Investigation numérique dans le Cloud

Principaux challenges et opportunités

Présentation par **PwC France**
Janvier 2020

pwc | Cyber Intelligence

Qui sommes nous ?

Philippe Baumgart
Associé Cyber Intelligence
philippe.baumgart@pwc.com
First Responder

Fahim Hasnaoui
Senior Manager Cyber Intelligence
fahim.hasnaoui@pwc.com
Former CISO et Pentester

Agenda

1. Overview
2. Challenges et opportunités
3. Cas concrets
4. Outils
5. Conclusion

Overview

Shadow-IT dans le Cloud

The Good, the Bad and the Ugly

The Bad …

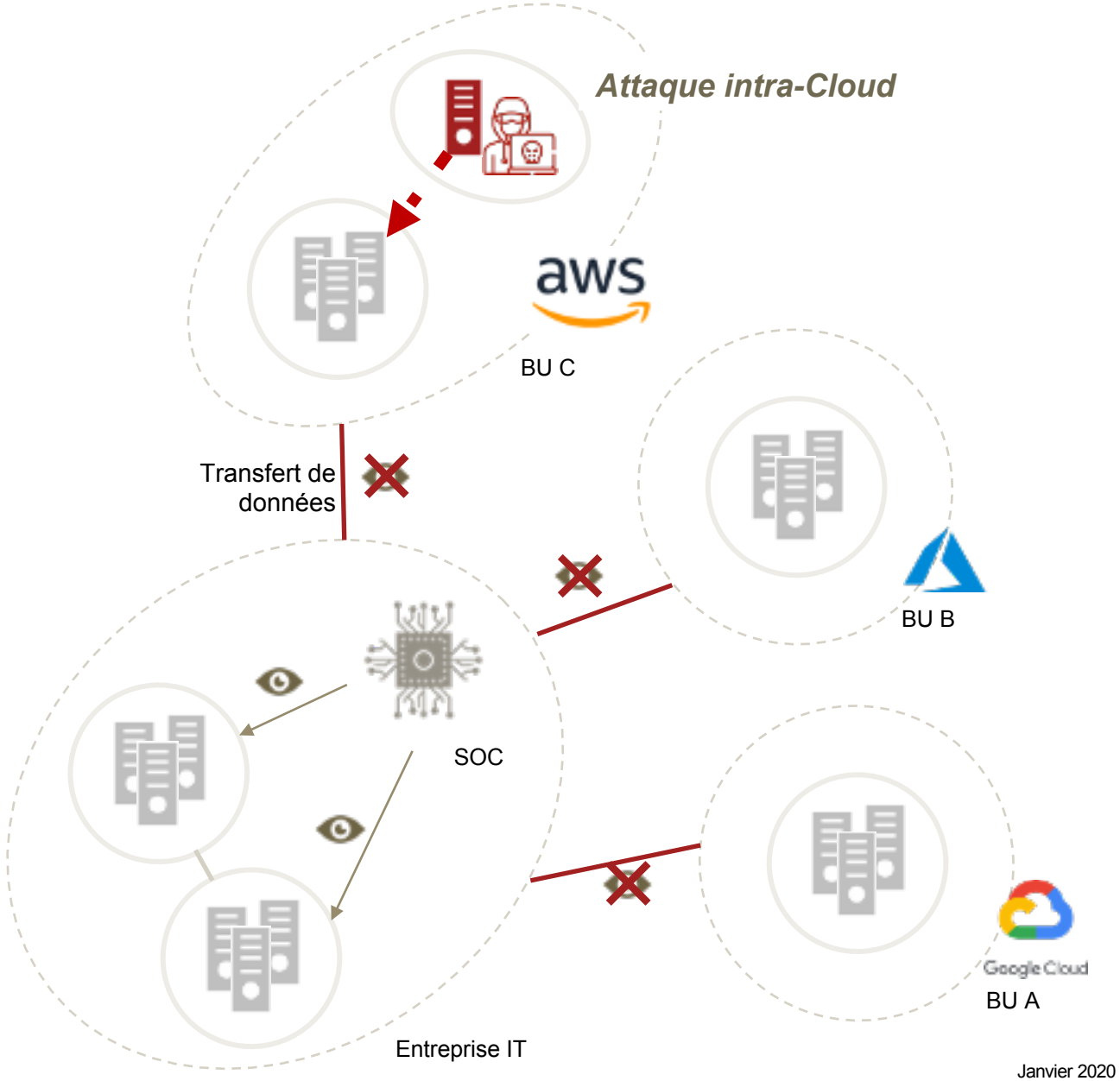
Dans un réseau classique, de nombreux assets peuvent rapidement être oubliés, perdus, et de fait deviennent vulnérables et vecteurs d'attaques sans une gestion rigoureuse de la CMDB, ni d'outils de scan permettant leur découverte.

…The Good

Dans le Cloud, ce problème ne se pose plus: Les APIs fournis par le fournisseur permet le listing complet des instances créés.

… and the Ugly

Chaque Business Unit, chaque projet dans l'entreprise à la **possibilité de créer une infrastructure de son côté**, sans que le **groupe ne soit au fait de ces réseaux** :Cela amène à des hétérogénéités de pratiques et de politiques de sécurité, et le SOC en est souvent exclus.

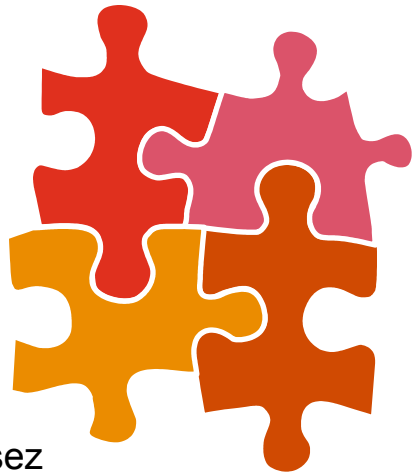


Une investigation différenciée

Une différence de concept mène à une approche différente

Un monitoring simple mais facultatif

Le Cloud offre de nombreuses manières de monitorer l'activité, voire de fournir des outils de détection d'activités malveillantes. Or, par défaut, ces fonctionnalités sont facultatives, ce qui rend une équipe de réponse à incidents aveugle quant aux mouvements qui s'y déroulent.



Une (trop) grande facilité de déploiement

Le Cloud permet de monter rapidement une architecture, en quelques minutes, et de donner une flexibilité dans le déroulement de nouveaux projets. Il échappe également rapidement au contrôle de l'entreprise, et amène à un Shadow IT hétérogène entre les projets, augmentant le nombre de points d'entrées dans l'entreprise, et de fait augmente le risque de compromission.

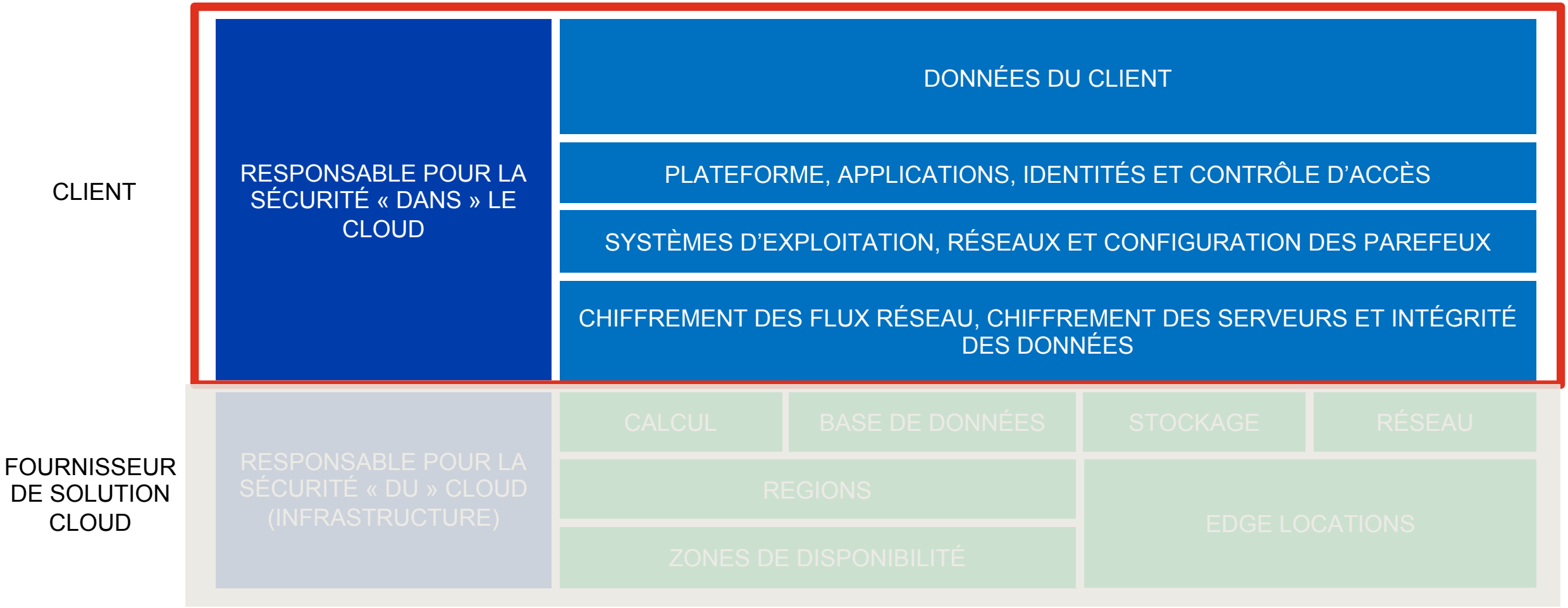
Une stratégie architecturale différente

Déployer des outils de sécurité dans le Cloud diffère assez d'une architecture classique : certains types d'équipements ne sont pas compatibles, ou contre-productifs car non adaptés à la logique du Cloud. La logique de gestion des flux et des zones réseau ne sont également pas les mêmes (Firewall vs. ACL notamment).

Challenges et opportunités

Les challenges du cloud

Une responsabilité partagée entre le client et le fournisseur de solution cloud



Un très net avantage pour le Cloud

Qui doit bien être maîtrisé

Challenges

- Les évènements disponibles en Cloud **sont différents d'une infrastructure "on-premise"**;
- Une entreprise peut rapidement avoir de multiples comptes dans de multiples Cloud, favorisant l'émergence de **comptes Shadow**, hétérogènes, ne suivant pas de politique de sécurité particulière;
- Les contrats envers les fournisseurs Cloud **sont rigides et difficilement négociables** (Notamment s'agissant des SLAs & SLOs);
- La localisation des données sont parfois **floues, et s'avère problématique** pour respecter les différentes législations nationales.

Opportunités

- Un **déploiement mondial, et instantané**;
- Un monitoring **facile d'accès**;
- L'infrastructure peut maintenant être **scriptée et automatisée;**
- La gestion des instances (ou Asset Management) **est grandement simplifié, avec une API native disponible**, qui liste toutes les instances créées;
- Grandement **moins cher**, et abstraction de la couche équipement (ou « Hardware »), qui devient **invisible** et gérée par le fournisseur Cloud;
- **Accès rapide** aux données, et i**solation immédiate** possible en cas d'attaque ou de propagation, sans attendre qu'une équipe soit disponible;
- Des fonctionnalités de backup et restauration **simples, et efficientes.**

Les tableaux de bord, un outil essentiel

Des informations précieuses en accès direct

Certaines informations (CPU, réseau, nombre de requêtes) sur des infrastructures “on-premise” peuvent ne pas ou difficilement être disponibles. Les fournisseur d’IaaS mettent à disposition différents tableaux de bord en temps réel utile lors d’investigation.

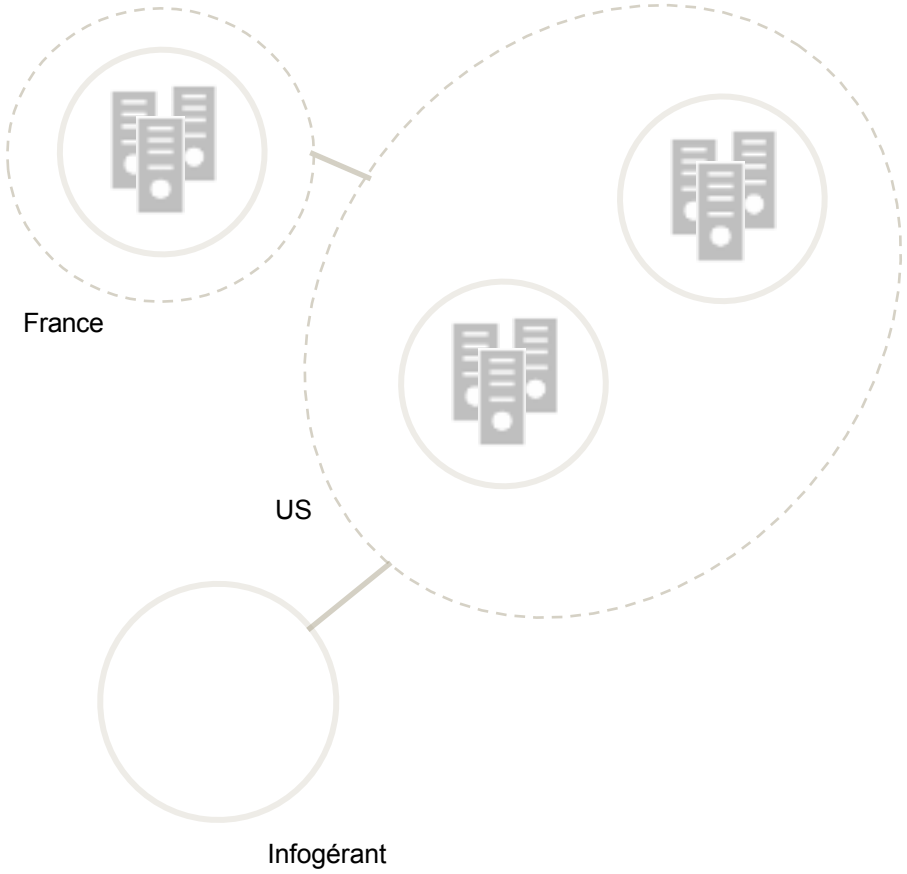
Ils permettent de mettre en évidence facilement :

- **l’exfiltration de données** (tableau de bord réseau)
- **les activités de rançongiciel** (tableau de bord CPU et I/O)

Cas concrets

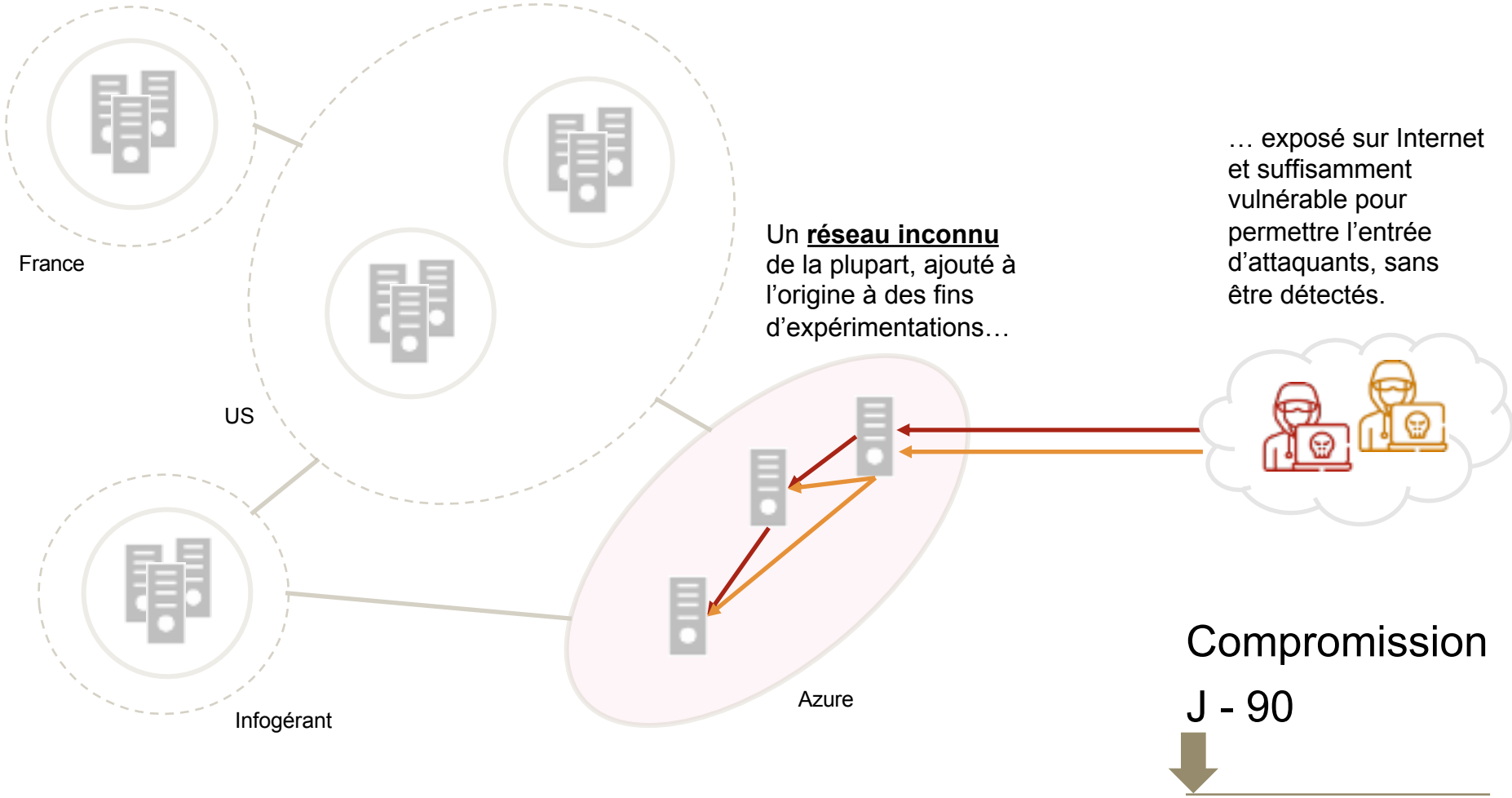
Une infrastructure type…

Pour un premier cas réel, sur Azure



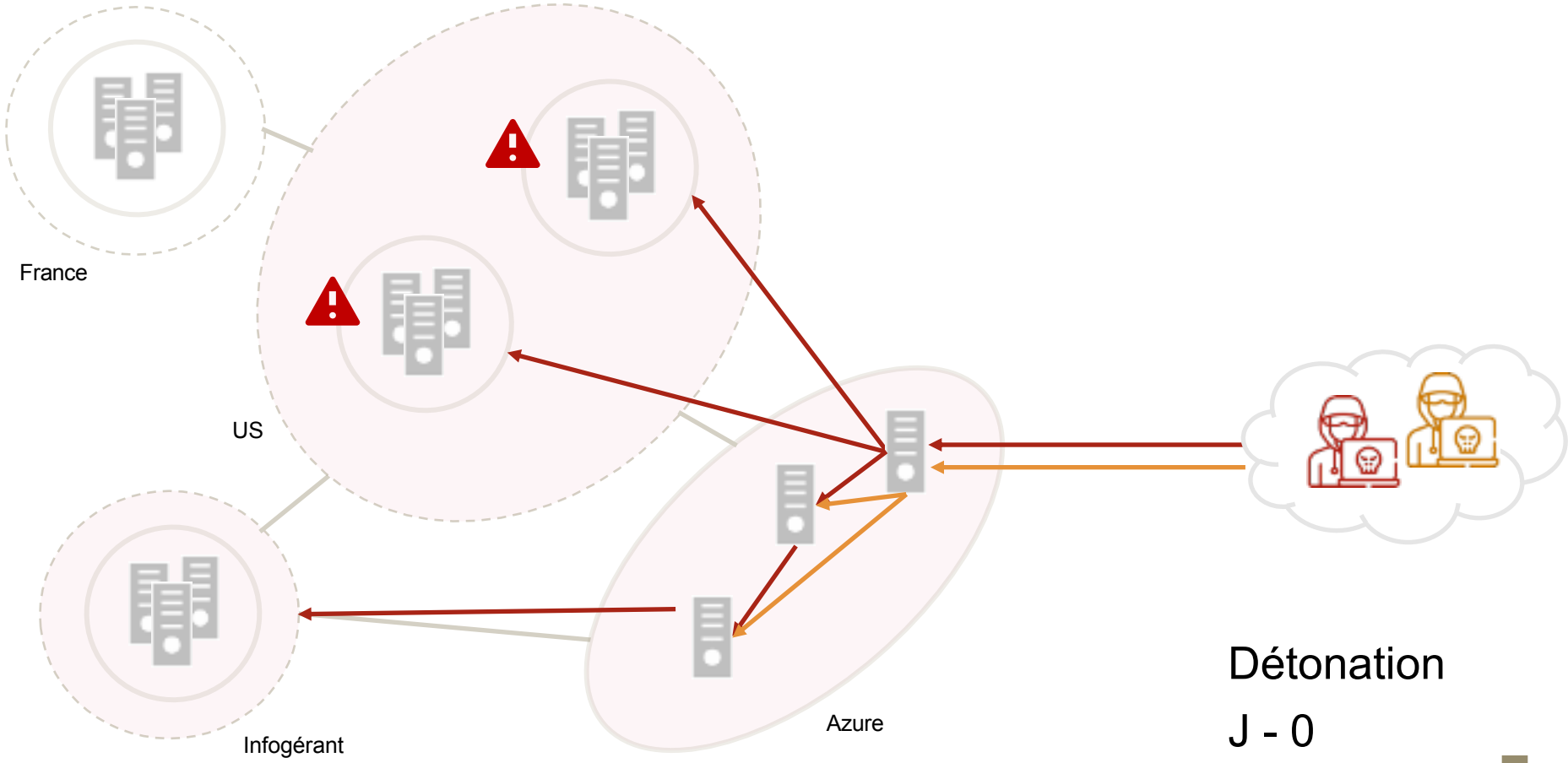
Une infrastructure type liée à un Cloud IAAS

Inconnue, Vulnérable, ne suivant pas les bonnes pratiques de l'entreprise



Une infrastructure type attaquée par un ransomware

Détecté tardivement lors d'alertes de disques durs pleins



Une base de données SaaS compromise

Un autre cas réel de ransomware, sur GCP

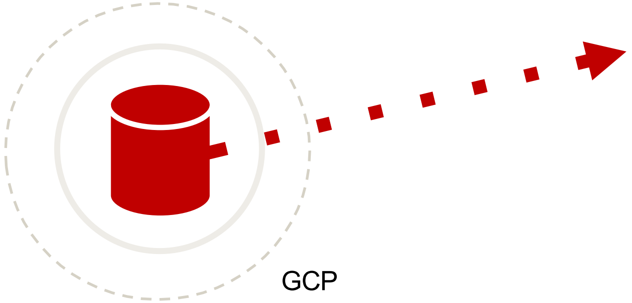
Serveur MySQL

Création de la base de données sans mot de passe pour le compte root

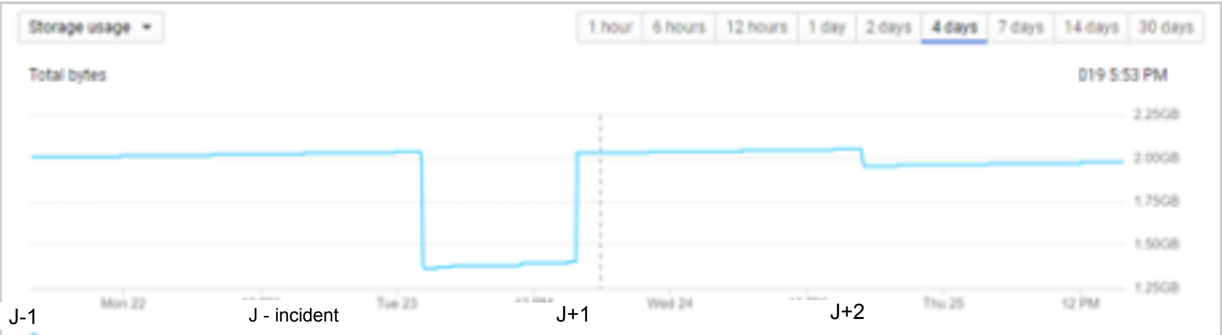
Jour J-365

Une base de données compromise

Un autre cas réel de ransomware, sur GCP analysé avec Stackdriver

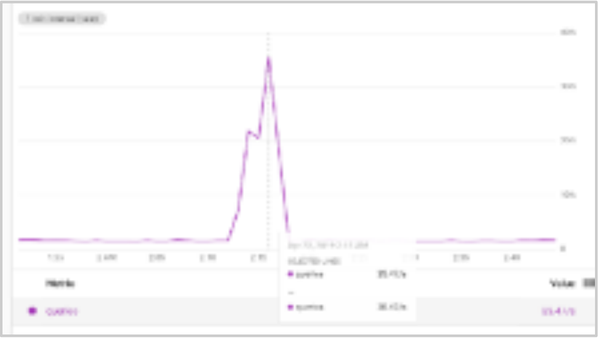


La suppression du contenu de la base de données est clairement visible via les tableaux de bord (perte de ~500 Mb)



Pendant l'exfiltration, 35 requêtes MySQL par seconde ont été enregistrées

Activités associées à un script automatique



Serveur MySQL

Création de la base de données sans mot de passe pour le compte root

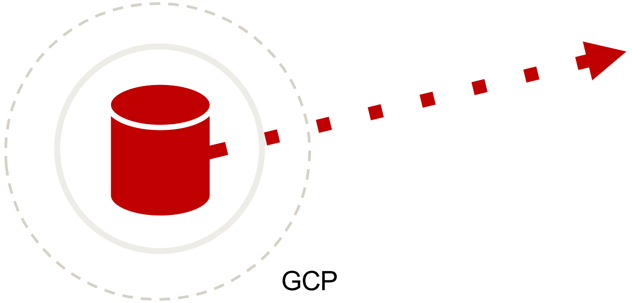
Détonation & Exfiltration de données

Et effacement de la base de données, avec une table Warning créée, dans chaque BDD ainsi, qu'une BDD "Please_read_me"

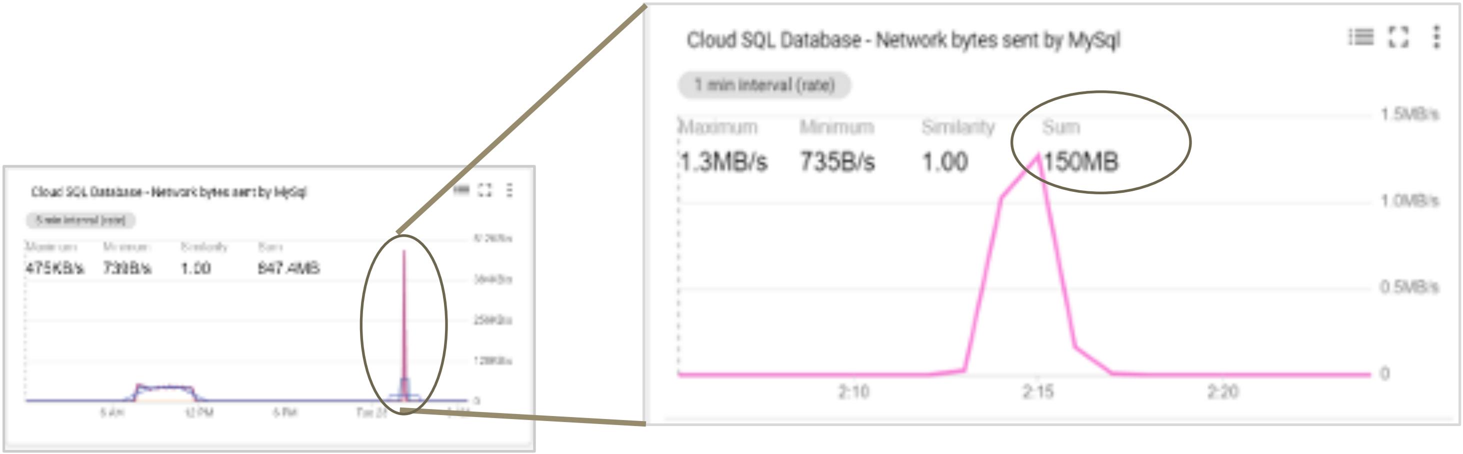
Jour · J-365 · J0

Une base de données compromise

Un autre cas réel de ransomware, sur GCP analysé avec Stackdriver



Le client avait de gros doutes sur l'exfiltration des données, le rendant réticent à prévenir les autorités compétentes.
Le dashboard GCP a été en mesure de confirmer nos suspicions :



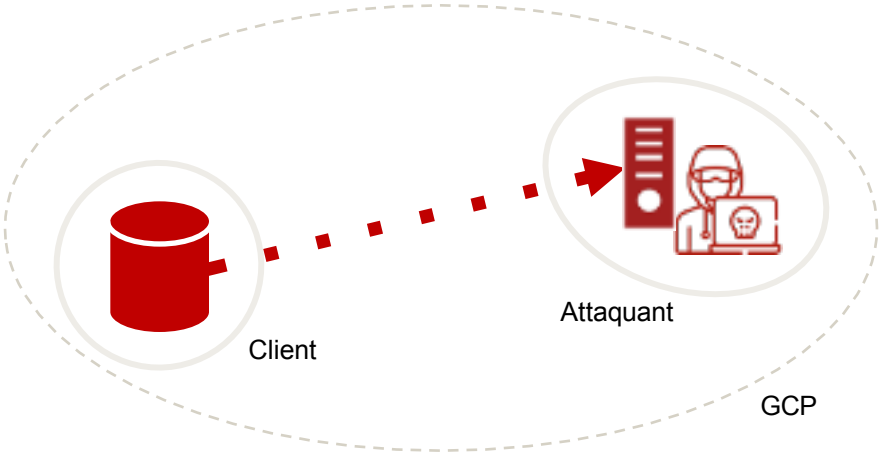
Serveur MySQL
Création de la base de données sans mot de passe pour le compte root

Détonation & Exfiltration de données
Et effacement de la base de données, avec une table Warning créée, dans chaque BDD ainsi, qu'une BDD "Please_read_me"

Jour **J-365** **J0**

Une base de données compromise

Un autre cas réel de ransomware, sur GCP analysé avec Stackdriver



Attaque intra-Cloud

La base de données n'était pas exposée publiquement, mais uniquement en interne GCP. Un attaquant avait acheté une instance pour pouvoir scanner en interne toutes les instances d'autres clients exposés, et ainsi les compromettre.

Serveur MySQL

Création de la base de données sans mot de passe pour le compte root

Détonation & Exfiltration de données

Et effacement de la base de données, avec une table Warning créée, dans chaque BDD ainsi, qu'une BDD "Please_read_me"

Découverte de l'incident

Un développeur se connecte et constate l'absence des données.

Confinement d'urgence

Suppression du compte root mise en place de règles de filtrage et restauration de la base de données.

Appel PwC

Pour investiguer sur l'incident concernant la base de donnée.

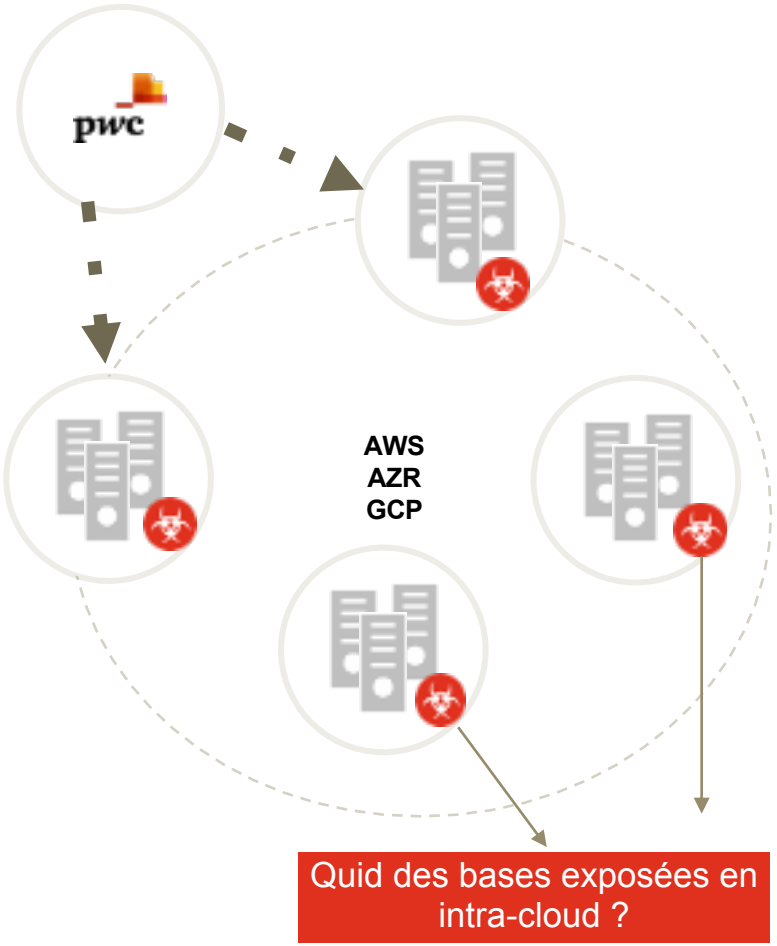
Première compréhension

L'attaque provenait de la partie intra cloud.

Jour · J-365 · J-0 · H+9 · H+11 · H+12 · J+3 ▶

Statistiques de « *ransomisation* » des bases externes NoSQL non sécurisées

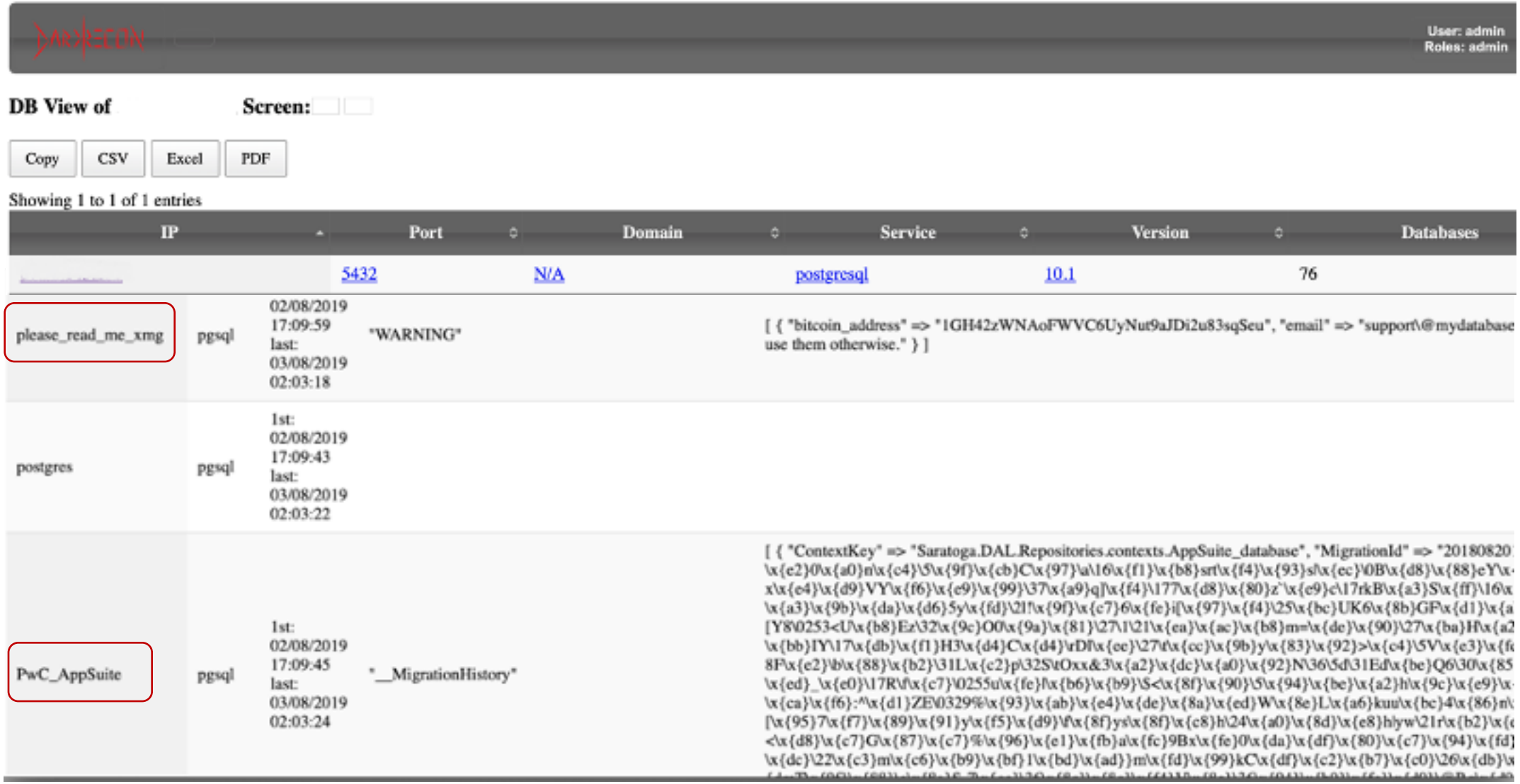
Nos observations sur l'exposition de bases de données* sur Internet



	mongoDB.	elasticsearch
aws	***19 658 bases exposées*** *8,6% de bases compromises*	***2832 bases exposées*** *11,2% de bases compromises*
	8690 bases exposées *3,4% de bases compromises*	***1781 bases exposées*** *9,8% de bases compromises*
Google Cloud	***4287 bases exposées*** *5,7% de bases compromises*	***1587 bases exposées*** *7,1% de bases compromises*

Source: DarkRecon ONYPHE

Personne n’est épargné …



User: admin
Roles: admin

DB View of **Screen:**

Copy CSV Excel PDF

Showing 1 to 1 of 1 entries

IP	Port	Domain	Service	Version	Databases
[redacted]	5432	N/A	postgresql	10.1	76

please_read_me_xmg	pgsql	02/08/2019 17:09:59 last: 03/08/2019 02:03:18	"WARNING"	[{ "bitcoin_address" => "1GH42zWNAoFWVC6UyNut9aJDi2u83sqSeu", "email" => "support\@mydatabase use them otherwise." }]
postgres	pgsql	1st: 02/08/2019 17:09:43 last: 03/08/2019 02:03:22		
PwC_AppSuite	pgsql	1st: 02/08/2019 17:09:45 last: 03/08/2019 02:03:24	"__MigrationHistory"	[{ "ContextKey" => "Saratoga.DAL.Repositories.contexts.AppSuite_database", "MigrationId" => "20180820 \x{e2}0\x{a0}n\x{c4}\5\x{9f}\x{cb}C\x{97}\a\16\x{f1}\x{b8}srt\x{f4}\x{93}s\x{ec}\0B\x{d8}\x{88}eY\x x\x{e4}\x{d9}VY\x{f6}\x{e9}\x{99}\37\x{a9}q]\x{f4}\177\x{d8}\x{80}z`\x{e9}c\17rkB\x{a3}S\x{ff}\16\x \x{a3}\x{9b}\x{da}\x{d6}5y\x{fd}\2l!\x{9f}\x{c7}6\x{fe}i[\x{97}\x{f4}\25\x{bc}UK6\x{8b}GF\x{d1}\x{a [Y8\0253<U\x{b8}Ez\32\x{9c}O0\x{9a}\x{81}\27\1\21\x{ea}\x{ac}\x{b8}m=\x{de}\x{90}\27\x{ba}H\x{a2 \x{bb}IY\17\x{db}\x{f1}H3\x{d4}C\x{d4}\rDl\x{ee}\27\f\x{cc}\x{9b}y\x{83}\x{92}>\x{e4}\5V\x{e3}\x{f 8F\x{e2}\b\x{88}\x{b2}\31L\x{c2}p\32S\tOxx&3\x{a2}\x{dc}\x{a0}\x{92}N\36\5d\31Ed\x{be}Q6\30\x{85 \x{ed}_\x{e0}\17R\f\x{c7}\0255u\x{fe}l\x{b6}\x{b9}\$<\x{8f}\x{90}\5\x{94}\x{be}\x{a2}h\x{9c}\x{e9}\x \x{ca}\x{f6}:^\x{d1}ZE\0329%\x{93}\x{ab}\x{e4}\x{de}\x{8a}\x{ed}W\x{8e}L\x{a6}kuu\x{bc}4\x{86}n\ [\x{95}7\x{f7}\x{89}\x{91}y\x{f5}\x{d9}\f\x{8f}ys\x{8f}\x{c8}h\24\x{a0}\x{8d}\x{e8}h\yw\21r\x{b2}\x{ <\x{d8}\x{c7}G\x{87}\x{c7}%\x{96}\x{e1}\x{fb}a\x{fc}9Bx\x{fe}0\x{da}\x{df}\x{80}\x{c7}\x{94}\x{fd} \x{dc}\22\x{c3}m\x{c6}\x{b9}\x{bf}l\x{bd}\x{ad}}m\x{fd}\x{99}kC\x{df}\x{c2}\x{b7}\x{c0}\26\x{db}\x

D’autres cas existent

Qui découlent d’une mauvaise utilisation/compréhension du Cloud

De nombreuses mauvaises configurations de Cloud sont à l’origine de compromission ou de fuite de données.

Les serveurs de stockage S3 d’Amazon peuvent être configurés de telle manière que les données deviennent accessibles par tous le monde.

« Cultura Colectiva » est un éditeur de médias mexicain qui, en 2019, a laissé en libre accès plus de 540 millions d'enregistrements Facebook détaillant les commentaires, les goûts, les réactions, les noms de comptes, etc. des utilisateurs du réseau social.

Les identifiants et clés permettant de s’authentifier auprès du Cloud doivent être protégés et ne pas être partagés.

L’authentification Amazon peut se faire par clé d’accès afin de faciliter l’automatisation des tâches avec une interface en ligne de commande (CLI). Il est possible de donner plus ou moins d’accès à une clé API donnée.

En 2016, « Uber » a subit une fuite de données de plus 56 millions d’utilisateurs (noms, prénoms, emails, numéros de téléphone). Une clé d’accès Amazon était présente dans un projet GitHub privé, qui a été compromis.

La "master API key" d'Accenture a fuité au travers d'un serveur S3 possédant des droits trop permissifs, pouvant ainsi entraîner une perte de contrôle total des données de l'entreprise sur ses environnement AWS.

Les fuites de données en quelques chiffres

Liées à des droits trop permissifs

240K Buckets S3 parsés

900M de documents indexés

7%

De l'ensemble des buckets S3 hébergés sur AWS ont des droits trop permissifs, permettant un accès non authentifié et illimité.

198M

En juin 2017, une liste de 198 millions de votants américains a été divulguée.

3M

En juillet 2017, 3 millions de fans de lutte enregistrés sur WWE ont vu leur données exposées au travers d'une fuite de leur données personnelles.

111Go

En décembre 2017, une base de données de plus de 111 gigaoctet contenant des informations relatives aux crédits de dizaines de milliers de personnes affiliées à la « National Credit Federation ».

20M

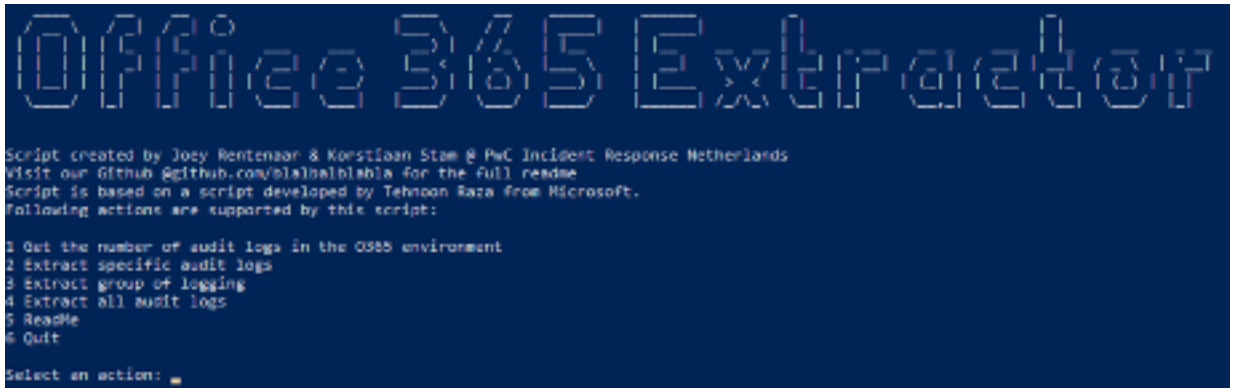
Les données d'identification de la population de l'Equateur ont été divulguées en septembre 2019 au travers d'un défaut de configuration d'AWS.

Outils

https://github.com/PwC-IR/Office-365-Extractor

O365 - Investigations BEC

Office 365 Extractor : Un outil PwC OpenSource



Challenges d'Office 365

Acquisition de données

- Extraire des données par le biais d'une session est limité:
  Données triées : max. 5000 entrées;
  Données non triées : max. 50000 entrées.

- Le script permet de n'extraire que les journaux pertinents :
  - Extraire tous les journaux;
  - Extraire des journaux spécifiques;
  - Extraire la journalisation des groupes (Azure, Exchange, Skype et Sharepoint).

Analyse des données

- Difficulté d'investiguer avec l'interface web d'Office 365, et seul un certain nombre d'entrées de journaux sont affichées;
- Le filtrage dans l'interface web est limité à quelques champs.

Solutions apportées par l'outil

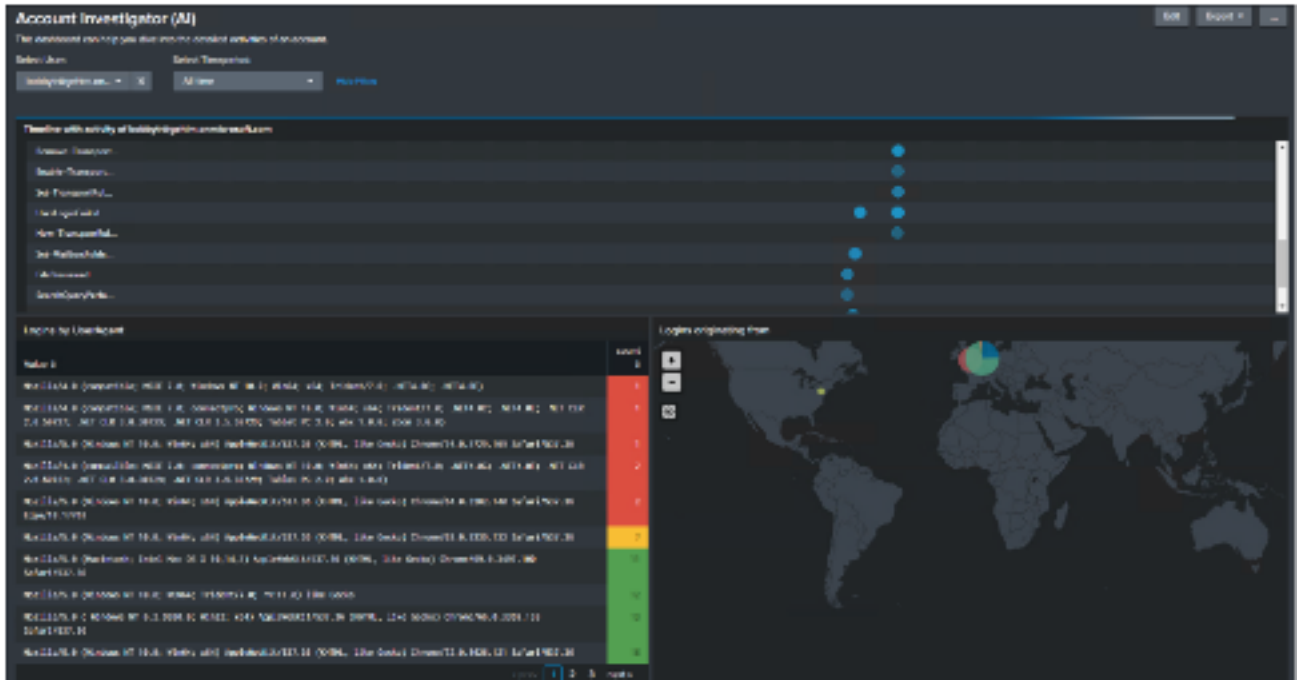
- Le nombre d'entrée est calculé, et utilisé pour calculer les intervalles de temps nécessaires à l'extraction des journaux;
- Le script va créer une nouvelle session par intervalle de temps pour s'assurer que le nombre maximum d'entrées n'est pas supérieure à 5000;
- Tous les journaux seront extraits et écrits dans un fichier CSV qui peut être facilement chargé dans une solution de centralisation des journaux (ElK-Stack, Splunk)

O365 - Investigations BEC

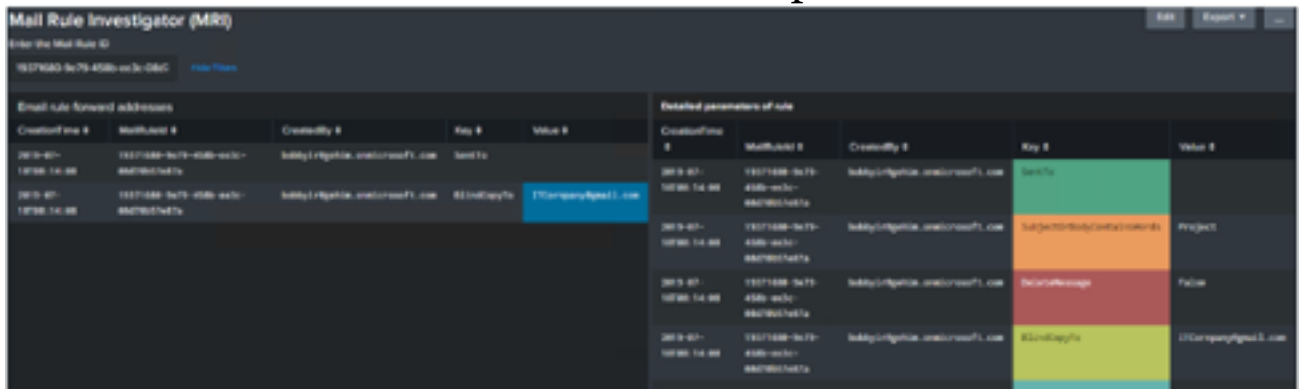
App Splunk pour visualisation

https://splunkbase.splunk.com/app/4667/

Activité de connexion suspecte



Activité des comptes



Activité des règles de routage

AWS - Investigations IaaS

Une boîte à outils complète favorisant des investigations exhaustives et en profondeur

Les sources de données DFIR

– CloudTrail: Log API (Get, List, Describe, Recon, Delete, Disable, Stop, Set…)

– CloudWatch: Monitoring des performances Système / Application et Laerting

– Config Logs : Traçabilité des actions réalisées au niveau de la configuration AWS

– S3 Bucket Logs : Traçabilité des accès aux buckets (Objets et Données)

– VPC Flows & WAF Logs: traçabilité des flux applicatifs et des communications réseau inter VPC

– Gestion des Habilitations
  - Certificat Manager
  - Key Management Service
  - Cloud HSM
  - Identity and Access Management (IAM)

Construction d'un environnement d'analyse

- Instance Investigation EC2 : Création d'une instance avec toolbox d'investigation dans un VPC isolé
- Incident Response S3 Bucket: Environnement pour extraire les traces d'investigation (Dump mémoire, images disques…)
- Role & compte IR : Création d'un compte d'investigation avec des droit Admin Read-Only
- Elastic Block Store(EBS): Les EBS permettent de faire des snapshots rapidement des disques des machines;

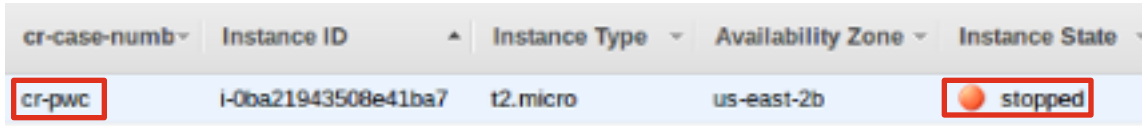
AWS - Investigations IaaS

Automatisation de la collecte de données avec « aws_ir »

AWS fournis **plusieurs APIs** afin de pouvoir automatiser au maximum certaines actions liés à un incident. Il est donc possible de les automatiser avec des outils, comme « aws_ir », un outil Open Source permettant **d'automatiser les taches suivantes** :

- **Isoler** les ressources compromises:
  - En isolant totalement l'instance du réseau,
  - En ajoutant un tag indiquant un incident sur la ressource et son ID.
- Faire un **snapshot** du disque tagué avec le nom de l'incident;
- Ajouter une **règle de filtrage** selon l'IP de la machine d'investigation (la ressource accepte les connexions ssh venant de l'ip de cette machine);
- Effectuer une **collecte de la mémoire** pour la déposer dans un S3 sécurisé;
- **Eteindre** la ressource compromise.

Snapshot du disque avec le tag du cas de réponse « cr-pwc »



Instance stopée avec le tag du cas de réponse « cr-pwc »

AWS - Investigations IaaS

Découverte du « RBAC » avec PMapper

IAM AWS

- IAM (Identify Access Management) permet de contrôler finement l'accès aux services et ressources AWS au moyen d'une gestion avancée des utilisateurs, groupes, rôles et permissions ;
- Fédération possible entre les annuaires d'entreprise (ex : Active Directory) et les identités AWS ;
- Possibilité d'intégrer une authentification fort (facteurs multiples).

Solutions apportées par l'outil

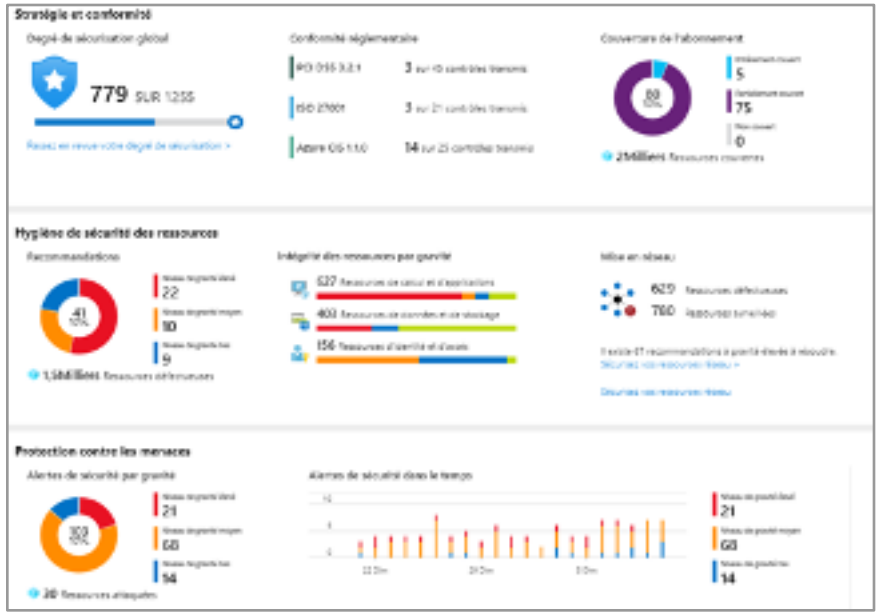
- PMapper (Principal Mapper) permet d'identifier rapidement les utilisateurs et rôles ayant accès à une action (ou ressource) donnée ;
- Utilise le simulateur d'API afin de déterminer les utilisateurs et rôles ayants des accès mutuels ;
- Affichage graphique des liens entre utilisateurs et rôles ;
- Moteur de requêtes permettant l'identification de scénarios complexes pouvant mener à une compromission ou élévation de privilèges.

AZR & GCP - Investigations IaaS SaaS

Consoles de sécurité & ATP

Un monitoring de vulnérabilités (AZR/IaaS)

Par défaut, Azure indique une notation sur le niveau de sécurisation de l'environnement. De même, il fournit des recommandations basiques de configuration, de sécurisation et de politiques de sécurité.



Advanced Threat Protection (ATP/IaaS)

Le module ATP fourni des fonctionnalités supplémentaires, notamment EPP et EDR sur toutes les instances dont l'agent Azure est déjà installé, le tout agrémenté d'une source de Threat Intelligence géré par Microsoft.

Un monitoring complet des ressources (AZR et GCP IaaS & SaaS)

GCP après souscription il est possible de générer des graph sur à peu près toutes les ressources des VMs via Stackdriver.

AZR c'est possible sans frais mais les graph sont beaucoup moins exploitables.

Conclusion

Une préparation nécessaire

Afin d'éviter de potentiels écueils

Se préparer avant un incident :

- Un suivi étroit des actifs du Cloud et Security by design;
- Des exercices de crise effectués de manière régulière;
- Cartographie des composants critiques
- Comptes et environnements dédiés pour l'investigation et le SOC;
- Identifier les journaux « utiles » permettant au SOC / équipe DFIR de détecter des anomalies et/ou des menaces.

Avoir des outils et procédures d'acquisition prêts à l'emploi :

- Equipe de réponse à incident formée aux méthodes de collecte cloud;
  - Récupération de données volatiles (ex: RAM), de disque;
  - Avoir une machine dans le Cloud prête à faire des analyses sur les ressources compromises du Cloud;
- Savoir isoler des machines afin d'éviter toute propagation.
- Documenter les procédures d'acquisition et mettre en place des protocoles de validation de l'intégrité des traces/preuves.

Revoir les contrats, SLA, SLO pour s'assurer du niveau **de support et d'assistance** du fournisseur de Cloud **en cas d'incident.**

Avoir **le service juridique** en soutient pour s'assurer de l'intégrité des preuves et valider les schémas d'acquisition tout au long de la procédure, et ce dans le cas d'utilisation judiciaire ultérieure.

Cyber Intelligence