Réseau et sécurité

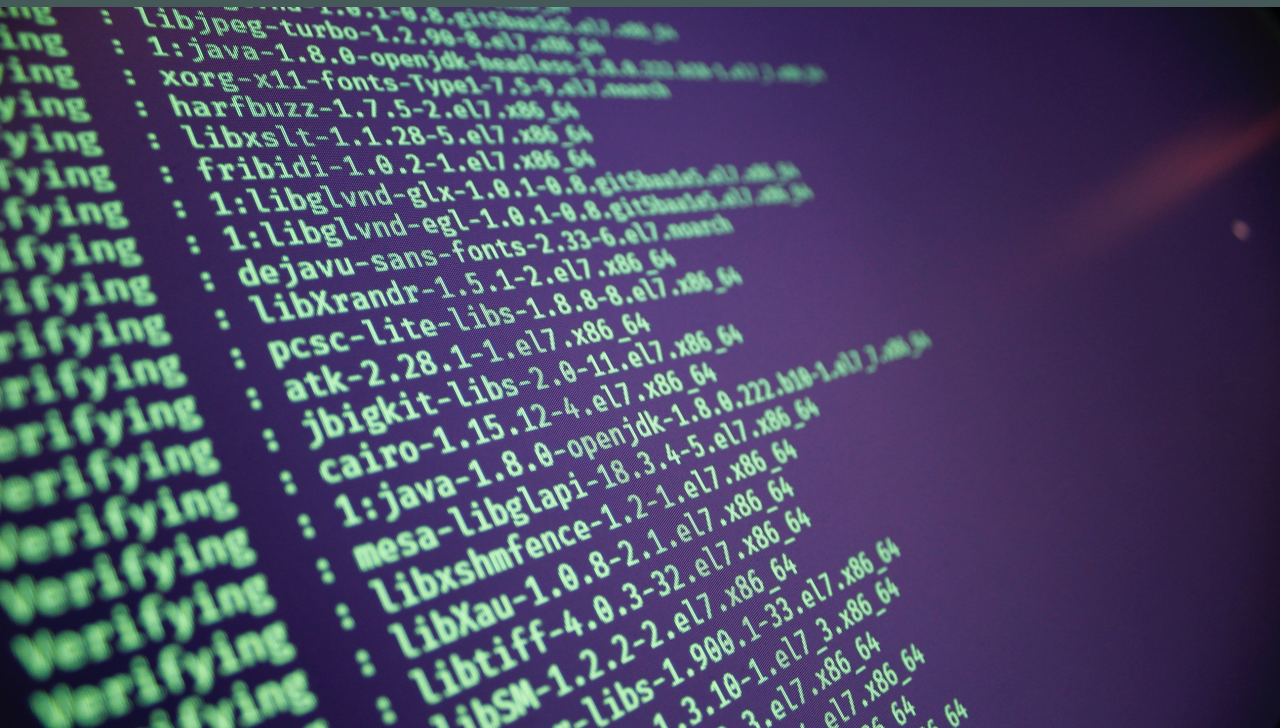
Conseil Scolaire Francophone de la C.-B.

Vincent Aury

Analyste –

Réseau & Cybersécurité

Table des matières



- Introduction
  - Qui suis-je ?
- Cybersécurité - Principes Fondamentaux
  - CIA vs DAD
  - The Cyber Kill Chain
  - Incident Response
- Audit de sécurité pour le CSF (26/01/2024)
  - Aperçu des tests effectués
- Contrôles de sécurité
  - Types de Security Controls
    - Contrôleur d'accès réseau (NAC)
    - Serveur VPN
    - Authentification Multifacteur
    - BYOD (Bring your Own Device)
    - Visibilité des données
    - Visibilité du réseau
- Backup System - Systèmes de sauvegarde
  - Office365 "System Backup"
- Infrastructure au CSF
  - L'importance d'une infrastructure forte

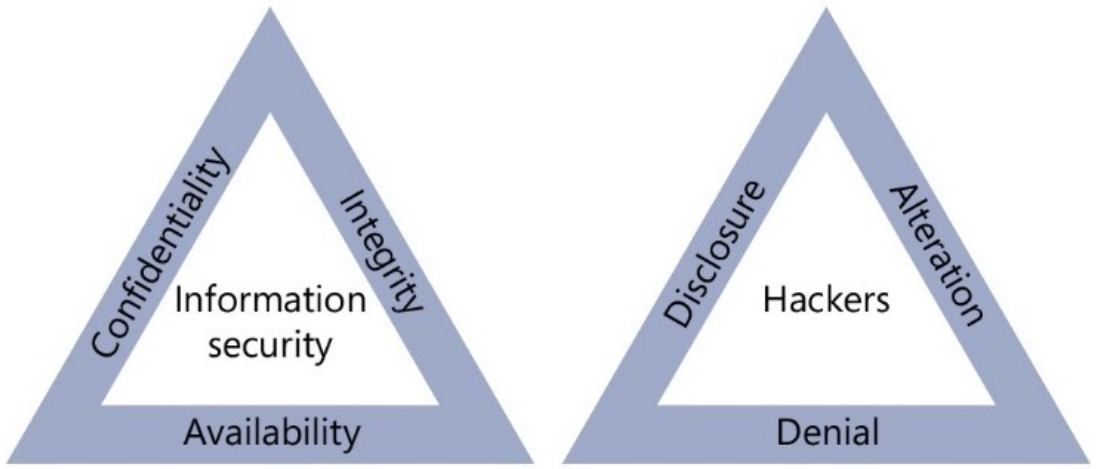
Introduction – Qui suis-je ?

- Vincent Aury
- Travail depuis 2013 pour le CSF
- Analyste Réseau et Cybersécurité
- Certifications actives:
  - CompTIA – Security+ (2020)
  - CompTIA – CyberSecurity Analyst+ (2021)
  - eJPT – Junior Pentester (2022)
  - CompTIA – Pentest+ (2024)

** Trois d'entre elles sont conformes à la directive 8570 du Département de la Défense (DoD-8570).*

Cybersécurité – Principes Fondamentaux

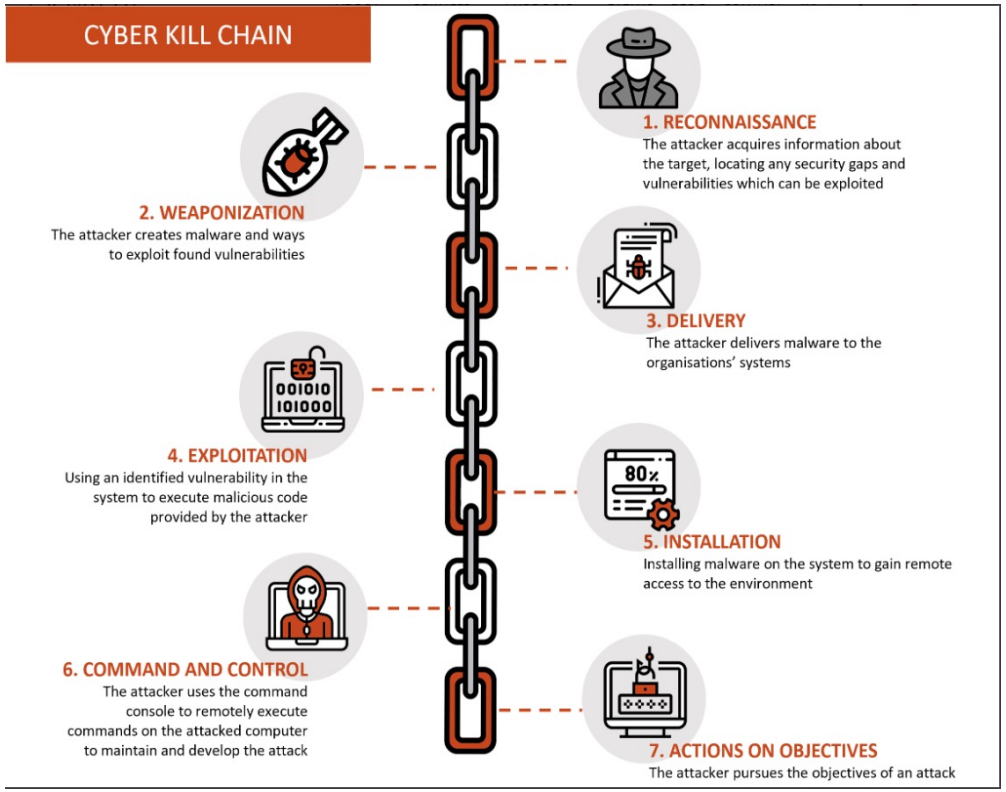
CIA vs DAD



En cybersécurité, le terme "CIA triad" fait référence à trois concepts fondamentaux qui sont essentiels pour assurer la sécurité des données. Ces trois concepts sont la Confidentialité (Confidentiality), l'Intégrité (Integrity) et la Disponibilité (Availability) des données.

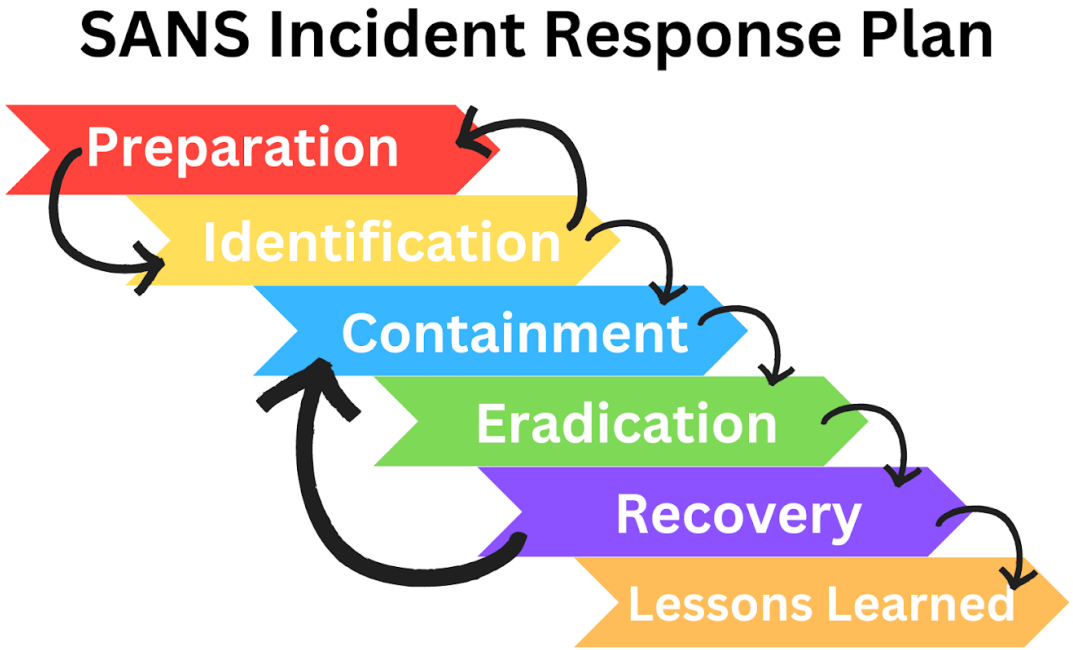
En contrepartie, le terme ”DAD triad”, Divulgation (Disclosure), Altération (Alteration) et Déni (Denial) définit les trois principales stratégies utilisées pour déjouer les objectifs de sécurité d'une organisation.

The Cyber Kill Chain



« **Cyber Kill Chain »** est un concept dérivé de la chaîne d'attaque militaire, une approche progressive destinée à identifier et à bloquer les activités ennemies. Développée initialement par Lockheed Martin en 2011, « Cyber Kill Chain » décrit les différentes phases de plusieurs cyberattaques courantes et, par extension, les points au niveau desquels l'équipe en charge de la sécurité informatique peut prévenir, détecter ou intercepter les cyberattaques.

Incident Response



Préparation : Cette phase consiste à se préparer à répondre aux incidents avant qu'ils ne se produisent. Cela comprend la création de plans de réponse aux incidents, la formation du personnel, la mise en place de systèmes de détection d'incidents et l'élaboration de politiques et de procédures pour gérer les incidents.

Identification : Dans cette phase, les équipes de sécurité informatique détectent et identifient un incident. Cela peut se faire par le biais de systèmes de détection d'intrusion, de surveillance des “logs”, de rapports d'utilisateurs ou d'autres méthodes de détection des activités suspectes.

Isolement : Une fois qu'un incident est identifié, la priorité est de limiter sa propagation et son impact. Cette phase implique d'isoler les systèmes affectés, de bloquer l'accès non autorisé, de désactiver les comptes compromis ou toute autre mesure nécessaire pour empêcher que l'incident ne s'aggrave.

Éradication : Après avoir contenu l'incident, l'étape suivante consiste à éliminer complètement la menace de l'environnement. Cela peut impliquer de supprimer les logiciels malveillants, de corriger les failles de sécurité, de restaurer les données à partir de sauvegardes, ou toute autre action nécessaire pour éliminer complètement la cause de l'incident.

Récupération : Une fois que la menace a été éradiquée, l'objectif est de rétablir les opérations normales aussi rapidement que possible. Cela peut inclure la restauration des systèmes à partir de sauvegardes, la réparation des dommages causés par l'incident, la réactivation des services désactivés et la réintégration des systèmes dans l'environnement de production.

Leçons apprises : Enfin, il est essentiel d'examiner l'incident pour comprendre ce qui s'est passé, pourquoi cela s'est produit et comment cela aurait pu être évité ou mieux géré à l'avenir. Cela implique souvent de mener une analyse post-mortem de l'incident, de documenter les leçons apprises et de mettre à jour les politiques, les procédures et les mesures de sécurité en conséquence.

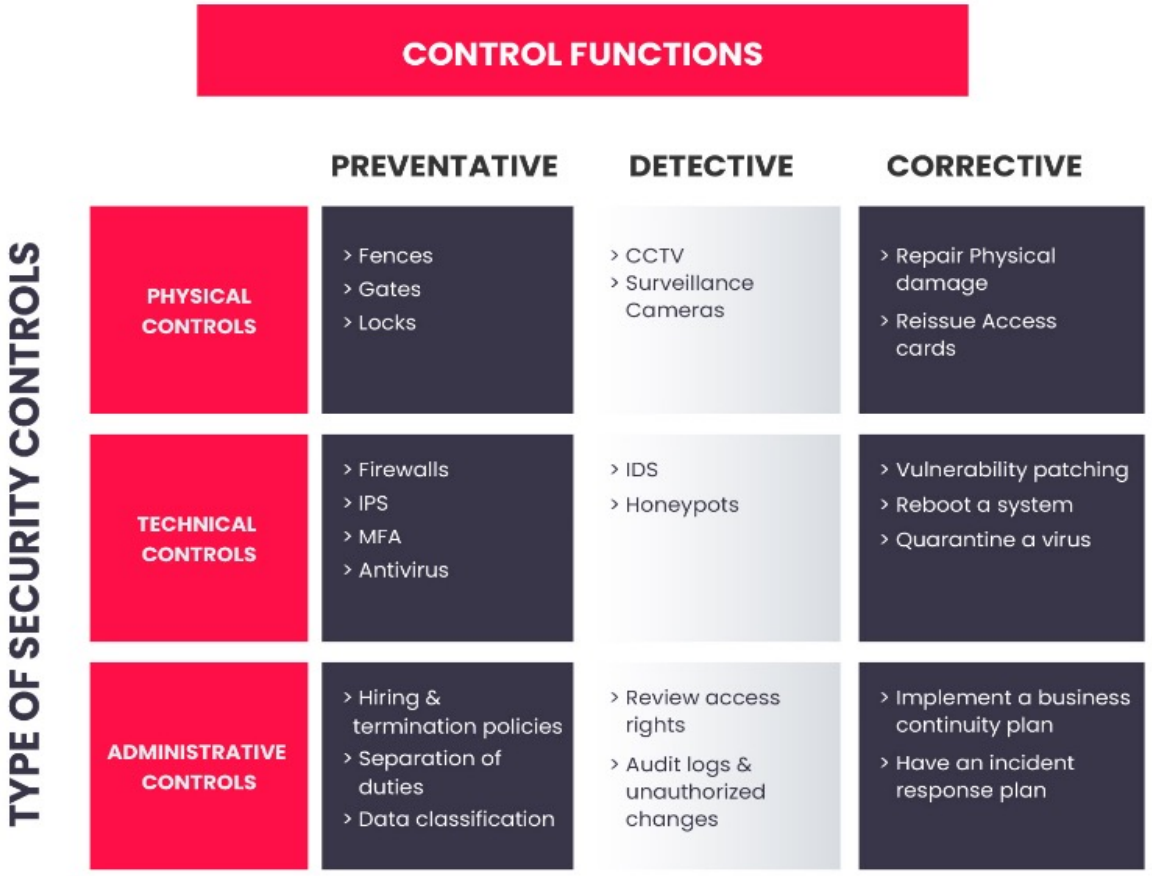
Security Audit -
Audit de sécurité pour le CSF (26/01/2024)

Aperçu des tests effectués

- ✓ Audit de sécurité du réseau externe
- ✓ Audit de sécurité du réseau interne
- ✓ Reconnaissance passive
- ✓ Reconnaissance active
- ✓ Énumération des services ouverts sur les servers
- ✓ Scanneur de vulnérabilité externe / interne + interprétation des résultats
- ✓ Audit de vulnérabilité pour les sites internet
- ✓ Audit de « Active Directory »
  - ✓ Tests des différents vecteurs d'attaques
  - ✓ Vérification du principe de « least privilege » pour les utilisateurs
  - ✓ Vérification des protocoles d'échanges désuets
- ✓ Communication des résultats pendant et après l'audit avec les coordonnateurs ainsi que le directeur du service technologique.
- ✓ Les vulnérabilités jugées critiques sont corrigées immédiatement, tandis qu'une fenêtre de maintenance a été planifiée pour le reste.

Security Controls - Contrôles de Sécurité

Quels sont les différents types de contrôles de sécurité ?



- Les contrôles préventifs tentent d'empêcher un incident de se produire.
- Les contrôles détecteurs tentent de repérer les incidents après qu'ils se sont produits.
- Les contrôles correctifs tentent d'inverser l'impact d'un incident.

- Les contrôles compensatoires sont des contrôles alternatifs utilisés lorsqu'un contrôle principal n'est pas réalisable.

Suivi des dernières améliorations techniques au CSF

Network Access Control

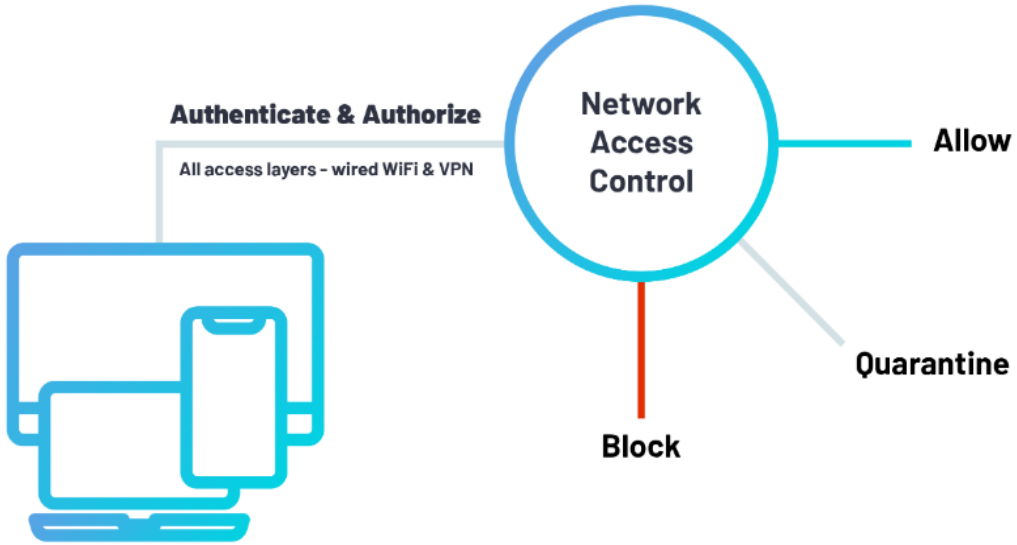
VPN Server

Multi Factor Authentication

BYOD

Data and Network Visibility

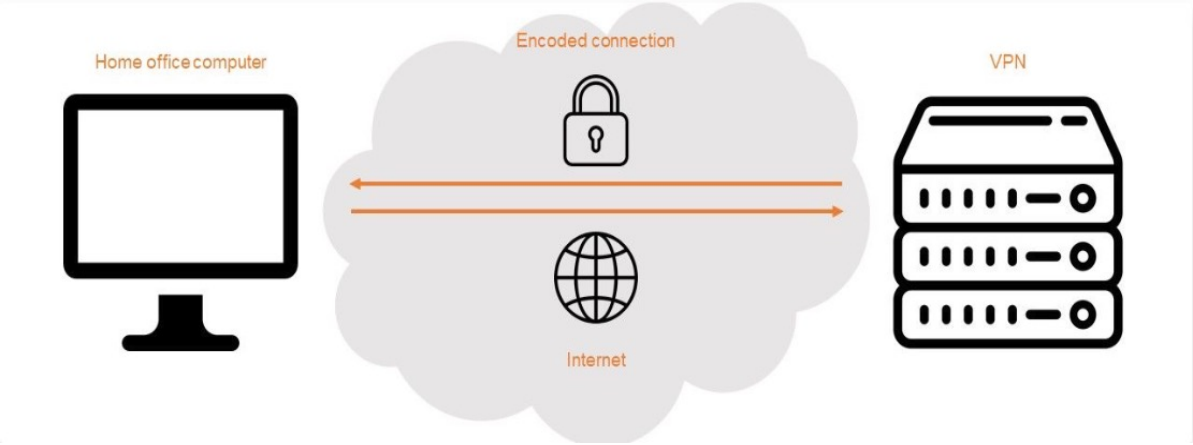
Network Access Control (NAC)



Le contrôleur d'accès réseau (NAC) restreint l'accès aux réseaux privés, empêchant les utilisateurs non autorisés d'y accéder. Il est crucial pour les entreprises qui veulent contrôler l'accès des utilisateurs externes, en particulier avec la montée du BYOD. Cela garantit que seuls les utilisateurs et appareils autorisés peuvent accéder au réseau, assurant ainsi la sécurité et la disponibilité opérationnelle.

Pendant les deux dernières années, nous avons mis en œuvre un contrôleur d'accès réseau pour renforcer la sécurité du réseau Wi-Fi CSF. Désormais, l'authentification des appareils sur le réseau sans-fil repose sur un modèle de certificats TLS client/serveur.

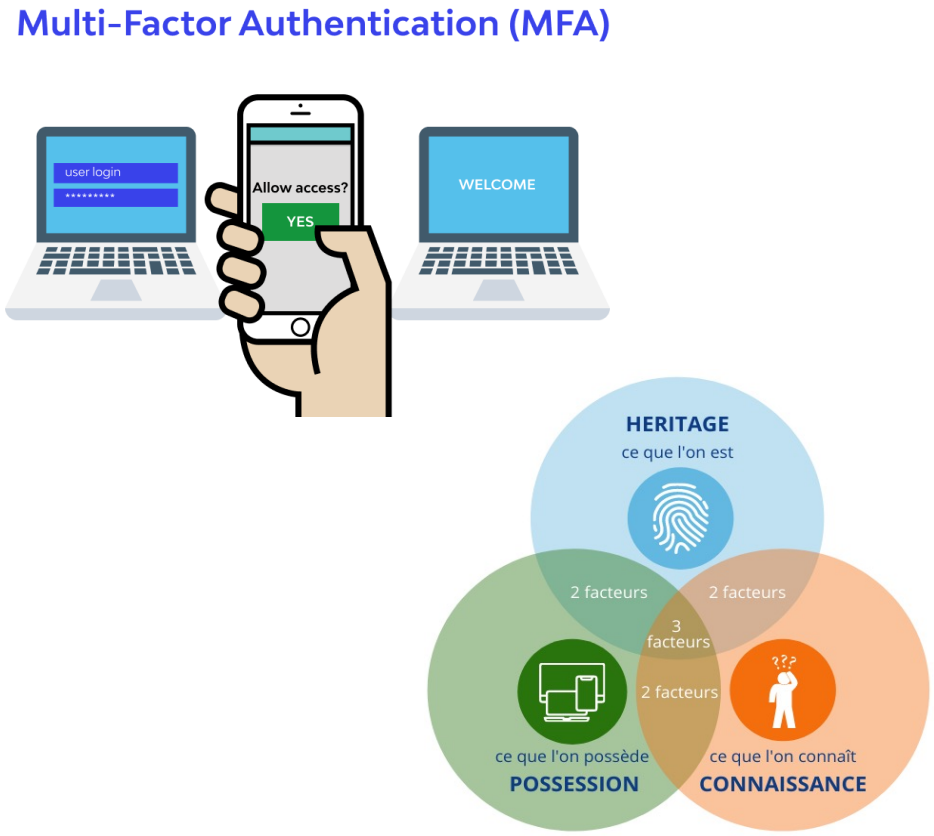
Serveur VPN (Virtual Private Network)



En informatique, un réseau privé virtuel, plus communément abrégé en VPN, est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics (internet).

Avec l'augmentation du nombre d'employés, la pandémie de COVID-19 donnant l’opportunité aux employés de travailler de la maison, des changements significatifs ont dû être apportés à notre serveur VPN pour l’adapter à la situation actuelle.

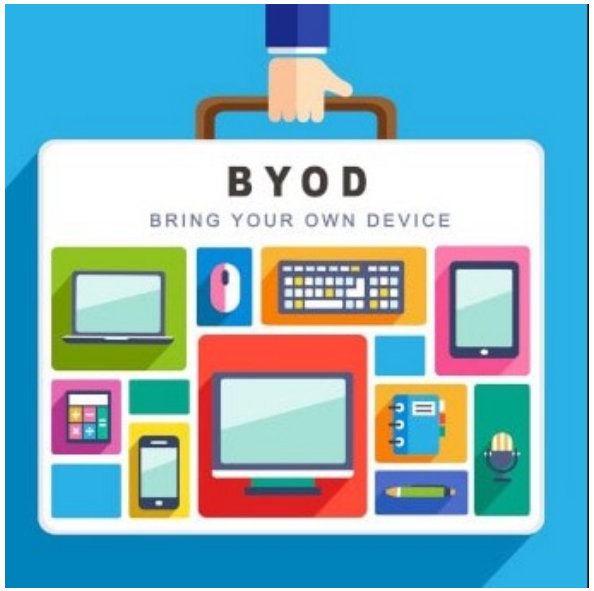
Authentification Multifacteur



L'authentification multifacteur (AMF) est un processus de sécurité qui nécessite généralement deux éléments ou plus pour vérifier l'identité d'un utilisateur lorsqu'il se connecte à un compte en ligne. Ces éléments peuvent inclure quelque chose que l'utilisateur sait (comme un mot de passe), quelque chose qu'il possède (comme un téléphone cellulaire) et quelque chose qu'il est (comme une empreinte digitale).

L'authentification multifacteur (AMF) ajoute une étape de sécurité en demandant aux utilisateurs plus qu'un simple mot de passe lors de la connexion à un compte en ligne. Bien que cela puisse sembler fastidieux, cela rend beaucoup plus difficile pour les pirates d'accéder aux données personnelles. En résumé, bien que l'AMF puisse être ennuyeuse, elle est cruciale pour protéger les données en ligne.

Bring Your Own Device

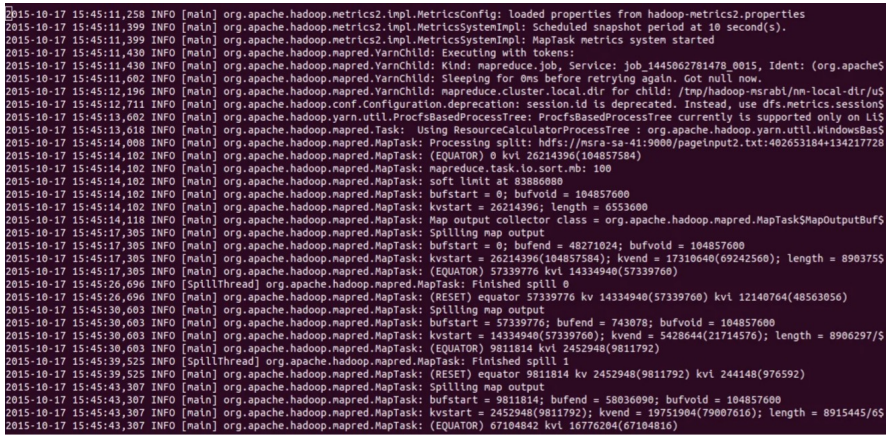


Le CSF autorise les employés à apporter leurs appareils personnels. Il est à noter cependant que le BYOD pose des défis de sécurité réseau car il implique:

- Une variété d'appareils et de systèmes d'exploitation, compliquant la mise en œuvre de politiques de sécurité uniformes.
- La difficulté à gérer les politiques de sécurité sur des appareils personnels.
- La complexité de contrôler le stockage et le partage des données sur des appareils personnels.
- Le besoin de gérer l'authentification et l'accès aux ressources de l'entreprise depuis de multiples appareils.
- La menace potentielle que représentent les appareils vulnérables pour l'intégrité du réseau.

Pour répondre à ces défis, le CSF doit mettre en place des stratégies de sécurité telles que l'utilisation de logiciels de gestion des appareils mobiles, la segmentation du réseau et l'authentification multi-facteurs.

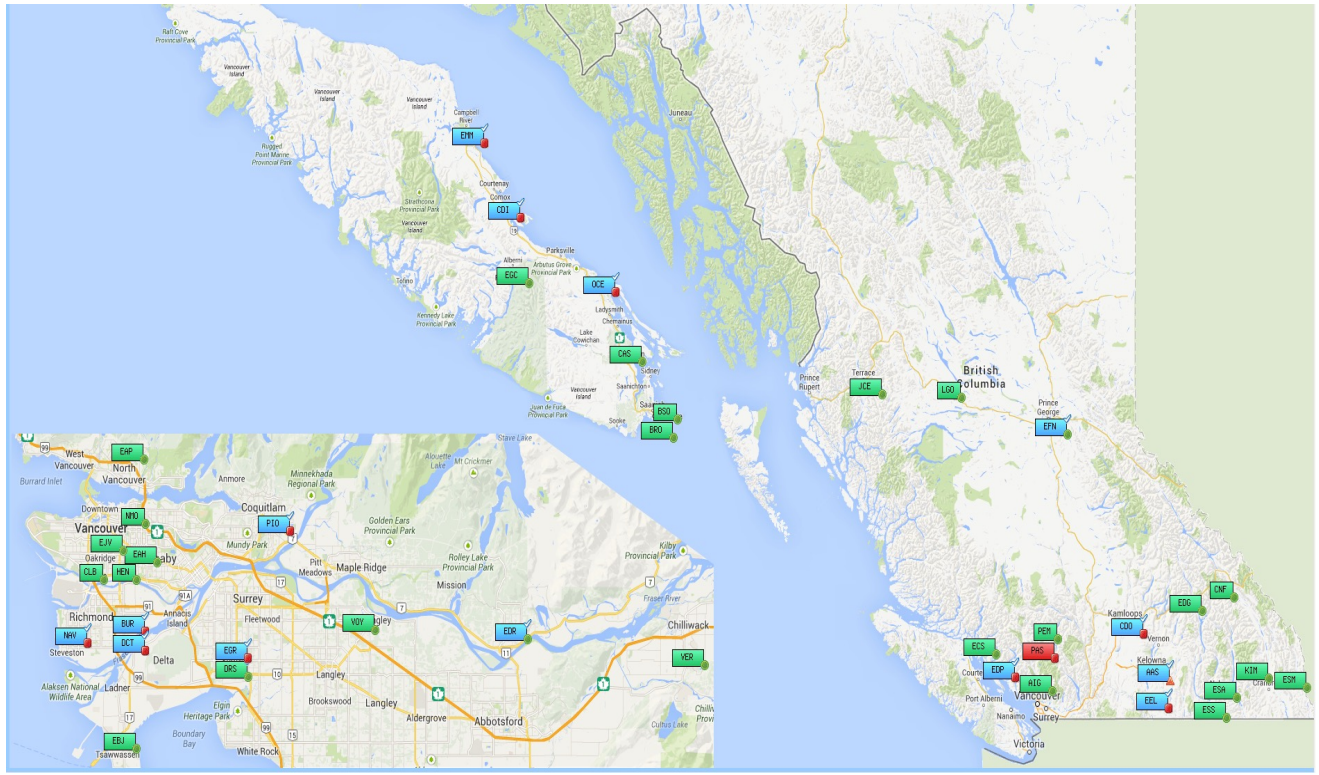
Visibilité des données et gestion des « logs »



La gestion des « logs » implique la collecte, le stockage, le traitement et l'analyse des données provenant de divers programmes et applications pour améliorer les performances du système, détecter les problèmes techniques, optimiser la gestion des ressources, renforcer la sécurité et garantir la conformité. Cependant, cette tâche peut devenir considérablement ardue lorsque nous sommes confrontés à des milliers de lignes de « logs » à analyser.

Au CSF, plusieurs outils ont été mis en place afin d'améliorer la visualisation des données et permettre ainsi une réaction plus efficace en cas de comportements anormaux. Avec le volume croissant du trafic réseau, il est essentiel de trier et d'analyser les informations de manière proactive pour anticiper d'éventuelles pannes ou même attaques.

Surveillance du réseau et système d'alertes



Nous employons des outils de surveillance et de détection de pannes pour garantir la sécurité et la disponibilité de notre réseau informatique.
Les alertes générées sont principalement transmises par courriel, nous permettant ainsi de réagir rapidement.

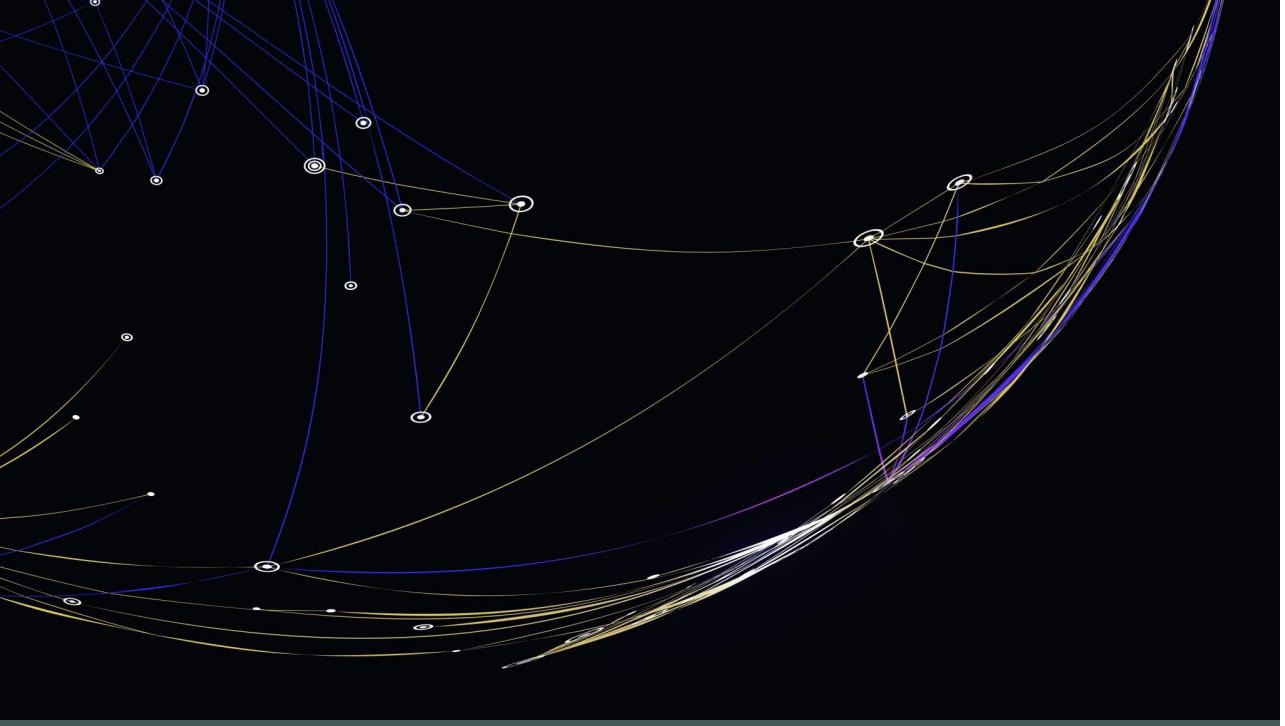
Nous travaillons en permanence dans l'amélioration et l'automatisation de ces systèmes visant à accroître notre efficacité opérationnelle.

Backup System -
Systèmes de Sauvegarde

Office 365 Système de Sauvegarde

La migration de Zimbra vers Office365/Outlook en ligne nous a contraint à revoir nos systèmes de sauvegarde et à trouver une nouvelle solution adaptée. Nous avons dû entreprendre des recherches pour trouver la meilleure option, procéder à sa configuration et à son implémentation afin de garantir la sauvegarde des données au sein du CSF.

L’infrastructure au CSF



Infrastructure vs Endpoints: l’importance d’une infrastructure forte

Bien que nous valorisions l'utilisation des ordinateurs et des iPads par nos enseignants et élèves en salle de classe, mais aussi les employés du CSF en géneral, il est primordial de reconnaître que sans une infrastructure solide, ces outils ne pourraient être pleinement exploités.

Il est souvent plus ardu de justifier les dépenses liées à quelque chose d'aussi abstrait que l'infrastructure par rapport à des appareils tangibles comme un ordinateur ou un iPad.

Cependant, en tant que conseil scolaire à la pointe de la technologie, nous nous devons d’accorder la priorité à la confidentialité, à l'intégrité et à la disponibilité des données, et ce, grâce à une infrastructure robuste.

Merci beaucoup!
Questions ?