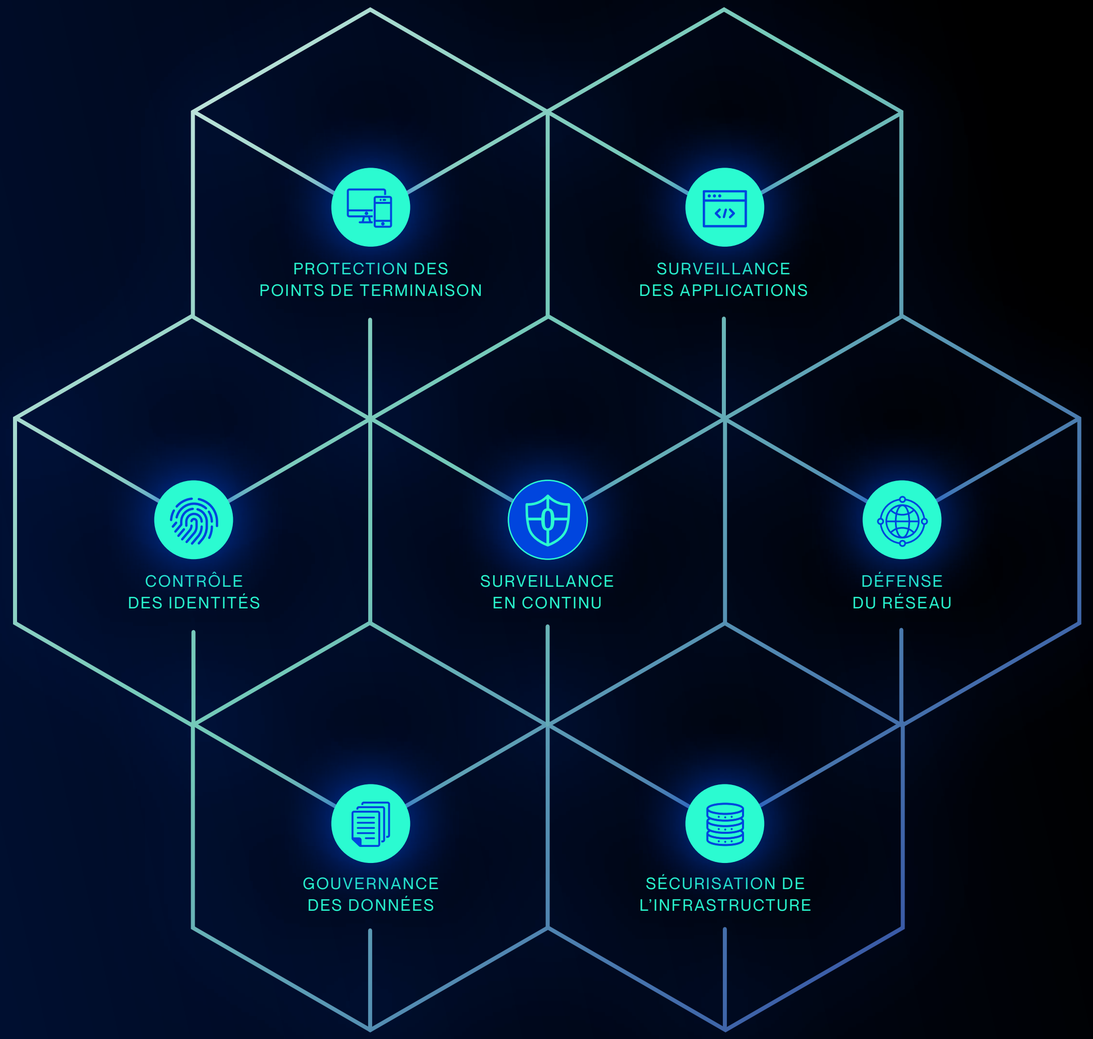
LES PILIERS DE LA CONFIANCE NULLE [ZERO TRUST]

La sécurité des systèmes TI évolue sans cesse, avec des menaces et des mesures de protection en constante progression. Appuyé par la méthodologie de la confiance nulle, ITI propose un guide en 6 étapes qui vous permet d'évaluer les stratégies de sécurité en place dans votre organisation et de les comparer avec les meilleures pratiques de l'industrie.



INTELLIGENCE TI.
INTELLIGENCE HUMAINE.

LES PILIERS DE LA CONFIANCE NULLE [ZERO TRUST]

FEUILLE DE ROUTE SÉCURITÉ

INTELLIGENCE TI.
INTELLIGENCE
HUMAINE.

SURVEILLANCE EN CONTINU

1

CONTRÔLE DES IDENTITÉS

Vérification de l'identité des usagers.

2

PROTECTION DES POINTS DE TERMINAISON

Validation de la posture et protection des appareils.

3

SURVEILLANCE DES APPLICATIONS

Appliquer les contrôles sur les applications et les API.

4

DÉFENSE DU RÉSEAU

Protection préventive des attaques et de leur propagation.

5

SÉCURISATION DE L'INFRASTRUCTURE

Protection de toutes les composantes du centre de données.

6

GOUVERNANCE DES DONNÉES

Garantir la confidentialité et l'intégrité des informations sensibles.

LES PILIERS DE LA CONFIANCE NULLE [ZERO TRUST]

CONTRÔLE DES IDENTITÉS

INTELLIGENCE TI.
INTELLIGENCE
HUMAINE.

1

Lors d'une tentative d'accès à une ressource, il est essentiel de vérifier l'identité de l'usager avec une authentification robuste et de garantir un accès conforme basé sur le principe du privilège minimal.

LISTE DE VÉRIFICATION

- ✓ Gestion des accès
- ✓ SSO et MFA
- ✓ Politiques de gestion d'identité et des mots de passe
- ✓ Accès conditionnel

SOLUTIONS À EXPLORER

- · Microsoft Entra ID
- · Microsoft Entra ID Protection
- · Microsoft Defender for Identity

LES PILIERS DE LA CONFIANCE NULLE [ZERO TRUST]

PROTECTION DES POINTS DE TERMINAISON

INTELLIGENCE TI.
INTELLIGENCE
HUMAINE.

Une fois l'accès accordé à un usager, il est essentiel de préparer vos appareils pour une circulation sécuritaire des données. Assurez-vous que les mises à jour sont effectuées régulièrement sur vos postes de travail et qu'ils sont équipés d'une solution avancée de protection comme un EDR.

LISTE DE VÉRIFICATION

✓ Validation de la posture des appareils
✓ Standardisation des postes par profils
✓ Protection des terminaisons
✓ Gestion des applications

SOLUTIONS À EXPLORER

· Microsoft Intune
· Microsoft Defender for Endpoints
· Microsoft Defender XDR

LES PILIERS DE LA CONFIANCE NULLE [ZERO TRUST]

SURVEILLANCE DES APPLICATIONS

INTELLIGENCE TI.
INTELLIGENCE
HUMAINE.

Qu'elles soient sur site ou dans l'infonuagique, les applications et les API sont des interfaces de consommation de données. Il est essentiel d'appliquer des mesures de contrôles évolués pour détecter les accès non autorisés et surveiller les configurations et les anomalies.

LISTE DE VÉRIFICATION

✓ Gestion des informations et évènements
✓ Protection des accès aux applications
✓ Filtrage et protection web (SWG et WAF)

SOLUTIONS À EXPLORER

· Microsoft Defender XDR
· Microsoft Defender for APIs
· Microsoft 365 Cloud App Security
· Zscaler Private Access (ZPA)
· Intune App protection policies (APP)
· Fortinet FortiWeb

LES PILIERS DE LA CONFIANCE NULLE [ZERO TRUST]

DÉFENSE DU RÉSEAU

INTELLIGENCE TI.
INTELLIGENCE
HUMAINE.

Toutes ces données transitent via le réseau. Les contrôles en place surveillent la circulation des données et offre une protection en temps réel du réseau en le segmentant et en le chiffrant, prévenant la propagation des attaques.

LISTE DE VÉRIFICATION

✓ Protection des réseaux infonuagique
✓ Accès et segmentation du réseau (NAC)
✓ Sécurisation des réseaux sans fil
✓ Protection réseau intersites
✓ Protection des télétravailleurs

SOLUTIONS À EXPLORER

· Cisco ISE
· Cisco Secure Access
· FortiGate, FortiClient EMS, FortiAuthenticator
· Aruba ClearPass
· Microsoft Defender for Cloud
· Zscaler Internet Access (ZIA)

LES PILIERS DE LA CONFIANCE NULLE [ZERO TRUST]

SÉCURISATION DE L'INFRASTRUCTURE

INTELLIGENCE TI.
INTELLIGENCE
HUMAINE.

Qu'elle soit constituée de serveurs locaux, de machines virtuelles, de conteneurs ou de microservices, l'infrastructure constitue toujours une cible privilégiée. Il faut évaluer sa version courante, sa configuration, ses accès et la surveiller pour détecter et bloquer les menaces.

LISTE DE VÉRIFICATION

✓ Protection des serveurs et des conteneurs
✓ Gestion des *patches* de sécurité
✓ Sauvegarde (airgap, immuabilité)
✓ Plan de relève

SOLUTIONS À EXPLORER

· Azure Kubernetes
· CommVault Backup & Recovery
· Microsoft Defender for Server
· Azure ARC
· Microsoft Defender for Cloud

LES PILIERS DE LA CONFIANCE NULLE [ZERO TRUST]

GOUVERNANCE DES DONNÉES

INTELLIGENCE TI.
INTELLIGENCE
HUMAINE.

Protéger les données, c'est veiller à leur sécurité même lorsqu'elles circulent en dehors du périmètre sécurisé de l'entreprise. L'objectif est de garantir la confidentialité et l'intégrité des informations sensibles, tout en assurant leur disponibilité lorsque nécessaire.

LISTE DE VÉRIFICATION

✓ Classification et protection des données
✓ Gestion du cycle de vie
✓ Archivage et chiffrement
✓ Gouvernance

SOLUTIONS À EXPLORER

· Microsoft Information Protection
· Microsoft Purview

LES PILIERS DE LA CONFIANCE NULLE [ZERO TRUST]

ÉTAPE TRANSVERSALE – **SURVEILLANCE EN CONTINU**

INTELLIGENCE TI.
INTELLIGENCE
HUMAINE.

Peu importe l'étape où se situe votre organisation dans son parcours sécurité, la surveillance en continu demeure votre meilleur allié. Pour détecter et répondre rapidement à tout incident de sécurité, la clé est d'être proactif. C'est d'ailleurs l'objectif premier d'un SOC, ou Centre des opérations de sécurité, qui surveille et analyse en temps réel vos réseaux, vos bases de données, vos applications et autres systèmes afin d'assurer la sécurité de l'information.

Enfin, effectuer des audits de sécurité et des tests de vulnérabilité sur une base régulière vous permet de cibler les points d'amélioration de votre infrastructure TI et d'atténuer les cybermenaces.

SOLUTIONS À EXPLORER

· Microsoft Sentinel
· Azure Security Center
· Hitachi SOCaaS
· Arctic Wolf MDR

INTELLIGENCE TI.
INTELLIGENCE
HUMAINE.

ITI PEUT VOUS AIDER À ANALYSER ET DÉPLOYER DES SOLUTIONS DE SÉCURITÉ SUR MESURE

Que ce soit par l'extension de votre équipe de sécurité TI interne ou pour vous aider à respecter les normes de votre industrie, n'hésitez pas à demander conseil à nos spécialistes.