# **Introduction générale**

Ce rapport de stage PFE décrit mon expérience au sein de Deloitte Morocco Cyber Center, où j'ai effectué un stage portant sur le thème du Zero Trust en gestion des accès et des identités. Ce stage s'inscrit dans le cadre de ma formation académique et a été réalisé dans le but de développer un démonstrateur d’outils IAM proposant une architecture Zero Trust.

Le rapport est structuré en quatre chapitres, couvrant les différentes étapes de mon stage. Le premier chapitre est consacré à la présentation de mon entreprise d'accueil, Deloitte Morocco Cyber Center. Nous examinerons son positionnement sur le marché de la cybersécurité ainsi que ses domaines d'expertise.

Le deuxième chapitre traite le contexte général du projet. Nous discuterons des enjeux actuels de la sécurité de l'information et de la nécessité pour les organisations d'avoir une approche solide de Zero Trust. Nous mettrons en évidence les défis et les opportunités qui ont motivé le développement de ce démonstrateur, ainsi que les objectifs fixés pour sa conception.

Le troisième chapitre est consacré à une étude détaillée du projet. Nous décrirons en détail l'architecture fonctionnelle et technique du démonstrateur, en nous concentrant sur les différentes phases de son élaboration, les méthodologies utilisées et les principaux éléments qui la composent. Nous expliquerons également comment ces outils peuvent être appliqués dans un environnement réel pour améliorer la sécurité de l'information d'une organisation.

Enfin, le quatrième chapitre se concentre sur la mise en œuvre et le déploiement du démonstrateur. Nous présenterons les différentes étapes à suivre pour la mise en œuvre des différents outils, en soulignant les résultats obtenus, les difficultés rencontrées et les enseignements tirés. Nous évoquerons également les perspectives et les recommandations pour l'amélioration continue du démonstrateur.

Ce rapport de stage a pour objectif de donner un aperçu de mon expérience au sein du Deloitte Morocco Cyber Center, ainsi que des résultats obtenus dans le cadre du projet de développement d’un démonstrateur d’outils IAM proposant une architecture Zero Trust. Il représente une opportunité de partager les connaissances et l'apprentissage acquis durant cette période de stage, tout en mettant en avant les compétences techniques et professionnelles développées.

Il convient de noter que certaines informations spécifiques relatives à l'entreprise d'accueil et aux projets des clients ont été omises ou rendues anonymes afin de respecter les obligations de confidentialité. Toutefois, cela n'affecte en rien la compréhension globale du rapport ou la présentation des résultats obtenus.

Dans la suite de ce rapport, nous discutons chaque chapitre en détail, en soulignant les aspects clés du projet et en fournissant des analyses approfondies.

# **Chapitre 1 : Présentation de l’entreprise d’accueil**

1. Introduction

Dans ce premier chapitre, nous introduisons l'organisme d'accueil, qui est l'entreprise prestataire du projet. Nous présentons brièvement la fiche technique de l'entreprise, en mettant en évidence des informations clés telles que son nom, son adresse et sa taille. Ensuite, nous abordons les domaines d'activité de l'entreprise, en soulignant les secteurs dans lesquels elle exerce ses activités principales. Enfin, nous donnons un aperçu de la structure et de l'organisation générale de l'entreprise, en mettant en avant les départements et les équipes qui la composent. Ces informations fournissent un contexte essentiel pour la suite de notre étude.

## Fiche technique de l’entreprise

Nous présentons dans ce qui suit l’organisme multinational Deloitte, sa filiale au Maroc Deloitte Morocco Cyber Center et l’équipe IAM qui nous a accompagné pour accomplir nos missions de stage PFE.

Les “Big Four” est le terme utilisé pour désigner collectivement les quatre plus grands ca- binets d’audit, à savoir Deloitte, Ernst & Young, KPMG et PwC. Deloitte est réputé être le plus ancien et le plus important de ces quatre grands cabinets avec plus de 175 ans d’excellence. Son chiffre d’affaires s’est élevé à **64.9 milliards** de dollarset **457,000** employésen 2023 couvrant plus de 150 pays.

Deloitte mobilise un ensemble de compétences diversifiées pour répondre aux enjeux de ses clients, de toutes tailles et de tous secteurs en visant la qualité la plus élevée en matière de prestation de services et de conseils professionnels sur différents métiers :

|  |  |
| --- | --- |
| Audit et Assurance | L’audit financier consiste à donner une opinion sur l’information financière mise à la disposition des marchés financiers et des différentes parties prenantes de l’entreprise |
| Consulting | Répondre aux demandes d’un paysage réglementaire complexe et changeant tout en restant flexible en allant jusqu’à l’externalisation. |
| Financial Advisory | Accompagner les entreprises dans la maîtrise de leurs risques financiers et la gestion de leurs ressources rares en alliant des compétences en organisation, modélisation et processus, en s'appuyant sur des outils éprouvés. |
| Juridique | Aider les entreprises à maîtriser et piloter leurs opérations, leurs tiers, leurs données et leurs projets. |
| Fiscalité | Anticiper des Cyber menaces toujours plus probables avec une approche stratégique de vigilance et de résilience. |
| Risk Advisory | Deloitte accompagne ses clients à connaître les risques, de les évaluer, les modéliser, afin de prendre des décisions éclairées. |

Table 1.1: Services de Deloitte

## Risk Advisory

Image de marque, impact de l’entreprise sur l’environnement, mise en conformité face à un environnement réglementaire complexe, protection des actifs numériques, Deloitte accompagne ses clients dans la gestion de tous ces risques s’articulant autour de 5 grandes catégories :

|  |  |
| --- | --- |
| STRATEGIC RISK | Aider les entreprises à identifier et maitriser les risques à fort impact sur leur stratégie en agissant sur la gouvernance, la réputation et le développement durable. |
| REGULATORY RISK | Répondre aux demandes d’un paysage réglementaire complexe et changeant tout en restant flexible en allant jusqu’à l’externalisation. |
| FINANCIAL RISK | Accompagner les entreprises dans la maîtrise de leurs risques financiers et la gestion de leurs ressources rares en alliant des compétences en organisation, modélisation et processus, en s'appuyant sur des outils éprouvés. |
| OPERATIONAL RISK | Aider les entreprises à maîtriser et piloter leurs opérations, leurs tiers, leurs données et leurs projets. |
| CYBER RISK | Anticiper des Cyber menaces toujours plus probables avec une approche stratégique de vigilance et de résilience. |

Table 1.2: Catégories de risques au sein de Risk Advisory

## Deloitte Morocco Cyber Center - DMCC

Le **DELOITTE MOROCCO CYBER CENTER** est un centre de Cyber Intelligence qui dispose d'un pool de spécialistes cybersécurité, de technologies et de services pour répondre au besoin croissant d'expertise cyber, et pour élargir l'offre de services de Deloitte Global sur le continent Africain.

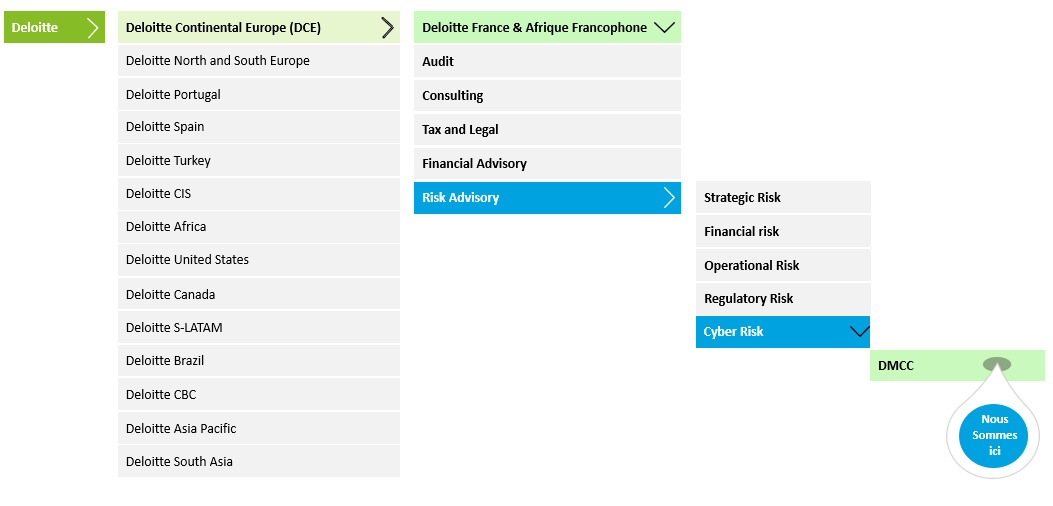


Figure 1.3: Deloitte Morocco Cyber Center

Le **DMCC** est le premier centre cyber en Afrique à offrir des services cyber en conformité avec les meilleures pratiques en matière de cybersécurité. Le centre se situe au cœur du **Casablanca Finance City**, la place économique et technologique connu comme le premier hub financier en Afrique.

Le **DMCC** vise à contribuer à favoriser l’emploi des experts et des ingénieurs Marocains diplômés des grandes écoles et universités d’ingénierie au Maroc en leur offrant le meilleur environnement de travail et l’opportunité de développer leurs compétences, et à développer un écosystème local en cybersécurité qui rayonnera au niveau national, régional et mondial.

Faisant partie d’un réseau de centre Deloitte de services cyber, avec un **mode opérationnel 24/7**, et un effectif de plus de **120 experts** dans le domaine, le centre **DMCC** fournit des services managés et un accompagnement rapproché à ses clients autour du globe sur les différents piliers couvrant l’ensemble des activités de la cybersécurité.

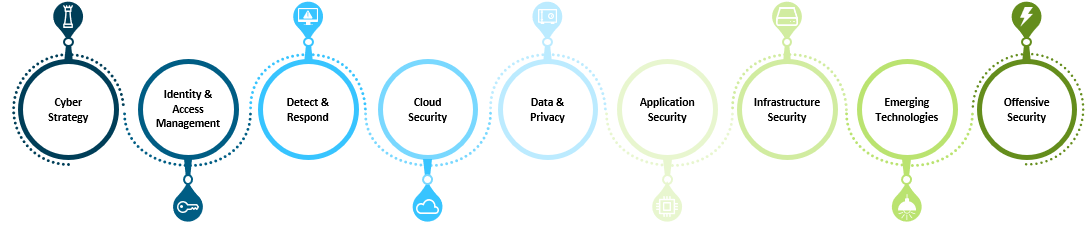


Figure 1.4: Services du DMCC

* **Identity & Access Management :** Aider les clients à assurer à la fois la sécurité des identités et des accès, et une expérience utilisateur fluide,
* **Cyber Strategy :** Accompagner les clients à faire coïncider leur stratégie cyber idéale avec leurs objectifs stratégiques sur l’ensemble du périmètre de l’entreprise,
* **Detect & Respond :** Mettre en place des programmes de cyber défense et de gestion des incidents afin de faire face, de se protéger et de remédier aux cybers attaques,
* **Cloud Security :** Réussir la migration de tous les processus métier d’une entreprise vers le Cloud et ce de manière sécurisée et privée,
* **Data & Privacy :** Aider à la gestion des informations personnelles, sensibles et confidentielles que nos clients collectent, traitent et partagent,
* **Application Security :** Sécuriser les applications tout au long du cycle de développement des systèmes,
* **Infrastructure Security :** Définir les bons mécanismes afin de sécuriser le réseau et les infrastructures des organisations,
* **Emerging Technologies :** Sécuriser les technologies de nouvelle génération, telles que l'Internet des objets (IoT) et les systèmes de contrôle industriel (ICS),
* **Offensive Security :** Aider les organisations à évaluer leur résilience face aux cyberattaques en testant et examinant leurs systèmes.

## Pilier Principal

Le pilier dans lequel j’ai effectué mon stage est le pilier Identity & Access Management (IAM) qui vise à aider les clients avec la gouvernance et la gestion des identités et des accès dans une ère où la cybersécurité est omniprésente. Deloitte accompagne la conception, l’analyse et l’implémentation de processus IAM garantissant une gouvernance et une gestion opérationnelle fiables des identités et des accès en se basent sur des référentiels reconnus sur le marché dans ses projets visant à renforcer la maturité des politiques IAM, et met son expertise des technologies ainsi que sa connaissance fine du marché à la disposition de ses clients, permettant ainsi d’appréhender avec sérénité des thématiques d’actualité, dont :

* + La fédération des identités et des accès dans le cloud ;
  + Le choix et la typologie de l’outillage IAM ;
  + Les politiques de sécurité et d’authentification ;
  + L’adaptabilité et la qualité des processus IAM ;
  + Le contrôle de l’accès aux ressources sensibles ;
  + La conformité aux cadres législatifs facilitée par l’outillage IAM/IAG.

Compte tenu de l’évolution rapide des métiers et des systèmes d’information vers plus d’ouverture et de synergie, Deloitte fournit l’expertise métier et technologique nécessaire pour répondre aux enjeux liés à la transformation numérique de ses clients :

* + Fédération des identités, intégration des filiales et ouverture aux partenaires ;
  + Protection des actifs, renforcement de la sécurité des données ;
  + Amélioration des processus d’intégration des nouveaux arrivants ;
  + Intégration des politiques d’entreprise en matière de gestion des accès et habilitations sensibles ;
  + Respect des cadres de conformité applicables au secteur d’activité ;
  + Maîtrise des coûts et des risques organisationnels et opérationnels.

Dans un environnement où les menaces et les risques liés à la cybercriminalité sont de plus en plus présents, il est essentiel pour les entreprises de développer une stratégie de cybersécurité solide qui réponde à leurs besoins spécifiques et qui soit alignée sur leurs objectifs globaux.

Le pilier IAM se concentre sur cette dimension stratégique et téchnique en travaillant étroitement avec les clients pour comprendre leurs objectifs, leurs défis et leurs priorités.

**Description du déroulement de stage**

Le 6 février 2023, j'ai entamé mon stage au sein de Deloitte MCC. La première journée a été consacrée à l'intégration, au cours de laquelle notre senior manager et l'équipe des ressources humaines nous ont présenté l'organisation et les activités de Deloitte. Nous avons également eu un aperçu des différents piliers et de l'équipe. Par la suite, nous avons entamé les formations d'intégration ainsi que les formations sur les différentes plateformes d'e-learning.

Une semaine plus tard, j'ai été intégré à mon pilier principal, qui est le pilier Cyberstrat, et on m'a attribué mon sujet de stage. J'ai commencé par effectuer des recherches approfondies sur le sujet, ainsi que sur les normes et les standards internationaux qui me guideront dans l'élaboration de ma solution. Ensuite, j'ai défini l'approche à suivre et les différents services que je devais aborder pour ma solution. J'ai entamé la phase de conception de ma solution tout en suivant des formations complémentaires qui m'ont aidé dans cette démarche. De plus, j'ai régulièrement eu des points de suivi avec mon encadrant pour discuter de l'avancement du projet et recevoir des suggestions d'amélioration.

Par la suite, j'ai été intégré dans une mission client en lien avec mon sujet de stage, où j'ai pu constater concrètement l'utilité de ma solution et sa contribution à l'amélioration de la qualité du travail. Cette expérience m'a permis de mettre en pratique mes connaissances et de voir les résultats concrets de mes efforts.

Dans l'ensemble, mon stage chez Deloitte MCC a été une occasion unique de développer mes compétences, d'acquérir une expérience précieuse dans le domaine de la cybersécurité, et de voir comment mes efforts peuvent avoir un impact réel sur les clients et leur activité. Je suis reconnaissante d'avoir eu cette opportunité au sein d'une entreprise réputée telle que Deloitte.

## Conclusion

En conclusion, ce premier chapitre nous a permis de poser les bases de notre rapport de stage en présentant l'organisme d'accueil, l'équipe Cyber du service Risk Advisory et le pilier Cyberstrat auquel j'ai été rattaché. Nous avons également décrit le déroulement de ma période de stage, mettant en évidence les différentes étapes et activités auxquelles j'ai participé.

Ce chapitre a été essentiel pour contextualiser notre expérience de stage et fournir une compréhension claire de l'environnement dans lequel nous avons évolué. Il a permis de mettre en lumière l'importance de la cybersécurité et de la stratégie en matière de cybersécurité dans les entreprises actuelles, où les risques liés à la cybercriminalité sont omniprésents.

À travers notre intégration dans l'équipe Cyberstrat, nous avons pu développer nos connaissances et nos compétences dans le domaine de la cybersécurité, en nous familiarisant avec les normes et les meilleures pratiques internationales. Nous avons également eu l'occasion de mettre en pratique nos connaissances en participant à une mission client, où nous avons constaté l'impact concret de nos travaux sur l'amélioration de la sécurité et de la qualité du travail au sein de l'entreprise cliente.

Ce premier chapitre jette les bases pour les chapitres à venir, où nous approfondirons les détails de notre projet, les méthodologies utilisées, les résultats obtenus et les enseignements tirés de notre expérience de stage.

## Contexte du projet

## Contexte générale

La « dé-périmètrisation » du système d’information (SI) d’entreprise, vision anticipatrice imaginée par le Jericho Forum au début des années 2000, est en passe de devenir une réalité grâce à l’adoption massive du Cloud et du télétravail.

D’un SI centralisé où les ressources sont pour la plupart hébergées au niveau des Datacenters de l’entreprise et où les utilisateurs travaillent majoritairement depuis les locaux de l’entreprise, nous évoluons vers un SI décentralisé où les ressources sont réparties entre les Datacenters et un ou plusieurs environnements Cloud, et où les utilisateurs peuvent travailler depuis n’importe où.

Face à une telle transformation qui a pour effet d’augmenter la surface d’attaque du SI et à une menace cyber qui trouve presque toujours le moyen de s’introduire dans le SI, les modèles de sécurité traditionnels, basés sur la mise en œuvre de périmètres de sécurité réseau et de zones de confiance sont remis en question.

Dans ce contexte, la philosophie Zero Trust connait un engouement important. Cependant, si les principes théoriques sont aujourd’hui relativement bien connus et compris, nombreuses sont les entreprises à s’interroger sur la démarche concrète de mise en œuvre d’un modèle Zero Trust.

## Objectifs

Le stage a pour objectifs de **démontrer la faisabilité d’une architecture Zero Trust** – **avec un focus sur l’architecture Zero Trust IAM** - et **d’évaluer son niveau de sécurité via la conception et la mise en œuvre d’un démonstrateur**.

## Travaux à réaliser

Sous la tutelle d’un.e consultant.e et le pilotage d’un.e manager, le/la stagiaire pourra être amené.e à réaliser une partie ou la totalité des travaux suivants :

* Définition des cas d’usage du démonstrateur et son architecture fonctionnelle
* Identification et étude des solutions du marché permettant la mise en œuvre d’une architecture Zero Trust
* Définition de l’architecture technique du démonstrateur
* Mise en œuvre du démonstrateur dans un environnement Cloud
* Evaluation du niveau de sécurité de la maquette et les limites des solutions actuelles

## Plan de projet

## Conclusion

# **Chapitre 2 : Etat de l’art** Introduction

Avant d'entrer dans notre sujet, il faut d'abord clarifier les définitions des principaux concepts

liés à notre projet, ce qui est l'objet de ce chapitre, où nous présenterons l'historique, la

définition et les avantages de Zero-Trust. Ce chapitre donne également un aperçu des

différentes briques sécuritaires du Zero-Trust, ainsi que de l'architecture de ZT proposée par

le NIST.

## Zero Trust

## Historique

Traditionnellement, les limites de sécurité étaient placées à la périphérie du réseau de

l'entreprise selon une approche classique de type "muraille et douves" du château.

Cependant, avec l'évolution de la technologie, les travailleurs distants et les charges de travail

distantes sont devenus plus courants. Les limites de sécurité ont donc nécessairement suivi et

se sont étendues non seulement à la périphérie de l'entreprise, mais également aux appareils

et réseaux auxquels l'utilisateur distant était connecté, ainsi qu'aux ressources auxquelles il

accédait. Cela a contraint les équipes de sécurité et de réseau à adapter les modèles de

sécurité et d'accès appliqués par les organisations pour répondre à ces exigences

commerciales, avec des degrés de succès mitigés. En 2010, l'analyste de Forrester John

Kindervag a introduit le terme "Zero Trust" dans l'influent document "No More Chewy

Centers: Introducing The Zero Trust Model Of Information Security". Ce document a capturé

des idées qui avaient été discutées dans l'industrie depuis quelques années, en particulier

celles promues par le Forum Jericho. Le document de Forrester a décrit le passage d'une

périphérie dure à une approche qui exigeait d'inspecter et de comprendre les éléments d'un

réseau avant qu'ils puissent gagner un niveau de confiance et d'accès. Avec le temps, Forrester

a développé ce concept en ce qui est maintenant connu sous le nom de cadre Zero Trust

eXtended (ZTX), qui comprend les données, les charges de travail et l'identité comme

composants clés de Zero Trust.

## Définition

Zero Trust est un modèle complet de sécurité pour protéger les ressources de réseau,

d'application et de données. Il se concentre sur l'utilisation d'un modèle de politique centré

sur l'identité pour contrôler l'accès. Bien que chaque entreprise ait des outils informatiques

et de sécurité en place, Zero Trust exige une approche holistique, avec l'identité au centre,

afin d'appliquer des politiques de sécurité qui tiennent compte du contexte et des attributs

dans tout l'environnement.

## Avantages de Zero Trust

Visibilité accrue de l'accès aux ressources : l'approche de la sécurité Zero trust exige que vous

déterminiez et classiez toutes les ressources du réseau. Cela permet aux entreprises de mieux

voir qui accède à quelles ressources pour quelles raisons et de comprendre les mesures à

appliquer pour sécuriser les ressources.

Diminution de la surface d'attaque : en mettant l'accent sur la sécurisation des ressources

individuelles, les entreprises qui appliquent les principes de Zero trust sont confrontées à une

réduction des risques d'attaques de pirates visant le périmètre du réseau.

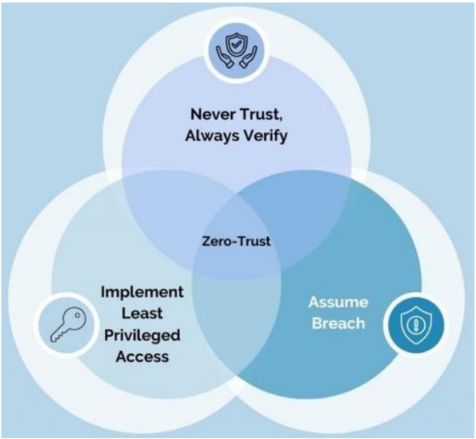
Amélioration du contrôle : la mise en œuvre d'une stratégie de sécurité Zero trust est associée

au déploiement d'une solution de surveillance et de journalisation continues de l'état des

ressources et de l'activité des utilisateurs. Cela permet aux entreprises de mieux détecter les

menaces potentielles et d'y répondre en temps utile.

## Principes du Zero Trust



Le modèle Zero Trust obéit à trois principes qui guident et étayent l’implémentation de la

sécurité. Ces principes sont les suivants :

Vérification explicite : Chaque accès est vérifié et autoriser en fonctions de plusieurs critères

: identité, emplacement, état de santé de l’équipement

Accès selon le privilège minimum : Le principe du privilège minimum dans le modèle Zero

Trust est souvent utilisé en conjonction avec deux autres principes : Just-In-Time Access (JIA)

et Just Enough Access (JEA).

• Le principe JIA permet de limiter l'accès des utilisateurs et des dispositifs à des

ressources sensibles pendant une période définie. Par exemple, un utilisateur peut

être autorisé à accéder à une ressource critique pendant une période spécifique pour

accomplir une tâche, après quoi l'accès est automatiquement révoqué. Cette mesure

réduit le risque d'utilisation non autorisée de ressources sensibles.

• Le principe JEA permet de limiter l'accès des utilisateurs et des dispositifs à un niveau

spécifique de privilège, en ne leur donnant accès qu'aux fonctions et aux informations

nécessaires pour accomplir leur travail, et rien de plus. De cette manière, les

utilisateurs ne peuvent pas accéder à des données sensibles ou des fonctions qui ne

sont pas nécessaires à leur travail.

En combinant les principes du privilège minimum, du Just-In-Time Access et du Just Enough

Access, les entreprises peuvent mettre en place des politiques de sécurité efficaces pour

minimiser les risques de violation de données, tout en permettant aux utilisateurs et aux

dispositifs de travailler de manière productive.

Supposition de violation. Le principe de supposition de violation dans le cadre du modèle de

sécurité Zero Trust implique d'adopter une approche proactive pour la sécurité des systèmes

d'information. Ce principe suppose que les menaces existent en permanence et vise à

détecter et à répondre aux violations de sécurité potentielles avant qu'elles ne causent des

dommages considérables. Pour y parvenir, il est crucial de procéder à une vérification

constante des utilisateurs, des dispositifs et des connexions, afin de minimiser les risques de

violation de données et de limiter les effets d'une telle violation.

## Composants clés de Zero Trust

Pour mettre en place une architecture Zero Trust efficace, plusieurs composants clés doivent

être pris en compte :

Authentification forte : pour s'assurer que les utilisateurs sont bien ceux qu'ils prétendent

être.

Micro-segmentation : pour diviser le réseau en zones distinctes et contrôler les accès entre

ces zones.

Visibilité en temps réel : pour surveiller les activités du réseau et détecter les éventuelles

anomalies.

Contrôle d'accès basé sur le contexte : pour prendre en compte les caractéristiques de chaque

session et déterminer les permissions d'accès appropriées.

Chiffrement bout en bout : pour garantir la confidentialité des données.

Validation continue : pour vérifier que tous les composants fonctionnent correctement.

Automatisation et orchestration : pour gérer l'ensemble de ces composants de manière

cohérente et efficace.

## Architecture Zero Trust selon NIST

Le choix du NIST comme référence pour la présentation de l'architecture Zero Trust repose

sur sa réputation en tant qu'autorité respectée dans le domaine de la cybersécurité. Grâce à

son expertise et à sa rigueur scientifique, ce dernier a pu identifier les composants essentiels

et fournir des lignes directrices précises pour la construction d'une architecture Zero Trust.

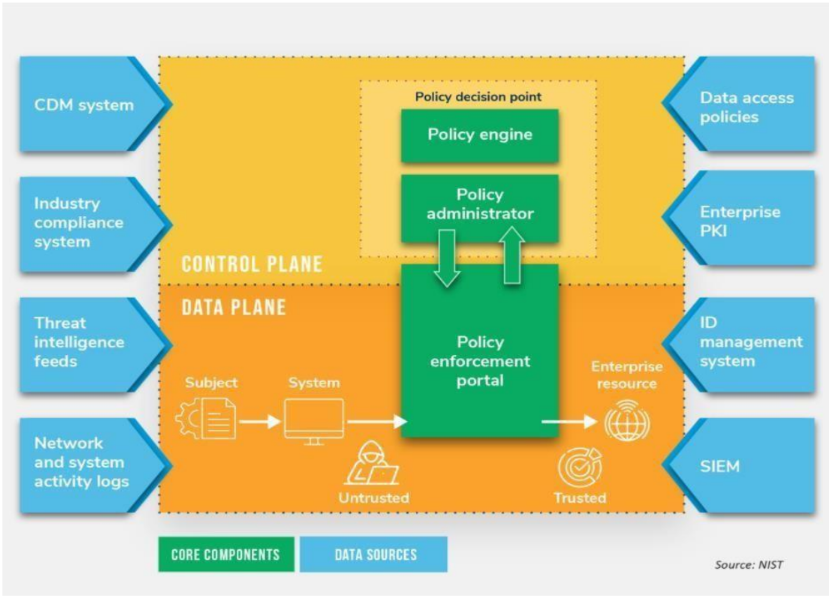
Le modèle de sécurité Zero Trust est un concept plutôt qu'une solution clé en main qu'une

entreprise peut simplement adopter. Cependant, le NIST a identifié les composants clés qui

peuvent aider à construire une architecture Zero Trust à travers son état de l'art. Une

architecture Zero Trust est généralement composée de deux parties : le Control Plane et le

Data Plane.



## Control Plane

Le control plane représente l’ensemble des composants chargés de collecter les informations

nécessaires à la retranscription du contexte et chargés de la prise de décision. Il est composé

du « policy decision point », lui-même composé du « policy engine » et du « policy

administrator ».

Policy engine :

Ce composant est responsable de la décision finale d'accorder l'accès à une ressource pour un

sujet donné. Le PE utilise la politique de l'entreprise ainsi que des données provenant de

sources externes pour alimenter un algorithme de confiance afin d'accorder, de refuser ou de

révoquer l'accès à la ressource.

Policy administrator :

Ce composant est chargé d'établir et/ou de fermer le chemin de communication entre un sujet

et une ressource. Il génère toute authentification spécifique à une session et tout jeton ou

justificatif d'authentification utilisé par un client pour accéder à une ressource d'entreprise. Il

est étroitement lié à la PE et s'appuie sur sa décision d'autoriser ou de refuser finalement une

session.

## Data plane

Le reste des composants se trouve dans le data plane. Le data plane représente l’ensemble

des composants avec lesquels l’utilisateur peut interagir. L’utilisateur peut interagir avec le

policy enforcement point mais pas avec le policy decision point qui est dans le control plane.

* Policy Enforcement Point :

Ce système est chargé d'activer, de surveiller et, éventuellement, de mettre fin aux

connexions entre un sujet et une ressource d'entreprise. Le pep communique avec le PA pour

transmettre des demandes et/ou recevoir des mises à jour de politiques de la part du PA. Il

s'agit d'un seul composant logique dans ZTA, mais il peut être divisé en deux composants

différents : le côté client et le côté ressource.

## Limites de Zero Trust

Le modèle de sécurité Zero Trust a été présenté comme une défense ultra-sécurisée contre

les menaces émergentes et non reconnues. Contrairement à la sécurité périmétrique, il ne

part pas du principe que les personnes à l'intérieur d'une organisation sont automatiquement

en sécurité. Au contraire, il exige que chaque utilisateur - interne et externe - soit autorisé

avant tout accès.

* Une approche fragmentaire de la cybersécurité zéro confiance peut créer des lacunes :

La cybersécurité à confiance zéro peut éventuellement conduire à une sécurité supérieure, mais en cours de route, elle peut exposer les entreprises à un risque accru. La plupart des

entreprises personnalisent leurs propres stratégies en utilisant une approche fragmentaire,

mais des lacunes ou des fissures peuvent se développer et rendre la confiance zéro moins

solide qu'annoncé. Dans le même temps, le démantèlement d'une solution existante peut

créer des failles de sécurité inattendues.

* La cybersécurité "zéro confiance" exige un engagement d'administration permanente :

Un autre obstacle souvent négligé au passage à un modèle de cybersécurité à confiance zéro

est la nécessité d'une administration permanente. Les modèles de confiance zéro reposent

sur un vaste réseau de permissions strictement définies, mais les entreprises sont en constante évolution. Les personnes occupent de nouveaux rôles et changent de site. Les

contrôles d'accès doivent être mis à jour à chaque fois pour garantir que les bonnes personnes

ont accès à des informations spécifiques. Le maintien de l'exactitude et de la mise à jour des

autorisations nécessite une saisie permanente.

* Impacte de Zero Trust sur la productivité :

L'introduction d'une approche de la cybersécurité fondée sur la confiance zéro peut

également affecter la productivité. Le défi principal de la confiance zéro est de verrouiller

l'accès sans 40 interrompre les flux de travail. Les gens ont besoin d'accéder à des données

sensibles pour travailler, communiquer et collaborer. Si une personne change de rôle et se

retrouve bloquée pendant une semaine pour accéder à des fichiers ou des applications, sa

productivité peut chuter. Dans le pire des cas, la perte de productivité devient un problème

plus important que la cybersécurité elle-même.

## Conclusion

En conclusion de ce chapitre, nous avons exploré en détail le concept de Zero Trust, son

historique, ses avantages, ses principes ainsi que ses composants et son architecture selon le

NIST. Nous avons également entamé notre exploration de la brique de l'IAM, en fournissant

une définition claire et en définissant son scope, qui comprend le magasin d'identité, le cycle

de vie de l'identité et la gestion des accès. Ces deux domaines sont des éléments essentiels

pour renforcer la sécurité des systèmes d'information et garantir un niveau de confiance approprié. Dans les prochains chapitres, nous approfondirons davantage ces sujets et

explorerons leurs interactions pour construire une infrastructure de confiance solide.

# **Chapitre 3 : – Etude comparatif et présentation des solutionsINTRODUCTION**

Dans ce chapitre nous allons découvrir les deux technologies IAM et Zero Trust en détail en

présentant leurs avantages et leurs contributions dans une architecture Zero Trust, nous

allons aussi comparer les éditeur leader dans les deux briques, et finalement présenter les

solutions choisies.