Les protections périmétriques

16 décembre 2022

claude@lemarson.com
https://www.lemarson.com

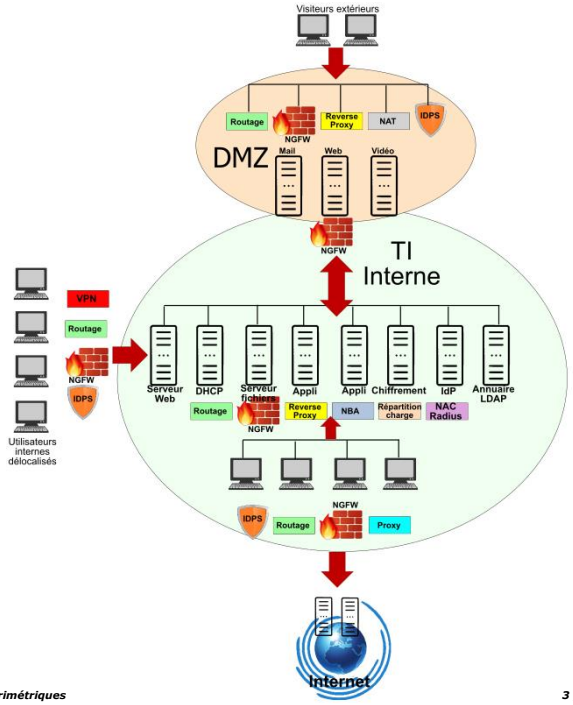
Sommaire

Les protections périmétriques

Le seul marché de la cybersécurité, qui induit l'usage d'Internet, représentera 266 milliards $ en 2027 (MarketsandMarkets). A titre de comparaison, Amazon a fait un CA de 469 milliards $ en 2021.

Architecture globale de protection périmétrique

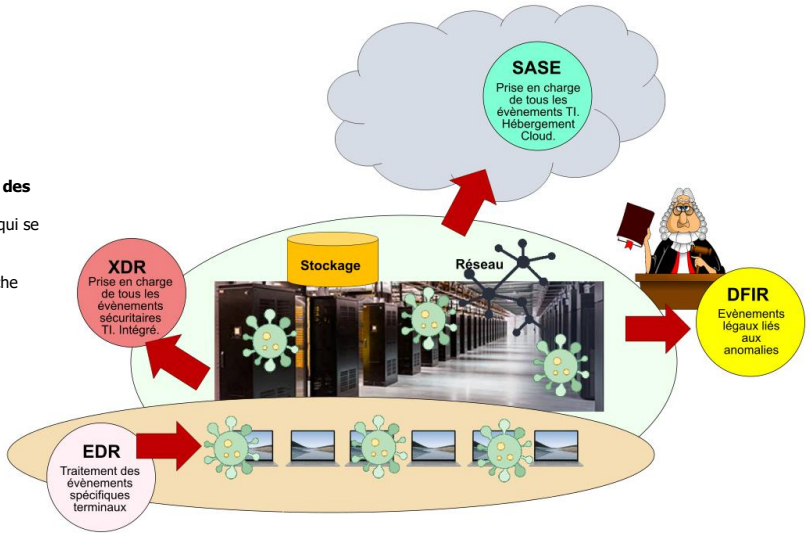
- Très difficile de s'y retrouver.
- Fort recouvrement des fonctionnalités.
- Désormais tout est dans tout…
- Pour s'y retrouver :
  - Donner une définition cohérente des services.
  - Faire la liste exhaustive des fonctions dont on a besoin, internes et externes, indépendamment des solutions.
  - Choisir entre une solution intégrée ou "best of breed".
  - S'assurer de la réalité du service demandé.



S'y retrouver dans les néologismes

La grande salade marketing des néologismes

- Toute une série de concepts qui se recouvrent en partie.
- On n'y comprend plus rien…
- Commençons par une approche globale…



Le principe du "zero trust"

- N'avoir confiance en personne…
- Pas une technologie mais un concept d'architecture dédié au renforcement de la sécurité d'accès aux ressources et aux services.
- La démarche Zero Trust consiste à réduire la « confiance implicite » accordée aux utilisateurs et aux activités menées par le biais des équipements. Les « protections périmétriques » ne disparaissent pas pour autant.
- Les principes :
  - Accès sur la base du plus faible niveau de privilège nécessaire pour réaliser une tâche.
  - On ne fait pas de différence dans les contrôles internes et externes : tous sont "suspects".
  - La politique d'accès aux ressources doit être dynamique et prendre en compte un grand nombre d'attributs (identités de l'accédant et de la ressource accédée, sensibilité des ressources sollicitées, analyse comportementale de l'utilisateur, horaires d'accès…).
  - Les authentifications et autorisations d'accès aux ressources font l'objet de réévaluations régulières.
- La transformation est progressive, c'est un ensemble d'opérations plus ou moins indépendantes
  - Gouvernance améliorée de l'identité (moyens d'authentification à l'état de l'art)
  - Cloisonnement des ressources granulaire et dynamique
  - Renforcement des moyens de détection
  - Conduite du changement

- Zero Trust : apparu chez Forrester en 2009 : mettre en place les outils et règles pour qu'un utilisateur ne puisse accéder qu'aux applications et données, auxquelles l'autorise ses droits.
- Remplacera le VPN dans le futur et le PAM (moindres privilèges).
- De nombreux prestataires sont présents : Akamai, Check Point, Centrify, Cloudflare, Fortinet, Mobile Iron, Okta, Palo Alto Networks, Trend Micro, Symantec…

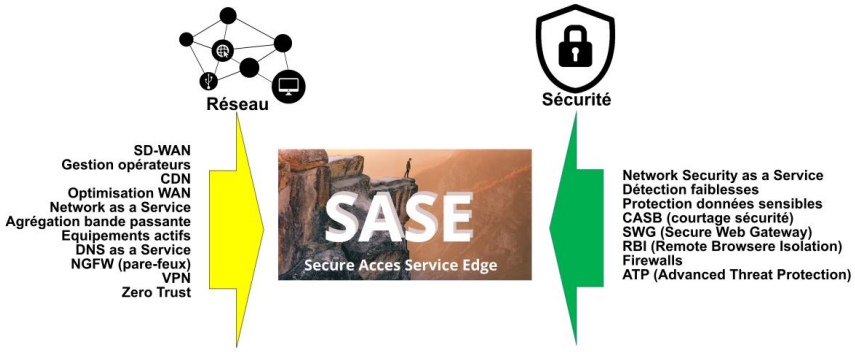
Le principe du moindre privilège

- Le principe du moindre privilège consiste à ne doter une tâche ou un usager que des droits stricts et minimum, nécessaires pour fonctionner.
- Il ne sert à rien de doter les usagers de droits exorbitants, qui ne leur seront pas utiles et seront sources de graves dysfonctionnements.
- Un administrateur pour 90 % de ses tâches n'aura pas besoin d'être déclaré "root user" sous Linux…
- Pour des raisons de respect hiérarchique, il ne faut **jamais** donner des droits admin à un responsable : il est la première cible des criminels. Plus on monte dans la hiérarchie, moins il faut donner de droits…
- Avantages (*) :
  - Une meilleure stabilité du système : les privilèges étant limités, les possibilités qu'une application puisse ralentir ou provoquer un crash système sont également limitées.
  - Une meilleure sécurité du système : l'exploitation d'une faille dans un logiciel pour prendre le contrôle de la machine est rendue plus difficile.
- De nombreux logiciels traitent cet aspect de manière indépendante, en plus des intégrés, SASE…

(*) : Wikipedia

L'approche holistique de la sécurité

Appréhender les problèmes de manière globale
Une autre manière de parler d'intégration



Penser à la mise en œuvre des PCA/PRA, directement liée aux capacités sécuritaires

L'approche holistique de la sécurité

Les solutions

Cynet 360
L'un des plus complets, fondé sur la technologie "Sensor Fusion", avec des possibilités de réaction automatiques ou non, provenant de tout type d'événement, quelle que soit sa granualarité : réseau global, serveurs, terminaux, fichiers, etc.

Palo Alto Cortex XDR
Solution très complète, quelle que soit la taille de l'entreprise. Fondé sur des mécanismes d'IA, pour anticiper sur les défaillances globales.

FireEye
L'offre regroupe les fonctions EDR, suivi réseau, "forensics", etc. Système très complet, qui analyse régulièrement l'environnement à protéger pour détecter de manière les risques potentiels

Sophos XDR Home et ¨Premium
Version "home" gratuite et entreprise. IA, management global Optix depuis le Cloud 24/7.

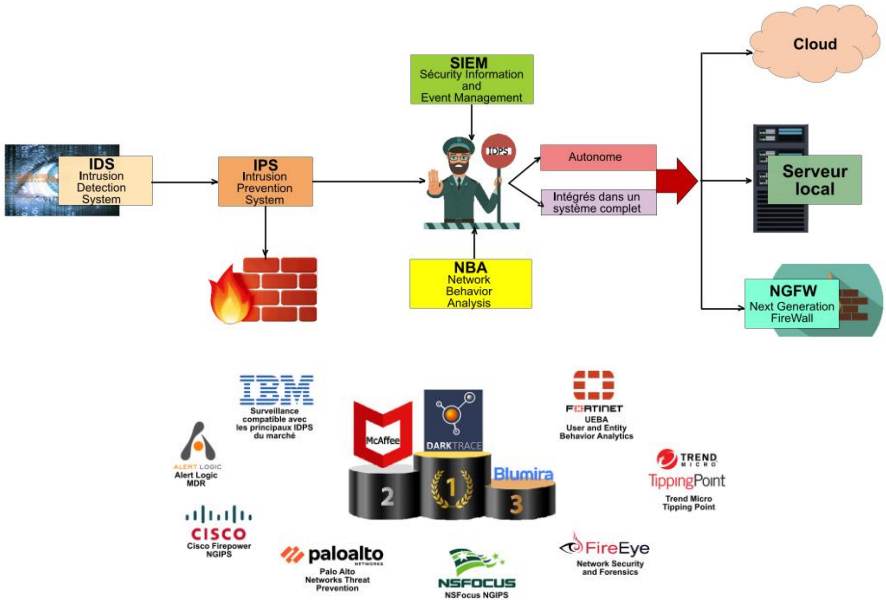
Rapid7
Sa spécialité : la détection de vulnérabilités multiples grâce à des méthodes avancées : analyse comportementale, analyse du trafic réseau, faiblesses humaines...

Fidelis Cybersecurity
XDR complet : analyse du réseau, DLP, détection d'anomalies endpoints, etc. Nombreuses fonctionnalités.

Microsoft Defender ATP
Solution complète "endpoint", découverte temps réel des vulnérabilités, expertise de traitement, gestion d'identités, bénéficie d'outils d'IA

Trend Micro XDR
Trend Micro a étendu le périmètre d'investigation XDR aux courriels, endpoints, serveurs, ressources IaaS et réseaux. Solution très significative, fondée sur des algorithmes IA.

Les intégrés IDPS



SASE : l'intégré de la sécurité périmétrique

- D'ici 2024 (Gartner), 40 % des entreprises auront mis en place une stratégie SASE (« Secure Access Service Edge »).
- Le SASE est synonyme de Cloud : c'est sa principale différence avec les solutions XDR.
- Regroupe les fonctions protectrices de détection des menaces, de protection des données, etc, réunies dans une plate-forme unique, hébergée dans le Cloud.
- Architecture de bout en bout, susceptible de protéger tout ce que contient le TI et de minimiser les attaques malveillantes.
- Ce modèle, très complet et à la pointe de ce « qui se fait de mieux » regroupe :
  - Un service de firewalls FWaaS.
  - Des services CASB (« Cloud Access Security Brokers »).
  - Un proxy inline (transparent) pour le trafic Web et Cloud (NG SWG).
  - L'implémentation des règles « zero trust ».
  - Des capacités d'authentification SSL/TLS.
  - Des outils pour surveiller les données en transit (DLP).
  - Des protections contre les attaques les plus récentes : ATP, UEBA, sandboxing…
  - Un regroupement et partage des informations sur les menaces : EDR, fichiers logs SIEM…
  - Le tout dans un périmètre logiciel SD-WAN avec une infrastructure réseau hyperscale de niveau opérateur et des points de présence partout dans le monde.
- SASE constitue l'avenir de la protection holistique. Compte tenu de son implantation exclusive dans le Cloud, elle est le complément indispensable d'une approche SD-WAN, dont elle ne peut pas être dissociée.
- Ses avantages :
  - Une faible complexité d'implantation et des coûts réduits, ce qui tient à son statut mono-fournisseur dans le Cloud, libéré de l'empilement habituel de briques plus ou moins compatibles.
  - Une grande souplesse et agilité de mise en œuvre.
  - Une meilleure maîtrise des performances.
  - Une gestion des accès complète, qui va plus loin que la simple adresse IP, avec des fonctions d'authentification.
  - Une plus grande efficacité d'usage du réseau.
- Une douzaine de prestataires sont présents sur le créneau : Cisco, Fortinet, Zscaler, Cato Networks…

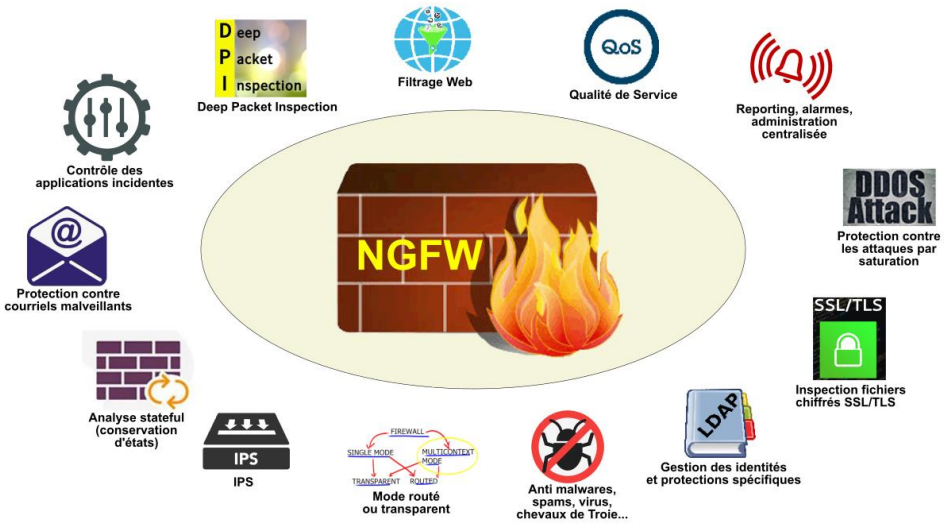
XDR, une extension de l'EDR

- XDR (« eXtended Detection and Response ») est une alternative du mode EDR (« Endpoint Detection and Response »), dans lequel chaque point à surveiller (« endpoint ») est doté d'un agent qui contrôle ce qui se passe et collecte des données qu'il émet à une ressource centralisée dans un datacenter. Mais EDR ne traite qu'une problématique, celle des terminaux.
- Comparativement à un EDR, XDR est une extension qui prend en compte tous les évènements susceptibles d'intervenir dans le TI, en termes de sécurité, tout en restant confiné au périmètre de l'entreprise : des problèmes de VPN, des attaques globales, le comportement des proxies et des reverse proxies, celui des pares-feux, le déferlement intempestif de messages, les tentatives de blocage en déni de service, etc.
- L'idée étant que tous les « endpoints » et équipements du TI, sans restrictions, vont constater ces « anomalies », qu'ils vont faire remonter vers une autorité centralisée, dans laquelle seront concentrées toutes les technologies d'IA et d'analyse comportementale, pour prendre des décisions liées à la poursuite des activités du TI. C'est ce que les prestataires appellent un SOC (« Security Operations Center »).

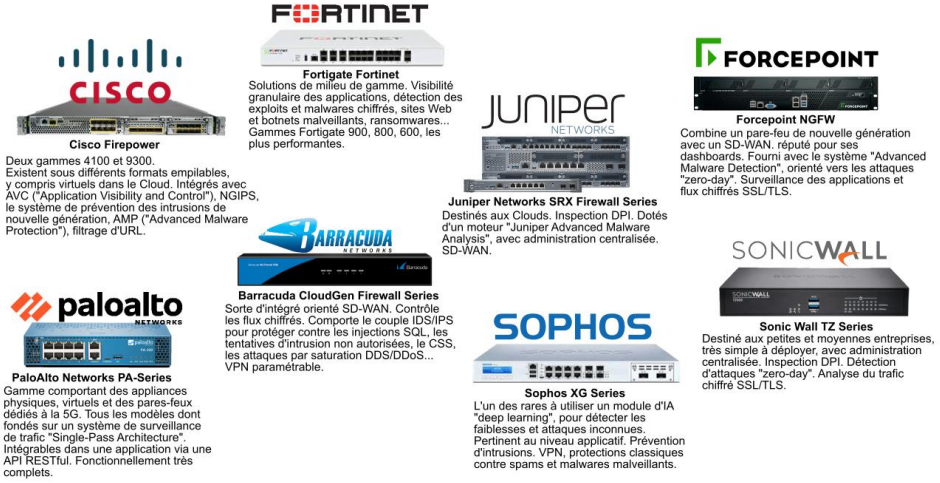
DFIR, le bras "légal" de la sécurité

- DFIR (« Digital Forensics and Incident Response »), regroupe tout ce qui permet de relever des indices, des faits et des éléments liés à une attaque ou dégradation informatique, en vue de les présenter à une administration légale. Qui peut être un juge.
- Il s'agit d'une approche holistique, car très globale, à qui on pourra reprocher un mélange des genres, puisqu'elle ne se contente pas d'explorer et de recueillir des informations et empiète sur le domaine d'autres outils, tels que la reprise sur incidents.
- Concerne surtout les professionnels de la sécurité et prestataires, car il ne faut pas détériorer la « scène du crime » et se contenter d'en faire ressortir les éléments utiles à l'enquête, sans les dégrader.
- Il existe de nombreux produits qui se réclament de l'approche DFIR, qui ont à peu près les mêmes caractéristiques :
  - Des moyens d'investigation cohérents et exhaustifs.
  - Des outils pour récupérer les données, quelles que soient les sources, équipements actifs réseaux, serveurs, terminaux, mobiles…
  - Des utilitaires de suivi et de reporting.
  - Des moyens pour s'améliorer, provenant des technologies d'apprentissage de l'Intelligence Artificielle.
- Il existe un grand nombre de solutions DFIR sur le marché : Lace Forensic Carver qui reconnaît plus de 180 types de fichiers différents (vidéo, images, textes, bases de données…), BlueBear, très efficace pour catégoriser de gros volumes d'informations, Digital Forensic Framework (DFR), Forensic Toolkit, Disk Drill, Magnet Forensics, Encase Forensic Software, Regripper (pour l'analyse des registres système), etc.
- La difficulté est de les positionner sans recouvrement avec d'autres produits déjà présents.

Pares-feux de nouvelle génération : NGFW



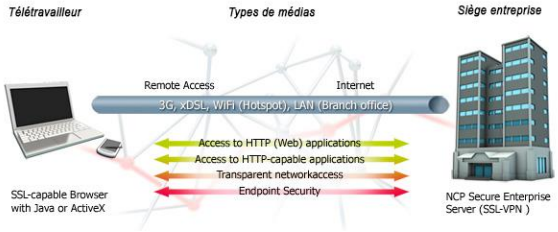
Pares-feux de nouvelle génération : NGFW



Les VPN de nouvelle génération

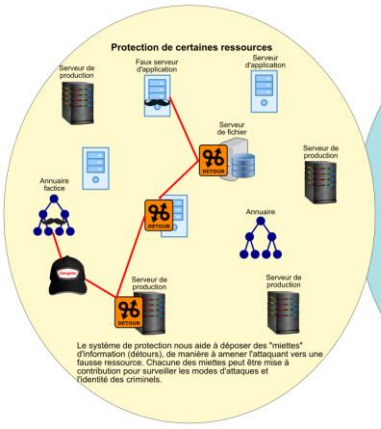
et l'alternative des proxy

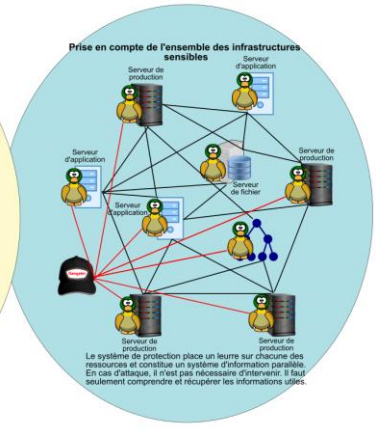
- VPN d'entreprise : Réseau Privé d'Entreprise
- Tunnel entre les ressources et les employés (sans passer par un
- Plutôt que de passer par Internet via un FAI, le VPN d'entreprise fournit un tunnel entre les ressources et les employés, quelle que soit leur localisation.
  - Chiffrement de bout en bout
  - Déploiement des serveurs avec des adresses IP dédiées
  - Bonne protection des données
  - Audit
  - Contrôles d'identités des usagers
  - Première approche de sécurisation, sans vocation universelle
- Proxy d'entreprise
  - Les demandes de connexion Internet passe par ce serveur avant d'atteindre l'adresse demandée. La réponse renvoyée passe par ce même serveur proxy (il y a des exceptions à cette règle), avant de retransmettre les données reçues.
  - Les proxy modernes font aussi office de pare-feu et de filtrage Web, fournissent des connexions réseau partagées, placent les données en cache pour accélérer le traitement des requêtes les plus courantes. Un bon serveur proxy protège les utilisateurs et le réseau interne des menaces externes et garantit un niveau élevé de confidentialité.



La technologie des leurres

- Deux générations.
- Génération 1 ("pots de miel"), peu utilisée : on dissémine des pièges sur les ressources les plus sensibles : serveurs de production, annuaires AD, machines virtuelles, etc, des mini-récepteurs, appelés "miettes", chargés de récolter des informations sur les attaques.
- Pas de perspective globale sur l'ensemble du SI, ce ne sont que des constats.
- Génération 2 ("security decoys" (leurres)) est plus générique. Elle concerne un plus grand nombre de ressources et monte d'un cran dans la compréhension des stratégies "belliqueuses".
  - Mise en place de leurres chargés de désorienter l'attaquant et de le rediriger vers des ressources factices, mais son périmètre est plus large et surtout s'appuie sur des mécanismes de détection et de compréhension par rapprochement, que l'on ne pratiquait pas auparavant.
  - Toujours transparente pour les usagers et les applications.
  - Technologie "œcuménique" : elle ne se fonde pas sur un fichier de signatures, qui n'a donc pas à être mis à jour. Elle est bien adaptée aux contextes nouveaux et "zero day".





La technologie des leurres

ACALVIO

Très spécialisé dans les environnements industriels, IoT et distribution points de vente.

Attivo NETWORKS

ThreadDefense Platform, détecte les attaques externes, les liens transverses, l'escalade de privilèges...

Aves netsec

Solution SaaS destinée aux entreprises, grandes et moyennes. Les leurres sont des "precision sensors". Offre gratuite ou premium.

Cymmetria, Récemment acquis par un fonds de pension. Solution MazeRunner, typique de la "deception technology". Très pertinente dans la compréhension des intentions malveillantes.

Counter Craft

Compagnie espagnole. Solution complète avec des modules de design des leurres, déploiement, monitoring et analyse des suivis.

illusive

L'une des solutions les plus populaires. Combinaison de plusieurs produits. Assistance à la mise en oeuvre.

Ridgeback Network Defense. Petite structure créée en 2014, avec un produit complet de "deceptive security".

SMOKESCREEN

Protection de type "deception", très diversifiée : institutions financières, énergie, grands comptes manufacturiers.

CYBERTRAP

Solution autrichienne très complète, qui aboutit à un TI totalement trompeur. Objectif : comprendre les intentions des attaquants et connaître leur identité.

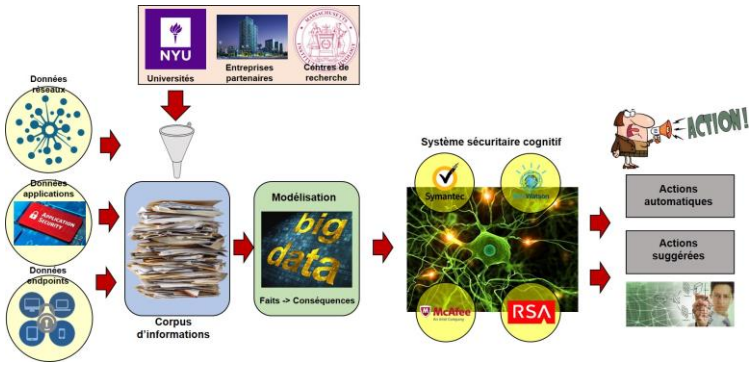
TRAPX SECURITY

DeceptionGrid, conforme à laux modèles d'attaque MITTRE ATT&CK. Relativement simple à installer, y compris sur de grandes infrastructures.

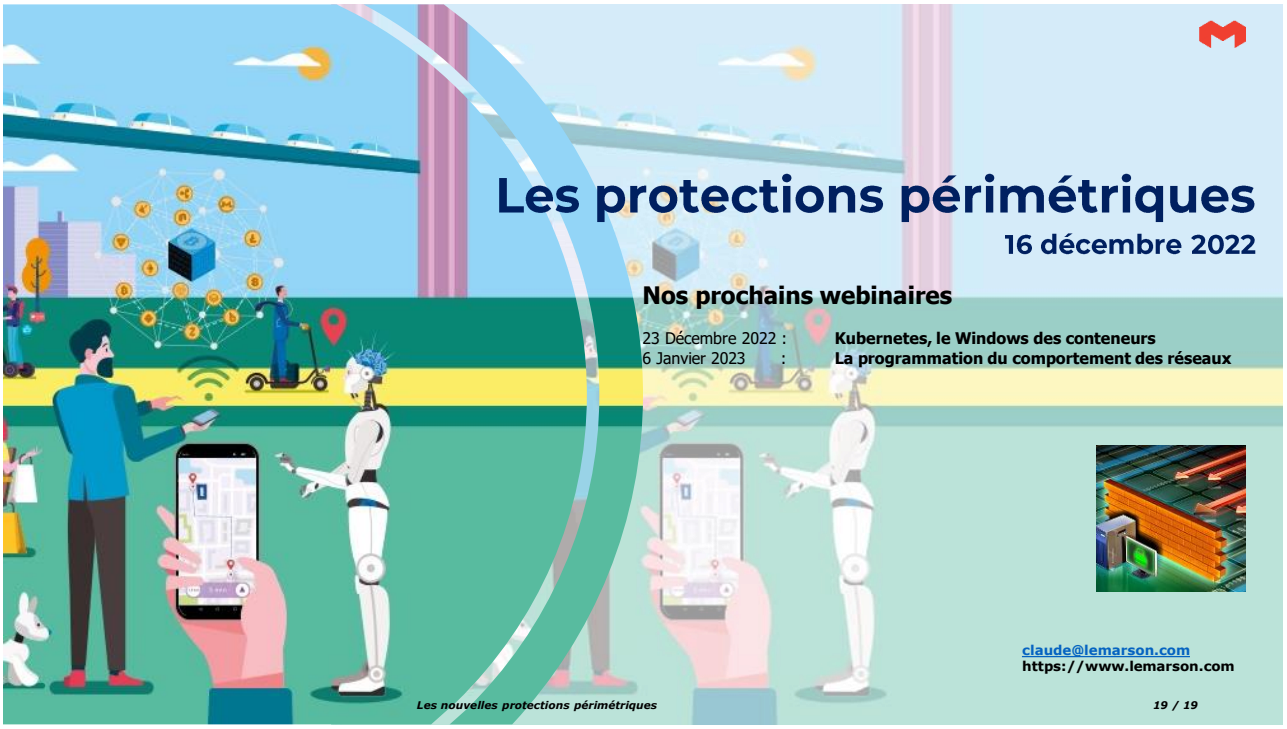
TOPSPIN SECURITY

Technologie israëlienne (centre de recherche à Herzliya), commercialisée par TopSpin. Annonce 2 000 clients.

La protection sera cognitive...ou ne sera pas



- Compte tenu de l'évolution des malwares et des technologies d'attaques, il faudra à la fois appliquer des techniques de protection périmétriques et de réaction cognitive.
- On ne se protègera plus contre un malware donné, mais contre une typologie d'attaques, avec une analyse cognitive de ses conséquences : ex de Watson.



Les protections périmétriques

16 décembre 2022

Nos prochains webinaires

23 Décembre 2022 : **Kubernetes, le Windows des conteneurs**
6 Janvier 2023 : **La programmation du comportement des réseaux**

claude@lemarson.com
https://www.lemarson.com