

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

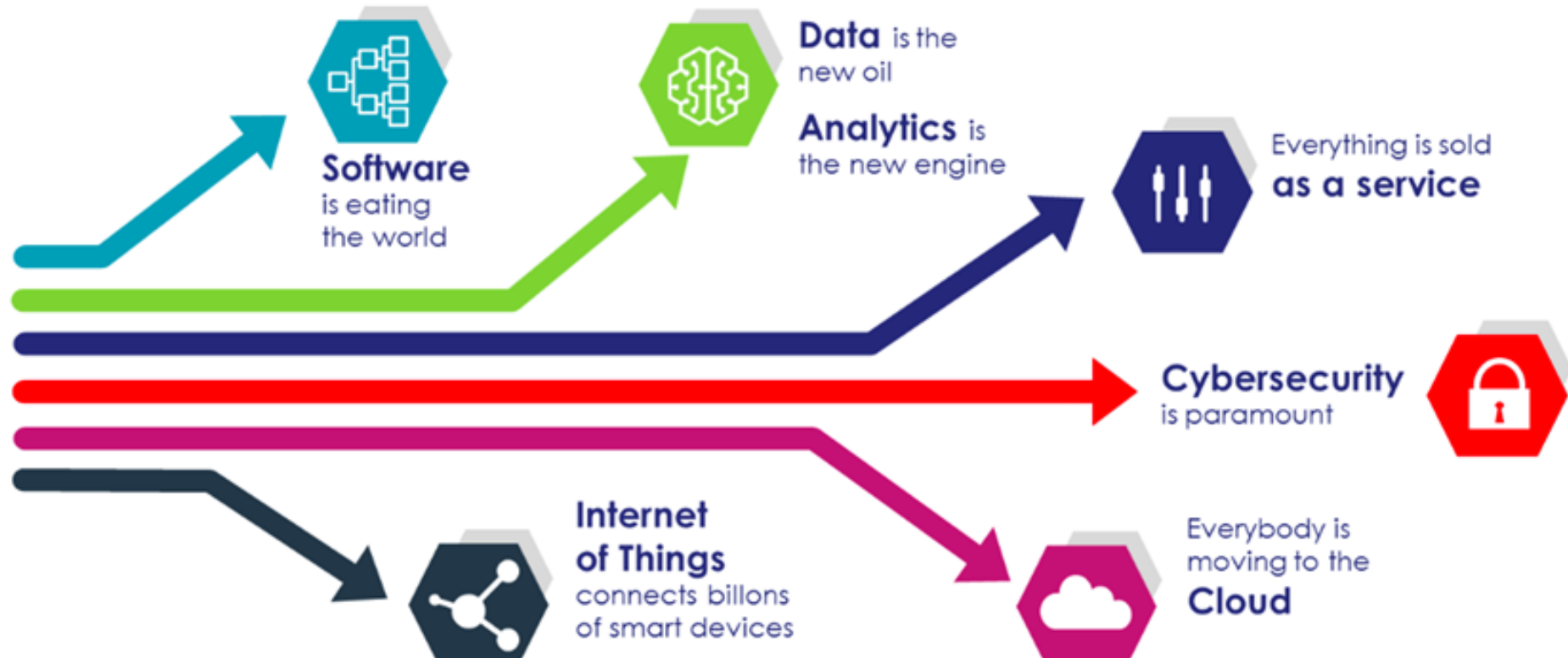


PROTÉGER les données en
atténuant les risques



et **TRANSFORMER LES
DONNÉES** en informations pertinentes

La cybersécurité est essentielle



Les acteurs de la cybercriminalité...

Cyber Bad Actor Landscape



1

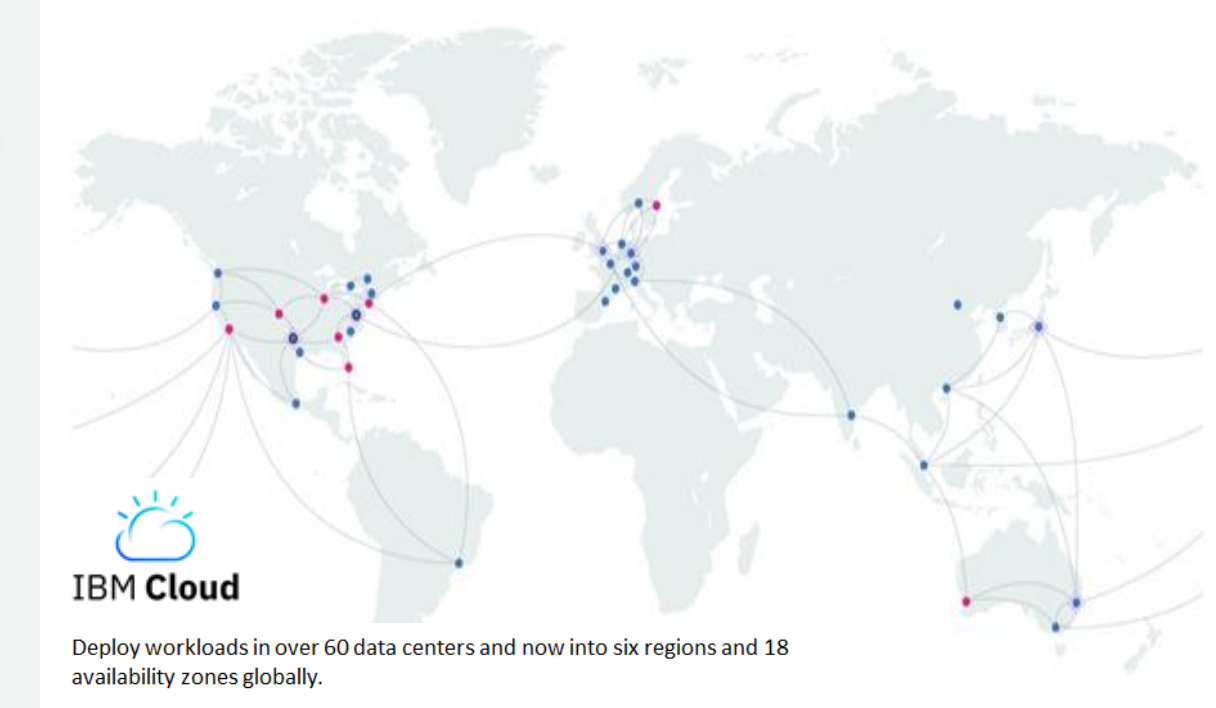
UN APERÇU DU MARCHÉ

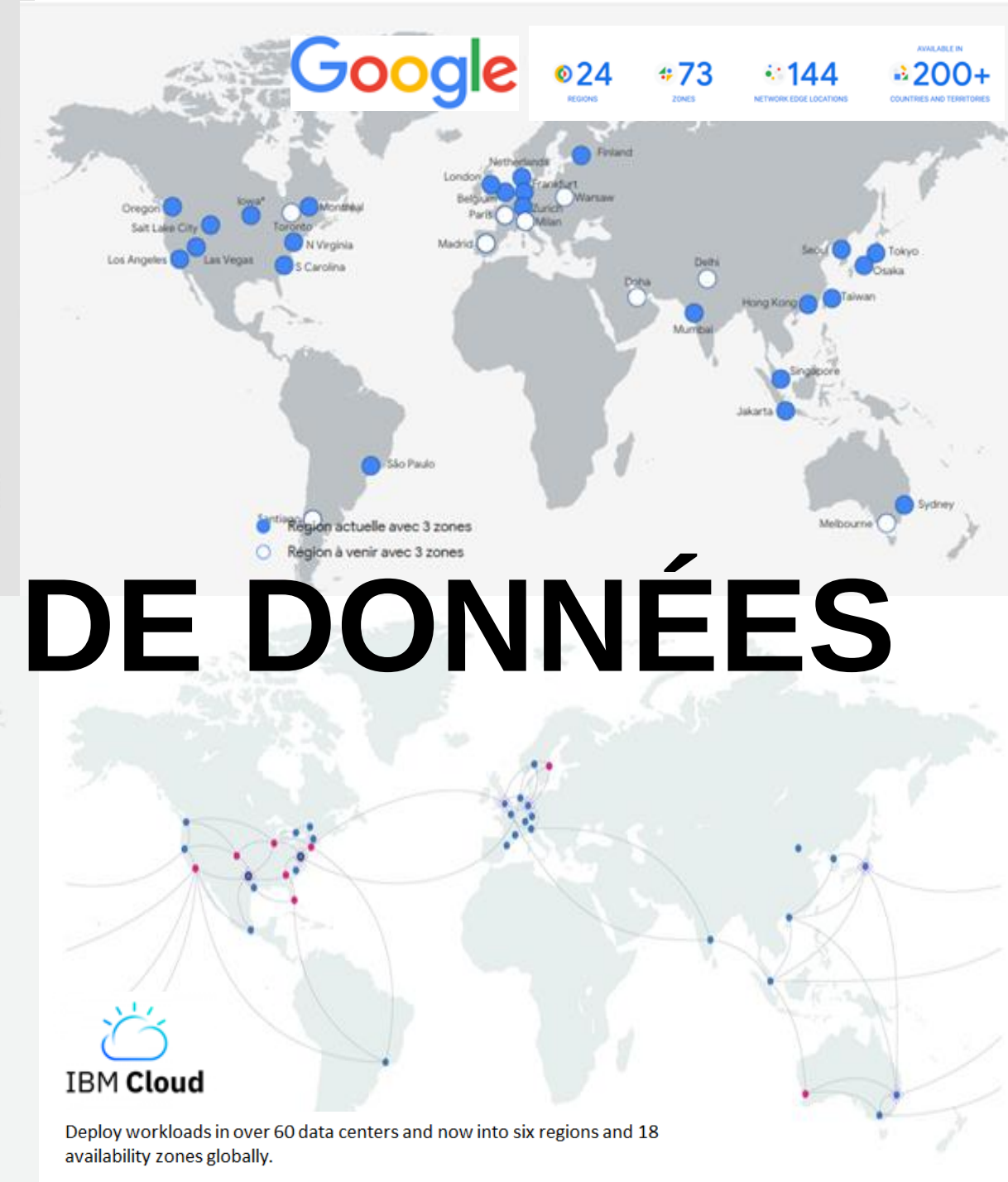


LE CLOUD EST-IL GÉNÉRALEMENT ADOPTÉ?

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







Aujourd'hui : 191 CENTRES DE DONNÉES

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.

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.



Water Nue Phishing Campaign Targets C-Suite Office 365 Accounts

DISCOVERED 10 DAYS AGO by [Asterhawk](#) (Public) | TLP: █ | [Write](#)
A series of ongoing business email compromise (BEC) campaigns that uses spear-phishing schemes on Office 365 accounts has been seen targeting business executives of over 100 States and Canada. The fraudsters, whom we named "Water Nue," primarily target accounts of financial executives to obtain credentials for further financial fraud. The phishing emails compromised, emails containing invoice documents with tampered banking information are sent to subordinates in an attempt to siphon money through fund transfer requests.
REFERENCE: <https://blog.trendmicro.com/trendlabs-security-intelligence/water-nue-campaign-targets-c-suites-office-365-accounts/>
TAGS: office, water nue, office 365
ADVERSARY: WATER Nue
TARGETED COUNTRIES: Canada, United States of America
ATT&CK ID: T1193 - Spearphishing Attachment

Indicators of Compromise (4) **Related Pulses (5)** Comments (0) History (0)



Phishing Campaign Targeting Executive Office 365 Accounts

DISCOVERED 9 DAYS AGO by [porter_redwall](#) (Public) | TLP: █ | [Write](#)
URLs (2) Domains (2)
<https://blog.trendmicro.com/trendlabs-security-intelligence/water-nue-campaign-targets-c-suites-office-365-accounts/>



Water Nue Phishing Campaign Targets C-Suite's Office 365 Accounts

DISCOVERED 10 DAYS AGO by [AmalMohammed](#) (Public) | TLP: █ | [Write](#)
URLs (2) Domains (2)
A series of ongoing business email compromise (BEC) campaigns that uses spear-phishing schemes on Office 365 accounts has been seen targeting business executives of over



Water Nue Phishing Campaign Targets C-Suite Office 365 Accounts

DISCOVERED 11 DAYS AGO by [CyberArk](#) (Public) | TLP: █ | [Write](#)
URLs (2) Domains (2)
office, water nue, office 365

Nearly 80% of Companies Experienced a Cloud Data Breach in Past 18 Months

June 5, 2020

KEYWORDS access management / cloud security / data breach / Identity Authentication / risk management

Ermetic, cloud access risk security company, **announced** the results of a research study conducted by global intelligence firm IDC which found that nearly 80% of the companies surveyed had experienced at least one cloud data breach in the past 18 months, and nearly half (43%) reported 10 or more breaches.

According to the 300 CISOs that participated in the survey, security misconfiguration (67%),



BUT SAAS APPLICATIONS ARE HACKED...



FORTUNE

Deloitte Gets Hacked: What We Know So Far

Office 365

INDEPENDENT

Parliament hit by cyber attack as hackers attempt to access MPs' email accounts

Office 365

Doki Infecting Docker Servers in the Cloud

DISCOVERED 10 HOURS AGO by [MARQUELL](#) (Public) | TLP: █ | [Write](#)
Filehash-ADS (1) Filehash-SHA512 (1) Filehash-SHA256 (1) YARA (1) Hostname (1)
Doki, Docker, Docker, Linux

Cloud Phishing from Google App Engine and Azure App Service

DISCOVERED 10 HOURS AGO by [MARQUELL](#) (Public) | TLP: █ | [Write](#)
URLs (2) Domains (1) Hostname (1)
o365-themed, phish, phishing

NextCloud Bruteforce Attempts

DISCOVERED 1 DAY AGO by [TheQuackLord](#) (Public) | TLP: █ | [Write](#)
Bruteforce IP addresses against a private NextCloud server. These IP addresses are external only, recorded with the Fail0verban IPS software. Fail0verban is configured to log the IP address of an adversary after 3 sets of failed login. Fail0verban, Apache, HTTP, BruteForce, NextCloud

A Big Catch: Cloud Phishing from Google App Engine and Azure App Service - Netskope

DISCOVERED 1 DAY AGO by [james_james](#) (Public) | TLP: █ | [Write](#)
URLs (1) Domains (1) Hostname (1)
Netskope Threat Labs has identified an ongoing O365 phishing campaign hosted in Google App Engine with the credential harvester mostly hosted in Azure App Service. This phishing campaign typically targets O365 users in o365-themed, phish, phishing

Flaws in SAP Solution Manager could have facilitated intrusions

DISCOVERED 10 DAYS AGO by [joshua234](#) (Public) | TLP: █ | [Write](#)
CVE-3
Used by 80% of the companies that make up the Global 2000 list of Forbes magazine, which ranks the world's largest publicly traded companies, according to estimates, SAP Solution Manager (SolMan)

Office365 Bruteforce IP - 070720

DISCOVERED 14 DAYS AGO by [QoS_Lunatic](#) (Public) | TLP: █ | [Write](#)
IP of a cloud VM trying multiple permutations of various user IDs to gain access to Australian MSO365 accounts

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 (%)	BUSINESS SIZE		Yes (%)
	Manufacturing	58%	 1,500 - 2,499		81%
	Banking	94%	 2,500 - 4,999		89%
	Health	81%	 5,000 - 9,999		79%
	Government	70%	 10,000 - 19,999		71%
	Retail	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.

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**.

Initial Access 5 techniques	Persistence 5 techniques	Privilege Escalation 1 techniques	Defense Evasion 5 techniques	Credential Access 4 techniques	Discovery 10 techniques	Lateral Movement 2 techniques	Collection 4 techniques	Exfiltration 1 techniques	Impact 4 techniques
Drive-by Compromise	Account Manipulation (3)	Valid Accounts (2)	Impair Defenses (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Data from Cloud Storage Object	Transfer Data to Cloud Account	Defacement (1)
Exploit Public-Facing Application	Create Account (1)		Modify Cloud Compute Infrastructure (4)	Steal Application Access Token	Cloud Service Dashboard	Use Alternate Authentication Material (2)	Data from Information Repositories (2)		Endpoint Denial of Service (3)
Phishing (1)	Implant Container Image		Unused/Unsupported Cloud Regions	Steal Web Session Cookie	Cloud Service Discovery		Data Staged (1)		Network Denial of Service (2)
Trusted Relationship	Office Application Startup (6)		Use Alternate Authentication Material (2)	Unsecured Credentials (2)	Network Service Scanning		Email Collection (2)		Resource Hijacking
Valid Accounts (2)	Valid Accounts (2)		Valid Accounts (2)		Network Share Discovery				
					Permission Groups Discovery (1)				
					Remote System Discovery				
					Software Discovery (1)				
					System Information Discovery				
					System Network Connections Discovery				

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!

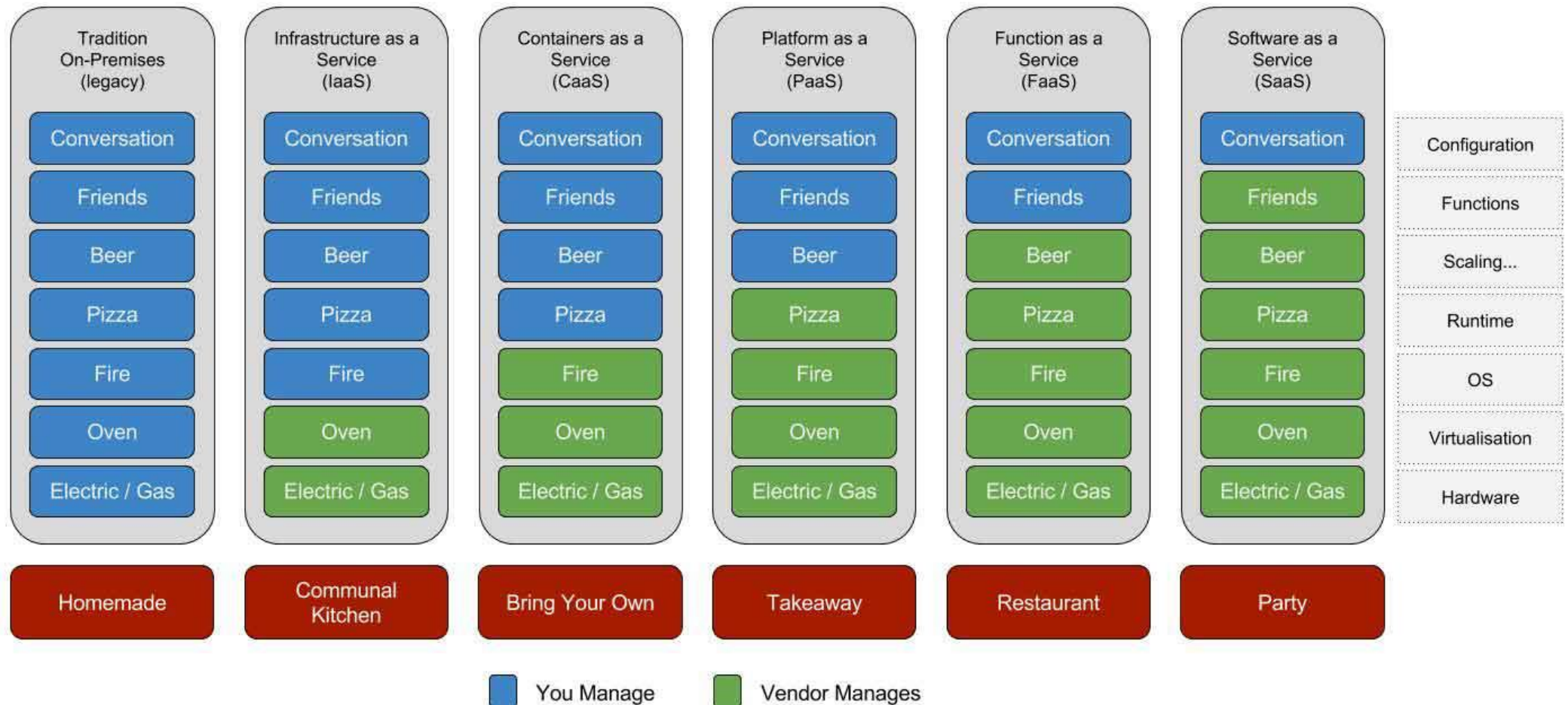
Fournisseur de services infonuagiques	Client
Sécurité physique de l'infrastructure	Gestion de l'identité des utilisateurs et contrôle des accès aux systèmes de services
Sécurité du CPU, stockage et matériel réseau	Sécurité des données
Sécurité des réseaux de base, tels que les coupe-feu	Gestion de la 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 relèvement	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

Le partage des responsabilités : qui fait quoi?



Pizza as a Service 2.0

<http://www.paulkerrison.co.uk>



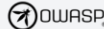
6

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)

- 0. Foreword by Eoin Keary
- 1. Frontispiece
- 2. Introduction
 - 2.1 The OWASP Testing Project
 - 2.2 Principles of Testing
 - 2.3 Testing Techniques Explained
 - 2.4 Manual Inspections and Reviews
 - 2.5 Threat Modeling
 - 2.6 Source Code Review
 - 2.7 Penetration Testing
 - 2.8 The Need for a Balanced Approach
 - 2.9 Deriving Security Test Requirements
 - 2.10 Security Tests Integrated in Development and Testing Workflows
 - 2.11 Security Test Data Analysis and

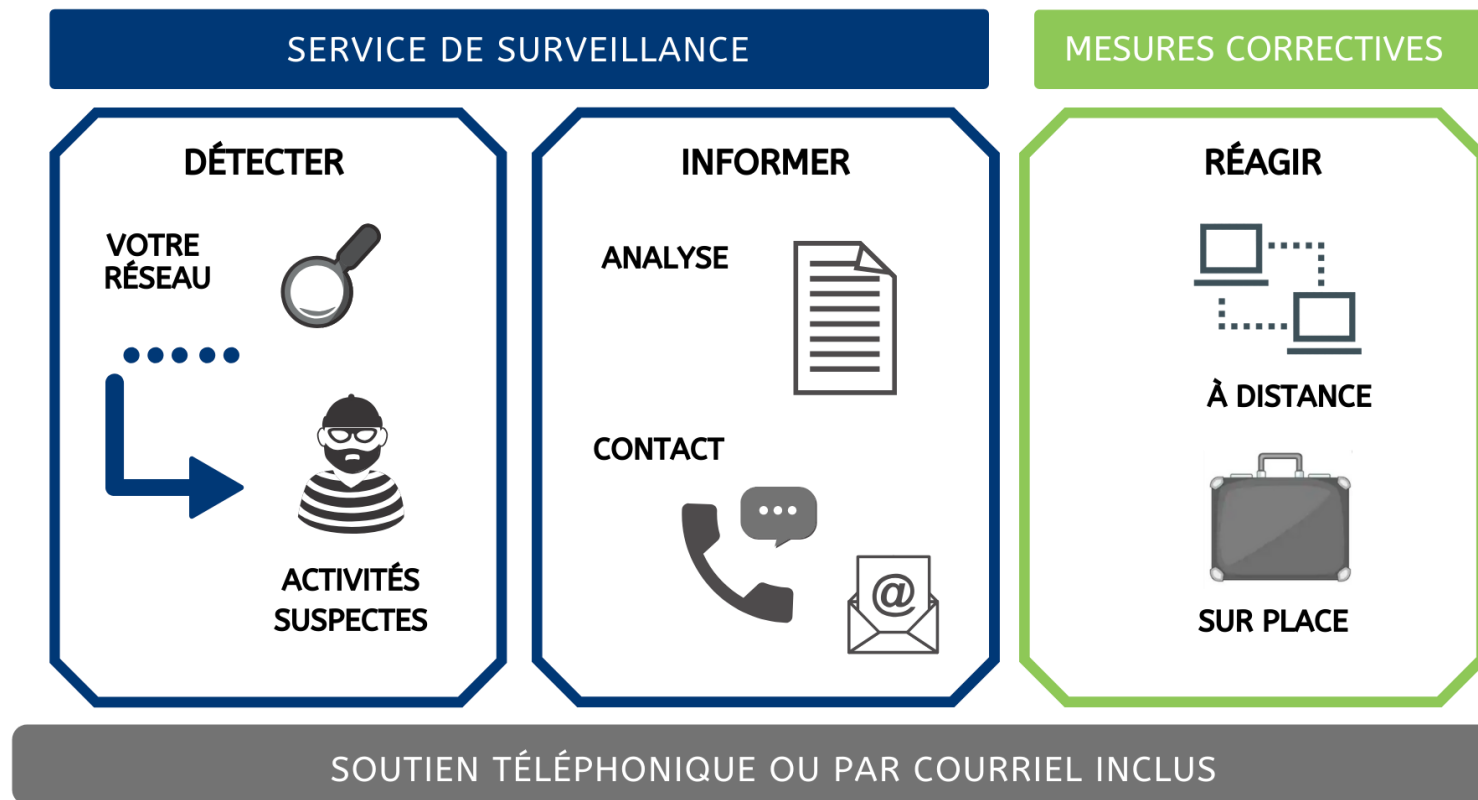
Table des content

1. INTRODUCTION	5
1.1 Contexte	5
1.2 Portée	5
2. CONFORMITE	6
3. LISTE DE TEST DÉTAILLÉ	7
3.1 Cloud AWS Penetration Test	8
3.1.1 AWS Patterns	8
3.1.2 AWS Metadata SSRF	8
3.1.3 AWS Shadow Admin	8
3.1.4 AWS - Gaining AWS Console Access via API Keys	8
3.1.5 AWS - Mount EBS volume to EC2 Linux	8
3.1.6 AWS - Copy EC2 using AMI Image	8
3.1.7 AWS SSH key push to EC2 instance	8
3.1.8 AWS Lambda - Extract function's code	8
3.1.9 AWS SSM Command Execution	8
3.1.10 AWS Golden SAML Attack	8
3.1.11 AWS Shadow Copy Attack	8
3.2 Cloud Azure Penetration Test	8
3.2.1 Azure Storage Account Blob	8
3.2.2 Azure AD Enumeration	8
3.2.3 Azure Password Spray	8
3.2.4 Azure Service principal signing	8
3.2.5 Azure AD connect - Password Extraction	9
3.2.6 MSOL Account and DCSync	9
3.2.7 Azure Single Sign On Silver Ticket	9
3.2.8 Azure Common Execution as NT System	9
3.3 Kubernetes	9
3.3.1 Listing Secrets	9
3.3.2 Access Any Resource or Verb	9
3.3.3 Pod Creation	9
3.3.4 Privilege to Use Pods/Exec	9



SURVEILLANCE DE VOS ACTIFS CLOUD POUR LES PROTÉGER

Services gérés : le SOC ESI

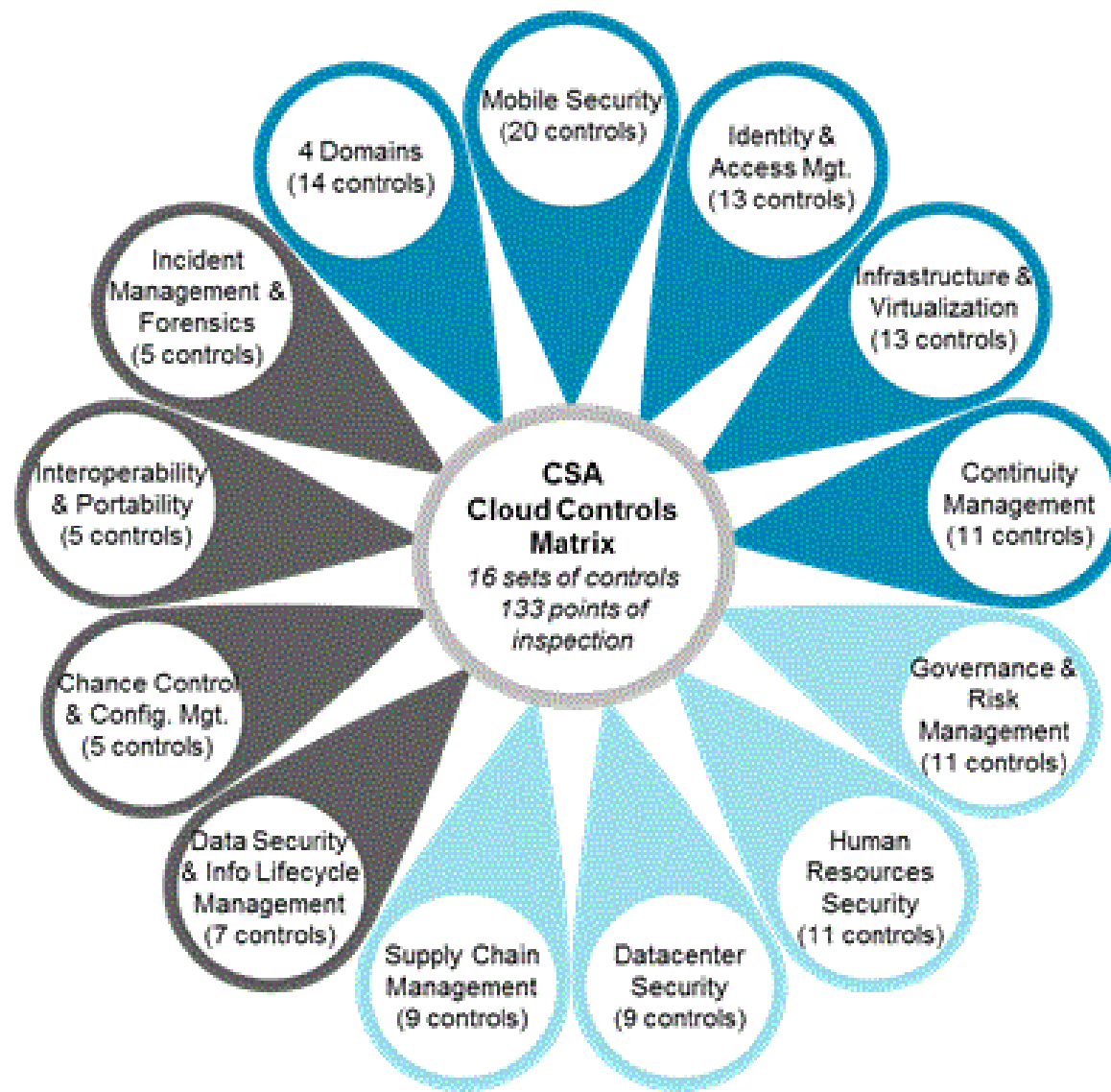


- Sonde installée sur une VM dans l'infrastructure du client pour la collecte de données
- Alertes analysées par des spécialistes en sécurité
- Client informé par ESI de toute menace à la sécurité de son infrastructure
- Aide à la mitigation des risques et correction des vulnérabilités

PLUS DE
CONTRÔLES =
PLUS DE RISQUES

CCMTM
Cloud Controls Matrix

CSA Cloud Control Matrix



Source: Cloud Security Alliance

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.

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