HOPE 3K | 10 ANS À VOTRE SERVICE
HOPE AND WE PERFORM

PRISALYA CONSULTING

LES NOUVELLES APPROCHES CYBERSÉCURITÉ

ÉTAT DES LIEUX ET PERSPECTIVES

Elmehdi ERROUSSAFI | Nabil HAMAOUI

Avril 2021

LES NOUVELLES APPROCHES
CYBERSÉCURITÉ

TAB MA

CONTEXTE

Toute entreprise est en train de naviguer dans l'ère de la révolution industrielle, où les technologies numériques, le digital, influent sur la stratégie commerciale et sur l'exécution opérationnelle.

Cette révolution met sous pression les différents acteurs de cet écosystème, pour innover et faire des investissements intelligents dans des technologies disruptives telles que : L'internet des Objets (IoT), le Cloud Computing, les technologies de le Big Data, et le fort usage des Advanced Analytics. Ce changement introduit aussi une métamorphose de la culture du travail au sein de l'organisation. Les maîtres mots sont l'agilité, la mobilité et la rapidité d'exécution avec une ambition d'efficacité à la hauteur des technologie et des capacités permises par ces dernières.

Il est donc nécessaire d'adapter les mécanismes de sécurité - réseau pour soutenir cette évolution. La mobilité, l'adoption de solutions Cloud, IoT et les technologies numériques sur les opérations industrielles et informatiques nécessitent de repenser l'architecture du réseau d'interconnexion pour intégrer des concepts et des abstractions de sécurité novatrice et résolument tournées vers le Cloud et l'agilité permise par les usages récents de l'outil numérique.

Les ingénieurs cherchent à simplifier mais aussi à renforcer la sécurité dans une proposition de modèle centré autour de l'utilisateur, mais surtout, respectant la réglementation en matière de cyber- sécurité dans le territoire Marocain. En effet, le royaume s'est doté d'un arsenal de lois et de décrets s'inspirant des cadres de bonnes pratiques, auquel, le publique et le privé sont assujettis.

La sécurité du réseau comme tout élément de cette architecture hybride doit répondre aux nouvelles exigences, d'être un moteur de développement à haute valeur ajoutée et un moteur métier. Le marché actuel des solutions de sécurité réseau a récemment subi une transformation et la naissance d'une nouvelle génération et d'une nouvelle vision de la sécurité en favorisant une efficacité, une visibilité et une automatisation en profondeur. HOPE3K, acteur majeur de la transformation numérique, bâtie dans l'opérationnel et axée objectif, avec son partenaire PRISALYA CONSULTING, Cabinet de conseil en cyber sécurité et métiers du risque, présentent dans ce document, un état de l'art de la cybersécurité moderne.

LE DES TIERES

AUTEUR

NABIL HAMAOUI

Fondateur et directeur associé de HOPE3K, créée en 2008, certifiée ISO9001 en Consulting, une entreprise novatrice qui continue de révolutionner l'industrie des services avec un CA de 51 Millions de DH en 2020, Fournisseur de spécialistes et d'experts dans le domaine de l'ICT.

Diplômé de l'INPT, passionné par le digital, Il a géré plusieurs projets d'envergure dans le secteur de l'informatique et des télécommunications pour le compte de clients institutionnels, privés et grands groupes. Il a aussi créé et lancé plusieurs produits digitaux et startups et supervisé plusieurs projets de recherche et de thèses de doctorat dans l'intelligence artificielle.

nabil.hamaoui@hope3k.net

AUTEUR

ER-ROUSSAFI ELMEHDI

Fondateur et directeur général de PRISALYA Consulting, un cabinet de conseil en Cybersécurité, transformation Digitale et Opérations IT. Basé à Casablanca, Maroc.

Auditeur certifié ISO 27001 LA, Chercheur doctorant et Ingénieur réseaux et télécoms diplômé de Télécom Saint-Etienne, Il a entamé une carrière dans les télécommunications entre des équipementiers à Paris, Berlin et il a intégré l'opérateur INWI pour le lancement de son réseau national. Durant ces 15 ans, il a développé une expertise dans le coeur des télécommunications, la DATA ainsi que la cybersécurité dans les réseaux de télécommunications mobile.

mehdi@prisalya.com

Elmehdi ERROUSSAFI | Nabil HAMAOUI

Avril 2021

EVOLUTION DU PARADIGME DE CYBERSECURITE

1940
AVANT LE CRIME

1943 : création du 1er ordinateur numérique du monde L'accès aux machines électroniques géantes était délicat.
1949 : théorisation et postulat du virus informatique par John von Neumann.

1950
PHREAKING TÉLÉPHONIQUE

Les racines technologiques et culturelles du piratage sont autant liées aux premiers téléphones qu'aux ordinateurs.
À la fin des années 50, le «phreaking téléphonique» est apparu pour détourner les protocoles en permettant de passer des appels gratuits.

1960
NOTION DU PIRATAGE MALVEILLANT

La toute première référence au piratage malveillant a été publiée dans le journal étudiant du Massachusetts Institute of Technology.

1970
NAISSANCE DE LA SÉCURITÉ INFORMATIQUE

La cybersécurité proprement dite a débuté en 1972 avec un projet de recherche sur ARPANET, précurseur d'Internet.
Le chercheur Bob Thomas a créé le programme Creeper qui pourrait se déplacer sur le réseau d'ARPANET, laissant la trace «Je suis la plante grimpante, attrape-moi si tu peux».

1980
NAISSANCE DE LA CYBERSÉCURITÉ

Les années 1980 ont été marquées par la guerre froide et les attaques de haut niveau du Pentagone, de la National CSS, AT&T et l'apparition des termes cheval de Troie et virus informatique. En 1985, le département américain de la Défense a publié les Trusted Computer System Evaluation Criteria (alias The Orange Book).

1990
LE MONDE PASSE EN LIGNE

Le nombre de nouveaux virus a explosé dans les années 90. Un chercheur de la NASA a développé le premier pare-feu. Vers la fin des années 1990, le courrier électronique proliférait et a ouvert un nouveau point d'entrée pour les virus.

2000
LES MENACES SE DIVERSIFIENT (WEB ET MI)

En 2007, Panda Security a combiné la technologie cloud et l'intelligence des menaces dans son produit antivirus.
l'Anti-Malware Testing Standards Organization (AMTSO) a été créée et a élaboré une méthode de test des produits cloud.

2010
LA NOUVELLE GÉNÉRATION

- Multi-factor authentication (MFA)
- Network Behavioural Analysis (NBA)
- Forensics
- Real-time protection
- Sandboxing
- Back-up and mirroring
- Web application firewalls (WAF)

Elmehdi ERROUSSAFI | Nabil HAMAOUI

Avril 2021

ANALYSER, COMPRENDRE, RÉSOUDRE

Impératifs méthodologiques

La prise en compte des enjeux de sécurité réseau par une équipe en support de clients agiles doit être continue (tout au long de la construction et de l'amélioration du service) et pragmatique puisqu'elle priorise les efforts en fonction du risque réel et assume l'existence de risques résiduels. Ce principe de management de la sécurité numérique par les risques est celui qui guide la démarche appropriée à chaque contexte. Nos équipes adoptent une méthode axée sur les menaces réelles, intentionnelles et ciblées. Plus précisément, nous devons concentrer nos efforts sur l'analyse des attaques ciblées, considérant les risques informatiques habituels, comme traitées par les approches classiques par conformité.

Ceci nous permettra de justifier, et cadrer les projets cibles, comme des objectifs de sécurité spécifiquement adaptés aux systèmes et aux réseaux étudiées et à l'écosystème spécifique de chaque entreprise, et non à réécrire les politiques ou à mettre en place des politiques de sécurité justifiées par un risque hypothétique.
Ensuite, et au vu de la complexité de l'écosystème, mais à la clarté du virage agile entamé par beaucoup d'entreprises, notre méthode ne doit pas chercher l'exhaustivité, mais plutôt l'efficacité.
Dès lors que l'on sait qu'un concept d'architecture de sécurité réseau viendra couvrir complètement plusieurs menaces, est il bien nécessaire de lister tous les scénarios à couvrir ? Notre méthode doit se baser sur une réelle connaissance des attaques avérées, pour faire le choix de la meilleure architecture, capable de justifier, de par son efficacité, de son implémentation et de son choix. L'exhaustivité des scénarios sera une résultante à l'adoption et à la gestion du changement. Notre méthode doit prendre en charge la complexité de l'écosystème. Les attaquants exploitent souvent des vulnérabilités annexes pour atteindre leur cible. Nous devons choisir une méthodologie qui prend en charge les parties prenantes qui interagissent avec le système : Infogérance, Fournisseurs, Partenaires, Directions Supports ...etc., avec pour objectif d'intégrer à la réflexion la menace que représentent ces parties prenantes et l'exposition qu'elles engendrent pour l'entreprise.
Notre méthode doit permettre de, configurer la granularité. Et nous entendons par cela, la capacité d'approfondir l'analyse par itération. La phase exploration permettra de lister nos risques sur le réseau, chaque itération permettra d'approfondir l'analyse et d'avoir une granularité plus fine des scénarios d'attaque plausibles et donc de définir les solutions d'architecture cible.
La méthodologie doit nous permettre de nous arrêter en cours de route pour permettre de définir l'architecture sans avoir besoin de continuer dans l'analyse fine des risques encourus, en vue de la multitude de risques qui peuvent apparaitre pour chaque Stream.
Enfin, la réglementation, principalement Marocaine et qui s'inspire fortement du standard ISO/IEC 27001 en termes de système de Management de la Sécurité de l'Information, et notamment dans les directives DNSSI, la loi cyber sécurité, mais aussi de la RGPD européenne en ce qui concerne la loi 09-08 et ses futures évolutions pour ne citer que ces réglementations.
Notre méthodologie doit être compatible avec ces standards et lois pour permettre une adhérence a la législation et une cohérence dans le rendu et dans les livrables.

Elmehdi ERROUSSAFI | Nabil HAMAOUI

Avril 2021

COMPARATIF DES FRAMEWORK D'ANALYSE DU RISQUE

Plusieurs entreprises, sont activées par un flux physique continu et un flux décisionnel qui opèrent de symbiose pour atteindre des objectifs déterminés. Ce qui a engendré l'implantation d'un système d'information fiable, puis un système mondial, opérant avec un contrôle continu et une exigence de sécurité maximal.

Compte tenu du niveau d'exposition aux risques et de la dépendance vitale du groupe vis à vis de son système d'information et de ses ressources numériques, il est crucial de prêter attention aux exigences de sécurité. La réalisation d'une architecture de sécurité, qui assure à la fois l'équilibre entre les exigences de sécurité et l'efficacité et l'agilité demandée par le virage numérique exige au préalable une analyse approfondie du contexte organisationnel. Elle nécessite également l'identification, l'analyse et la gestion des risques encourus par l'entreprise. Nous avons conduit une étude des méthodologies d'analyse de risques pour retrouver la méthode la plus adaptée à cette mission.

L'analyse (ou identification) des risques implique l'identification de plusieurs aspects :

•**L'actif :** défini comme tout ce qui a de la valeur pour l'entreprise.

• **La menace :** une cause potentielle d'un incident indésirable, qui peut entraîner des dommages à un système ou à l'organisation entière. La vulnérabilité est une faiblesse d'un actif ou d'un groupe d'actifs qui peut être exploitée par une ou plusieurs menaces.

• **L'exigence :** un besoin documenté singulier de ce qu'un actif particulier devrait être, faire ou respecter

• **L'impact** peut être défini comme la gravité des conséquences d'un événement ou d'un incident. Dans le contexte de la sécurité de l'information, l'impact est une perte de disponibilité, d'intégrité et de confidentialité des informations.

PREMIERS CRITÈRES DE SÉLECTION DU MODÈLE DE DIAGNOSTIC

Dans une approche comparative, nous avons listé l'ensemble des méthodologies d'analyse de risque appliquée au domaine ainsi qu'au contexte et aux impératifs listés dans le paragraphe précèdent.

Les critères suivants ont été retenu dans cette sélection :

- Choix des méthodes et non des guidelines
- Mises à jour et maintien de la base de connaissance
- Choix des méthodes ouvertes et documentées avec notoriété.
- Choix des méthodes adaptées au risque Cyber

Une première Analyse donne le tableau suivant des différentes méthodes explorées :

Nom de la méthode	Méthode ou Guideline?	Adaptée au Risque Cybersécutité?	Documentation	Mise à jour
OCTAVE	Methode	Oui	Ouvert	À jour
Mehari	Methode	Oui	Ouvert	À jour
Ebios RM	Methode	Oui	Ouvert	À jour
ISO 27005	Guideline	Oui	Disponible	À jour
NIST SP800-30	Guideline	Oui	Ouvert	À jour
MIGRA	Methode	Oui	Payant/Propriétaire	À jour
Information Risk Assessment Method 2 (IRAM)	Methode	Non	Payant/Propriétaire	À jour
RiskIT	Guideline	Non	Dispobible	N/A

Figure 1 – Premiers critères de sélection de la méthode

DEUXIÈMES CRITÈRES DE SÉLECTION DU MODÈLE DE DIAGNOSTIC

Sur les trois méthodes sélectionnées OCTAVE, MEHARI et EBIOS RM, nous avons appliqué des critères de sélections relatifs aux impératifs dictés par le marché local, la réglementation et les méthodologies ayant prouvé leur efficacité.

- Origine du modèle
- Approche de la méthode
- Prise en charge de la réglementation
- Identification des menaces réelles (scénarios).
- Complexité (L'efficacité VS l'exhaustivité, Itérations et Granularité)
- Parties prenantes externes et analyses spécifiques

Ces critères nous ont permis d'identifier la méthode EBIOS RM comme étant la méthode la plus adaptée au besoin de la majorité des entreprises marocaines comme le montre le tableau comparatif suivant :

Complexité	Approche	Origine	Réglementation	Parties prenantes externes	Menaces Réelles	Complexité
OCTAVE	Elevée	Workshops, collaborative	Académique	Moyen	Non	Bas
MEHARI	Moyenne	Analyse basée sur des formules et une base de connaissance	Commerciale	Bas	Non	Bas
EBIOS RM	Basse	Workshop, Collaborative, Encadrement et méthodologie de contrôle	Gouvernementale	Fort	Oui	Haut

Figure 2 – Deuxièmes critères de sélection de la méthode

MÉTHODOLOGIE EBIOS RM

La méthode EBIOS Risk Manager adopte une approche de management du risque qui part du plus haut niveau (grandes missions de l'objet étudié) pour s'intéresser progressivement aux éléments métier et techniques, en étudiant les chemins d'attaque possibles.
Elle vise à obtenir une synthèse entre « conformité » (réglementaire, lois, politiques) et « scénarios » (menaces réelles, faiblesses techniques, réelles carences) par le repositionnement de ces deux approches complémentaires là où elles apportent le plus de valeur ajoutée.
Selon EBIOS Risk Manager, l'appréciation des risques par scénarios se concentre donc sur les menaces intentionnelles et ciblées.

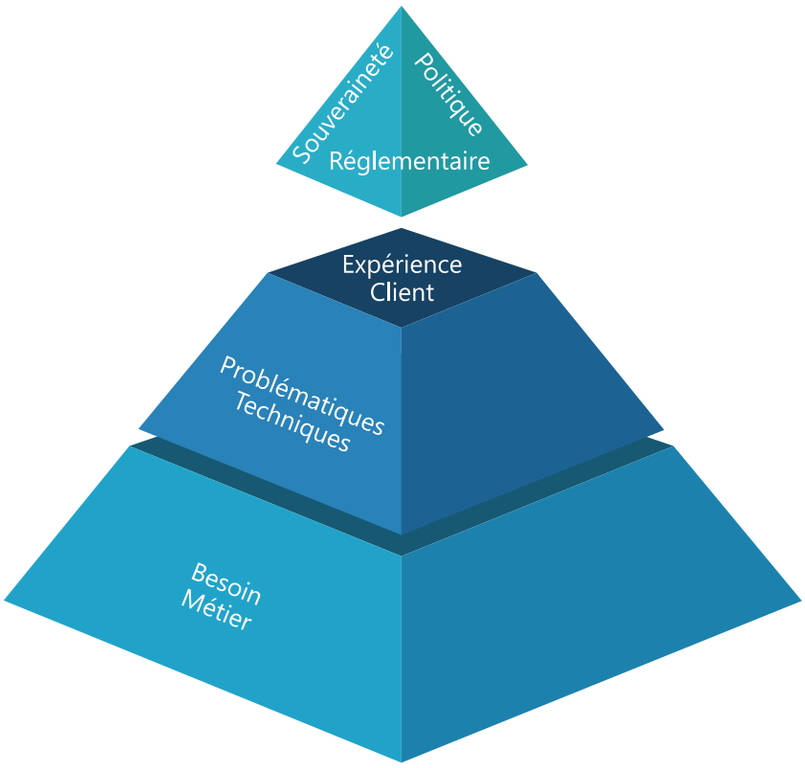

Security
Computer
Internet attack
Protect
Mobile devices

DÉROULEMENT DE NOS ATELIERS

AU-DELÀ DE LA MÉTHODOLOGIE

EBIOS RM est une démarche dont le but est de répondre à un besoin de connaissance des risques cyber qui impactent aujourd'hui les systèmes d'information les plus sensibles. À l'origine de cette démarche se trouve l'ANSSI, le « cyber gendarme » de la sécurité en France, qui l'a conçue pour répondre à des cas d'usage d'organismes concernés par le cyber risque – on appelle ce système des opérateurs d'importance vitale (OIV). Il faut toujours prendre en compte en parallèle les impératifs réglementaires ainsi que l'évolution business croissante.

Pyramides Cybersécurité



Parfois une politique Up-Buttom conduit à une absence de coopération du bas de la pyramide et la sécurité dans ce cas mène à l'obscurité.
Une autre façon de faire est de renverser la pyramide mais en gardant toujours le lead au cadre règlementaire et en travaillant toujours à l'intérieur de ce cadre réglementaire, qui lui-même change au cours du temps.
Cette méthodologie va respecter bel et bien le cadre réglementaire tout en restant proche de l'opérationnel et répondre d'une manière réaliste aux besoins cybersécuritaires des utilisateurs, du métier et du réglementaire.
Notre approche consiste à traiter les objectifs (protection contre les menaces, défendre la souveraineté) tout en préservant l'ouverture de l'internet. Cette ouverture est un prérequis, car elle permet de faire du cyberespace une plate-forme pour l'innovation et la création de nouvelles sources de richesse. Pour que des règles, des normes et des théories soient opérationnalisées elles doivent obligatoirement être proches du réel et des gens de l'opérationnel afin de prendre en considération les contraintes sectorielles, organisationnelles et le background socio-culturel.
L'humain est toujours au centre de notre approche pour mieux légiférer, éduquer, sensibiliser, convaincre, et de pouvoir s'adresser au politique, au secteur économique et aux développeurs de technologies.

ATELIERS ET LIVRABLES

Notre méthodologie, à plusieurs étapes, peut faire dire que l'approche est à géométrie variable. Il n'est pas nécessaire de suivre les cinq ateliers pour ruéssir la méthode : N'en exploiter qu'une partie est possible.
Ce qui implique que chacun personnalise ses objectifs, et donc sa méthode. Ci-après les ateliers prévus par la méthode :

ATELIER 1 – CADRAGE ET SOCLE DE SECURITE

À l'issue de l'atelier, les éléments suivants doivent être identifiés :

• Les éléments de cadrage : objectifs de l'analyse des risques, rôles et responsabilités, cadre temporel ;
• Les métriques (Échelles de besoins DICT, échelle de gravité, échelle de vraisemblance, les métriques, etc.) ;
• Le périmètre métier et technique : Valeurs métiers et biens supports
• Les événements redoutés et leur niveau de gravité ;
• Le socle de sécurité : liste des référentiels applicables, état d'application, identification et justification des écarts.

ATELIER 2 – SOURCES DE RISQUE

À l'issue de l'atelier, les éléments suivants doivent être identifiés :

• La liste de couples SR/OV prioritaires retenus pour la suite de l'étude ;
• La liste des couples SR/OV secondaires susceptibles d'être étudié dans un second temps;

ATELIER 3 – SCENARIOS STRATEGIQUES

À l'issue de l'atelier, les éléments suivants doivent être identifiés :
• Niveau de menace des parties prenantes: (Dépendance x Pénétration) / (Maturité x Confiance)
• Les parties prenantes critiques sélectionnées ;
• Les scénarios stratégiques et événements redoutés associés ;
• Les mesures de sécurité retenues pourl'écosystème.

ATELIER 4 – SCENARIOS OPERATIONNELS

À l'issue de l'atelier, les éléments suivants doivent être identifiés :

• La liste des scénarios opérationnels et leur vraisemblance.

ATELIER 5 – TRAITEMENT DU RISQUE

À l'issue de l'atelier ou des séries d'ateliers, les éléments suivants doivent être identifiés

• Une synthèse de l'ensemble des scénarios de risques étudiés.

• Liste des mesures de sécurité complémentaires ;
• La synthèse des risques résiduels ;
• Le plan de traitement des risques (mesures de sécurité complémentaires spécifiques+ Mesures de sécurité Écosystème+ Mesures de sécurité de renforcement du socle de sécurité)

ETUDE DE MARCHE DES FOURNISSEURS

Il faut conduire une étude de marché des solution existantes ainsi qu'un comparatif des possibilités et composantes de chaque solution. Ensuite, proposer de ce fait une grille d'évaluation comparative des solutions explorées.

REDACTION DES APPELS D'OFFRES

Rédiger :

•La liste des investissements CAPEX/OPEX à prévoir pour supporter l'architecture proposées
• Une rédaction de l'annexe technique des différentes solutions demandées.
• Une proposition de grille d'évaluation pour chaque RFP proposé.

DESIGN DE L'ARCHITECTURE

Suite à l'exercice précédent, l'équipe va produire les premiers livrables issu de la mission :

• Évaluation des capacités actuelles de protection du réseau
• Énoncé des besoins pour le contexte du réseau couvrant les exigences légales, de conformité et d'affaires
• Exigences de cybersécurité pour faire face à l'exposition aux cybermenaces en ce qui concerne la surface d'attaque
• Élaboration de la conception fonctionnelle et technique

PLAN STRATEGIQUE ET FEUILLE DE ROUTE

Il faut proposer la stratégie qui comportera :

• Définition de la feuille de route de la protection des réseaux de cybersécurité priorisée en fonction des besoins et du contexte.
• Un plan de projet annuel.

SELECTION ET EVALUATION

Sélection et attribution des projets de RFP préparés.

NOUVELLES TECHNOLOGIES DE LA CYBERSECURITE DU CLOUD

Selon le National Institute of Standards and Technology (NIST) : «Le Cloud Computing est un modèle permettant un accès réseau omniprésent, pratique et à la demande à un pool partagé de ressources informatiques configurables (par exemple, réseaux, serveurs, stockage, applications et services) qui peuvent être rapidement provisionnés et libérés avec un effort de gestion ou une interaction avec le fournisseur de services minimal.

Un fournisseur de services cloud devrait être en mesure d'accepter un trafic réseau fiable et de bloquer le trafic réseau malveillant. La sécurité de l'infrastructure du réseau cloud doit être en mesure de bloquer et de se protéger contre les attaques par déni de service (DDoS), de détecter et de prévenir les intrusions et d'autoriser la journalisation et la notification. Les défenses DoS sont basées sur la sécurité du réseau, qui devrait filtrer efficacement les requêtes et identifier les envahisseurs pour éviter les attaques malveillantes. Les systèmes IDS / IPS détectent ou bloquent les attaques de logiciels malveillants, les signatures de virus et les signatures de spam, mais sont également sujets à de faux positifs. La journalisation et la notification permettent aux utilisateurs du cloud d'avoir un aperçu de la santé de la cybersécurité du réseau.

Elmehdi ERROUSSAFI | Nabil HAMAOUI

Avril 2021

ACCES AU RESEAU EN MODE ZERO-TRUST (ZTNA)

Selon Forrester Research, une solution Zero Trust doit :

• • Assurer que seul le trafic connu et autorisé ou la communication d'application légitime est autorisé en segmentant et en activant la stratégie de couche 7.

• • Tirer parti d'une stratégie d'accès les moins privilégiés et appliquer strictement le contrôle d'accès.

• • Inspecter et enregistrer tout le trafic. Sinon, il peut être assez simple pour un attaquant d'accéder au réseau d'une entreprise.

Ces principes peuvent être simples à mettre en oeuvre dans un réseau d'entreprise, mais comment s'appliquent ils au cloud ?

Vous pouvez appliquer les mêmes concepts au cloud en pilotant l'accès via une passerelle de sécurité pour un accès sécurisé aux moins privilégiés. Cependant, il est devenu clair que la mise en oeuvre d'une passerelle ne suffit pas pour Zéro Trust dans le cloud. Votre implémentation doit inspecter tout le trafic pour toutes les applications, sinon elle ne fournit pas vraiment de confiance zéro.

ADOPTION DU SECURITY ACCESS SERVICE EDGE (SASE)

Les solutions SASE sont idéalement fournies sous forme de services (Selon Gartner), mais peuvent être livrées sous forme d'Appliance clé en main.

L'utilisation de technologies de mise en réseau (SD-WAN, optimisation WAN, optimisation d'itinéraire et plus) pour offrir la meilleure expérience réseau possible à toute entité qui se connecte - groupe (un site), utilisateurs, appareils, applications, services et système IoT - indépendamment de lieu.

Dans le même temps, ils restreignent également les restrictions en fonction de l'identité et du contexte en temps réel (tel que l'emplacement) conformément aux politiques de sécurité / conformité de l'entreprise et évalués en permanence tout au long de la session.

Bien qu'il existe des dizaines de caractéristiques associées à SASE, quatre attributs principaux sont essentiels :

• Empreinte globale SD-WAN. Les fournisseurs de services SASE devraient fournir, en effet, un service SD-WAN mondial avec son propre réseau privé composé de points de présence (PoP) dans le monde entier. Le trafic est acheminé sur leur réseau, évitant ainsi les problèmes de latence de l'Internet mondial. Inspection distribuée et application des politiques.

• L'inspection de sécurité et l'application des politiques sont réparties sur les POPs d'un fournisseur SASE. Le trafic n'est pas renvoyé au « siège » pour l'inspection de sécurité. Les services de sécurité de base comprennent SWG, CASB, ZTNA et FWaaS.

• Architecture native du cloud. Un service SASE doit utiliser une pile logicielle cloud native convergée et multi-locataires et non un service de dispositifs de réseau et de sécurité discrets enchaînés. Les solutions SASE livrées sous forme de CPE doivent être des boîtiers clé en main, « allumez-le et oubliez-le », comme le dit Gartner.

• Axé sur l'identité. La sécurité et l'accès au réseau sont fournis en fonction de l'identité de l'utilisateur et non d'une adresse IP. L'identité peut être le nom de l'utilisateur, mais elle tiendra également compte de l'appareil utilisé et de l'emplacement de l'utilisateur.

CLOUD SECURITY POSTURE MANAGEMENT (CSPM)

Il y a eu de nombreuses failles de haut niveau qui ont suscité l'intérêt des entreprises pour une technologie émergente appelée CSPM, ou Cloud Security Posture Management. En termes simples, il nettoie l'environnement cloud et alerte l'entreprise des problèmes et des risques potentiels.

Prenons l'exemple d'un ancien employé d'Amazon Web Services (AWS) qui a volé des données de millions de demandes de crédit en exploitant un pare-feu d'applications Web (WAF) mal configuré. Dans un autre exemple, un partenaire de joaillerie Walmart a exposé les données de millions de clients. De toute évidence, une meilleure protection des données dans le cloud est nécessaire.

CSPM est un terme relativement nouveau dans le monde des capacités de sécurité. Au cours des dernières années, la CSPM est devenue populaire car de plus en plus d'organisations ont adopté une méthodologie axée sur le cloud. CSPM leur permet de surveiller le risque et de résoudre automatiquement certains problèmes de sécurité. Il n'y a pas de frais de configuration supplémentaires, et les utilisateurs bénéficient d'un déploiement évolutif et d'informations sur la sécurité.

Au fur et à mesure que l'espace cloud augmente, il devient important de suivre et de protéger les données sensibles contre les erreurs de configuration. Étant donné que l'environnement cloud s'est étendu dans de nombreux domaines, les entreprises peuvent utiliser CSPM pour consolider les éventuelles erreurs de configuration et créer une plate-forme transparente pour le relais d'informations. Lorsqu'ils utilisent CSPM, ils peuvent se conformer à des cadres tels que HIPAA, SOC2 et CIS v1.1. Cela renforce la confiance des clients dans votre entreprise et la sécurité du cloud. Des outils logiciels tels que Cloud Access Security Brokers (CASB) sont de plus en plus utilisés en conjonction avec CSPM. Un CASB protège le flux de données entre l'architecture informatique interne et les environnements cloud et étend les politiques de sécurité d'une organisation au-delà de son infrastructure interne. CSPM peut détecter des problèmes tels que le manque de cryptage, une gestion incorrecte des clés de cryptage, des autorisations de compte supplémentaires, etc.

Selon un rapport de Gartner, la majorité des attaques réussies sur les services cloud résultent d'une mauvaise configuration et CSPM peut atténuer ces risques. La CSPM présente de nombreux avantages, notamment :

- Recherche d'une connectivité réseau mal configurée
- Évaluation du risque lié aux données
- Détection des autorisations de compte extrêmement permissives
- Surveillance continue de l'environnement cloud pour détecter toute violation de politique
- Possibilité de remédier automatiquement aux erreurs de configuration dans certains cas
- Conformité aux normes communes pour les meilleures pratiques telles que HIPAA, SOC2 et PIC

SECURITE DES ARCHITECTURES MICRO-SERVICE

L'avènement des Architectures « Micro-services » offre une multitude d'avantages pour répondre efficacement aux demandes métiers (agilité, rapidité, évolution).
Cependant, ce changement architectural impose une revue profonde des principes de sécurité. En effet, avec une surface d'attaque volatile, une réorganisation des rôles au sein des équipes de développement et de support, l'utilisation de différents logiciels, une gestion particulière des magasins de données, il est important de reconsidérer la sécurité informatique dans son ensemble pour répondre à ces nouveaux défis.

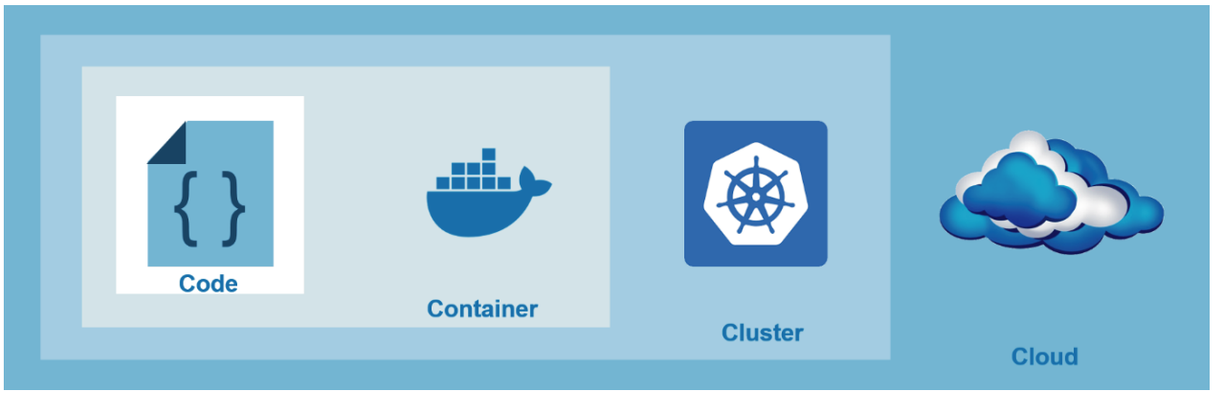


Figure 3 – Les 4 niveaux de sécurité

Il convient donc de mettre en place des nouveaux programmes de sécurité pour répondre à cette architecture, qu'on peut diviser en deux phases :

• La phase de création et déploiement : Consiste à appliquer les règles de sécurité lors de la créationdes conteneurs ainsi que leur déploiement dans le système informatique via des procédures automatisée.

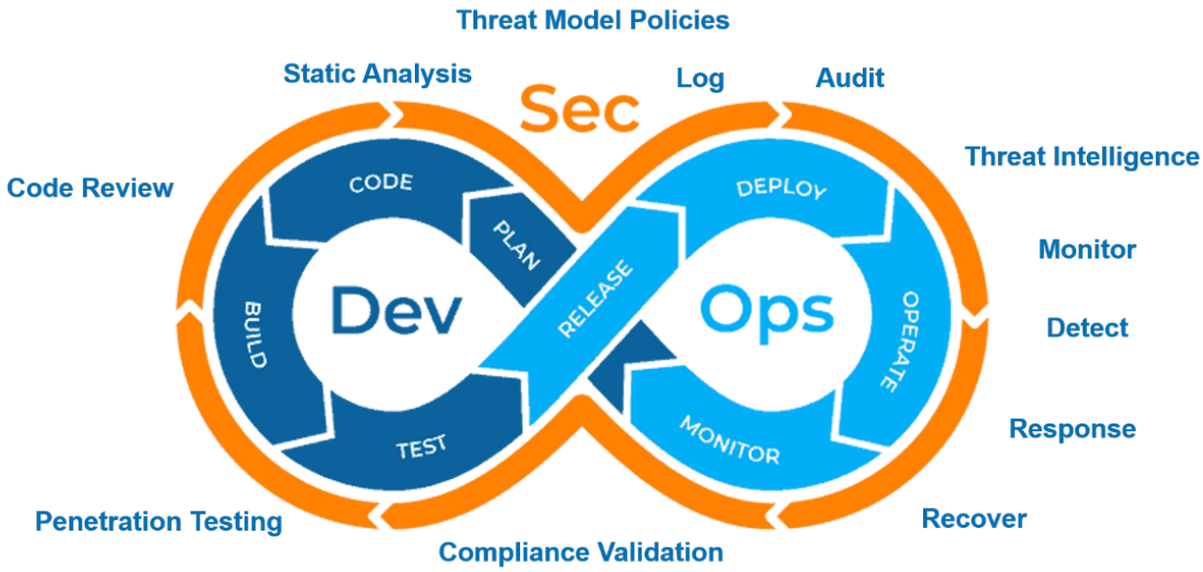


Figure 5 – Le cycle DevSecOps

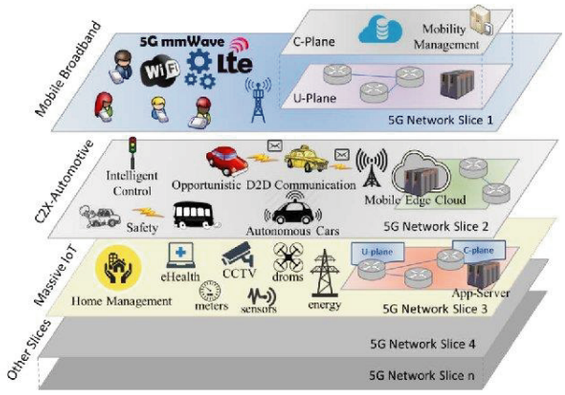
• La phase d'exécution : La sécurité dans cette phase englobe toutes les fonctions de surveillance, d'analyse d'incident, de réponse à incident ainsi que des fonctions avancées comme la corrélation d'incidents. L'ensemble de l'activité de chaque micro-service doit être correctement horodaté et enregistré de manière centralisée. Ceci afin de permettre une prise en charge complète et efficace des fonctions de sécurité.

Elmehdi ERROUSSAFI | Nabil HAMAOUI

Avril 2021

SECURITE DES ARCHITECTURES MICRO-SERVICE

Les technologies SDN (Software Defined Networks) et NFV (Network Functions Virtualisation) devraient révolutionner à terme les architectures des réseaux, et permettre de déployer des nouveaux services de manière beaucoup plus rapide et avec des coûts significativement réduits. Elles changeront complètement l'écosystème des infrastructures de Télécommunication dans les années à venir. La Virtualisation des Fonctions Réseau NFV est un élément déterminant pour optimiser l'utilisation des ressources du réseau en virtualisant des fonctions habituellement mises en oeuvre dans le matériel propriétaire, réduisant ainsi pour les opérateurs les coûts d'investissement et d'exploitation. La solution NFV est basée sur le principe de séparation entre une couche matérielle banalisée et standardisée de type « Data Center » et une couche logicielle applicative implantant des fonctions nécessaires au fonctionnement du réseau d'un opérateur (services de la couche 4 à la couche 7 tels que firewall, NAT, Load balancer, système d'inspection de paquets, etc).



Les architectures de matériel de routage et switching IP évoluent en parallèle suivant la standardisation poussée par l'ONF (Open Networking Foundation) appelée SDN (Software Defined Networking), visant à séparer la couche de transport IP et la couche de contrôle du routage IP, avec la mise en place d'un protocole « ouvert » appelé Openflow, permettant à la couche de contrôle d'inter-opérer avec des matériels de constructeurs différents. Le SDN est donc complémentaire de la technologie NFV et permet de mettre en place des solutions purement logicielles rendant possible le contrôle d'un réseau IP soit d'entreprise, soit d'opérateur. L'idée principale du SDN est d'éloigner le plan de contrôle du matériel réseau et d'activer le contrôle externe des données via une entité logicielle logique appelée contrôleur. Le contrôleur, qui gère le contrôle du flux de paquets pour permettre une mise en réseau intelligente, est situé entre les périphériques réseau et les applications. Dans cette architecture, le contrôle du réseau devient programmable. Avec le contrôleur, les administrateurs pourront facilement gérer le réseau 5G et introduire de nouveaux services ou des modifications.

Pour cette raison, le paradigme SDN 5G permettra une augmentation de la flexibilité et de la programmabilité des réseaux 5G, en comblant le fossé entre les besoins de l'entreprise et les systèmes de gestion. Un réseau 5G intelligent, virtualisé et programmable permettra aux fournisseurs d'innover, tant dans leurs opérations que dans leurs offres de services. Ils pourront fournir de nouveaux services à la demande, améliorant ainsi leur efficacité globale.

Cette virtualisation permet de créer simultanément plusieurs réseaux logiques, appelés tranches (ou slices), pilotés par des interfaces de programmations (API). Un découpage en tranche (network slicing) qui offre la possibilité aux opérateurs de délivrer différents niveaux de services (en termes de fiabilité, de latence, de capacité de bande passante, de couverture…) à partir de la même infrastructure. De quoi privilégier, par exemple, une plus grande connectivité pour une voiture autonome que pour un simple smartphone.

CONCLUSION

De par son expertise dans l'exécution des missions IT, de transformation digitale, de design d'architectures et de conseil réaliste, notre ambition est d'être un réel contributeur stratégique en matière de cybersécurité et dans l'évolution des réseaux et systèmes. Notre méthodologie est prouvée pour faire l'analyse du gap, ainsi que la mise à disposition d'une équipe de qualité pour assurer la production des livrables. En prenant en considération les prérequis du client, ainsi que le contexte réglementaire local, avec l'ambition de livrer un projet d'architecture complet, tenant compte, non seulement des contraintes, mais surtout des ambitions du business.

HOPE AND WE PERFORM

Casablanca, Maroc
contact@hope3k.net
www.hope3k.net

Casablanca, Maroc
contact@prisalya.com
www.prisalya.com

HOPE 3K 10 ANS À VOTRE SERVICE

HOPE AND WE PERFORM

PRISALYA CONSULTING