2600
Ecole de cybersécurité

École 2600

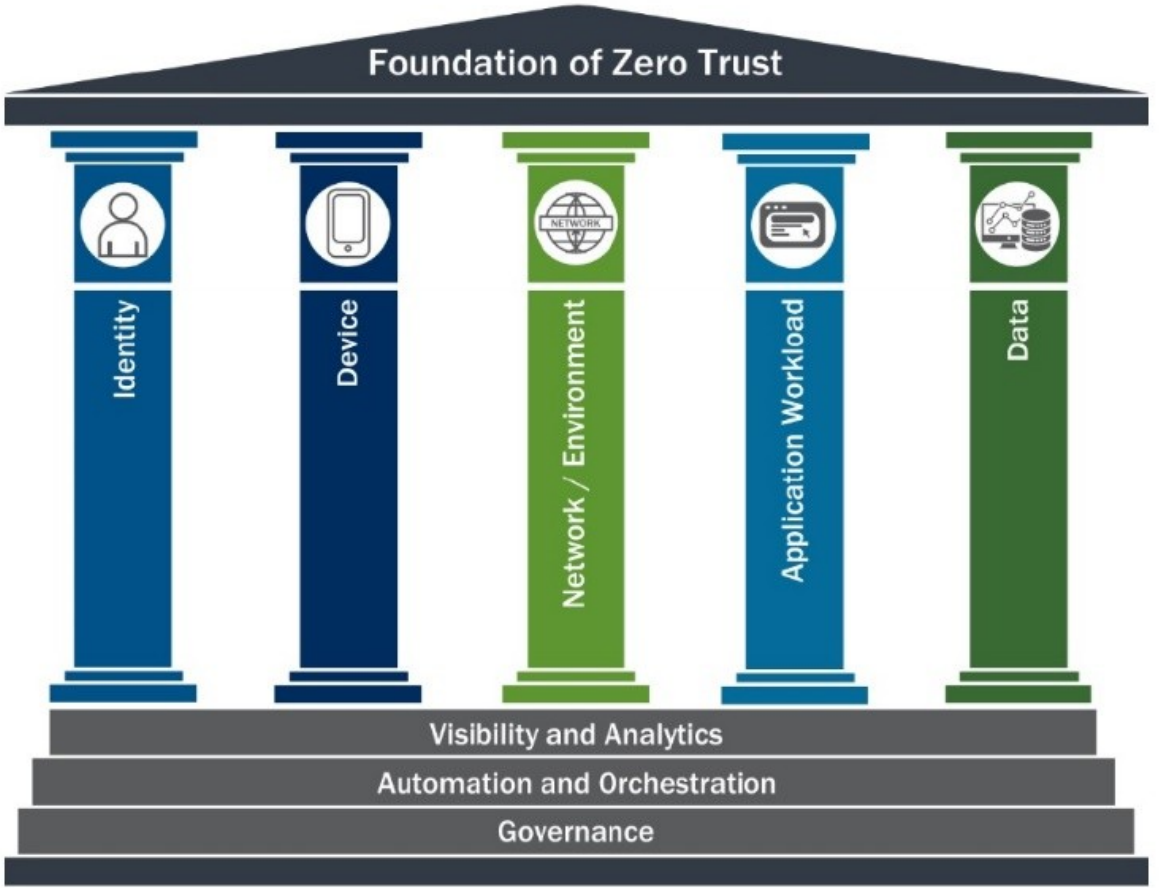
Cours Zero Trust

Implémentation 1

Juillet 2023

Les briques techniques du Zero Trust

Socles et piliers du Zero Trust



Source : CISA

Pilier **identité**

- L'identité est le « nouveau périmètre », puisque le réseau ne délimite plus les frontières du SI
- Utilisateur (humain) ou service, l'identité qui est à l'initiative de la demande d'accès à la ressource doit être au centre de la décision prise par le composant de contrôle d'accès dynamique
- Elle doit être administrée correctement (socle gouvernance), ainsi que les droits d'accès correspondants (respect du principe de moindre privilège)
  - Y compris lors des changements de rôles
  - Et lorsque l'employé quitte l'organisation
- Le risque sur l'identité est calculé en se basant sur le contexte, à travers l'analyse de signaux qui pourra déclencher par exemple une demande d'authentification multi-facteurs
- Envisager IDaaS comme « meilleure solution » technique

Pilier **appareils**

- La sécurité et la conformité des appareils doivent être assurées :
  - Par une gestion des politiques de sécurité
    - Dont on s'assurera qu'elles sont bien respectées, ex. solutions EMM
  - Par l'application sans délai des correctifs de sécurité, des mises à jour de l'OS, des signatures antimalware, etc.
  - Par la mise en œuvre d'outils de type EDR/MTD avec remontée vers l'outil de supervision central, pour la détection et réponse aux menaces
  - Par l'utilisation, si nécessaire, de dispositifs de sécurité physique et/ou cryptographique renforcée
    - Ex. TPM/HSM, dispositifs matériels permettant de prouver l'identité (ou même l'intégrité) de l'appareil
- L'état sanitaire de l'appareil est pris en compte dans l'évaluation du risque par le composant de contrôle d'accès dynamique

Quelques définitions

- IDaaS (*identity as a service*) ⇒ gestion des identités via un service Cloud
- EMM (*enterprise mobility management*) ⇒ gestion de configuration et sécurité d'un parc d'appareils mobiles et postes de travail portables hors site
- EDR (*endpoint detection & response*) ⇒ solution de sécurité conçue pour protéger les dispositifs d'extrémité, tels que les postes de travail et serveurs
- MTD (*mobile threat defense*) ⇒ sorte d'EDR pour appareils mobiles
- TPM (*trusted platform module*)
  - Composant matériel destiné principalement au stockage sécurisé de clés cryptographiques
  - Puce intégrée dans le système qu'elle protège
- HSM (*hardware security module*)
  - Boîtier matériel destiné au stockage, à la gestion et à l'utilisation sécurisés de clés cryptographiques
  - Composant externe directement relié à un système hôte, ou partagé entre plusieurs hôtes au sein d'un centre de données par exemple

Pilier **réseau / environnement**

- La taille du réseau interne se réduit à mesure que les ressources migrent vers le Cloud
  - Mais certaines ressources critiques restent tout de même hébergées sur site et doivent être protégées, dans « l'esprit Zero Trust »
  - Les bonnes pratiques d'isolation réseau sont à respecter, en explorant les solutions de micro-segmentation
  - Conservation du VPN pour l'administration depuis des postes sécurisés
- Les applications et ressources qui migrent dans le Cloud doivent également être protégées avec les composants réseau disponibles sur la plateforme (segmentation, FWaaS, etc.)
- Dans les deux cas (interne ou Cloud), la détection passe par des solutions d'analyse de flux réseau et par la consolidation des logs en provenance des équipements
  - À destination des outils de supervision (voir socles)

Pilier **applications / « *workload* »**

- Les nouvelles applications et services doivent être développés en tenant compte de la sécurité dès la conception (*security by design / by default*) tout en s'appuyant sur des outils de modélisation des menaces et de détection des vulnérabilités
  - Particulièrement les API et applications SaaS, qui sont plus exposées car accessibles depuis Internet
- Les architectures de référence servent de guide pour implémenter les bonnes pratiques (ex. https://www.redhat.com/architect/application-enterprise-architecture)
- Les outils de gestion et de contrôle de la posture de sécurité des applications sont utilisés pour s'assurer de bien détecter toute erreur de configuration (ex. CSPM)
- Les outils de type CASB (*Cloud Access Security Broker*) permettent de découvrir et contrôler les applications SaaS, tout en bloquant les applications non-autorisées et en protégeant les données sensibles

Quelques définitions : outils pour le Cloud

- **CASB** (*Cloud Access Security Broker*) qui offre généralement une gamme de fonctionnalités telles que la prévention des pertes de données (DLP), la protection contre les cyber-menaces et les politiques pour aider les organisations à sécuriser leur utilisation des services Cloud
- **CSPM** (*Cloud Security Posture Management*) qui se focalise essentiellement sur la gestion de la conformité en environnement Cloud
- **CWPP** (*Cloud Workload Protection Platform*) facilitant la protection au niveau des charges applicatives (*workload*) en environnements distribués
- **CIEM** (*Cloud Infrastructure Entitlement Management*) qui surveille les identités Cloud et leurs droits
- **CNAPP** (*Cloud Native Application Protection Platform*) qui permet aux équipes de sécurité et développeurs d'identifier, de hiérarchiser et de corriger les risques de sécurité, juridiques et de conformité en mode cloud natif

Pilier **données**

- Pour la grande majorité des organisations, les données sont les actifs informationnels les plus importants
- La mise en place d'une **classification** est le moyen d'identifier les données sensibles de manière à les protéger (ex. chiffrement) et à s'assurer qu'elles ne fuitent pas, de manière intentionnelle ou non
  - La mise en place d'une classification peut (ou devrait selon l'ISO 27001) être complétée par l'identification d'un propriétaire en mesure d'évaluer la légitimité des demandes d'accès
- Si elles doivent être partagées en interne ou externe, les outils de collaboration doivent assurer qu'elles sont accessibles uniquement par les personnes désignées dotées des droits nécessaires
- Un suivi du partage des données et des délais de fin d'accès limite les risques de fuite, de même que l'apposition de labels sur les données sensibles et l'usage d'un DLP (*data loss prevention*)
- Une gestion correcte des données personnelles permet de renforcer la conformité en les identifiant et les protégeant en accord avec les réglementations (ex. RGPD)

Classification des informations

- Tenir compte des besoins métier et des exigences applicables
  - Exigences de confidentialité, intégrité et disponibilité (et éventuellement d'autres critères comme la traçabilité)
- Les actifs supports peuvent également être classifiés conformément à la classification des informations qu'ils contiennent
- Les propriétaires des informations devraient être responsables de leur classification
  - À mettre à jour tout au long du cycle de vie de l'information
- La classification peut être déterminée en fonction du niveau d'impact qu'aurait une compromission de l'information (cf. exemple rappelé page suivante)
  - Sur chacun des critères confidentialité, intégrité, disponibilité, etc.
  - *Besoin de disponibilité souvent associé à la notion de durée d'interruption ou de perte de données maximales admissibles (DMIA/PDMA ou en anglais* RTO/RPO*)*

2600
Ecole de cybersécurité

Exemple d'échelle de niveaux d'impact

Type d'impact	Nul Niveau 0	Peu significatif Niveau 1	Gênant Niveau 2	Grave Niveau 3	Critique Niveau 4
Financier	Aucun	Compris entre 0 et 150 k€	Compris entre 150 k€ et 500 k€	Compris entre 500 k€ et 1 M€	Supérieur à 1 M€
Juridique	Aucun	Condamnation(s) civile(s) avec un montant peu élevé de dommage et intérêts	Condamnation(s) civile(s) avec un montant élevé de dommage et intérêts	Condamnation(s) pénale(s) contre un préposé et sanctions financières / dommage et intérêts	Condamnation(s) pénale(s) contre un (des) dirigeant(s) de l'établissement ou décision de suspension de l'activité de l'établissement
Organisation	Aucun	Retard léger dans la réalisation des activités	Retard moyen dans la réalisation des activités	Retard important dans la réalisation des activités	Désorganisation durable et non maitrisée d'un ou plusieurs processus pouvant entraîner l'arrêt d'activités
Image	Aucun	Réclamations potentielles internes ou externes	Réclamations avérées internes ou externes n'occasionnant pas la perte des clients	Réclamations avérées internes ou externes occasionnant la perte des clients	Atteinte grave à la réputation de l'établissement et perte massive de clients
Réglementation	Aucun	Infraction(s) mineure(s) à une réglementation sans sanction	Infraction(s) mineure(s) à une réglementation avec sanction	Infraction(s) majeure(s) à une réglementation avec sanction	Infraction(s) majeure(s) à une réglementation avec sanction pouvant causer un préjudice très important à l'établissement

Les **socles**

- Les 3 socles **Gouvernance**, **Automatisation et Orchestration** et **Visibilité et Analyse** sont transverses et s'appliquent donc à l'ensemble des piliers
- **Gouvernance**
  - Des **identités** ⇒ ensemble de processus de gestion des identités s'appuyant sur les différents référentiels d'identité, y compris les annuaires Cloud
  - Des **applications** ⇒ contrôler qu'elles sont bien déployées dans le respect des politiques de sécurité et qu'elles y restent conformes dans le temps
  - Des **données** ⇒ associer des processus (par ex. demandes d'accès, demande d'ouverture d'un site collaboratif, demande de partage externe…) à des outils techniques qui en assurent l'automatisation
- **Visibilité et Analyse** ⇒ assurer la détection d'attaques ou simplement de leurs prémices sur l'ensemble des piliers
- **Automatisation et Orchestration** de nombreuses tâches ⇒ sert à obtenir plus rapidement des réponses pour contrer le plus rapidement possible une compromission et ainsi en éviter la propagation

Focus sur le socle **Visibilité et Analyse**

- Le socle Visibilité et Analyse doit être capable de corréler de multiples alertes pour les inclure dans des scénarios d'attaques facilitant les investigations présentés aux analystes du SOC, en lien avec l'intelligence des menaces
- Exemples :
  - Alerte sur un utilisateur accédant depuis un nouvel appareil
  - Détection de l'installation de composants particuliers sur un poste
  - Alerte sur des accès non habituels à de multiples sites collaboratifs
  - Événements qui, une fois corrélés, feront suspecter une attaque avec usurpation d'identité…
- Utilisation quasi-obligatoire des technologies IA (*machine learning*) et *big data* pour assurer l'ingestion, le traitement et la corrélation d'alertes sur des volumes gigantesques de données (cf. solutions type SIEM avancé / XDR) tout en minimisant les faux-positifs (qui submergent les analystes du SOC) et en s'appuyant sur l'automatisation pour la réponse aux incidents (ex. SOAR)