< DÉTECTION DANS LE CLOUD >

Panorama des outils d’aide à la détection

CAMPUS CYBER 2025

< SOMMAIRE >

1. INTRODUCTION 03

2. LES MENACES À DÉTECTER 04
2.1 DÉFINITION D'UNE MENACE INTERNE
2.2 PROFILS DES ATTAQUANTS INTERNES
2.3 RISQUES INHÉRENTS À LA MENACE INTERNE
2.4 DÉFINITION D'UNE MENACE EXTERNE DANS LE CONTEXTE DU CLOUD
2.5 EXPOSITION SPÉCIFIQUE DU CLOUD PUBLIC AUX MENACES EXTERNES
2.6 RISQUES INHÉRENTS À LA MENACE EXTERNE

3. QUELS OUTILS POUR COUVRIR LES MENACES 10
3.1 DES OUTILS DÉJÀ PRÉSENTS DANS VOTRE SYSTÈME D'INFORMATION
3.1.1Durcissement
3.1.2 Scanners
3.1.3 Détection
3.1.4 Réponses
3.2 DES OUTILS TRADITIONNELS POUVANT ÊTRE LIMITÉS DANS LE CLOUD
3.2.1 Différences d'environnement notables
3.2.2 Complexité à corréler les signaux
3.2.3 De nouveaux outils pour répondre aux besoins de sécurité du Cloud
3.3 LES PLATEFORMES CNAPP
3.3.1 Qu'est-ce qu'une CNAPP ?
3.3.2 Détection des comportements anormaux et réponse à incident
3.3.3 Comment la CNAPP répond-t-elle aux besoins de sécurité ?
3.3.4 Comment ces différents modules travaillent-ils ensemble pour offrir une plateforme de sécurisation complète ?
3.3.5 Focus « Application & Development Life Cycle »
3.3.6 « Posture Management »
3.3.7 Focus « Détection & Réponse aux menaces »
3.3.8 Choisir et adopter une solution CNAPP
3.4 QUELLE STRATÉGIE ADOPTÉE ?

4. QUELLE GOUVERNANCE ASSOCIÉE ? 26
4.1 OBJECTIFS DE LA GOUVERNANCE DE LA SÉCURITÉ DU CLOUD
4.2 PRINCIPES DE LA GOUVERNANCE DE LA SÉCURITÉ DU CLOUD
4.3 BONNES PRATIQUES POUR LA GOUVERNANCE DE LA SÉCURITÉ DU CLOUD

5. TENDANCES FUTURES 28

6. CONCLUSION 29

7. GLOSSAIRE 30

1. INTRODUCTION

Le Cloud est aujourd'hui présent dans la plupart des organisations, quelles que soient leurs activités et leur volume d'affaire.

En effet, d'après le rapport de CISCO 2022, 92 % des entreprises questionnées utilisent plusieurs Clouds publics pour en exploiter tout le potentiel et améliorer l'agilité opérationnelle, la sécurité, la performance des applications et la résilience de leurs opérations.

L'utilisation de ce type de solution génère cependant de nouvelles problématiques de sécurité liées à l'évolution de la surface d'attaque du système d'information (exposition sur Internet, mauvaises configurations, etc.). Plusieurs options de sécurité s'offrent alors aux organisations :

- Utiliser les outils traditionnels, qui peuvent néanmoins être limités sur le Cloud,
- Utiliser un outil spécialisé de type CNAPP (Cloud Native Applications Protection Platform),
- Hybrider des outils traditionnels avec un CNAPP.

Ce livret a pour ambition de vous présenter de façon synthétique un panorama de ces solutions et un guide de choix en fonction de vos contraintes. Il s'adresse à tout acteur confronté à la problématique de sécurisation de ses applications Cloud. Il vise cependant tout particulièrement les PME / ETI souvent moins aguerries sur ces sujets en raison de leurs ressources plus limitées.

Nous détaillerons dans un premier temps le périmètre abordé ainsi que les termes et les concepts utilisés dans ce document. Nous développerons ensuite les types de menaces à détecter. Nous présenterons, dans un troisième temps les outils disponibles pour couvrir les besoins puis nous fournirons des bonnes pratiques et des exemples de gouvernances associées à la mise en œuvre de ces outils. Nous terminerons avec une vision prospective de notre sujet intégrant notamment les besoins émergents.

Bonne lecture !

2. LES MENACES À DÉTECTER

2.1 DÉFINITION D'UNE MENACE INTERNE

Dans le cadre de la sécurité de l'information, un agent menaçant est toujours présent. Il peut s'agir d'un acteur humain, d'un agent numérique ou d'un contexte environnemental défavorable. En ne se focalisant que sur l'aspect humain comme source de menace, une dissociation est réalisée entre la menace humaine interne à l'organisation et qui dispose de droits et privilèges sur le système d'information et la menace dite externe; car sans légitimité d'accès sur le système d'information ciblé.

2.2 PROFILS DES ATTAQUANTS INTERNES

La menace interne est considérée comme étant la principale source de menaces en termes de fréquence et donc de probabilité d'attaque sur les systèmes d'information. Le potentiel d'attaque associé à cette source de menace diffère selon le profil technique ou hiérarchique de l'attaquant, les accès qui lui sont consentis. A ce titre, l'impact d'une attaque interne présente des niveaux différents selon les paramètres qui la caractérise tels que la motivation de l'attaquant, les ressources mobilisables, le temps accordé à la préparation et à l'exécution de l'attaque, l'expertise de l'attaquant ou celle qui est à sa disposition.

Sur ce dernier point, la connaissance est souvent un des éléments qui rendra une attaque interne plus pertinente et donc plus aboutie. En effet, l'attaquant interne agit dans un environnement qui est le sien et donc qu'il domine. De plus, il se définit comme étant un acteur clairement identifié au sein de la structure et donc qui bénéficie d'un accès légitime à certaines ressources du système d'information, avec des privilèges plus ou moins élevés. En effet, selon que l'attaquant détient un profil associé à des privilèges étendus sur les ressources du système d'information ou pas, la facilité et la profondeur d'action peuvent être plus ou moins importantes.

Une liste théorique de profils d'attaquants internes peut ainsi être dégagée :

- L'utilisateur bureautique travaillant dans des domaines transverses, ne bénéficiant ni de connaissances poussées du système d'information, ni de privilèges élevés sur les ressources.
- Le gestionnaire métier avec des accès privilégiés à certaines ressources.
- L'exploitant.
- L'administrateur.
- L'utilisateur temporaire de type stagiaire ou autre.

Cette distinction en profil n'a de sens que dans le cas où l'organisme a recours aux bonnes pratiques de sécurité en termes de gestion des identités et de gestion fine des droits. En effet, si l'accès aux ressources n'est pas restreint par défaut, il peut être considéré qu'un seul rôle opère sur le système d'information.

2.3 RISQUES INHÉRENTS À LA MENACE INTERNE

1.Menace sur les API de gestion et de provisionnement (management plane)

Dès lors qu'un attaquant interne dispose de privilèges sur les infrastructures, il peut modifier les paramètres de configuration ou divulguer des éléments sensibles tels que des clés de chiffrements ou des secrets. La finalité d'une attaque interne au niveau des API et du provisionnement peut être une remise en cause du fonctionnement nominal de la plateforme ou l'ouverture d'un accès à destination d'un attaquant externe. Dans ce cas, l'attaque interne rentrera dans la catégorie des prérequis pour l'attaquant externe et sera à ce titre la première phase du mode opératoire de l'attaque externe.

En substance, l'attaque interne peut amoindrir le niveau de contrôle des accès distants ou livrés des secrets qui permettront d'utiliser les API par une faiblesse des mesures de sécurité ou grâce à la mise à disposition de moyens légitimes.

Si l'attaquant interne monte son attaque sans complicité externe, la motivation est principalement soit une atteinte au fonctionnement de la plateforme, soit une fuite des données. Selon les modalités d'attaque utilisées, l'attaquant interne pourra rendre impossible toute scalabilité de la plateforme et ainsi remettre en cause sa résilience de la plateforme. Pour ce qui est de la fuite de données, l'attaquant interne pourra directement extraire de la donnée via une API, sous la forme d'un flux légitime notamment.

2. Risques de « Lock-in » et de disponibilité du fournisseur

L'attaquant interne peut disposer de privilèges élevés sur la plateforme mais également n'être qu'un simple utilisateur bureautique, sans privilèges particuliers au niveau de la plateforme logique ou physique. Toutefois, l'attaquant interne peut détenir un rôle organisationnel et décisionnel majeur et à ce titre, avoir des impacts négatifs sur la sécurité de la plateforme si ses choix ne sont pas éclairés et pertinents.

En effet, s'agissant de la sélection des fournisseurs, par exemple, une analyse succincte voire inexistante du niveau d'adhérence avec un fournisseur peut conduire à une remise en cause ponctuelle ou durable dans la délivrance des services ceci peut avoir une incidence sur la survie de l'entité dans le cas où des précautions suffisantes et des solutions de repli n'ont pas été prises en amont.

3. Risques sur la souveraineté et sur la localisation des données (réglementaires)

Comme pour le cas d'un « Lock-in » vu précédemment, la maîtrise des choix techniques et leur validation préalable permettent de s'affranchir de déconvenues telles que le non-respect de la législation et de la réglementation opposable.

Dans le cas de l'attaquant interne qui dispose de pouvoirs décisionnels ou techniques et qui ne respecterent pas les obligations juridiques soit dans ses choix ou dans ses pratiques, fait peser l'organisation et son dirigeant un risque de condamnation et d'amende substantielle.

L'évolution du cadre juridique actuel tend à clarifier et à généraliser le principe de souveraineté des données, avec des contraintes fortes en termes de lieu de stockage de l'information et de contrôle d'accès à ces données.

4. Mauvaise configuration des équipements

La configuration des équipements est une activité majeure qui nécessite d'être définie, validée et contrôlée dans le temps. Toute mauvaise configuration peut engendrer des dysfonctionnements et rendre inefficace toute mesure de protection.

Toute administration, exploitant ou responsable hiérarchique qui viendrait à négliger les phases de validation et de recette de ces configurations, qui n'assurerait pas la sauvegarde de ces configurations ou le contrôle de leur changement dans le temps, apparente son manque de rigueur à une attaque interne.

2.4 DÉFINITION D'UNE MENACE EXTERNE DANS LE CONTEXTE DU CLOUD

Une **menace externe** est toute tentative malveillante ou accidentelle d'interruption, d'accès non autorisé ou d'exploitation d'un système d'information provenant de l'extérieur de l'organisation. Contrairement aux menaces internes (qui proviennent de l'intérieur de l'entreprise, par exemple des employés ou des partenaires), les menaces externes viennent d'individus, de groupes ou de forces non affiliées à l'organisation.

2.5 EXPOSITION SPÉCIFIQUE DU CLOUD PUBLIC AUX MENACES EXTERNES

Le **Cloud public** présente certaines caractéristiques qui le rendent potentiellement plus exposé aux menaces externes, mais aussi quelques aspects qui, paradoxalement, peuvent le rendre plus sécurisé.

1. Surface d'attaque plus large :

- Le cloud public est accessible via internet, ce qui élargit la surface d'attaque comparé aux infrastructures sur site, notamment en raison du nombre croissant de points d'entrée accessibles aux attaquants.
- Les entreprises utilisant le Cloud ne contrôlent pas directement les infrastructures physiques ou les plateformes, ce qui peut rendre plus complexe la gestion de la sécurité.

2. Mutualisation des ressources :

- Le Cloud public fonctionne souvent selon un modèle de mutualisation des ressources, ce qui signifie que plusieurs utilisateurs partagent les mêmes infrastructures physiques. Bien que des mécanismes de séparation soient en place, une faille dans l'isolation des utilisateurs pourrait permettre à une attaque visant un utilisateur d'en affecter d'autres.

3. Accès à distance :

- Le Cloud étant accessible de n'importe où, cela permet une grande flexibilité pour les utilisateurs, mais ouvre également la porte à des attaques à distance, comme le phishing ou le détournement de sessions, surtout si des pratiques de sécurité faibles sont mises en œuvre (comme l'utilisation de mots de passe simples ou le manque de multi-authentification).

4. Responsabilité partagée :

- Dans le Cloud public, le fournisseur de services Cloud est responsable de la sécurité de l'infrastructure (sécurité physique, pare-feu, etc.), mais l'entreprise cliente est responsable de la sécurité de ses propres données, configurations, et de l'accès à ses applications. Cette responsabilité partagée peut parfois créer des zones grises et des vulnérabilités si les deux parties ne prennent pas les mesures adéquates.

5. Automatisation et gestion à grandes échelles :

- Les services de Cloud public sont conçus pour s'adapter à de grandes échelles, ce qui peut compliquer la détection des anomalies et des menaces en temps réel, surtout dans des environnements massifs et automatisés.

2.6 RISQUES INHÉRENTS À LA MENACE EXTERNE

1. Vulnérabilités au niveau des hyperviseurs

Ce risque est lié à la mutualisation des ressources. L'hyperviseur est la technologie permettant d'assurer l'isolation des ressources entre différents clients. Si cet hyperviseur présente une vulnérabilité, un attaquant peut potentiellement « sortir » de sa machine virtuelle (VM Escape) et accéder à d'autres VM d'autres clients hébergés sur le même serveur physique.

2. Menace sur les API de gestion et de provisionnement (management plane)

Ce risque est lié à la manière dont le Cloud est géré à travers des API mais aussi à l'exposition de la console d'administration sur Internet (menace liée à l'accès à distance et à la gestion automatique). Ces interfaces de gestion (API et console) sont particulièrement critiques car elles permettent de provisionner les différentes ressources mais, aussi de gérer les clefs utilisées et les firewalls de l'infrastructure.

Les acteurs externes pourront tenter de prendre le contrôle de l'infrastructure à travers la console de gestion tandis que les acteurs internes pourront modifier le code d'infrastructure (IaC) utilisé pour créer cette dernière.

3. Risque « d'Effet domino » lié à une faille du fournisseur de Cloud

Beaucoup d'entreprises sont hébergées sur les mêmes infrastructures dans les mêmes sites. En cas de panne d'un site, beaucoup de clients tenteront de migrer en même temps vers un site de repli. Si les ressources sont en nombre insuffisantes dans le site de repli, tous les clients ne pourront pas exécuter leur DRP (Disaster Recovery Plan) et pourront donc être victime de Déni-De-Service.

De même, une faille affectant un service ou un middleware affectera beaucoup de clients d'un seul coup et limitera l'assistance que le fournisseur de Cloud peut apporter à chaque client.

4. Dé-provisionnement et effacement de données incomplets

Quand un contrat Cloud se termine ou lorsqu'une entreprise cesse d'utiliser une ressource, cette entreprise est dépendante des pratiques et garanties du fournisseur pour s'assurer que les données sont réellement effacées et pas seulement inaccessibles.

5.Visibilité limitée (log, monitoring)

Cette menace liée à la responsabilité partagée résulte de l'opacité de certaines couches d'infrastructure Cloud qui ne sont pas accessibles aux clients. Par exemple, le client ne pourra pas avoir accès à des logs critiques comme ceux de l'hyperviseur ou encore des firewalls physiques. Ce manque de visibilité entrave les capacités d'audit et de détection d'incidents (qui pourront être manquées ou détectées tardivement).

3. QUELS OUTILS POUR COUVRIR LES MENACES

3.1 DES OUTILS DÉJÀ PRÉSENTS DANS VOTRE SYSTÈME D'INFORMATION

La majorité des menaces mentionnées dans «*Les menace à détecter*» existent dans vos environnements on-premise. Ainsi, de nombreux outils peuvent déjà être présents pour y remédier. Ces derniers répondent à plusieurs objectifs :

- **Durcir** votre système d'information en appliquant une configuration sécurisée.
- **Scanner** les composantes du système d'information pour identifier la surface d'attaque (exposition Internet, vulnérabilités exploitables, etc.).
- **Détecter** les comportements malveillants en temps réel.
- **Répondre** aux menaces via la génération d'alertes et remédiation manuelle ou automatique.

3.1.1 Durcissement

Un défaut de configuration peut être exploité par un attaquant. Pour prévenir, des gestionnaires de configuration existent. Ces derniers permettent d'appliquer une configuration uniforme à un ensemble de composants du système d'information. Il est par exemple commun d'avoir une même configuration appliquée à l'ensemble des stations de travail.

Utiliser ces outils facilite la maîtrise de vos configurations. D'une part grâce à un déploiement centralisé de la configuration, d'autre part en facilitant le contrôle dans le temps. L'audit pouvant être effectué sur la configuration témoin en complément d'une vérification du taux de couverture.

Exemple : les *Group Policy Object (GPO)* pour les serveurs et stations de travail Windows.

3.1.2 Scanners

La surface d'attaque de votre système d'information peut être divisée en deux parties : externe et interne.

L'externe correspond à un attaquant n'ayant pas d'accès à votre système d'information. Il doit donc trouver un moyen d'y pénétrer. Afin de couvrir ce risque, les External Attack Surface

Management (EASM) permettent de scanner les actifs exposés sur Internet. Il s'agit de surveiller et de sécuriser l'empreinte numérique accessible au public, y compris les sites web, les serveurs, les API et les services Cloud.

A contrario, l'interne suppose que l'attaquant est déjà dans votre système d'information. Son but est donc de s'élever en privilège en se concentrant sur des machines vulnérables. Le Common Vulnerabilities and Exposures (CVE) référence l'ensemble des vulnérabilités connues. Pour en assurer la remédiation, les outils de gestion de vulnérabilités permettent d'identifier les composantes systèmes vulnérables et assure la traçabilité de remédiation.

Pour les applications spécifiquement, il existe plusieurs tests :

1. Statique (SAST) : examine le code source à la recherche de vulnérabilités connues sans exécuter le programme.
2. Dynamique (DAST) : effectue une analyse de sécurité pendant l'exécution de l'application.
3. Interactif (IAST) : combine le SAST et DAST.

3.1.3 Détection

Chaque action sur votre système d'information peut être tracée. Il devient alors intéressant de définir les signaux liés à un comportement suspect pour le détecter au plus tôt.

Certains outils spécialisés intègrent une capacité de collecte des informations, corrélation et génération d'alertes. C'est le cas de l'Endpoint Detection and Response (EDR) pour les stations de travail et serveurs, ainsi que Network Detect and Response (NDR) pour le réseau.

La multitude d'outils et signaux à collecter peut néanmoins poser un problème. De plus, vos équipes peuvent avoir besoin de créer des alertes personnalisées non couvertes par les outils cités ci-dessus.

Pour répondre à cela, l'outil Security Information and Event Management (SIEM) permet de centraliser les signaux et alertes d'autres outils, ainsi que la création de nouvelles alertes.

3.1.4 Réponses

Une fois en capacité de détecter les évènements malicieux, il faut pouvoir y répondre. Pour des écosystèmes minimalistes, cela peut faire sens de traiter chaque alerte manuellement. Dès que l'on passe à des environnements plus vastes, cela peut vite devenir compliqué sans outils. Pour répondre au besoin, les Security Orchestration Automation and Response (SOAR) permettent d'automatiser les réponses pour les alertes les plus fréquentes par exemples. De même, les outils de gestions de tickets permettront d'orchestrer la remédiation entre les différentes équipes.

3.2 DES OUTILS TRADITIONNELS POUVANT ÊTRE LIMITÉS DANS LE CLOUD

3.2.1 Différences d'environnement notables

L'environnement Cloud est, par définition, différent de l'on-premise. Le tableau ci-dessous détails les principales différences.

	Cloud Public	On-premise
Scalabilité	**Caractéristique** : Hautement dynamique. Les ressources (machines virtuelles, conteneurs, micro-services) sont créées, modifiées et supprimées rapidement selon la demande. **Impact** : Maintenir un inventaire fiable et un taux de couverture des outils est complexe.	**Caractéristique** : Les infrastructures sont plus fixes, et les ressources sont souvent prévisibles et moins fluctuantes. **Impact** : Le travail d'inventaire et de couverture des outils est moins complexe.
Responsabilité	**Caractéristique** : Modèle de responsabilité partagée entre le fournisseur de services Cloud et l'utilisateur. **Impact** : Les outils doivent s'adapter aux offres PaaS, IaaS et SaaS.	**Caractéristique** : L'entreprise est responsable de toute la pile de sécurité, de l'infrastructure aux applications. **Impact** : Les outils sont conçus pour un contrôle complet de bout en bout.
Gestion de la configuration	**Caractéristique** : La majorité des services Cloud proposent une gestion de configuration « clic bouton » pouvant être automatisé via scripts. **Impact** : Les erreurs de configurations sont plus probables. L'exposition de vos ressources sur Internet, par exemple, peut s'effectuer en quelques clics.	**Caractéristique** : La gestion de la configuration demande un niveau d'expertise plus élevé. **Impact** : L'environnement on-premise est plus mature et statique. La surface d'attaque est généralement maîtrisée.

3.2.2 Complexité à corréler les signaux

Les outils classiques adressent unitairement les menaces. Il est alors complexe de corréler les signaux unitaires pour affiner la compréhension d'une attaque de bout en bout. Prenons l'exemple de l'attaque d'un serveur Windows : une vulnérabilité connue permet à un attaquant de compromettre entièrement le serveur. Cela nécessite à minima deux outils pour comprendre la chaîne :

1. Gestionnaire de vulnérabilité : être capable d'identifier préventivement la vulnérabilité.
2. EDR : identifier le comportement suspect en temps réel.

Chaque outil répondant à son besoin, il est à votre charge de corréler ces évènements pour comprendre l'attaque.

3.2.3 De nouveaux outils pour répondre aux besoins de sécurité du Cloud

La singularité des environnements Cloud couplé à un besoin grandissant de vision plateforme a permis à de nouvelles solutions de sécurité d'émerger, les Cloud Native Application Protection Platform (CNAPP). La prochaine partie de l'article en détail les objectifs et le fonctionnement.

3.3 LES PLATEFORMES CNAPP

De nombreux acteurs proposent des plateformes de sécurité dédiées à la sécurisation des environnements cloud.

Ces plateformes sont appelées des CNAPP (Cloud-Native Application Protection Platforms), qui est un terme créé par le Gartner en 2021 pour décrire une plateforme proposant plusieurs modules de sécurité, dans le but de protéger, détecter et répondre aux menaces de sécurité pesant sur le Cloud.

3.3.1 Qu'est-ce qu'une CNAPP ?

Une Cloud-Native Application Protection Platform (CNAPP) est une plateforme unifiée conçue pour sécuriser les environnements cloud-native. Ils incluent des applications et des services développés sous les principes Cloud-Native comme les conteneurs, les microservices, l'infrastructure en tant que code (IaC), et les fonctions serverless. Le CNAPP intègre plusieurs solutions de sécurité cloud pour offrir une protection complète, couvrant tant la sécurité de l'infrastructure que celle des applications.

Sécurité de l'Infrastructure du Socle d'Hébergement
Cette composante vise à valider la sécurité de l'infrastructure Cloud sous-jacente, qui héberge les applications et les données. Cela inclut la gestion des identités et des accès (IAM) pour s'assurer que seules les entités autorisées accèdent aux ressources critiques et la sécurisation des réseaux pour prévenir les accès non autorisés et mouvements latéraux non maitrisés. Il vérifie que les bonnes pratiques de sécurité sont en place afin de garantir la disponibilité, l'intégrité, la confidentialité des données et de l'infrastructure. Enfin il collecte les événements se produisant sur l'environnement pour assurer la surveillance en continu et alerter de potentielles menaces.

Sécurité Applicative et Intégration DevSecOps(Shift Left)
Cette composante se concentre sur la sécurisation des applications elles-mêmes, ainsi que sur l'intégration des pratiques de sécurité dès le début du cycle de développement, conformément aux principes DevSecOps.
Elle implique l'intégration d'outils de sécurité dans le pipeline CI/CD pour automatiser les contrôles de sécurité à chaque étape du développement. Cela inclut des scans du code applicatif et du code de déploiement afin de détecter les vulnérabilités, les erreurs de configuration et les données sensibles le plus tôt possible, avant le déploiement.

3.3.2 Détection des comportements anormaux et réponse à incident

La détection des comportements anormaux repose sur l'analyse continue des activités pour identifier des anomalies signalant des menaces potentielles. En utilisant des techniques de machine learning et d'analyse comportementale, le système établit une ligne de base des comportements normaux et détecte toute déviation significative. Les outils de surveillance analysent en temps réel les logs, les accès utilisateurs et les flux réseau, générant des alertes en cas de comportements suspects.

Ces alertes sont intégrées aux SOC, permettant une réponse rapide et coordonnée aux incidents. Les équipes de sécurité peuvent alors mener des investigations approfondies sur les ressources concernées et activer des «boutons rouges» prédéfinis pour neutraliser les menaces en fonction de leur criticité.

3.3.3 Comment la CNAPP répond-elle aux besoins de sécurité ?

Une plateforme CNAPP regroupe plusieurs modules spécialisés pour assurer une protection complète des environnements Cloud-native. Chaque module a une fonction spécifique et participe à la sécurité globale de l'infrastructure et des applications.

3.3.4 Module de gestion de la posture de sécurité

- **CSPM : Cloud Security Posture Management**
  En plus des traditionnels scanner de vulnérabilité, ce module permet de cartographier et d'analyser la configuration des services Cloud, de l'infrastructure, des machines et des applications afin d'identifier et résoudre les mauvaises configurations qui peuvent exposer les ressources à des risques.

- **DSPM : Data Security Posture Management**
  Ce module se concentre sur la sécurisation des données tout d'abord en les cartographiant puis en analysant les accès à la recherche d'anomalies, assurant ainsi la confidentialité et l'intégrité des données sensibles.

- **ASPM : Application Security Posture Management**
  Ce module donne accès à un large éventail de solutions de test AppSec, notamment les tests statiques de sécurité des applications (SAST), les tests dynamiques de sécurité des applications (DAST) à la recherche de vulnérabilité applicative. Il permet aussi l'analyse de la composition des logiciels (SCA) permettant de donner une visibilité permanente sur les risques de sécurité.

- **SDLC-SP : Software Development Life Cycle Security Posture**
  Ce module intègre des pratiques de sécurité tout au long du cycle de vie du développement logiciel. Il assure qu'à chaque phase du projet (développement, compilation, déploiement, exploitation) on puisse détecter de potentiels problèmes de sécurité dans le but de les corriger au plus tôt, évitant l'effet tunnel et le report des corrections à des livraisons ultérieures.

- **CIEM : Cloud Infrastructure Entitlement Management**
  Ce module analyse les identités et les autorisations pour s'assurer que seules les entités autorisées ont accès aux ressources critiques et qu'il n'existe pas de chemin de compromission via l'accumulation de rôles et permissions non maitrisés. Il permet également de se conformer au principe de moindre privilège en garantissant que chaque identité à le bon niveau de droit.

- **CDR : Cloud Detection & Response**
  Ce module fournit des capacités de détection et de réponse pour identifier rapidement les menaces au niveau des interfaces de management de l'infrastructure (control plane) et au niveau des interfaces de données (data plane). Il permet également de réagir de manière appropriée aux menaces en donnant les outils nécessaires pour stopper ou réduire l'impact d'un incident de sécurité.

- **CWPP : Cloud Workload Protection Plateform**
  Ce module assure la protection des charges de travail dans les environnements Cloud (machines virtuelles, conteneurs) en détectant et bloquant les menaces via une visibilité sur le système de fichier, les processus exécutés, les opérations réseaux et les appels systèmes.

3.3.4 Comment ces différents modules travaillent-ils ensemble pour offrir une plateforme de sécurisation complète ?

Focus « Cloud Security Posture Management »

Bien que **la sécurité doive être prise en compte au plus tôt dans le cycle de vie du projet (Shift Left)**, les fonctionnalités de « security posture management » sont parmi les premiers modules que l'on utilise pour sécuriser son infrastructure Cloud. En effet, après une première étape de construction de la « landing zone » et des premiers déploiements applicatifs, les équipes sécurité vont chercher à gagner en visibilité face à une infrastructure cloud qui devient de plus en plus étendue et complexe. L'utilisation de ce module est accélérée également par sa simplicité de mise en œuvre, basé sur un connecteur simple et permettant au CNAPP de solliciter les API du Cloud provider pour y récupérer tous les déploiements et configuration des services, ainsi que la possibilité de réaliser des scans de sécurité.

Connecter et activer les modules de gestion de la posture de sécurité à son infrastructure Cloud la toute première fois, révèle une masse non négligeable de findings (vulnérabilités et misconfigurations). Il y a alors **une dette de sécurité à remédier que l'outillage CNAPP doit nous permettre de prioriser notamment au travers du module CSPM.**

Le Cloud Security Posture Management (CSPM) est un module essentiel pour la gestion de la sécurité dans les environnements Cloud. Il comporte plusieurs fonctionnalités de base :

- **Inventaire des ressources** Cloud et des configurations.
- **Scanner de vulnérabilité** sur les registres de code, d'image et les workloads.
- **Analyse et prévention des configurations** dangereuses et non conformes aux bonnes pratiques (misconfigurations) sur les services Cloud, les charges de travail, les applications.
- **Revue de conformité** de l'environnement Cloud vis-à-vis des référentiels de sécurité (benchmark et politiques de sécurité interne).
- **Analyse de la surface d'exposition** des ressources.

Cartographier les services et ressources

Le CNAPP fournit une visibilité complète des ressources Cloud et de leurs configurations. Cela commence par un inventaire exhaustif, rendu possible grâce à des connecteurs qui, avec des permissions étendues sur l'infrastructure Cloud, découvrent les ressources et configurations via leurs APIs respectives.

Scanner les ressources

Les CSPM disposent également de scanners de workload sans agent, permettant de récupérer les configurations systèmes (OS, services systèmes et réseaux), détecter les vulnérabilités dans les logiciels et librairies, et identifier des secrets ou données sensibles. Ces scanners utilisent des fonctionnalités de snapshot ou d'image, permettant d'inspecter les machines ou conteneurs de manière indépendante sans affecter leur fonctionnement. Pour assurer une sécurité continue, les scans de configuration et de vulnérabilité sont effectués dès la création de la ressource, lors de ses modifications et à intervalles réguliers par la suite. Cette surveillance continue assure que toute nouvelle vulnérabilité ou configuration incorrecte est rapidement identifiée et résolue.

Analyser la conformité

Les configurations découvertes sont analysées et comparées à un ensemble de règles de conformité issues de plusieurs sources, telles que les standards internationaux de sécurité (CIS, OWASP, NIS, CSA, PCI DSS, etc.), les cybermenaces identifiées par les éditeurs (« Cyber Threat Intelligence ») ou encore des règles personnalisées qui reflètent les politiques de sécurité spécifiques de l'entreprise.

Ces analyses permettent aux équipes de gouvernance de la sécurité d'obtenir une vision claire et documentée de la conformité de l'infrastructure Cloud. Les règles de conformité aident à identifier et atténuer plusieurs risques de sécurité appelé « findings » :

- Exposition non maitrisée des ressources.
- Rôles IAM et permissions excessivement larges.
- Secrets non protégés.
- Données sensibles non protégées ou trop largement accessibles.
- Absence de configurations de sécurité recommandées.

Analyser les risques pour prioriser les actions de remédiation

Une fois que la base de données des ressources Cloud et des findings associés (misconfigurations, vulnérabilités, ressources sensibles exposées…) est établie, la plateforme doit évaluer le risque global permettant aux équipes sécurité de prioriser les actions de remédiation. En effet, il est souvent impossible de corriger tous les findings immédiatement, et certains d'entre eux représentent des risques plus graves que d'autres. L'accent doit être mis sur les menaces de sécurité, c'est-à-dire la combinaison de plusieurs findings qui ensemble augmentent significativement le risque. Nous pouvons donner quelques exemples de combinaison de findings :

- Une vulnérabilité critique, dont l'exploit est connu, est détecté sur un workload exposé à un internet.
- Une clé d'accès détectée dans une ressource permettant d'accéder à une autre ressource contenant des données sensibles (stockage, base de données…).
- Un compte de service donnant accès à des permissions d'administrations avancées de ressources cloud et pouvant être utilisé à partir d'une ressource accessible par beaucoup d'utilisateur.

Ces combinaisons révèlent des scénarios où les findings individuels se combinent pour créer des menaces plus significatives, nécessitant une priorisation stricte et une remédiation proactive pour garantir la sécurité de l'infrastructure Cloud.

3.3.5 Focus « Application & Development Life Cycle Posture Management »

L'Application & Development Life Cycle Posture Management est essentiel pour garantir que la sécurité est intégrée tout au long du processus de développement. Cette approche permet de détecter et de résoudre les problèmes de sécurité avant qu'ils ne soit déployés, évitant ainsi l'effet tunnel et réduisant les efforts de remédiation a posteriori. Elle permet également d'appliquer des politiques de sécurité strictes afin de bloquer les déploiements non conformes et d'identifier l'origine des problèmes et les équipes de développement qui en sont responsables.

Scanner le code développé

Grâce à des modules intégrés directement dans l'environnement de développement (IDE) ou dans le gestionnaire de code source (VCS), la plateforme CNAPP va être en capacité de scanner le code source développé à la recherche de problèmes de sécurité via différents tests :

- **Les tests de sécurité statiques (SAST) :** analysent le code source de l'application pour détecter les vulnérabilités avant même que le code ne soit exécuté. Ils permettent de repérer des problèmes tels que ceux identifiés par l'OWASP Top Ten : injection SQL, Cross-Site Scripting, Secrets…

- **L'analyse de la composition des logiciels (SCA) :** L'analyse SCA scrute les bibliothèques et les dépendances utilisées dans le code pour identifier les composants vulnérables et obsolètes.

- **Les scanner IAC :** vérifient le code utilisé pour déployer l'infrastructure afin d'assurer que les configurations sont sécurisées et n'exposent pas les ressources à des risques non maitrisés. Les CNAPP offrent généralement la possibilité de créer des politiques de sécurité contrôlant que certaines « misconfigurations » ne puissent être déployées en production.

Scanner l'application déployée

- **Les tests de sécurité dynamiques (DAST) :** analyse les applications en cours d'exécution, permettant de découvrir les vulnérabilités lorsque l'application interagit avec des utilisateurs ou d'autres systèmes. Le type de scanner est capable de détecter des problèmes liés à l'authentification et la gestion des sessions ou encore des API non sécurisées pouvant entrainer des fuites de données ou des accès non autorisés.

Focus Détection & Réponse aux menaces

Malgré les bonnes pratiques de sécurité implémentées grâce aux modules de CSPM, certains risques continuent à peser sur l'infrastructure Cloud. Ces risques peuvent être atténués au travers d'une détection et réponse adaptée aux environnements Cloud.

Surveillance et Détection dans un environnement Cloud

En matière de détection cloud, il est important d'inclure plusieurs composantes dans le scope de surveillance pour assurer une sécurité optimale. Les trois grandes composantes à surveiller sont les suivantes :

1. **Le Control Plane (gestion des services cloud)** : Ce composant inclut les services de gestion de l'infrastructure Cloud comme la gestion de l'identité et des accès (IAM), la gestion des réseaux, ainsi que d'autres services clés qui contrôlent l'architecture et la sécurité du cloud.

La surveillance du control plane permet de détecter et de répondre aux modifications non autorisées de l'infrastructure, aux accès non conformes et aux configurations potentiellement dangereuses.

2. Le Data Plane (gestion des données): Ce composant correspond aux services de traitement et de stockage des données. Il englobe les bases de données, le stockage d'objets, les fonctions ou applications qui traitent directement les données des utilisateurs et des applications. La surveillance du data plane vise à identifier les activités suspectes ou anormales liées à l'accès aux données, aux transferts de données, et aux opérations de traitement.

3. Les Workloads (charges de travail): Cela inclut l'hébergement des applications comme les machines virtuelles, les conteneurs, les fonctions et autres unités de traitement des tâches dans le Cloud. La surveillance des workloads permet de repérer les comportements inhabituels ou non conformes des applications, de détecter des logiciels malveillants, et de vérifier l'intégrité des systèmes en temps réel.

Détecter les comportements malveillants sur le Control Plane & Data plane

La surveillance du Control Plane et du Data Plane est cruciale pour identifier et répondre aux menaces potentielles dans un environnement Cloud. Cela passe par l'ingestion et l'analyse de tous les événements Cloud, notamment ceux relatifs aux appels API, qu'ils proviennent d'un accès programmatique (CLI, SDK, IAC) ou de l'utilisation de la console d'administration. Ces modules sont souvent désignés sous le terme de CDR (Cloud Detection and Response).

Le CDR est connecté à l'infrastructure Cloud, souvent via un service de notification et de file de messages, et reste en attente de nouveaux événements (logs). Une fois notifié, le CDR récupère les logs à partir d'un service de stockage sécurisé du fournisseur Cloud. Il peut alors analyser les métadonnées des événements pour détecter des indices d'attaque (IOA), en se basant sur plusieurs facteurs comme :

- La criticité de l'opération effectuée.
- L'identité de l'appelant (par exemple, l'adresse IP et le rôle attribué).
- L'analyse des événements antérieurs pour identifier des patterns de menace.

Les CDR les plus avancés intègrent des capacités de machine learning pour établir une baseline de comportements normaux et détecter les anomalies. Cette technologie permet de repérer des comportements suspects qui pourraient échapper aux méthodes de détection traditionnelles basées sur des signatures statiques. Au-delà du machine

learning, ces systèmes peuvent également exploiter des capacités d'intelligence artificielle pour effectuer des analyses prédictives et renforcer la détection des menaces complexes.

De plus, la performance d'un CDR repose aussi sur l'intégration d'une solide base de Cyber Threat Intelligence (CTI). Une CTI robuste inclut des informations sur la réputation des IP, des patterns connus d'attaques et des signatures de menaces. Elle doit être continuellement mise à jour pour refléter les dernières menaces et techniques émergentes.

Un aspect critique souvent sous-estimé est la capacité de ces systèmes à fournir des réponses automatisées ou semi-automatisées en cas de détection d'anomalies. Ces réponses peuvent inclure :

- **Isolation automatique des ressources compromises** : pour limiter la propagation de la menace.
- **Révocation des accès compromis** : pour empêcher l'utilisateur ou le système compromis d'exercer davantage d'actions malveillantes.

  Alertes et notifications en temps réel : pour informer les équipes de sécurité, facilitant une intervention rapide.

Détecter les comportements malveillants sur les workloads (agent CWPP)

Une approche pour la détection des comportements malveillants sur les workloads pourrait être la simple collecte des logs systèmes à la manière d'un SIEM (Security Information and Event Management) couplée à des règles de détection. Cette méthode se limite à centraliser et analyser les journaux d'événements générés par les workloads. Bien que cette approche soit moins coûteuse, elle ne fournit pas une couverture complète et efficace pour détecter les menaces avancées.

Afin d'assurer une sécurité optimale, une approche plus intensive et couvrante consiste à utiliser des agents installés sur les workloads pour une surveillance complète et en temps réel, tout en mettant en œuvre des capacités de blocage plus ou moins fortes selon la typologie des menaces.

Une solution **CWPP (Cloud Workload Protection Platform)** intègre idéalement les fonctionnalités d'un agent EDR (Endpoint Detection and Response), tout en ajoutant des capacités Cloud Native comme la **détection sur les nœuds Kubernetes** pour surveiller l'exécution des conteneurs, ainsi que la détection des usages des services Cloud à travers les workloads. Il est à noter que les agents utilisent

de plus en plus la technologie eBPF moins intrusif sur le noyau du système d'exploitation et donc limite les risques de problèmes système.

Ces agents sont configurés pour collecter et rapporter en temps réel diverses informations comme **les logs du système d'exploitation, les activités réseau** (connexions entrantes et sortantes, les ports utilisés), **les activités des processus, les modifications des fichiers.**

La télémétrie collectée par les agents est ensuite remontée au module CDR (Cloud Detection and Response) pour enrichir les événements liés aux workloads avec des informations supplémentaires. Cela inclut des données antérieures ou ultérieures d'accès potentiellement malveillants ou de déplacements latéraux, permettant ainsi de :

- **Tracer un chemin de compromission** : identifier les étapes et les moyens par lesquels une attaque s'est propagée dans le système.
- **Déterminer un blast radius** : évaluer l'étendue de l'impact potentiel de l'attaque sur l'infrastructure.
- **Requalifier la criticité d'une attaque** : ajuster l'évaluation de la sévérité d'une attaque en fonction de nouvelles détections.

Lorsqu'un comportement malveillant est détecté, plusieurs réponses peuvent être déclenchées automatiquement ou manuellement comme l'**alertes et notifications en temps réel, l'isolation du workload, le blocage des processus suspects, la révocation d'accès compromis…**

3.3.8 Choisir et adopter une solution CNAPP

Investir dans une solution CNAPP représente un engagement financier significatif. Pour justifier cet investissement auprès de la direction, plusieurs arguments peuvent être avancés :

- **Optimisation des ressources** : En centralisant les outils et les équipes, le CNAPP permet de réaliser des économies d'échelle et d'améliorer le retour sur investissement à moyen terme.
- **Réduction des erreurs humaines** : L'automatisation des tâches de sécurité diminue les risques liés aux erreurs manuelles et renforce la fiabilité des opérations.
- **Amélioration de la détection des menaces** : la création d'un datalake unifié, véritable levier d'efficacité pour les intelligences artificielles dédiées à la cybersécurité.
- **Adaptabilité aux nouveaux usages** : Le CNAPP facilite l'intégration rapide de la sécurité des nouveaux cas d'usage, tel que l'intelligence artificielle.

- **Gestion du multicloud**: Grâce à une politique de sécurité cohérente sur l'ensemble des environnements Cloud, le CNAPP simplifie la gestion des infrastructures multicloud et réduit les risques de configuration incohérente.

Le choix d'une solution CNAPP doit être guidé par plusieurs critères : les fonctionnalités offertes, le coût total de possession, la conformité aux réglementations en vigueur, la souveraineté des données et les exigences spécifiques des donneurs d'ordre. Il est essentiel d'évaluer ces solutions dans le contexte particulier de l'entreprise pour assurer une adéquation optimale.

Enfin, il est fortement recommandé de se faire accompagner par des experts du domaine pour garantir le succès de l'implémentation. De nombreux prestataires proposent des services adaptés à différents niveaux de maturité, et des dispositifs publics, tels que le « diagnostic cyber », peuvent faciliter les premières étapes de cette transformation.

En somme, l'adoption d'un CNAPP constitue une démarche stratégique pour renforcer la sécurité des environnements Cloud. Elle permet non seulement de répondre aux défis actuels en matière de cybersécurité, mais aussi de préparer l'entreprise aux évolutions futures du paysage numérique.

3.4 QUELLE STRATÉGIE ADOPTÉE ?

Trois stratégies possibles sont proposées, pilotées par le besoin de sécurité Cloud :

1. **Outils CSP uniquement**: capitaliser sur l'intégration native des outils CSP pour élever rapidement le niveau de sécurité.
2. **100% CNAPP**: approcher la gestion des risques via une plateforme centralisée capable de corréler rapidement les évènements de sécurité.
3. **Mode hybride CNAPP et outils existants**: capitaliser sur l'existant et tirer bénéfice des nouveaux outils de sécurité Cloud.

< QUELS OUTILS POUR COUVRIR LES MENACES >

Le tableau ci-dessous propose des axes de réflexion pour le choix de la stratégie en fonction de plusieurs paramètres.

Stratégie	#1 - Outil CSP uniquement	#2 – 100% CNAPP	#3 – Mode hybride CNAPP et outils existants
Pourquoi ?	- Intégration simple - Environnement mono-cloud	- Peu ou pas d'outils existants - Environnement multi-cloud et /ou hybride	- Rationalisation - Capitaliser sur l'existant - Environnement multi-cloud et /ou hybride
Complexité d'implémentation	Moyenne - Activation des outils natifs simples - Nouvelle expertise requise	Complexe - Définition d'une nouvelle gouvernance - Nouvelle expertise requise	Complexe - Définition d'une nouvelle gouvernance - Nouvelle expertise requise - Beaucoup d'équipes à solliciter
Pourrait convenir à...	- Petite entreprise (e.g., start up) < 50 employés - Pas ou peu d'historique - Team IT restreinte	- Peu ou pas d'outils existants - Environnement multi-cloud et /ou hybride	Grande entreprise (e.g., CAC 40) > 1000 employees - Fort historique - Outillage existant pour la majorité des risques

Nb : Pour les services délégués au vendeur, les responsabilités respectives des parties prenantes doivent être clairement définies pour assurer la sécurité, conformité et les opérations (établissement d'un RACI).

4. QUELLE GOUVERNANCE ASSOCIÉE ?

L'informatique est un domaine qui gère des processus métiers et qui, à ce titre, doit évoluer avec les besoins opérationnels. Au-delà de cette adaptation aux métiers de l'entreprise, l'évolution constante des technologies et des composants eux-mêmes, nécessitent un suivi régulier et des prises de décision. C'est la raison pour laquelle une gouvernance de l'informatique doit être mise en place.

La gouvernance informatique est essentielle pour permettre d'aligner les opérations informatiques avec les stratégies commerciales et ainsi de gérer efficacement les données pour assurer leur usage. La question de la protection des données est un des pendants cruciaux de cette gouvernance pour garantir l'accessibilité, la qualité de la donnée numérique et sa diffusion auprès de l'audience désignée.

L'adoption du Cloud public pour répondre aux besoins informatiques impose de mettre en place une gouvernance de la sécurité des informations rigoureuse, en utilisant un cadre éthique solide.

4.1 OBJECTIFS DE LA GOUVERNANCE DE LA SÉCURITÉ DU CLOUD

- **Conformité**: Assurer que les opérations Cloud respectent les obligations légales et réglementaires.
- **Protection des données**: Protéger les informations sensibles contre tout accès non autorisé.
- **Transparence et responsabilité**: Établir des politiques claires pour augmenter la responsabilité et la confiance.
- **Efficacité opérationnelle**: Rationaliser les opérations en standardisant les processus de sécurité.

4.2 PRINCIPES DE LA GOUVERNANCE DE LA SÉCURITÉ DU CLOUD

- **Responsabilité**: Définir des rôles et des responsabilités clairs.
- **Approche basée sur les risques**: Évaluer et supprimer, accepter, partager ou atténuer les risques.
- **Transparence**: Favoriser la confiance en rendant les règles claires.
- **Alignement avec la conformité**: Respecter les exigences légales et réglementaires mais aussi métiers et liées à l'état de l'art.
- **Intégration de la sécurité**: Intégrer la sécurité dans tous les aspects des opérations Cloud.
- **Surveillance et amélioration**: Effectuer une surveillance continue et des évaluations régulières.

4.3 BONNES PRATIQUES POUR LA GOUVERNANCE DE LA SÉCURITÉ DU CLOUD

- **Définir des politiques claires**: Garantir que tous les membres comprennent leurs responsabilités.
- **Évaluer régulièrement la conformité**: Maintenir les cadres de gouvernance alignés sur les obligations légales.
- **Contrôles d'accès robustes**: Utiliser des contrôles d'accès basés sur les rôles.
- **Surveillance continue**: Fournir un aperçu en temps réel de la posture de sécurité.
- **Intégrer la sécurité au cycle de vie du développement**: Inclure des considérations de sécurité à toutes les étapes.
- **Collaborer avec les fournisseurs de services Cloud**: Maintenir des communications claires avec les fournisseurs.
- **Audits et évaluations réguliers**: Évaluer le succès du cadre de gouvernance.
- **Former et éduquer le personnel**: Investir dans l'éducation et la formation des employés.

5. TENDANCES FUTURES

La démocratisation des technologies d'intelligence artificielle constitue l'un des faits majeurs de ces dernières années. Mises à disposition à la fois des attaquants, des défenseurs et des collaborateurs d'entreprises, elles créent de nouveaux besoins en termes de détection mais génèrent également de nouvelles opportunités d'amélioration d'efficacité des solutions de détection.

Une autre évolution notable est le choix de plus en plus fréquent de la part des organisations d'un hébergement multicloud ce qui implique plus de communication entre les différents outils.

Les offres issues des leaders du marché sont en train de s'adapter à ces nouveaux besoins en intégrant les fonctionnalités suivantes :

Architecture Zero Trust

Le modèle Zero Trust, qui suppose qu'aucune entité à l'intérieur ou à l'extérieur du réseau ne peut être digne de confiance, deviendra une pierre angulaire de la sécurité du Cloud. La mise en œuvre de Zero Trust implique une vérification continue, des contrôles d'accès stricts et une micro-segmentation pour minimiser la surface d'attaque. Pour cela, les différents composants du CNAPP pourront aider à adresser certains besoins.

Intelligence artificielle et apprentissage automatique

L'IA et le ML joueront un rôle de plus en plus essentiel dans l'identification et l'atténuation des menaces. Ces technologies peuvent analyser de vastes quantités de données, détecter des anomalies et prédire des attaques potentielles, permettant ainsi des mesures de sécurité proactives.

Sécurité de la data et de l'usage des IA génératives

La gestion de la posture de sécurité de l'IA est une approche globale visant à maintenir la sécurité et l'intégrité des systèmes d'intelligence artificielle et d'apprentissage automatique. L'AI-SPM aidera a l'identification et la résolution des vulnérabilités, des erreurs de configuration et des risques potentiels.

Les solutions CNAPP sont pour la plupart développées aux Etats Unis ou en Israël, ce qui peut légitimement interroger sur notre souveraineté en termes de détection sur des Clouds qui sont également souvent opérés par des acteurs extra-européens. Si ces CNAPP sont généralement hébergés en Europe, le développement d'une nouvelle offre souveraine, issue d'acteurs européens, permettrait de combler un besoin lattent, notamment en termes de conformité à certaines directives. Mais le champ fonctionnel à couvrir serait extrêmement large et très peu d'acteurs semblent mesure de relever ce défi à court ou moyen terme.

< CONCLUSION >

4. CONLUSION

Pour protéger votre environnement Cloud, le curseur entre les outils traditionnels, ceux proposés par les CSPs et la plate-forme CNAPP doit être défini en fonction de votre contexte. Les stratégies proposées dans cet article fournissent des bases de réflexion.

Sous le prisme Cloud, les outils CNAPP offrent l'opportunité de centraliser les opérations de sécurité. Ils peuvent néanmoins trouver leurs limites dans les environnements hybrides, où les menaces on-premise restent à couvrir.

A noter que, l'adoption d'un CNAPP ne se résume pas à l'intégration d'un outil technologique. Elle nécessite une organisation adaptée, des ressources humaines qualifiées et une gouvernance rigoureuse en capacité de qualifier et traiter les alertes de sécurité. La réussite de cette démarche repose sur une stratégie globale, alignée sur les objectifs de l'entreprise et les exigences réglementaires.

Pour les environnements à faible empreinte Cloud, l'adoption des outils natifs Cloud pour améliorer rapidement la posture de sécurité peut être une option intéressante.

Au-delà des capacités techniques de chaque option, la réflexion doit inclure plusieurs composantes complémentaires en fonction de votre contexte : gouvernance associée à l'outil, souveraineté, expertise disponible.

< GLOSSAIRE >

6. GLOSSAIRE

1. CONCEPTS DE BASE

- **Zero Trust**: Modèle de sécurité qui stipule qu'aucune entité, qu'elle soit interne ou externe, ne doit être automatiquement fiable. Chaque accès doit être vérifié et validé.
- **Privilège escalation**: Technique utilisée par les attaquants pour obtenir des niveaux d'accès plus élevés que ceux qui leur sont normalement accordés.
- **Exfiltration & intégrité**: Exfiltration fait référence au transfert non autorisé de données hors d'un réseau, tandis que l'intégrité se réfère à la garantie que les données n'ont pas été altérées de manière non autorisée.
- **Discovery**: Processus de recherche et d'identification des actifs, des ressources et des vulnérabilités dans un environnement informatique.

2. GESTION DES IDENTITÉS ET DES ACCÈS

- **IAM (Identity and Access Management)**: Système qui gère les identités numériques et les autorisations d'accès aux ressources d'une organisation.
- **CIEM (Cloud Infrastructure Entitlement Management) :** Gestion des droits d'accès et des autorisations dans les environnements Cloud pour garantir une sécurité appropriée.

3. SÉCURITÉ DES APPLICATIONS

- **DevSecOps**: Pratique qui intègre la sécurité dans le processus de développement et d'exploitation des logiciels, favorisant une collaboration entre les équipes de développement, de sécurité et d'exploitation.
- **SAST (Static Application Security Testing)**: Technique de test de sécurité qui analyse le code source d'une application pour identifier les vulnérabilités sans exécuter le programme.
- **DAST (Dynamic Application Security Testing)**: Test de sécurité qui évalue une application en cours d'exécution pour détecter les vulnérabilités en simulant des attaques.
- **SCA (Software Composition Analysis)**: Analyse des composants logiciels tiers pour identifier les vulnérabilités et les licences associées.
- **ASPM (Application Security Posture Management)**: Évaluation et amélioration de la sécurité des applications tout au long de leur cycle de vie.
- **Shift Left**: Pratique qui consiste à intégrer les tests et la sécurité plus tôt dans le cycle de développement pour détecter et corriger les problèmes plus rapidement.
- **SDLC-SP (Software Development Life Cycle - Security Practice)**: Pratiques de sécurité intégrées dans le cycle de vie du développement logiciel.

< GLOSSAIRE >

4. SÉCURITÉ DES DONNÉES

- **DSPM (Data Security Posture Management)**: Gestion de la sécurité des données pour garantir leur protection contre les menaces et les violations.

5. SÉCURITÉ DES RÉSEAUX

- **NDR (Network Detection and Response)**: Solutions de sécurité qui se concentrent sur la détection des menaces dans le trafic réseau et la réponse à ces incidents.
- **SIEM (Security Information and Event Management)**: Système qui collecte, analyse et gère les données de sécurité pour détecter et répondre aux incidents.
- **Hunting**: Pratique proactive de recherche de menaces et d'anomalies dans les systèmes afin de détecter des activités malveillantes non signalées par les outils de sécurité.
  Forensics: Analyse détaillée des systèmes informatiques pour identifier, récupérer et analyser des données suite à un incident de sécurité.

6. CLOUD SECURITY

- **CNAPP (Cloud Native Application Protection Platform)**: Plateforme intégrée de protection des applications cloud-native, offrant des solutions pour la sécurité tout au long du cycle de vie de l'application.
- **CSPM (Cloud Security Posture Management)**: Outil de sécurité qui aide à identifier et corriger les configurations de sécurité inappropriées dans les environnements Cloud.
- **CKSPM (Cloud Key Security Posture Management)**: Gestion de la sécurité des clés dans les environnements Cloud, veillant à leur protection et à leur gestion appropriée.
- **KSPM (Kubernetes Security Posture Management)**: Outils et pratiques pour assurer la sécurité des déploiements Kubernetes en identifiant les vulnérabilités et en gérant les accès.
- **CWPP (Cloud Workload Protection Platform)**: Plateforme dédiée à la protection des charges de travail dans le Cloud contre les menaces et les vulnérabilités.
- **SSPM (SaaS Security Posture Management)**: Outils pour gérer la sécurité des applications SaaS, y compris la gestion des accès et des configurations.

< GLOSSAIRE >

7. OUTILS ET AUTOMATISATION

- **Ansible**: Outil d'automatisation de l'infrastructure qui permet la gestion des configurations, le déploiement d'applications et l'orchestration.
- **Puppet**: Outil d'automatisation et de gestion de configuration permettant de gérer les infrastructures de manière déclarative.
- **IaC (Infrastructure as Code)**: Pratique de gestion de l'infrastructure à l'aide de code, permettant l'automatisation et la gestion de l'infrastructure par des scripts.
- **Pipeline CI/CD**: Processus d'intégration continue (CI) et de déploiement continu (CD) qui permet l'automatisation du développement, des tests et des déploiements d'applications.
- **ECR (Elastic Container Registry)**: Service de stockage et de gestion d'images de conteneurs, souvent utilisé avec des solutions comme Docker et Kubernetes

8. MICROSERVICES ET CONTENEURS

- **Micro-segmentation**: Technique de sécurité qui divise le réseau en segments plus petits pour limiter les mouvements latéraux d'attaquants et améliorer le contrôle d'accès.
- **Conteneur**: Unité standardisée de logiciel qui regroupe le code et toutes ses dépendances, permettant une exécution cohérente dans divers environnements.
- **Microservice**: Architecture logicielle où une application est constituée de petits services indépendants, chacun exécutant une fonction spécifique.
- **Kubernetes**: Plateforme open source de gestion de conteneurs qui automatise le déploiement, l'évolutivité et la gestion des applications conteneurisées.
- **CRD/KDR (Cloud Resource Discovery/Kubernetes Resource Discovery):** Processus de découverte des ressources dans les environnements cloud ou Kubernetes pour mieux comprendre la posture de sécurité.

< GLOSSAIRE >

9. NORMES ET ORGANISATIONS

- **CIS (Center for Internet Security)** : Organisation à but non lucratif qui développe des bonnes pratiques et des benchmarks de sécurité pour aider les organisations à sécuriser leurs systèmes.
- **OWASP (Open Web Application Security Project)** : Fondation mondiale qui se consacre à la sécurité des applications web et fournit des ressources, des outils et des standards.
- **NIST (National Institute of Standards and Technology)** : Organisme américain qui fournit des normes et des directives pour améliorer la sécurité informatique.
- **CSA (Cloud Security Alliance)** : Organisation qui promeut les meilleures pratiques en matière de sécurité dans les environnements cloud.
- **PCI DSS (Payment Card Industry Data Security Standard) :** Norme de sécurité pour protéger les informations des cartes de paiement, exigeant que les entreprises respectent des mesures de sécurité spécifiques.

10. ANALYSE ET GESTION DE LA SÉCURITÉ

- **AI SPM (Artificial Intelligence Security Posture Management)** : Utilisation de l'intelligence artificielle pour analyser et améliorer la posture de sécurité d'une organisation.
- **GPO (Group Policy Object)** : Fonctionnalité de Windows permettant de gérer et de configurer les paramètres des utilisateurs et des ordinateurs au sein d'un réseau.
- **Log** : Enregistrement chronologique des événements et des activités d'un système, utilisé pour le diagnostic, l'audit et la sécurité.

< Studio des Communs >

CAMPUS CYBER

POUR EN SAVOIR PLUS : **WIKI.CAMPUSCYBER.FR**
ADRESSE MAIL DE CONTACT : **COMMUNAUTES@CAMPUSCYBER.FR**
5 - 7 RUE BELLINI 92800, PUTEAUX

CE PROJET A ÉTÉ FINANCÉ PAR LE GOUVERNEMENT DANS LE CADRE DU PROGRAMME D'INVESTISSEMENTS D'AVENIR