

Sécurité dans les environnements infonuagiques

Module 1 : Introduction à l'infonuagique (Partie 2)

Armstrong Foundjem, Ph.D

Polytechnique Montréal

Automne 2022

Plan du module

- ① Actualités: cyberattaques sur le cloud
- ② Risques de sécurité liés au cloud
- ③ Propriétés de sécurité: Triade CIA

1 Actualités

2 Risques de sécurité

3 Propriétés de sécurité

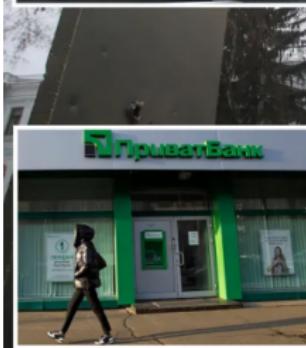
Actualités

- **VIASAT attack:** La Russie déconnecte des milliers d'Ukrainiens d'Internet en exploitant les failles des communications satellites (NYT 2022)



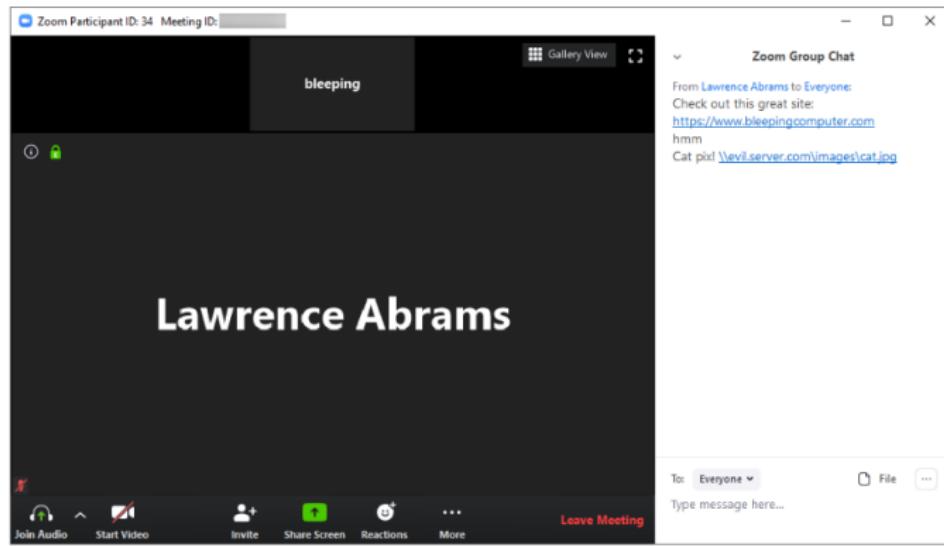
Actualités

- La Russie cause l'arrêt des sites du gouvernement Ukrainien (défense, armée) et deux grandes banques Ukrainiennes: PrivatBank et Oschadbank (NYP 2022)



Actualités

- Des pirates usurpent Zoom afin de voler les accès aux comptes Microsoft en imitant le message d'invitation aux réunions Zoom (BleepingComputer, 2021).



Sondage ☺: <https://app.wooclap.com/events/QHDXRL>.

wooclap

1 Actualités

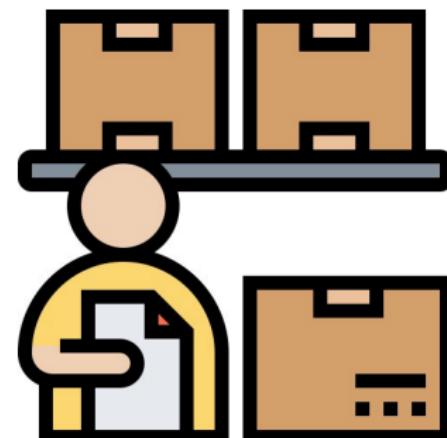
2 Risques de sécurité

3 Propriétés de sécurité

Actifs dans le cloud

• Actifs de données

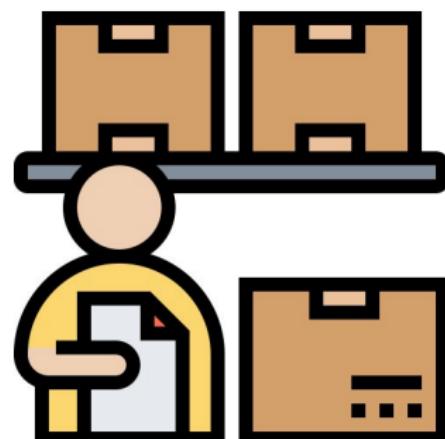
- identifiants d'accès
- clés de chiffrement
- les données d'affaires
 - clients, employés
 - code en production
 - artefacts logiciels
 - rapports d'analyse
 - produits/services
- métadonnées (BDs, services)
- configurations
 - serveurs
 - accès
 - rôles
 - réseaux
 - stockage



Actifs dans le cloud

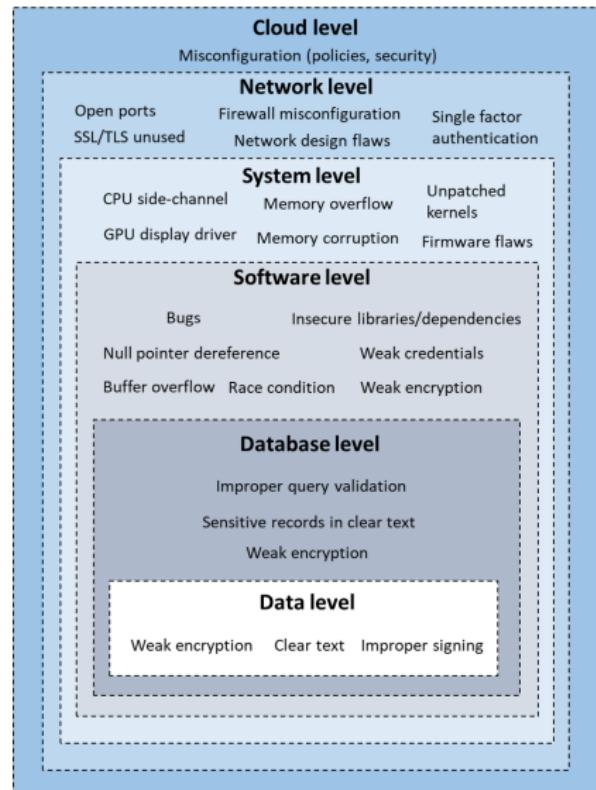
• Actifs opérationnels

- instances VMs (inclus. conteneurs)
- infra. réseaux
 - VPN
 - VLAN
 - VPC
- infra. stockage
 - Buckets
 - Active Directory
 - RDBMS / NoSQL
- infra. physiques connectés au cloud
 - data centers
 - technologie opérationnelle (OT)



Vulnérabilités des actifs cloud

- niveau des données
 - au repos/transit/en cours
- niveau de la base de données
- niveau logiciel
- niveau du système
 - OS
 - Machines virtuelles
 - Matériel
- niveau réseau
 - protocole TCP/IP
 - configuration Pare-feu
- niveau cloud
 - configurations
 - des contrôle d'accès

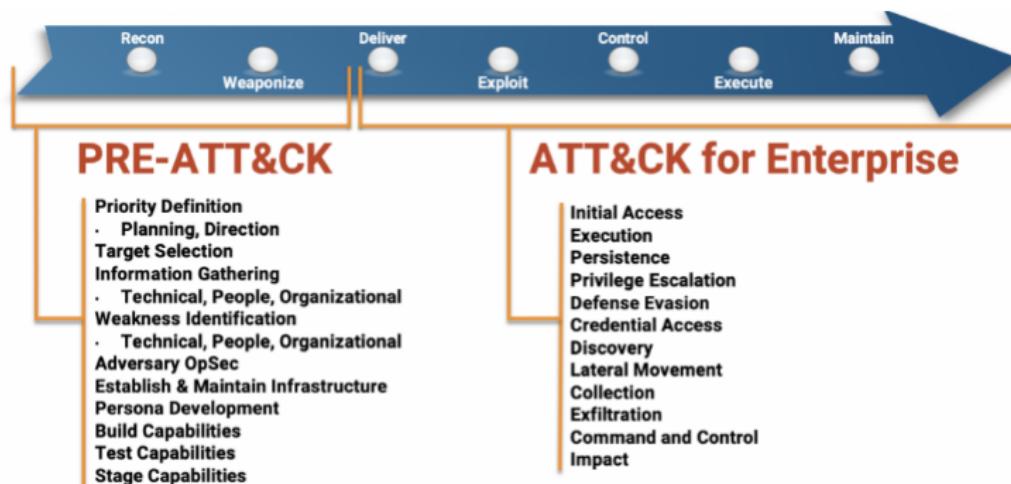


Sondage ☺: <https://www.wooclap.com/XOMOFT>.

wooclap

Menaces sur le cloud > ATT&CK Kill chain

- ATT&CK (Adversary Tactics, Techniques, and Common Knowledge) est un standard développé par MITRE
- Contient des descriptions de **tactiques, techniques, et procédures** (TTPs) des attaques
- Permet d'automatiser les menaces via des mécanismes SOAR (Security Orchestration, Automation and Response)



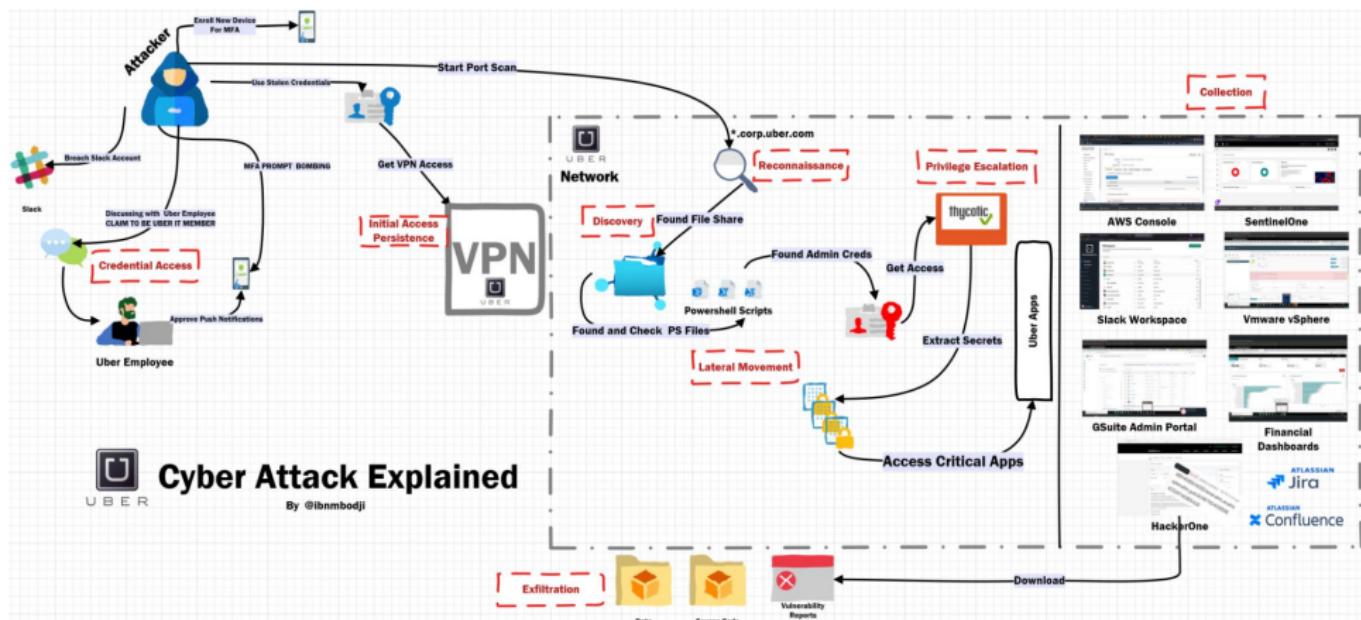
Menaces sur le cloud > Matrice des menaces

Ref.: <https://attack.mitre.org/matrices/enterprise/cloud/>

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
5 techniques	1 techniques	5 techniques	2 techniques	7 techniques	7 techniques	13 techniques	3 techniques	5 techniques	1 techniques	7 techniques
Drive-by Compromise	User Execution (1)	Account Manipulation (5)	Domain Policy Modification (1)	Domain Policy Modification (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Automated Collection	Transfer Data to Cloud Account	Account Access Removal
Exploit Public-Facing Application		Create Account (1)	Valid Accounts (2)	Hide Artifacts (1)	Forge Web Credentials (2)	Cloud Infrastructure Discovery	Taint Shared Content	Data from Cloud Storage Object		Data Destruction
Phishing (1)		Implant Internal Image		Impair Defenses (3)	Multi-Factor Authentication Request Generation	Cloud Service Dashboard	Use Alternate Authentication Material (2)	Data from Information Repositories (3)		Data Encryption for Impact
Trusted Relationship		Office Application Startup (6)		Modify Cloud Compute Infrastructure (4)	Network Sniffing	Cloud Service Discovery		Data Staged (1)		Defacement (1)
Valid Accounts (2)		Valid Accounts (2)		Unused/Unsupported Cloud Regions	Steal Application Access Token	Cloud Storage Object Discovery		Email Collection (2)		Endpoint Denial of Service (3)
				Use Alternate Authentication Material (2)	Steal Web Session Cookie	Network Service Discovery				Network Denial of Service (2)
				Valid Accounts (2)	Unsecured Credentials (2)	Network Sniffing				Resource Hijacking
						Password Policy Discovery				
						Permission Groups Discovery (1)				
						Software Discovery (1)				

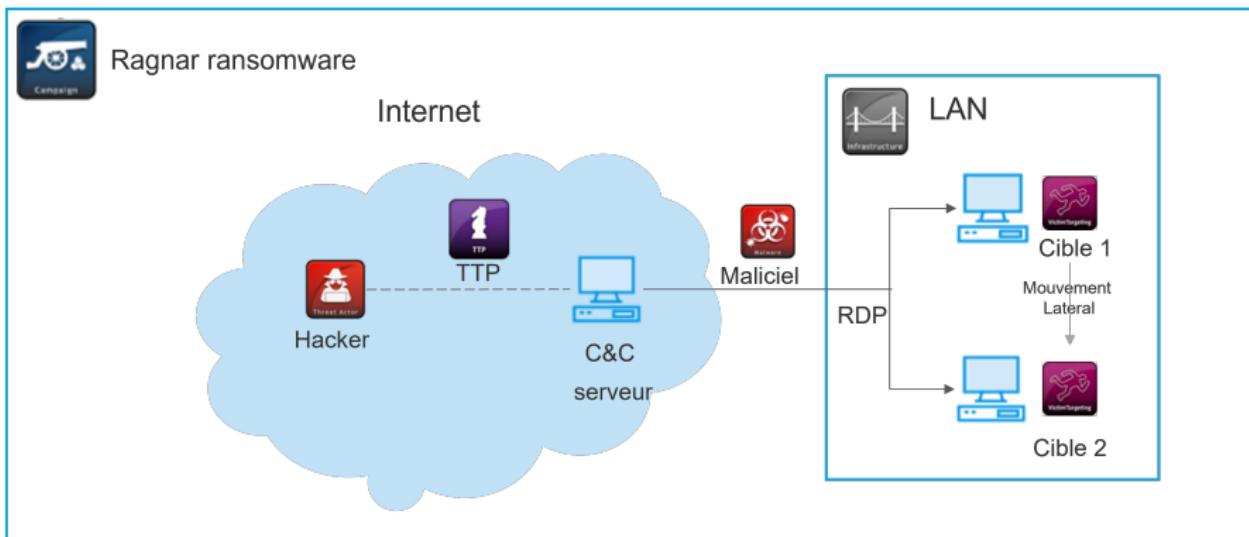
Menaces sur le cloud > Matrice des menaces: Exemple

Cas de l'attaque MFA fatigue - 16 Sept. 2022



Menaces sur le cloud > Matrice des menaces: Exemple

Cas du rancongiciel Ragnar



Menaces sur le cloud > Matrice des menaces: Exemple

Description des TTPs Ragnar dans ATT&CK

Nom de la phase	Description de l'événement	Action de l'attaquant	Action de la cible	Liste des techniques utilisées
#1 Transfert et Installation du ranconiciel sur l'hôte	Un programme est délivré par email en utilisant des méthodes d'ingéieries sociales. La victime télécharge le fichier paraissant normal et l'installe.	L'attaquant s'assure que la cible exécutera le fichier malveillant	La cible télécharge la pièce jointe ou clique sur un lien malicieux sans le savoir.	<ul style="list-style-type: none"> T1193 – SpearPhishing Attachment T1189 – Drive by Compromise
#2 Exécution et manipulation de services	Ragnar clone/créé des services suspicieux (sc.exe), manipule l'hôte en utilisant des appels système (Windows API), utilise l'infrastructure de gestion Windows (WMIC) pour lister/contrôler/modifier les processus et interroger les registres (reg.exe query)	Utilisation du gestionnaire de contrôle des services (SC), des appels systèmes Windows, de l'utilitaire WMIC et Reg pour la manipulation des services et registres.	N/A	<ul style="list-style-type: none"> T1035 – Service Execution T1106 – Execution through API T1047 – Windows Management Instrumentation T1012 – Query Registry T1057 – Process Discovery
#3 Activation de la persistance et évasion	Ragnar interagit avec la partition primaire du disque (DRO), manipule les registres Run Keys (reg.exe), alloue la mémoire virtuelle et écriture des données dans un processus distant (wmic.exe), supprime les clés instantanées (vssadmin.exe), déploie des VMs Windows pour éviter la détection des AVs (vrun.exe), et patch les processus en cours.	Utilisation des utilitaires Reg et WMIC pour la manipulation des registres et processus. Utilisation de l'utilitaire VSSADMIN et exécution du programme VRUN pour contourner les AVs.	N/A	<ul style="list-style-type: none"> T1067 – Bootkit T1060 – Registry Run Keys/Startup Folder T1055 – Process Injection T1107 – File Deletion T1063 – Security Software Discovery T1179 – Hooking
#4 Mouvement latéral	Le ranconiciel utilise le protocole RDP et l'utilitaire WMIC pour infiltrer les autres machines	Utilisation du protocole RDP et l'utilitaire WMIC pour le mouvement latéral.	N/A	<ul style="list-style-type: none"> T1076 – Remote Desktop Protocol T1110 – BruteForce T1210 – Exploitation of Remote Services
#5 Commande et contrôle	Le ranconiciel communique avec les serveurs C&C et crypte des fichiers avec la clé téléchargée en utilisant le chiffrement RSA-2048.	Utilisation des protocoles réseaux (incluant RDP) et cryptage des fichiers à l'aide chiffrement RSA-2048.	N/A	<ul style="list-style-type: none"> T1032 – Standard Cryptographic Protocol T1022 – Data Encrypted
#4 Exfiltration	Ragnar collecte des données locaux et les exfiltre sur les serveurs C&C.	Utilisation de l'utilitaire WMIC	N/A	<ul style="list-style-type: none"> T1041 – Exfiltration Over Command and Control Channel T1005 – Data From Local System T1486 – Data Encrypted for Impact



Menaces sur le cloud > Matrice des menaces: Exemple

Execution des TTPs Ragnar sur Caldera

The screenshot shows the ATT&CK profile interface for the "Hunter" profile. The profile is described as "Discover host details and steal sensitive files". The ordering of TTPs is as follows:

- 1 Find files (COLLECTION | DATA FROM LOCAL SYSTEM)
- 2 Identify active user (DISCOVERY | SYSTEM OWNER/USER DISCO...)
- 3 Find local users (DISCOVERY | ACCOUNT DISCOVERY: LOCAL ACC...)
- 4 Identify local users (DISCOVERY | ACCOUNT DISCOVERY: LOCAL ACC...)
- 5 Snag broadcast IP (DISCOVERY | SYSTEM NETWORK CONFIGURATIO...)
- 6 Find user processes (DISCOVERY | PROCESS DISCOVERY)
- 7 View admin shares (DISCOVERY | NETWORK SHARE DISCOV...)
- 8 Find domain controller (DISCOVERY | REMOTE SYSTEM DISCOV...)
- 9 Discover antivirus programs (DISCOVERY | SOFTWARE DISCOVERY: SECURITY ...)
- 10 Permission Groups Discovery (DISCOVERY | PERMISSION GROUPS DISCOV...)
- 11 Identify Firewalls (DISCOVERY | SOFTWARE DISCOVERY: SECURITY ...)
- 12 Discover Mail Server (DISCOVERY | REMOTE SYSTEM DISCOV...)
- 13 Get Chrome Bookmarks (DISCOVERY | BROWSER BOOKMARK DISCOV...)
- 14 Create staging directory (COLLECTION | DATA STAGED)
- 15 Stage sensitive files (COLLECTION | DATA STAGED)
- 16 Compress staged directory (EXFILTRATION | ARCHIVE COLLECTED DATA: ARC...)
- 17 Exfil staged directory (EXFILTRATION | EXFILTRATION OVER C2 CHAN...)

Profile details:
Profiles are collections of ATT&CK TTPs, designed to create specific effects on a host or network. Profiles can be used for offensive or defensive use cases.

Buttons: VIEW, Save, Delete profile.

Sondage ☺: <https://www.wooclap.com/0NBFBM>.

wooclap

Menaces sur le cloud > Top 10 menaces

- Les menaces sur le cloud selon la norme OWASP:

1. Responsabilité et risque lié aux données

- parties tierces/fournisseurs
- configurations des politique de sécurité

2. Fédération des identités des utilisateurs

- identités partagés entre les fournisseurs
- intégration des identités

3. Conformité légale et réglementaire

- different règlements des pays (Canada, EU)

4. Continuité et résilience des activités

- responsabilité partagée avec le fournisseur
- contrat lié à la qualité de service

5. Confidentialité des utilisateurs et utilisation secondaire des données

- exploitation des sites sociaux (Twitter, Facebook)

Menaces sur le cloud > Top 10 menaces (OWASP)

- Les menaces sur le cloud selon la norme OWASP (suite):

6. Intégration de services et de données

- sécurité des données propriétaires
- en transit/en utilisation par les services

7. Multiloccation et sécurité physique

- risques liés au partage de services/ressources

8. Analyse des incidents et cybercrimes

- Données venant de plusieurs zones géographiques
- Différentes lois sur la gestion des données

9. Sécurité des infrastructures

- conception de l'architecture
- partagée avec le fournisseur (patches, renforcement)

10. Exposition dans un environnement hors production

- faible mesure de sécurité
- données sensibles en clair

Sondage ☺: <https://app.wooclap.com/events/QHDXRL>.

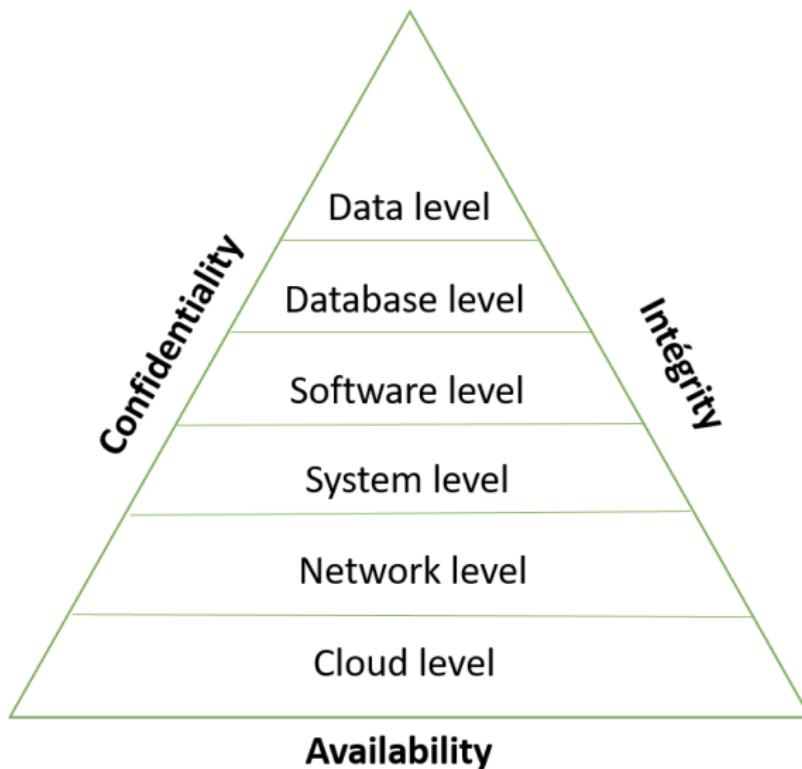
wooclap

1 Actualités

2 Risques de sécurité

3 Propriétés de sécurité

Triade CIA



Triade CIA > Confidentialité

- Gestion des identités et accès
 - utilisateurs/ressources/groupes
 - roles/permissions
- Protection
 - des données (repos, transit, utilisation)
 - des machines virtuelles
 - des images conteneurs/applications
 - exécution (statique/dynamique)
 - des fonctions serverless
 - des pipelines (code, services)
 - des buckets/bases de données
- Gestion des clés de chiffrement
 - Apporter votre propre clé (BYOK)
 - Garder votre propre clé (KYOK/HYOK)
- Protection des réseaux
 - Veille sécurité (journalisation, prévention/détection intrusions)
 - Configurations réseaux

Triade CIA > Intégrité

- Intégrité
 - des données (repos, transit, utilisation)
 - des machines virtuelles
 - des images conteneurs/applications
 - exécution (statique/dynamique)
 - des fonctions serverless
 - des pipelines (code, services)
 - des buckets/bases de données
- Intégrité des clés de chiffrement
 - Apporter votre propre clé (BYOK)
 - Garder votre propre clé (KYOK/HYOK)
- Intégrité des réseaux
 - Veille sécurité (journalisation, prévention/détection intrusions)
 - Configurations réseaux

Triade CIA > Disponibilité

- Disponibilité des ressources sur le cloud
 - routeurs/load balancers/passerelles/pare-feux
 - des machines virtuelles
 - des images conteneurs/applications
 - des fonctions serverless
 - des services API
 - des buckets/bases de données
- Disponibilité des données (repos, transit, utilisation)



Matrice de contrôle Cloud (CCM v4)

- Liste de contrôles de sécurité de la Cloud Security Alliance (CSA)
- sur les principes de sécurité
- à suivre par les fournisseurs Cloud

Security Controls Domain	
1. Application & Interface Security	10. Identity & Access Management
2. Audit Assurance & Compliance	11. Interoperability & Portability
3. Business Continuity Mgmt. & Ops Resilience	12. Infrastructure & Virtualization Security
4. Change Control & Configuration Mgmt.	13. Logging & Monitoring
5. Cryptography, Encryption & Key Mgmt.	14. Security Incident Mgmt., E-Discovery & Cloud Forensics
6. Datacenter Security	15. Supply Chain Mgmt., Transparency & Accountability
7. Data Security & Privacy Lifecycle Mgmt.	16. Threat & Vulnerability Management
8. Governance, Risk, and Compliance	17. Universal End-point Management
9. Human Resources Security	

Credits: CSA