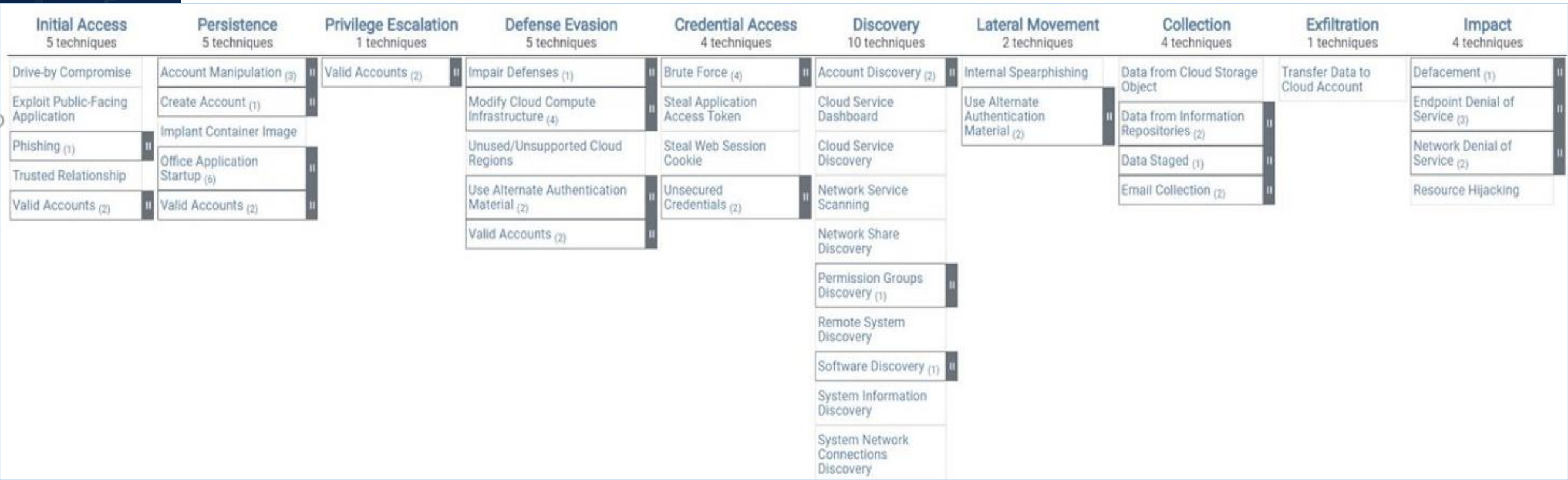
Source: IDC Cloud Security Survey Highlights – Top Identity and Data Access Risks (2020)

3

COMMENT LE CLOUD EST-IL PIRATÉ?

Qu'est-ce que le MITRE ATT&CK?

- Mitre est une organisation américaine basée au Massachusetts
- ATT&CK signifie : *Adversarial Tactics Techniques & Common Knowledge*
- Matrice cloud : Tactiques et attaques visant spécifiquement AWS, GCP, Azure, Azure AD, Office365, SaaS.



4

DÉMO

Démo # 1

- Détournement de navigateur (browser hijack)

Démo # 2

- Démarrage d’application Office (page d’accueil Outlook)

Démo # 3

→ Vol de jeton de demande d’accès (fausse demande)

Démo # 4

- Données provenant du stockage objet cloud (AWS S3 Bucket)

5

RESPONSABILITÉS *NUAGEUSES…*

La matrice des responsabilités partagées du cloud : qui fait quoi?

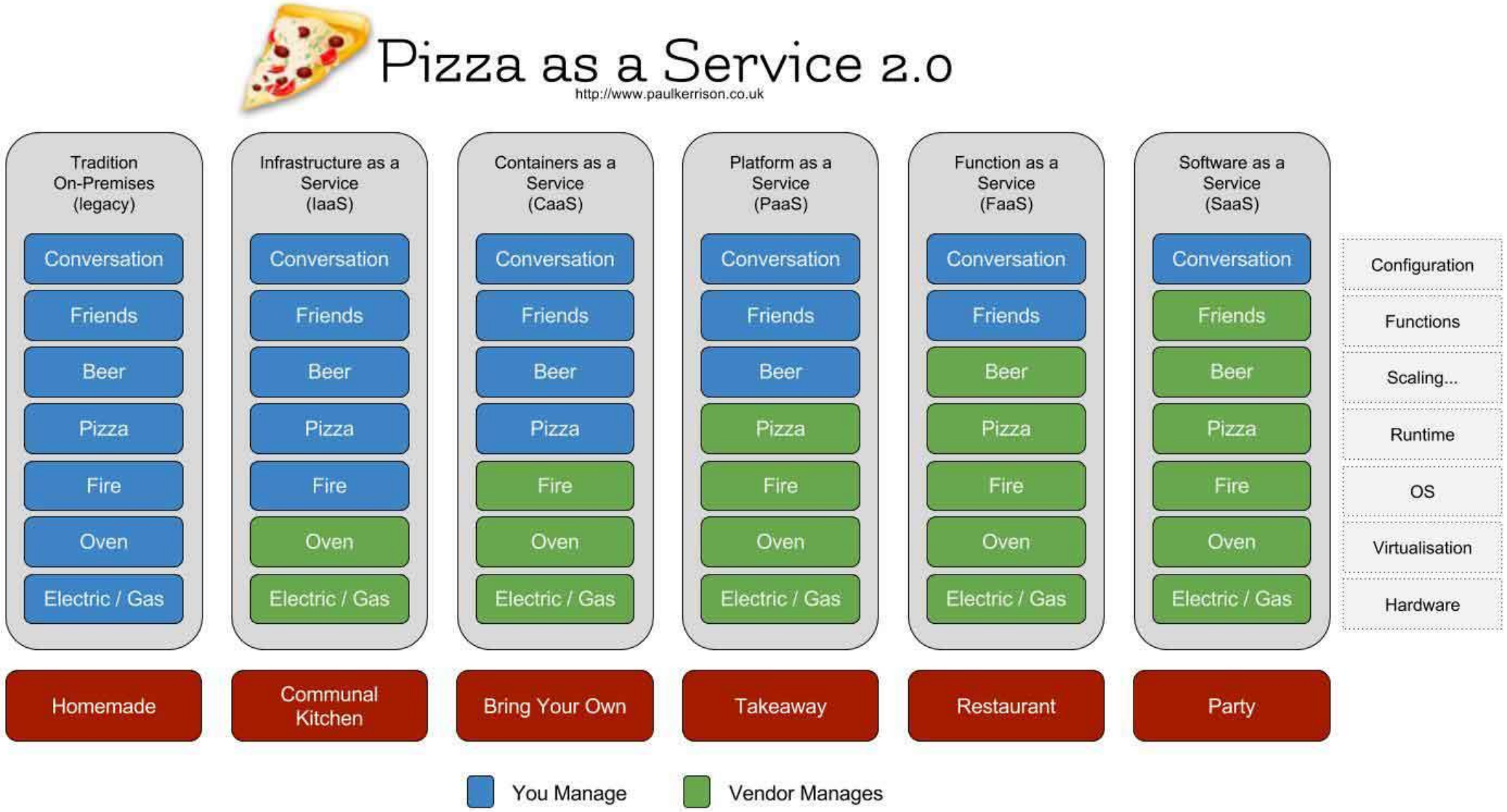
- Responsabilités partagées :
  - En 2017 Gartner estimait que 95% de la responsabilité reposait sur les épaules du client
  - En 2018, le RGPD affirmait que c'était presque 100%
- En définitive, la sécurité de vos données est VOTRE responsabilité!

Fournisseur de services infonuagiques	Client
Sécurité physique de l'infrastructure	Gestion de l'identité des utilisateurs et contrôle des accès aux systèmes de services
Sécurité du CPU, stockage et matériel réseau	Sécurité des données
Sécurité des réseaux de base, tels que les coupe-feu	Gestion de la sécurité et contrôle des terminaux qui accèdent aux services cloud, y compris le matériel, les logiciels, les systèmes d'application et les droits des appareils
Sécurité du stockage infonuagique, tel que les copies de sauvegarde et service de relève	Comportement des utilisateurs
Gestion de l'identité et contrôle des accès	Informations d'identification de l'organisation et des employés (mots de passe forts mais dans un stockage non sécurisé?)
Planification pour reprise après sinistre et continuité des affaires pour l'infrastructure	Les API de vos applications

Source: https://cloudsecurityalliance.org/blog/2019/09/05/how-to-share-the-security-responsibility-between-the-csp-and-customer/

ESI TECHNOLOGIES

Le partage des responsabilités : qui fait quoi?

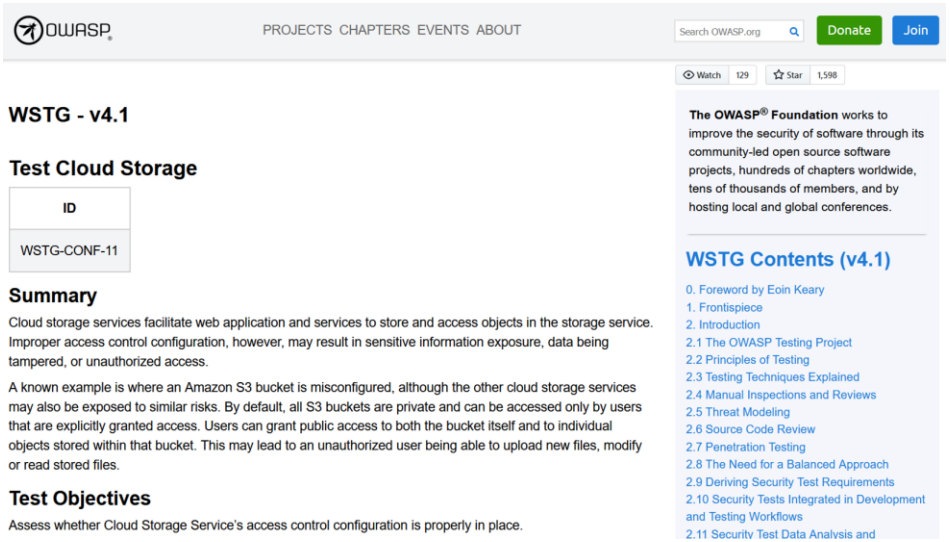


6

SOLUTIONS ET PISTES DE RÉFLEXION

TESTS RÉGULIERS

- Tests d’applications et sites Web
- OWASP 4.1 comprend maintenant une vérification de contrôles de sécurité dans le cloud
- Surveillance des actifs infonuagiques



OWASP PROJECTS CHAPTERS EVENTS ABOUT Search OWASP.org Donate Join

Watch 129 Star 1,598

WSTG - v4.1

Test Cloud Storage

ID
WSTG-CONF-11

Summary

Cloud storage services facilitate web application and services to store and access objects in the storage service. Improper access control configuration, however, may result in sensitive information exposure, data being tampered, or unauthorized access.

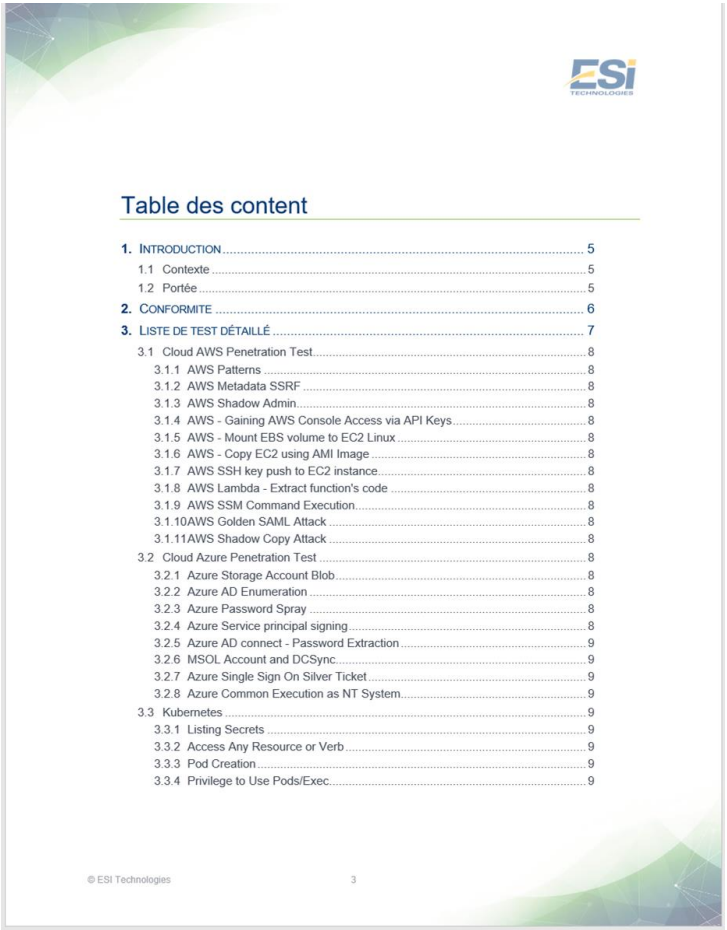
A known example is where an Amazon S3 bucket is misconfigured, although the other cloud storage services may also be exposed to similar risks. By default, all S3 buckets are private and can be accessed only by users that are explicitly granted access. Users can grant public access to both the bucket itself and to individual objects stored within that bucket. This may lead to an unauthorized user being able to upload new files, modify or read stored files.

Test Objectives

Assess whether Cloud Storage Service's access control configuration is properly in place.

The OWASP® Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.

WSTG Contents (v4.1)



ESI TECHNOLOGIES

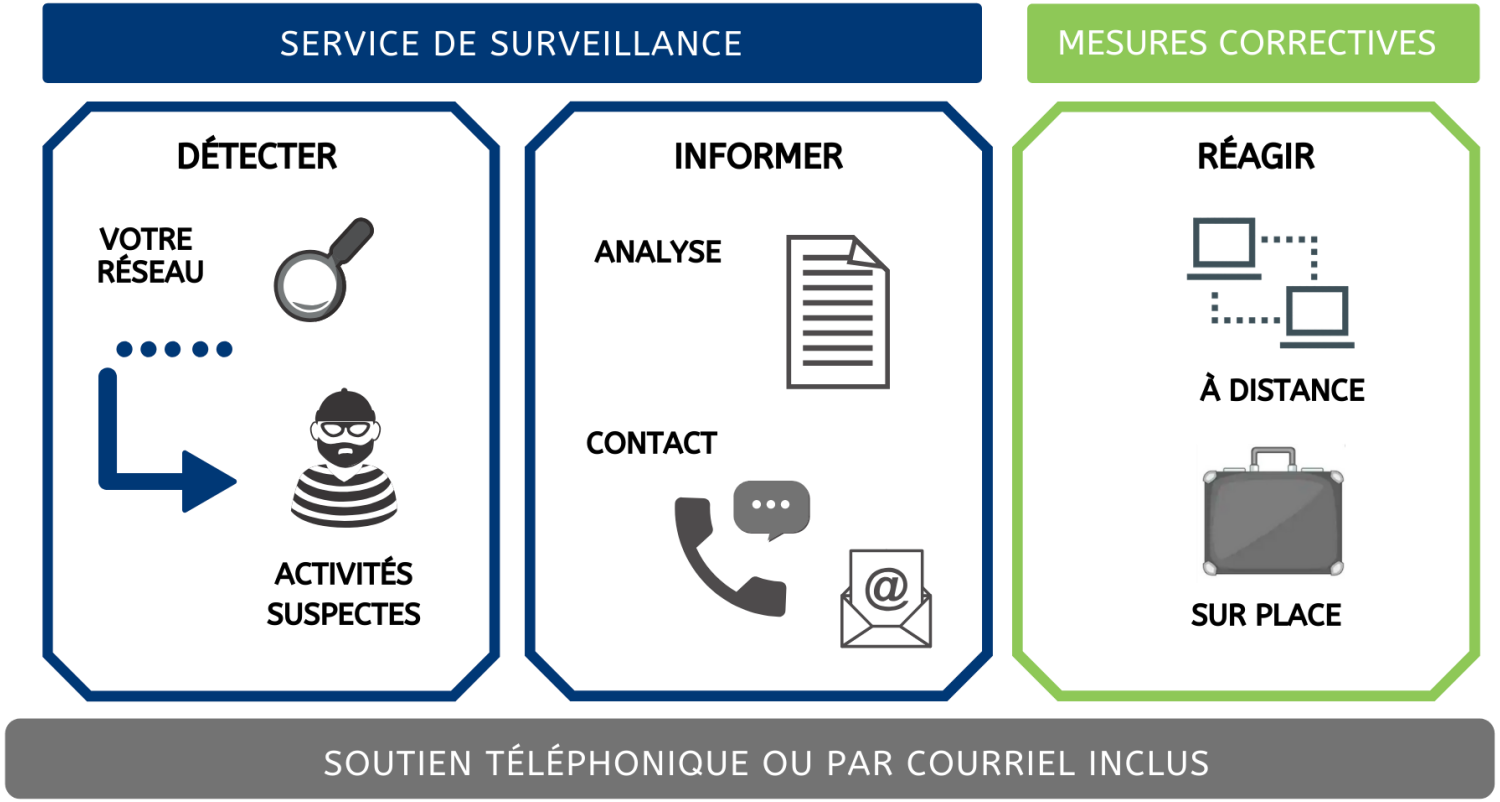
Table des content

OWASP Open Web Application Security Project

ESI TECHNOLOGIES

SURVEILLANCE DE VOS ACTIFS CLOUD POUR LES PROTÉGER

Services gérés : le SOC ESI

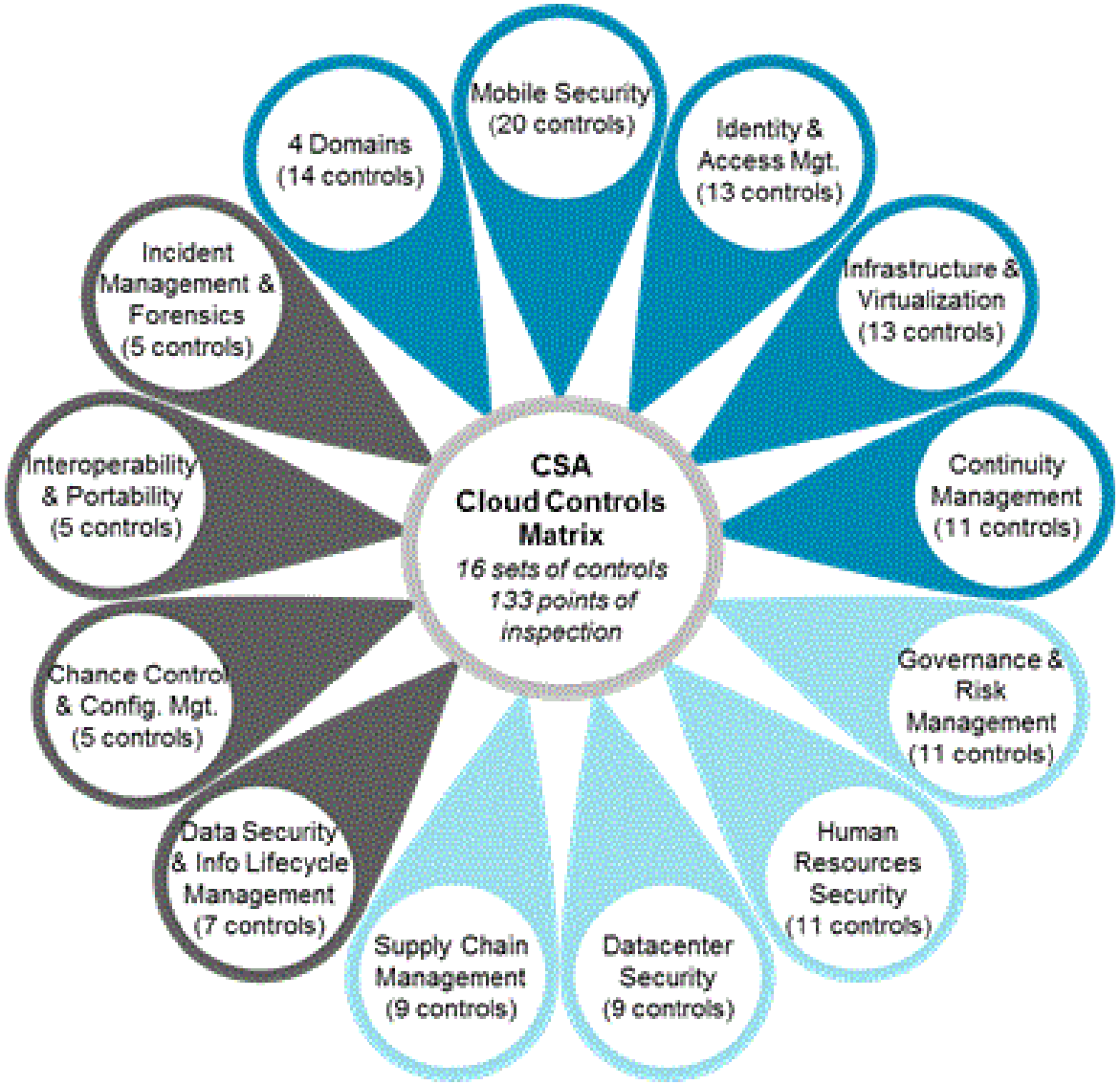


- → Sonde installée sur une VM dans l'infrastructure du client pour la collecte de données
- → Alertes analysées par des spécialistes en sécurité
- → Client informé par ESI de toute menace à la sécurité de son infrastructure
- → Aide à la mitigation des risques et correction des vulnérabilités

PLUS DE CONTRÔLES = PLUS DE RISQUES

CCM™
Cloud Controls Matrix

CSA Cloud Control Matrix



Source: Cloud Security Alliance

ESI TECHNOLOGIES

SI LES RISQUES SONT SI NOMBREUX, POURQUOI LES ORGANISATIONS VONT-ELLES VERS LE CLOUD?

→ **L'agilité de l'organisation** devient un objectif important

1. As the pandemic situation evolves and organizations move through the stages of recovery, their business focus will shift along with their technology investment priorities.
2. Technology plays a critical role in helping organizations maintain business resiliency through the downturn & recession, ultimately preparing for a return to growth & "the next normal" where digital capabilities will be vital to success.
3. Until COVID-19 is eradicated and/or a vaccine is widely available, we should expect waves of new COVID-19 infections and lockdowns. For many businesses this means they revert to an earlier stage, i.e., to recession, slow down or even crisis mode.
4. In this dynamic and uncertain environment, technology suppliers must adapt in order to meet their customers' needs at the corresponding stage. Some organizations may arrive in the next normal without experiencing any significant growth.

Source; IDC presentation 2020: Future of enterprise

ESI TECHNOLOGIES

CHERCHEZ-VOUS UNE SOLUTION CLOUD SÉCURITAIRE?

- ESI possède une équipe de migration pour vous aider à migrer votre organisation vers un environnement infonuagique sécuritaire
- Le cloud ESI est hébergé dans deux centres de données
- Le SOC ESI surveille cet environnement 24/7
- Des services professionnels connexes sont disponibles pour vous conseiller
- Vous cherchez à faire un premier pas vers le cloud? ESI vous offre :
  - BaaS
  - IaaS
  - PaaS

5 PISTES DE RÉFLEXION

1. Amazon, Microsoft, Google Cloud ne sont pas imprenables
2. Vous êtes ultimement responsable de la sécurité de vos actifs dans le cloud
3. Les tests Web doivent être effectués régulièrement
4. La surveillance est une bonne chose pour garder un œil sur vos actifs dans le cloud
5. ESI peut fournir des conseils pour garantir l'agilité de votre entreprise

ESI Technologies
Toronto – Montréal – Québec - ÉU

Thanh Nguyen, CISSP
Marco Estrela, PMP – 514 236-0056
Sans frais : 1 800 260-3311