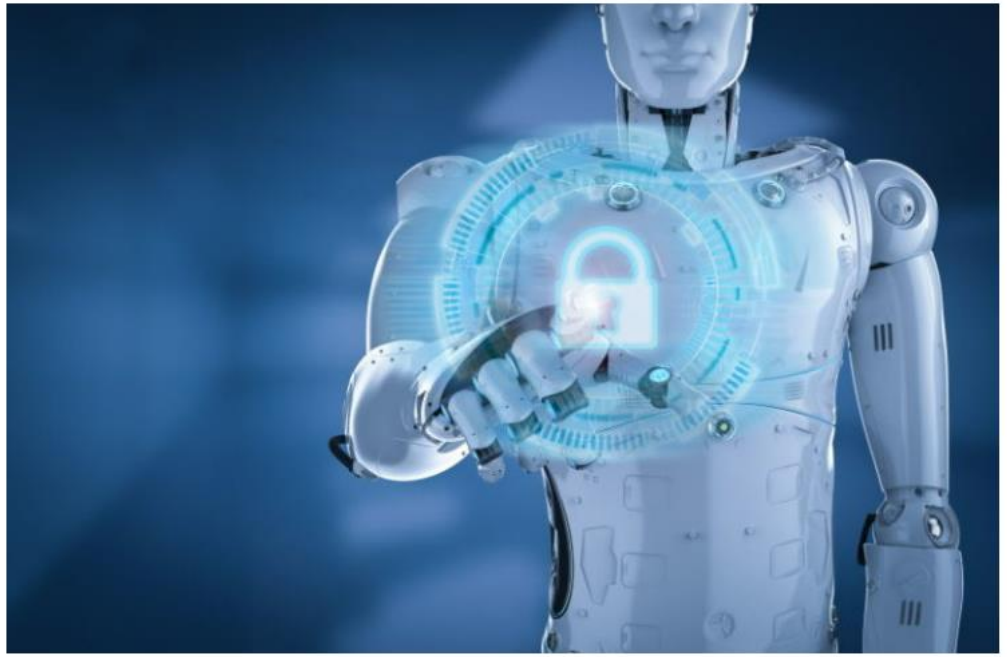
IIBA Geneva Chapter

IA et Cybersécurité

10:50 – 11:35

Yannis Martin



Compte tenu de cybermenaces et des groupes malveillants toujours plus innovants et dynamiques, les capacités de cyberdéfense des entreprises sont réduites le plus souvent à une suite d'outils complexes à gérer dans un centre d'opérations de sécurité (SOC).

Les SOAR (Security Orchestration, Automation, and Response) ont été développées pour intégrer et automatiser de nombreuses tâches et process afin d'aider les équipes SOC à répondre aux incidents.

Mais qu'en est-il de l'automatisation sans analyse fine des données crées ?

Nous verrons comment le Machine Learning et l'IA servent à apporter des éléments de réponses à cette problématique.

En partenariat avec

nistin

SMP Société suisse de management de projet

SWORD UPGRADE YOUR BUSINESS

IIL EMEA

Qim info

SMP Société suisse de management de projet

REDSEN CONSULTING

IA et Cybersécurité

L'IA AU SERVICE DE L'ENTREPRISE

CONGRÈS DE BUSINESS ANALYSE IIBA GENEVA

06 OCTOBRE 2022

https://www.thelocal.fr/20171208/11-everyday-moments-in-france-when-you-really-need-to-say-bonjour/

Préambule

Rappel de la séance

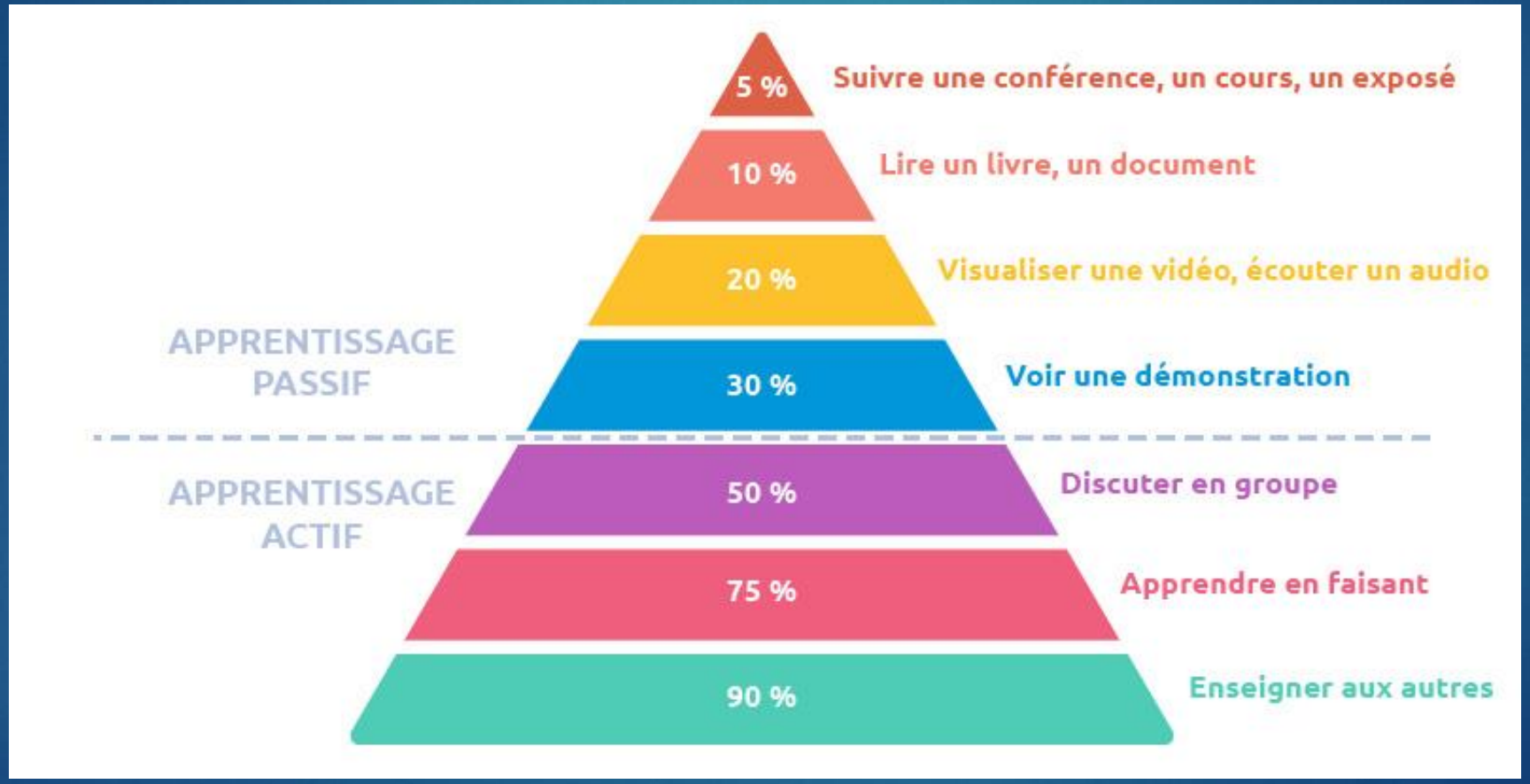
- Compte tenu de cybermenaces et des groupes malveillants toujours plus innovants et dynamiques, les capacités de cyberdéfense des entreprises sont réduites le plus souvent à une suite d'outils complexes à gérer dans un centre d'opérations de sécurité (SOC).
- Les SOAR (Security Orchestration, Automation, and Response) ont été développées pour intégrer et automatiser de nombreuses tâches et process afin d'aider les équipes SOC à répondre aux incidents.
- Mais qu'en est-il de l'automatisation sans analyse fine des données crées ?
- Nous verrons comment le Deep Learning et l'IA servent à apporter des éléments de réponses à cette problématique.

Votre Intervenant

Yannis MARTIN :

- Manager de Transition depuis 5 ans,
- 13 ans d'expérience en Management des SI,
- Enseignant/Formateur depuis 2019, (CERI Université d'Avignon : LIA)
- EICnam : Ingénieur IRSM,
- CNAM : M2 Mention Travail et développement,
  - Spécialité Travail, emploi et organisation. (voie recherche) GRH et sociologie.

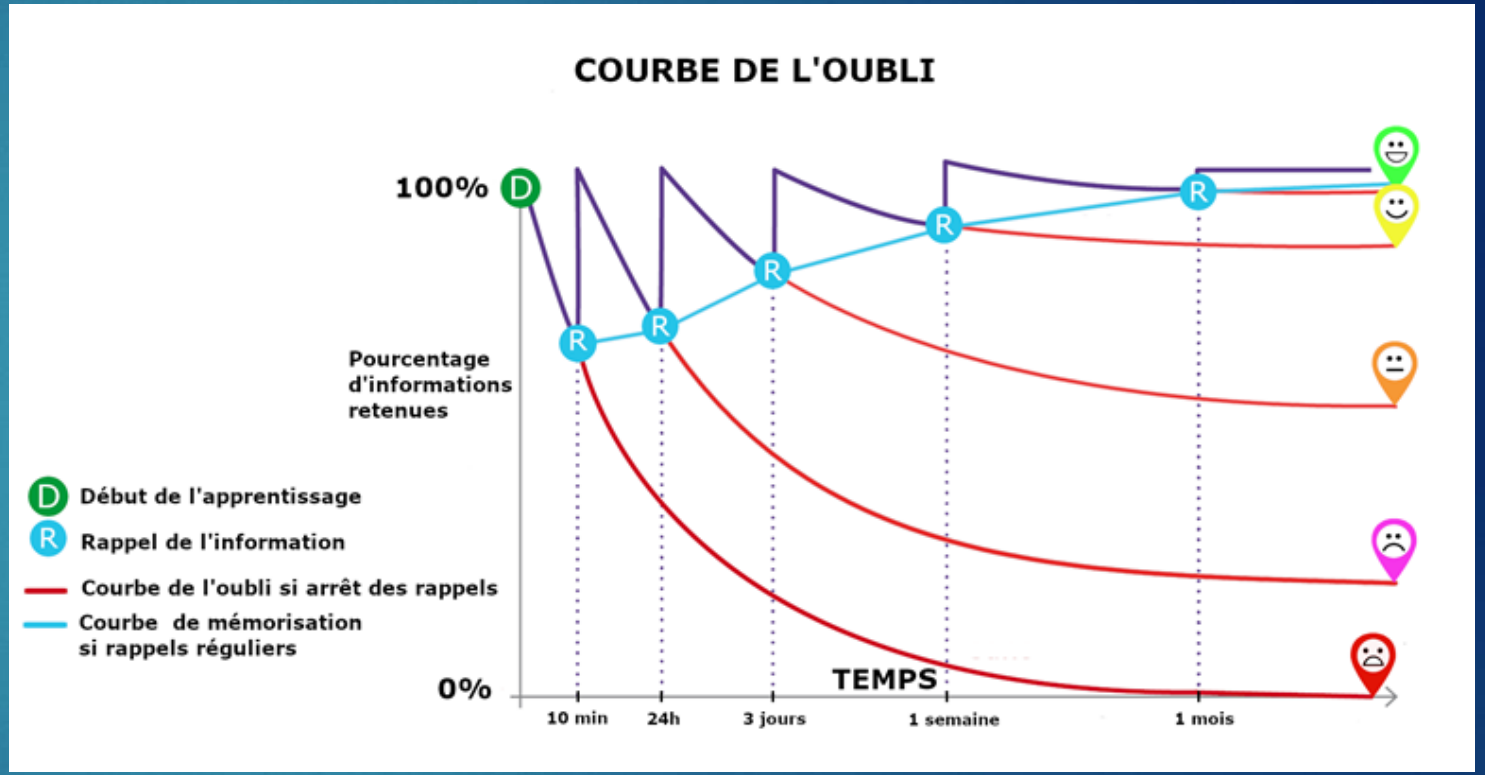
Pyramide d'apprentissage



https://mobiteach.fr/news/comment-rendre-vos-formations-interactives/

Courbe de l'oubli et du réapprentissage : Hermann Ebbinghaus (1885)

La Courbe d'Ebbinghaus est une technique destinée à améliorer la rétention d'informations. Elle consiste à se remémorer une information donnée (un cours, un livre, un mots, du vocabulaire…) grâce à des rappels réguliers. Elle part du principe que plus une information est répétée dans le temps, plus elle s'ancre dans notre mémoire.



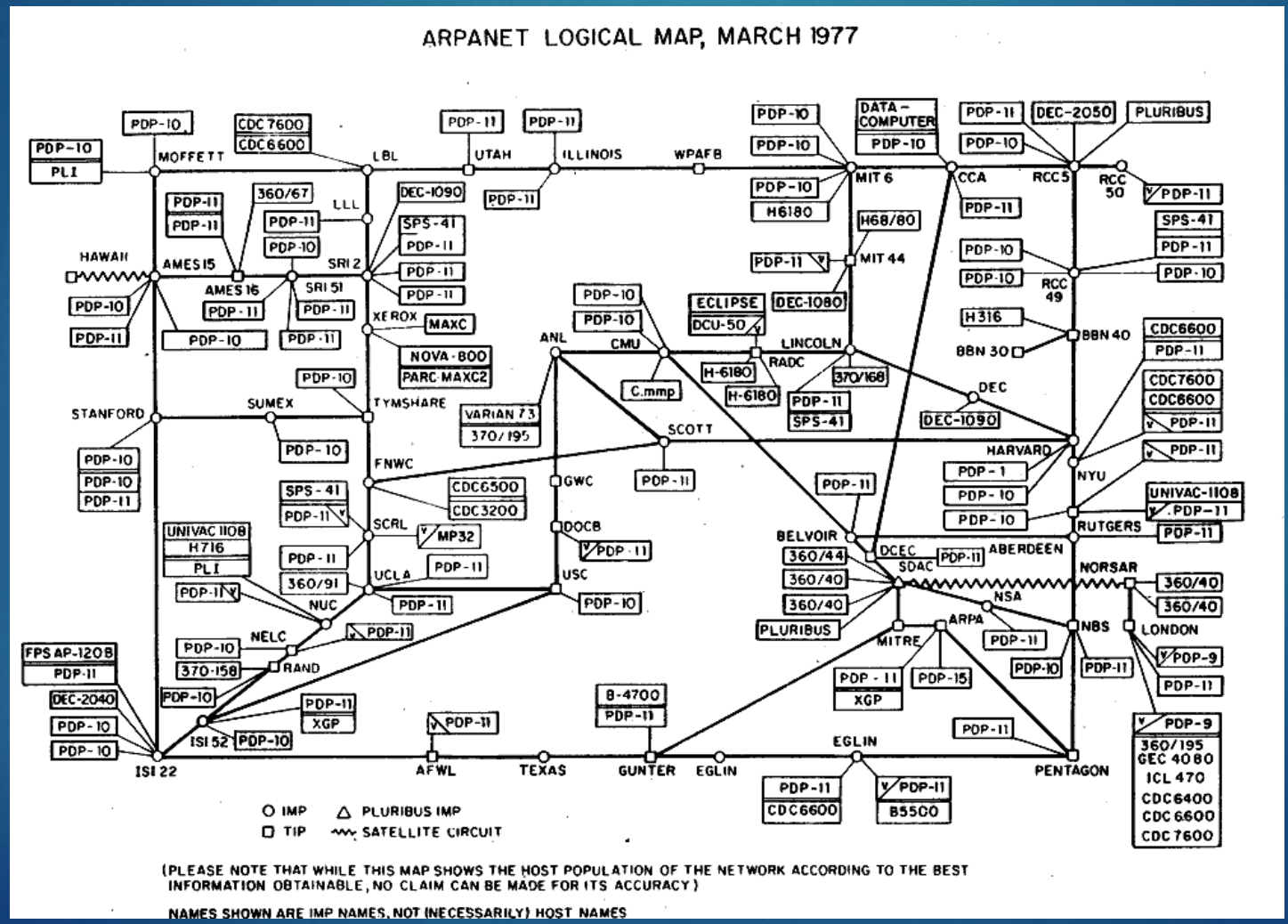
Agenda

- Introduction
- Des risques Cyber réels
- L'IA au service de la cybersécurité
- Quelques outils
- Conclusion

Agenda

- Introduction
- Des risques Cyber réels
- L'IA au service de la cybersécurité
- Quelques outils
- Conclusion

1969 - 1984 : Aux États-Unis, naissance et développement d'Arpanet

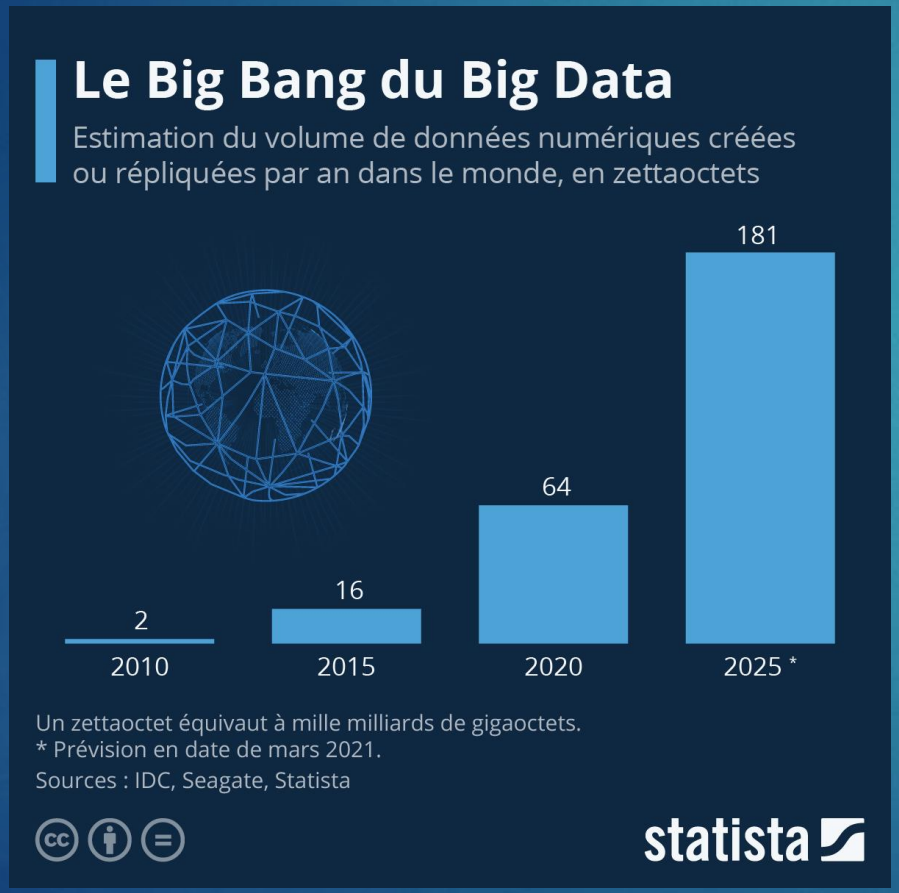


1969 - 1984 : Aux États-Unis, naissance et développement d'Arpanet

- Arpanet est mis en service le 29 octobre 1969 à partir de l'université de Californie à Los Angeles (UCLA). C'est avant tout un réseau de communication basé sur la commutation de paquets et le principe de transparence d'une information transmise de bout en bout entre égaux (peer to peer).
- Le but recherché est la mise en communication d'applications installées sur des ordinateurs hétérogènes, en vue de partager les ressources informatiques matérielles et logicielles, les données et les moyens humains pour opérer des applications géographiquement réparties.

https://www.inria.fr/fr/arpanet-internet-en-france-dates-reperes#:~:text=Arpanet%20est%20mis%20en%20service,%C3%A9gaux%20(peer%20to%20peer).
05/10/2022

Evolution du volume de données numériques

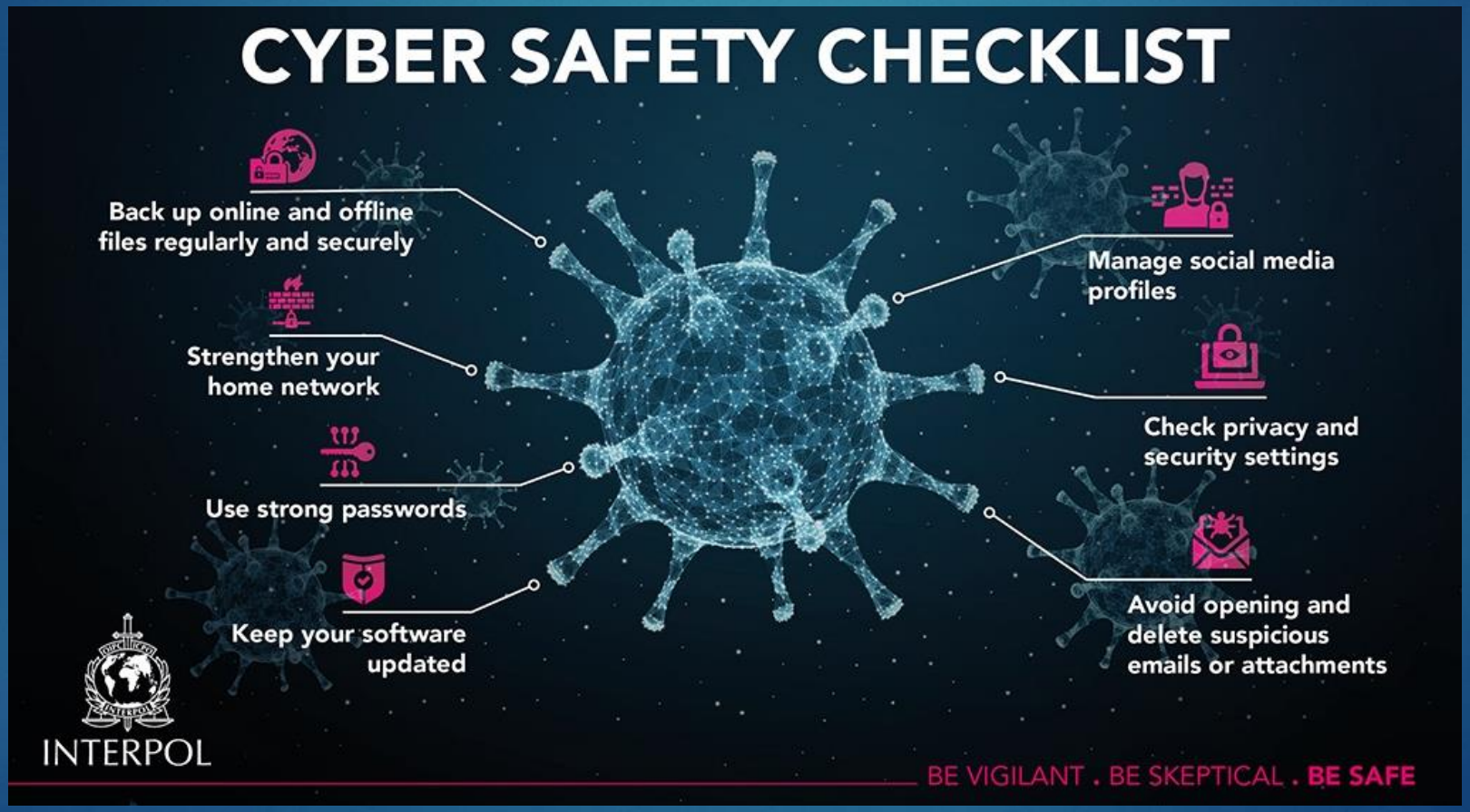


https://fr.statista.com/infographie/17800/big-data-evolution-volume-donnees-numeriques-genere-dans-le-monde/
05/10/2022

Un volume d'attaques difficile à appréhender au quotidien

https://www.fireeye.com/cyber-map/threat-map.html
05/10/2022

Des changements ouvrant de nouvelles cibles aux pirates



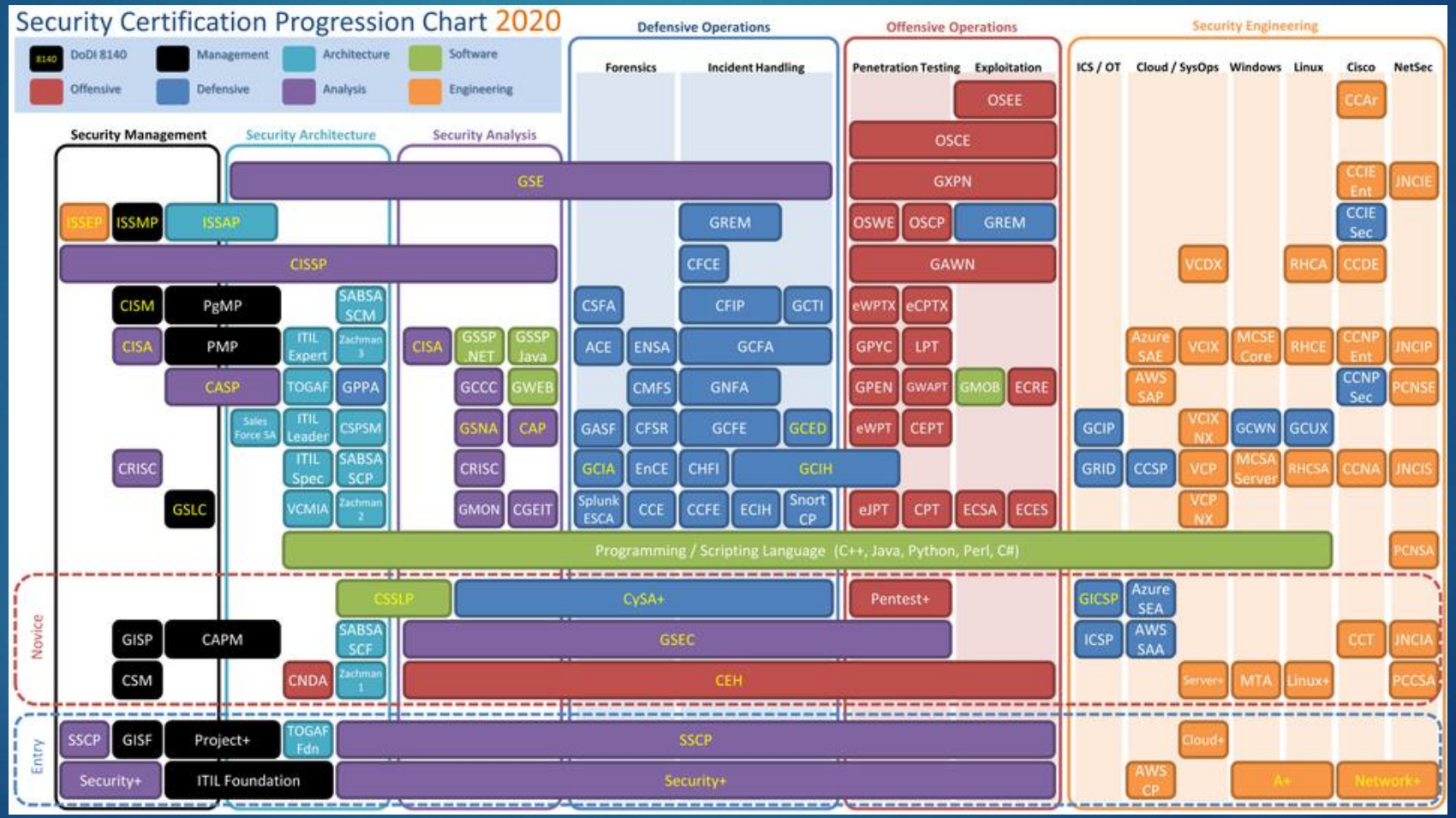
https://www.interpol.int/fr/Infractions/Cybercriminalite/Cybermenaces-liees-au-COVID-19
05/10/2022

De nouveaux usages Evolutions marché Cyber 2020 ➔ 2021

https://www.silicon.fr/securite-marche-2021-415159.html#
05/10/2022

Market Segment	2020	2021	Growth (%)
Application Security	3,333	3,738	12.2
Cloud Security	595	841	41.2
Data Security	2,981	3,505	17.5
Identity Access Management	12,036	13,917	15.6
Infrastructure Protection	20,462	23,903	16.8
Integrated Risk Management	4,859	5,473	12.6
Network Security Equipment	15,626	17,020	8.9
Other Information Security Software	2,306	2,527	9.6
Security Services	65,070	72,497	11.4
Consumer Security Software	6,507	6,990	7.4
Total	**133,776**	**150,409**	**12.4**

Une gouvernance complexe : Liste non exhaustive de certifications



Agenda

- Introduction
- Des risques Cyber réels
- L'IA au service de la cybersécurité
- Quelques outils
- Conclusion

La transformation numérique

- L'interconnexion des outils informatiques avec Internet présente un certain nombre de risques, parmi lesquels on peut citer :
  - L'exfiltration de données depuis l'entreprise vers Internet, portant ainsi atteinte à leur confidentialité voire à la réputation de l'entreprise si elles sont diffusées ;
  - L'intrusion depuis Internet pour porter atteinte à l'intégrité ou la disponibilité du SI et des outils de production de l'entreprise ;
  - L'usurpation d'identité ;
  - Le détournement du SI de l'entreprise pour des usages frauduleux ou délictueux.

Les enjeux de la sécurité des S.I.

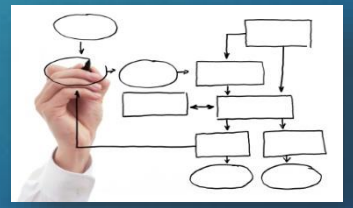
Impacts financiers

Impacts sur l'image et la réputation

Sécurité des S.I.

Impacts juridiques et réglementaires

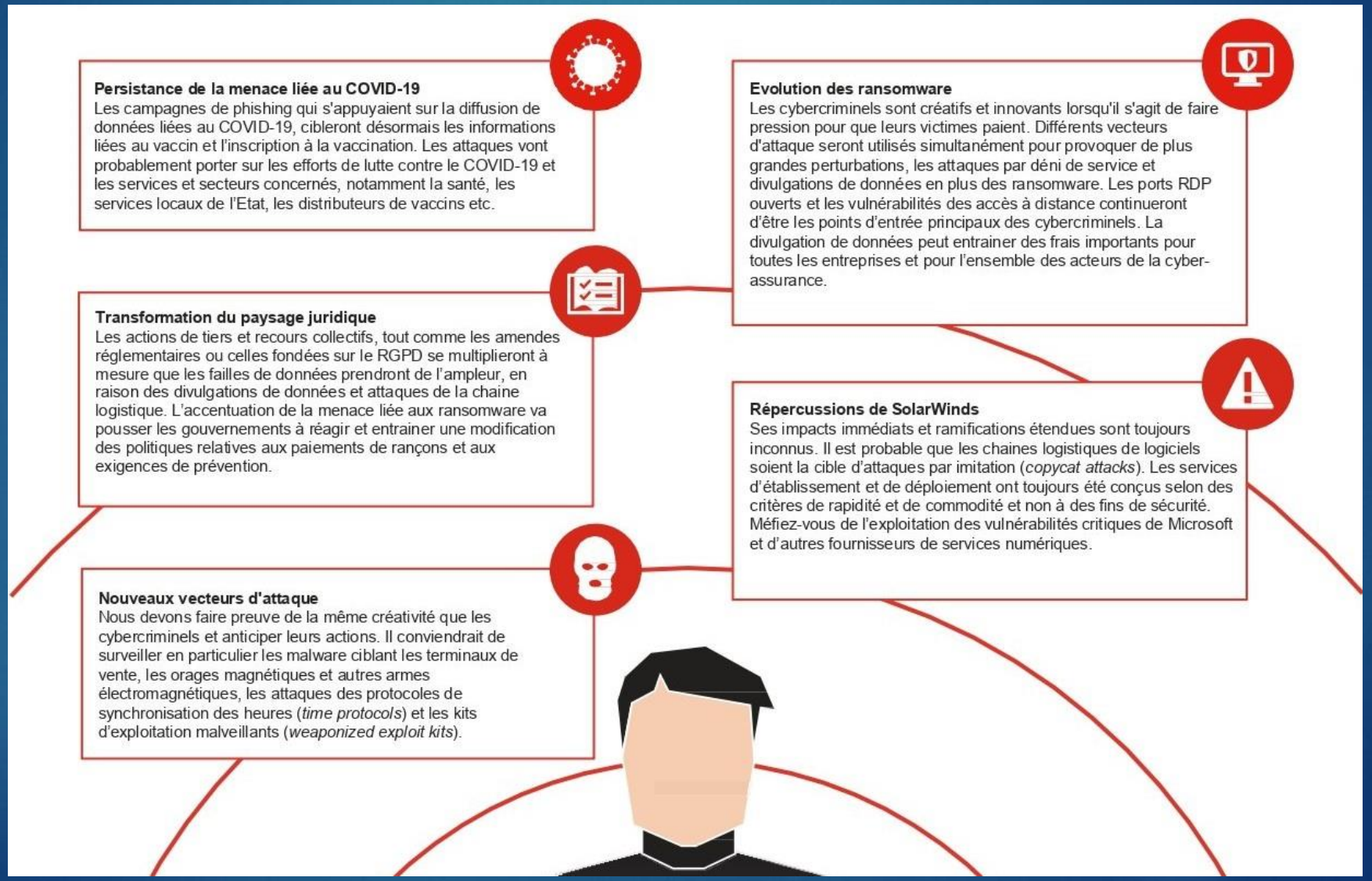
Impacts organisationnels



Pourquoi les pirates s'intéressent-ils aux S.I. des organisations ou au PC d'individus ?

- **Gains financiers** (accès à de l'information, puis monétisation et revente)
  - Utilisateurs, emails
  - Organisation interne de l'entreprise
  - Fichiers clients
  - Mots de passe, N° de comptes bancaire, cartes bancaires
- **Utilisation de ressources** (puis revente ou mise à disposition en tant que « service »)
  - Bande passante & espace de stockage (hébergement de musique, films et autres contenus)
  - Zombies (botnets)
- **Chantage**
  - Déni de service
  - Modifications des données
- **Espionnage**
  - Industriel / concurrentiel
  - Étatique

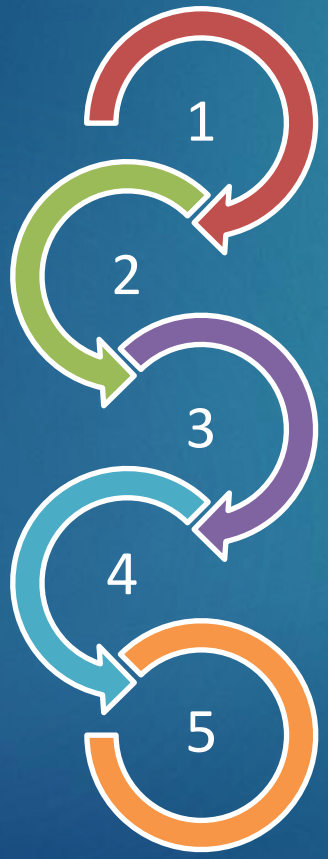
Principales Menaces 2021



https://www.hiscox.fr/blog/les-5-principaux-risques-cyber-2021
05/10/2022

La nouvelle économie de la cybercriminalité

- Une majorité des actes de délinquance réalisés sur Internet sont commis par des groupes criminels organisés, professionnels et impliquant de nombreux acteurs



des groupes spécialisés dans le **développement de programmes malveillants** et virus informatiques

des groupes en charge de l'**exploitation et de la commercialisation** de services permettant de réaliser des attaques informatiques

un ou plusieurs **hébergeurs** qui stockent les contenus malveillants, soit des hébergeurs malhonnêtes soit des hébergeurs victimes eux-mêmes d'une attaque et dont les serveurs sont contrôlés par des pirates

des groupes en charge de la **vente des données volées**, et principalement des données de carte bancaire

des **intermédiaires financiers** pour collecter l'argent qui s'appuient généralement sur des réseaux de **mules**

La nouvelle économie de la cybercriminalité

- Quelques chiffres pour illustrer le marché de la cybercriminalité…

de 2 à 10 $ le prix moyen de commercialisation des **numéros de cartes bancaires** en fonction du pays et des plafonds

5 $ le tarif moyen de location pour 1 heure d'un **botnet**, système permettant de saturer un site internet

2.399 $ le prix de commercialisation du **malware** « Citadel » permettant d'intercepter des numéros de carte bancaire (+ un abonnement mensuel de 125 $)

Les impacts de la cybercriminalité sur la vie privée (quelques exemples)

- **Impact sur l'image / le caractère / la vie privée**
  - Diffamation de caractère
  - Divulgation d'informations personnelles
  - Harcèlement / cyber-bullying
- **Usurpation d'identité**
  - « Vol » et réutilisation de logins/mots de passe pour effectuer des actions au nom de la victime
- **Perte définitive de données**
  - malware récents (rançongiciel) : données chiffrées contre rançon
  - connexion frauduleuse à un compte « cloud » et suppression malveillante de l'ensemble des données
- **Impacts financiers**
  - N° carte bancaire usurpé et réutilisé pour des achats en ligne
  - Chantage (divulgation de photos ou d'informations compromettantes si non paiement d'une rançon)

Ces impacts – non exhaustifs – ne signifient pas qu'il ne faut pas utiliser Internet, loin de là !

Il faut au contraire apprendre à anticiper ces risques et à faire preuve de discernement lors de l'usage d'Internet/smartphones…

Les impacts de la cybercriminalité sur les infrastructures critiques

- Infrastructures critiques = un ensemble d'organisations parmi les secteurs d'activité suivants, et que l'État français considère comme étant tellement critiques pour la nation que des mesures de sécurité particulières doivent s'appliquer
  - Secteurs étatiques : civil, justice, militaire…
  - Secteurs de la protection des citoyens : santé, gestion de l'eau, alimentation
  - Secteurs de la vie économique et sociale : énergie, communication, électronique, audiovisuel, information, transports, finances, industrie.

- Ces organisations sont classées comme **Opérateur d'Importance Vitale (OIV).** La liste exacte est classifiée (donc non disponible au public).

Quelques exemples d'attaques

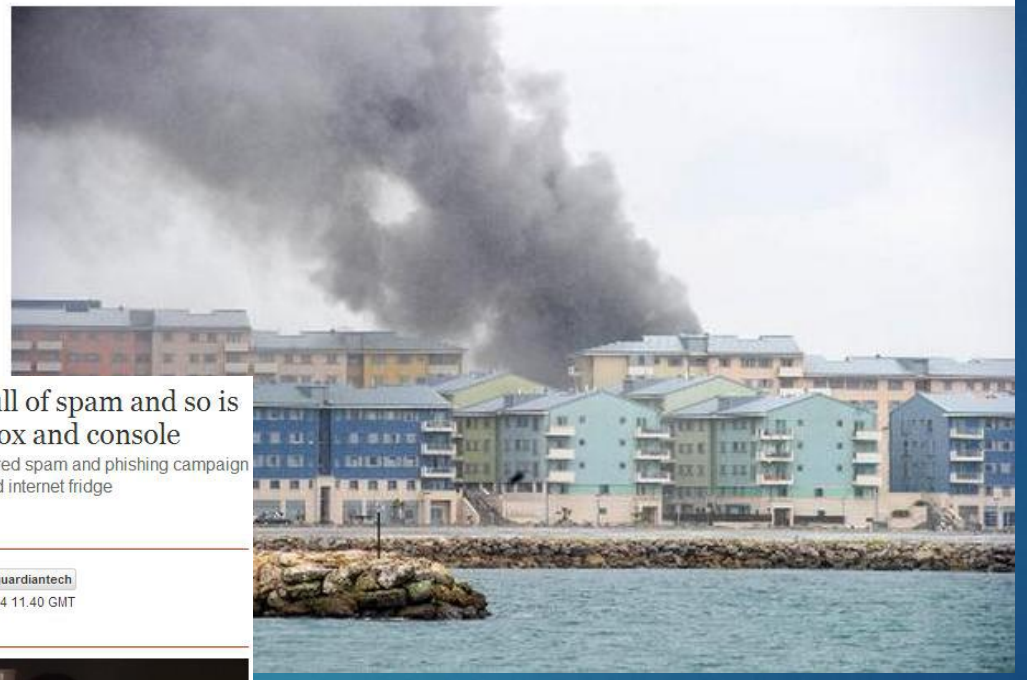
Bug informatique à La Poste : "Tout est rentré dans l'ordre"

par **Caroline Piquet**
le 30 juillet 2013 à 15h50 , mis à jour le 30 juillet 2013 à 18h59.

A la suite d'une panne informatique, les opérations de prélèvements et de virements bancaires accusent un retard de 24 heures. Ce mardi, les clients ne pouvaient accéder à leurs soldes sur Internet et il leur était impossible de retirer de l'argent aux distributeurs automatiques.

Gibraltar: un incendie interrompt des services de paris en ligne

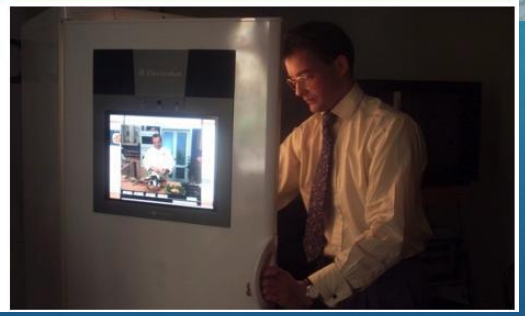
AFP, 20/04 23:31 CET



Help! My fridge is full of spam and so is my router, set-top box and console

Security company says it discovered spam and phishing campaign run over Christmas, which involved internet fridge

Charles Arthur
Follow @charlesarthur Follow @guardiantech
theguardian.com, Tuesday 21 January 2014 11.40 GMT
Jump to comments (19)



Une panne informatique paralyse Wall Street pendant 3 heures

Edité par **MYTF1News** avec **AFP**
le 23 août 2013 à 06h50 , mis à jour le 23 août 2013 à 07h02.

Un avion espion « plante » le système informatique d'un aéroport

Par Pierre Dandumont 5 MAI 2014 12:30 - Source: NBC News | 0 COMMENTAIRE

Panorama de quelques menaces

Hameçonnage & ingénierie sociale

Fraude interne

Violation d'accès non autorisé

Virus informatique

Déni de service distribué

Hameçonnage & ingénierie sociale

L'hameçonnage (anglais : « **phishing** ») constitue une « attaque de masse » qui vise à abuser de la « naïveté » des clients ou des employés pour récupérer leurs identifiants de banque en ligne ou leurs numéros de carte bancaire…

1. Réception d'un mail utilisant le logo et les couleurs de l'entreprise
2. Demande pour effectuer une opération comme la mise-à-jour des données personnelles ou la confirmation du mot de passe
3. Connexion à un faux-site identique à celui de l'entreprise et contrôlé par l'attaquant
4. Récupération par l'attaquant des identifiants/mots de passe (ou tout autre donnée sensible) saisie par le client sur le faux site

Quelques exemples d'attaques, ce qui pourrait arriver

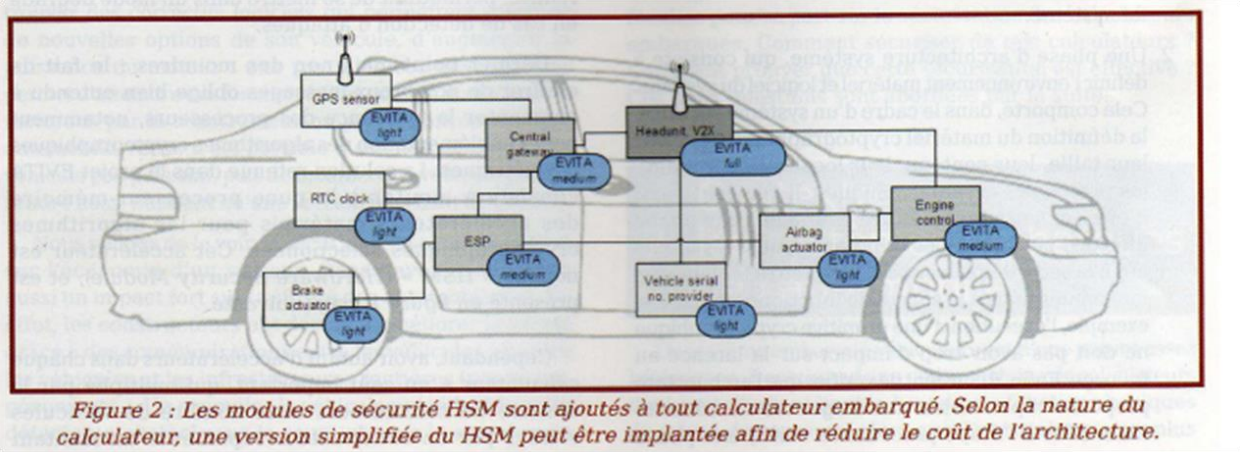
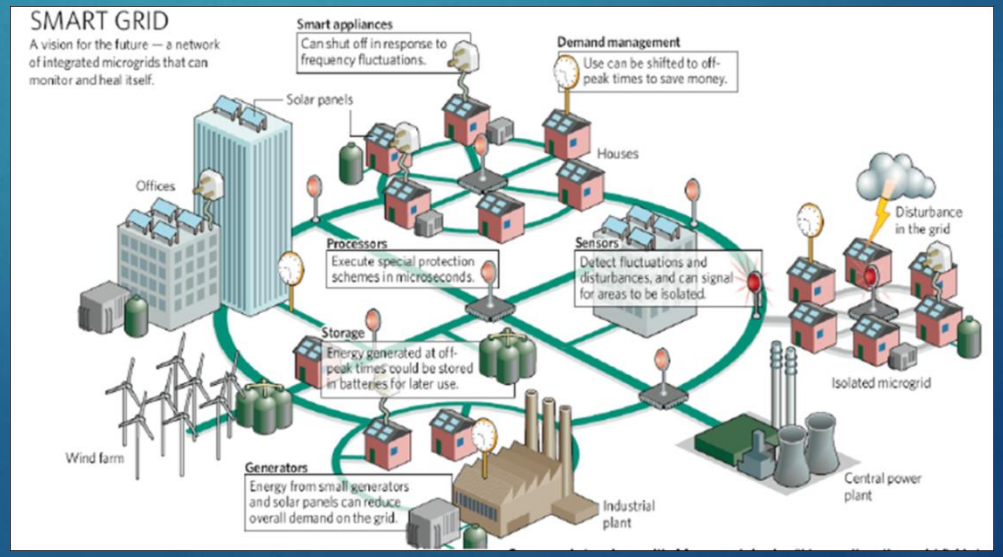


Figure 2 : Les modules de sécurité HSM sont ajoutés à tout calculateur embarqué. Selon la nature du calculateur, une version simplifiée du HSM peut être implantée afin de réduire le coût de l'architecture.

Cyberattaques sur la voiture connectée envisagées depuis 2020
Exemple : Prise de contrôle du système de frein

Déploiement des smart grid prévu à l'horizon 2030
Exemple : Blackout sur une grille.



Cybersécurité : Faites votre choix en conscience | Yann Allain | TEDxRennes

- Question :
  - Qui a un ordinateur ?
  - Qui sait qu'il faut un antivirus, ou un firewall ?
  - Qui a pensé à regarder le firewall de sa voiture ou frigo connecté ?
  - Qui a surveillé récemment le pacemaker de Mamie ?
- Imaginons qu'un pirate vous appelle :
  - Alors en voiture pour débloquer les freins ?
  - Ou la mamie pour danser toute la nuit ?

Hacker un pacemaker, c'est possible et c'est dangereux

10:12 - vendredi 19 octobre 2012 - Par Johann Mise - Source : France Info

Zoom

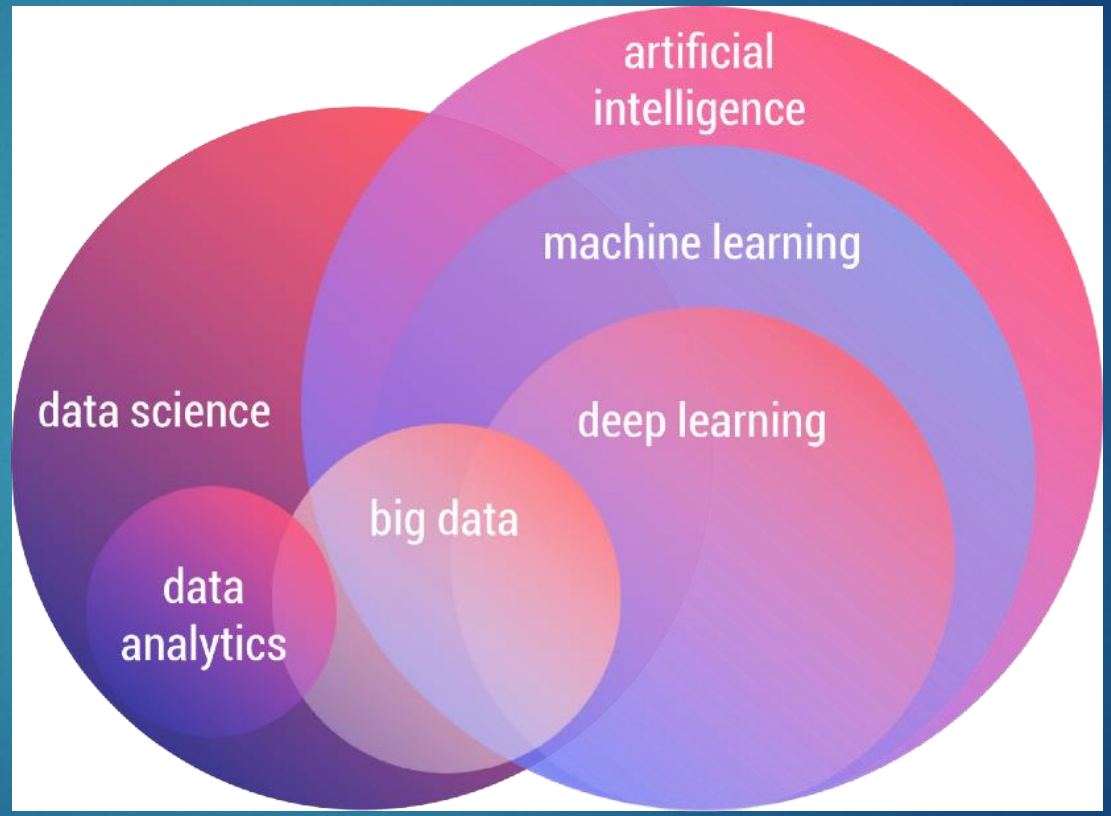
https://www.youtube.com/watch?v=r5OEIY7oz6I
05/10/2022

Agenda

- Introduction
- Des risques Cyber réels
- L'IA au service de la cybersécurité
- Quelques outils
- Conclusion

IA comme support de la data science

- **L'intelligence artificielle (IA)** est conçue pour donner aux ordinateurs la pleine capacité de réponse de l'esprit humain. Cette science englobe de nombreuses autres technologies, à l'instar du Machine Learning et du Deep Learning.
- **Le Machine Learning (ML)** utilise les schémas comportementaux existants pour prendre des décisions à partir des données et des conclusions antérieures. L'intervention humaine est toujours requise pour implémenter des modifications. Le Machine Learning est probablement la discipline de cybersécurité basée sur l'IA la plus pertinente à ce jour.
- **Le Deep Learning (DL)** fonctionne de la même manière que le ML. Il prend des décisions à partir de schémas antérieurs, mais effectue des ajustements de manière autonome. Dans le domaine de la cybersécurité, le Deep Learning relève du Machine Learning, sur lequel nous nous concentrerons davantage ici.



https://towardsdatascience.com/4-intersecting-domains-that-you-can-easily-confuse-with-artificial-intelligence-2233cb6ad7d1

05/10/2022

Nous ne sommes pas les seuls à vouloir utiliser l'IA

En août dernier, le réseau Retadup a été démantelé. Il comptait plus de 850.000 machines contrôlées par des pirates, c'est ce que l'on appelle un « botnet ».

« Le botnet qui se contente ***de paralyser un site, c'est fini.*** *Sa capacité à cartographier les failles est redoutable,* remarque Gaël Musquet.

Souvent les cibles sont observées pendant des semaines ou des mois. Et comme le botnet est international, il offre une furtivité incomparable. »

De telles puissances de calcul servent aujourd'hui à **casser des mots de passe, miner des cryptomonnaies ou injecter des virus ou des cryptolockers**, ces logiciels qui cryptent les données et exigent une rançon.

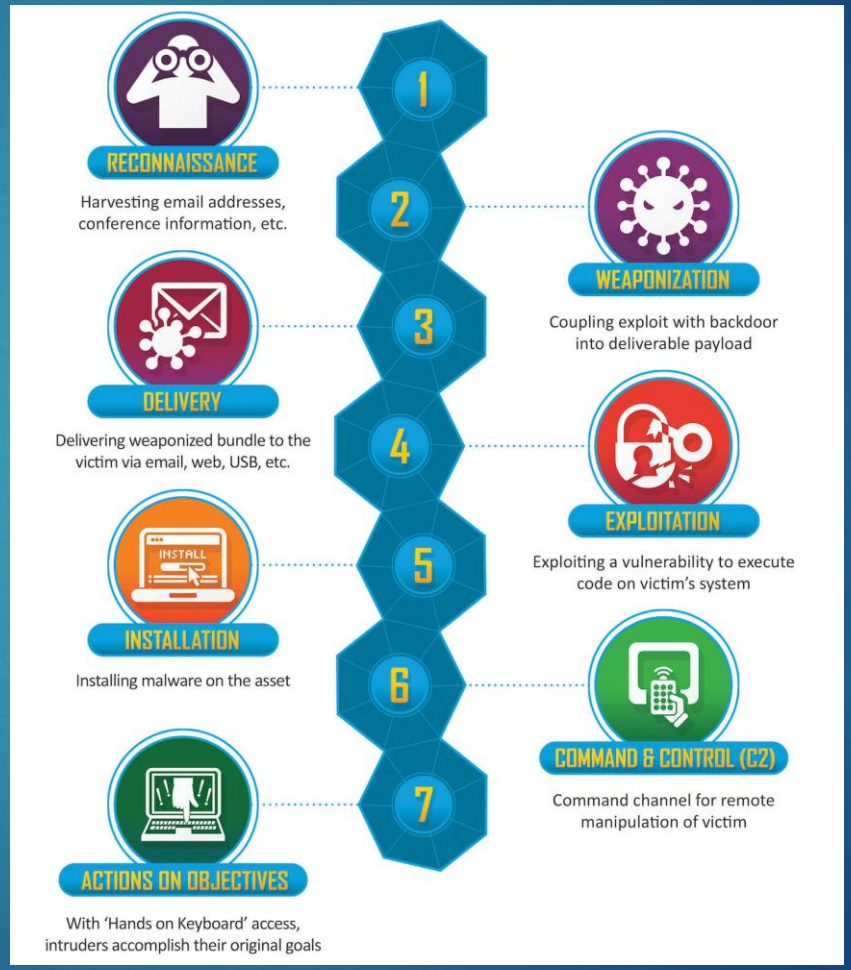
https://www.lesechos.fr/thema/cybersecurite-pme/cybersecurite-la-course-sans-fin-pour-contrer-les-menaces-1189065
05/10/2022

Bien comprendre la chaîne d'une cyberattaque

On résume par trop souvent l'attaque comme les dernières étapes et on omet les premières étapes du cycle.

Il faut savoir que les pirates peuvent être present sur les systems depuis un long moment.

> "Une chaîne d'hôtels était piratée depuis au moins quatre ans après analyse post-leaks en 2018."



https://www.lemondeinformatique.fr/actualites/lire-bien-comprendre-la-chaine-d-une-cyberattaque-72336.html
05/10/2022

L'IA, un outil permettra de basculer de réaction à la prévention.

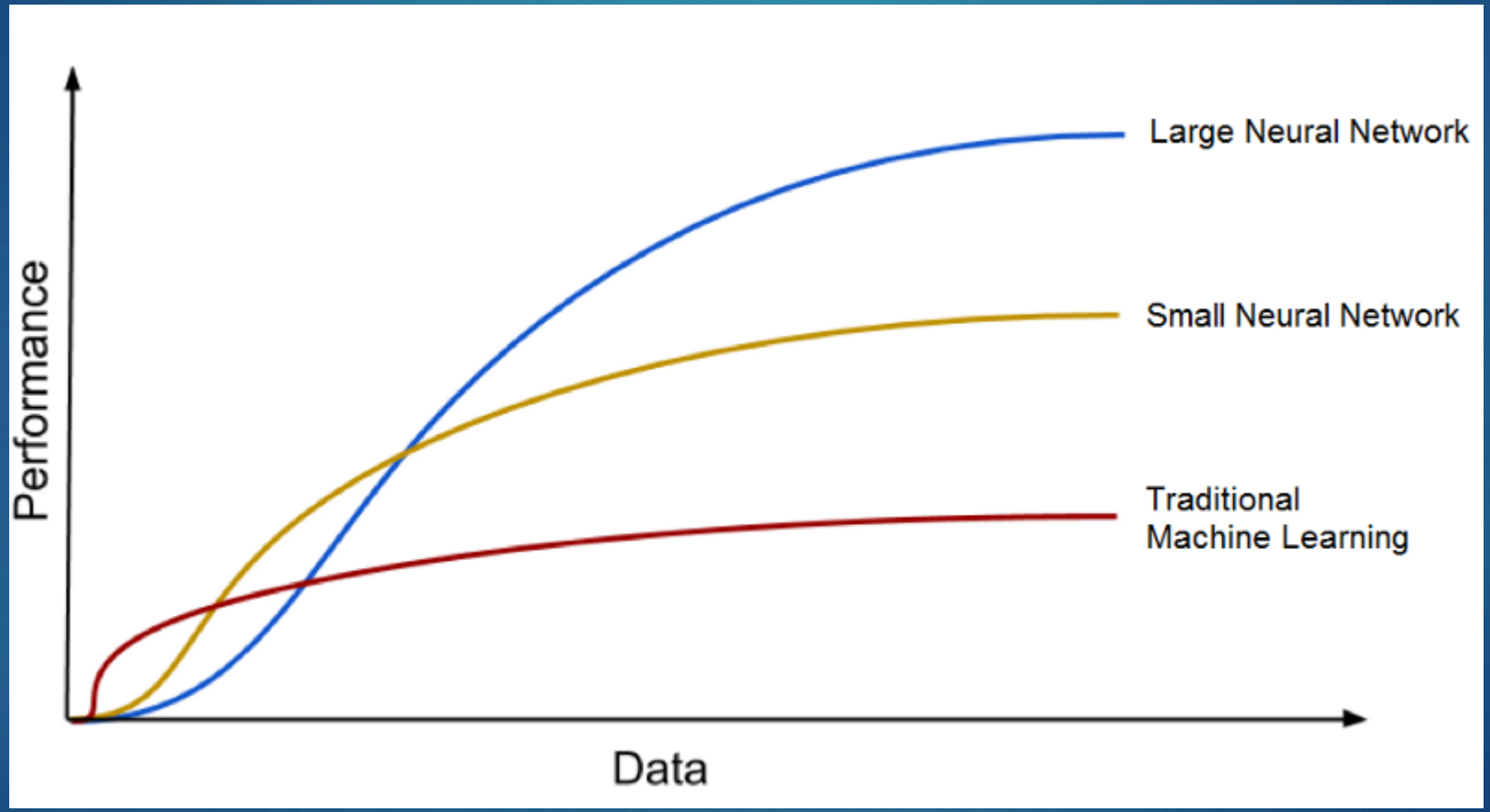
- Il est facile de mettre en relation des informations pour appréhender **les attaques connues** à l'aide d'un **SIEM** mais qu'en est il pour **les attaques inconnues** ?

- Pour ce qui n'est pas connu, nous allons utiliser la force de l'apprentissage de l'IA.
  - Les données modélisées comportement machine/humain,
  - Ces informations nous permettrons de voir en amont la structuration de l'attaque,

- Seulement 39% des entreprises se disent être suffisamment préparées en cas de cyber-attaques de grande ampleur, mais elles se protègent mieux avec environ 12 solutions mises en place. L'ensemble de ces solutions sont jugées adaptées aux besoins des entreprises (83%).

https://www.opinion-way.com/fr/component/edocman/?task=document.viewdoc&id=2199&Itemid=0
05/10/2022

Cybersécurité : Un intérêt certain pour le deep learning.



https://builtin.com/artificial-intelligence/ai-vs-machine-learning
05/10/2022

NIST Cybersecurity Framework

Le cadre de cybersécurité du NIST est un ensemble de directives pour atténuer les risques de cybersécurité organisationnelle, publié par l'Institut national américain des normes et de la technologie sur la base des normes, directives et pratiques existantes.

https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework
05/10/2022

How Vulnerable Are You To a Cyber Attack?

1 IDENTIFY

Identify and control who has access to your business information

Conduct background checks

Require individual user accounts for each employee

Create policies and procedures for cybersecurity

2 PROTECT

Limit employee access to data and information

Install Surge Protectors and Uninterruptible Power Supplies (UPS)

Patch your operating systems and applications routinely

Install and activate software and hardware firewalls on all your business networks

Secure your wireless access point and networks

Set up web and email filters

Use encryption for sensitive business information

Dispose of old computers and media safely

Train your employees

3 DETECT

Install and update anti-virus, anti-spyware, and other anti-malware programs

Maintain and monitor logs

4 RESPOND

Develop a plan for disasters and information security incidents

5 RECOVER

Make full backups of important business data and information

Continue to schedule incremental backups

Consider cyber insurance

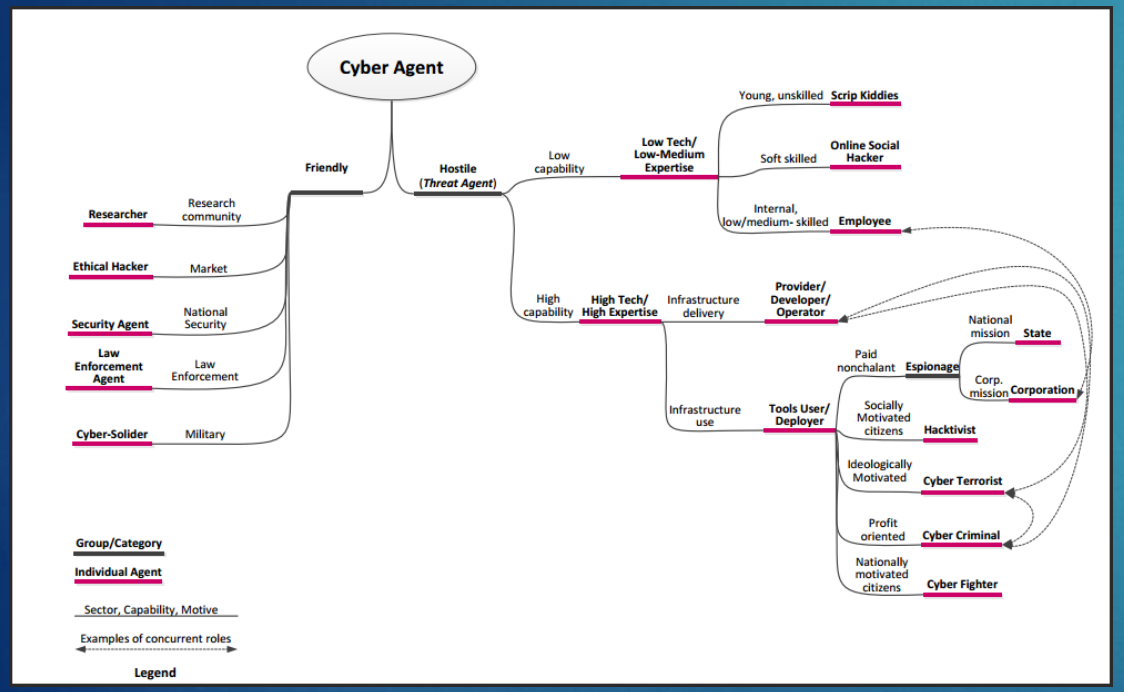
Make improvements to processes/ procedures/ technologies

https://www.nist.gov/blogs/how-vulnerable-are-you-cyber-attack-self-assessment-tool-manufacturers
05/10/2022

Quelques cas d'usage

DE LA RÉACTION À LA PRÉVENTION

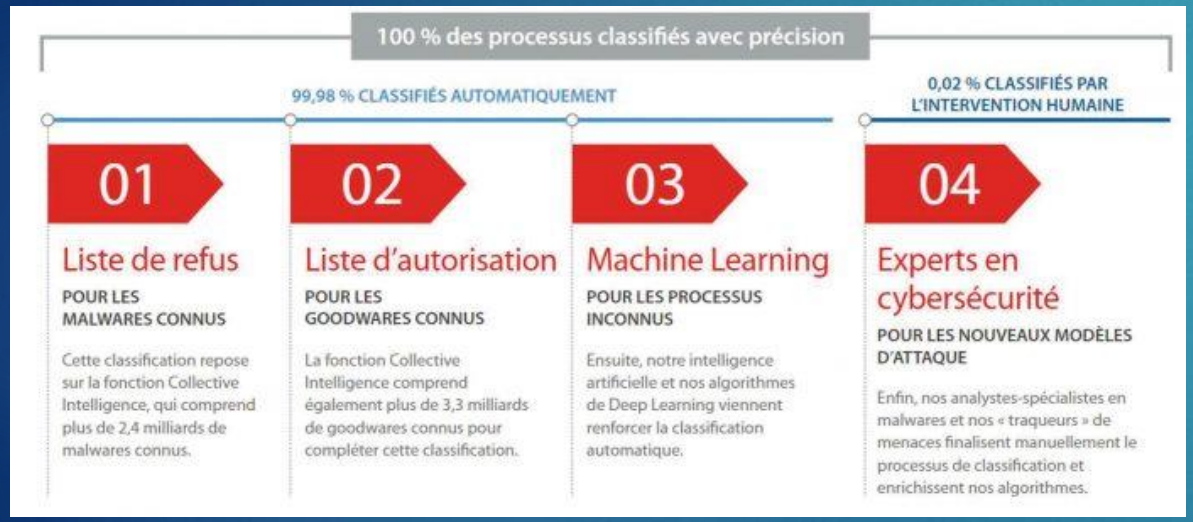
CTI : Cyber Threat Intelligence



- La **CTI** ou Cyber Threat Intelligence est l'activité liée à la collecte d'informations sur les menaces ou les acteurs de la menace. Elle peut contribuer à atténuer les évènements préjudiciables car les défenseurs disposent alors de données utiles pour prendre la bonne décision. La **CTI** est basée sur de multiples types de sources comme le renseignement open source, le renseignement via les réseaux sociaux, le renseignement humain, le renseignement technique, ou même le renseignement via des analyses du web profond et sombre (deep & dark web).

https://medium.com/swlh/cyber-threat-intelligence-cti-in-a-nutshell-1-71a03916fd92
05/10/2022

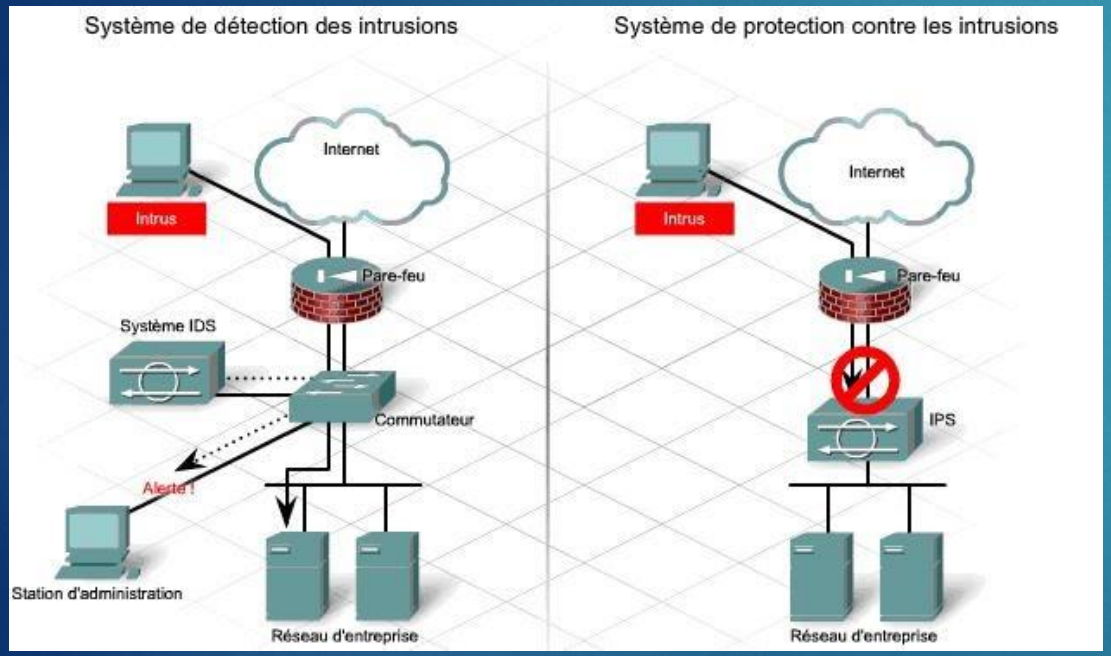
IA intégrée à l'infrastructure



- Aujourd'hui, en 2020, le deep learning a été perfectionné, et ce taux de réussite de 99,9 % est toujours valable en ce qui concerne le spam, le phishing et le blocage des logiciels malveillants. Mais c'est la recherche de logiciels malveillants qui a évolué. Le scanner Gmail traite quelque 300 milliards de pièces jointes chaque semaine, à la recherche de documents malveillants à bloquer. Parmi les documents bloqués, Google affirme que 63 % d'entre eux sont différents. C'est cette menace en constante évolution provenant de documents malveillants qui a incité Google à déployer une nouvelle génération de scanners reposant sur le machine learning (apprentissage automatique) : le deep learning.

https://www.forbes.fr/technologie/gmail-fait-appel-au-deep-learning-pour-lutter-contre-les-spam/
05/10/2022

IDS/IPS : Intrusion Detection/Prevention System



- En analysant les logs, c'est-à-dire l'ensemble des informations recueillies à un point précis du réseau de l'entreprise, des algorithmes statistiques « *identifient des enchaînements d'événements et les qualifient de normaux ou d'anormaux* », explique Thomas Anglade. Ils alertent ensuite le centre de sécurité de l'entreprise (SOC) quand des comportements jugés anormaux dans le passé se reproduisent ou quand de nouveaux comportements jamais analysés apparaissent. Ce processus d'analyse continu des actions effectuées au sein du réseau est désigné sous l'acronyme UEBA (*user and entity behavior analytics*).

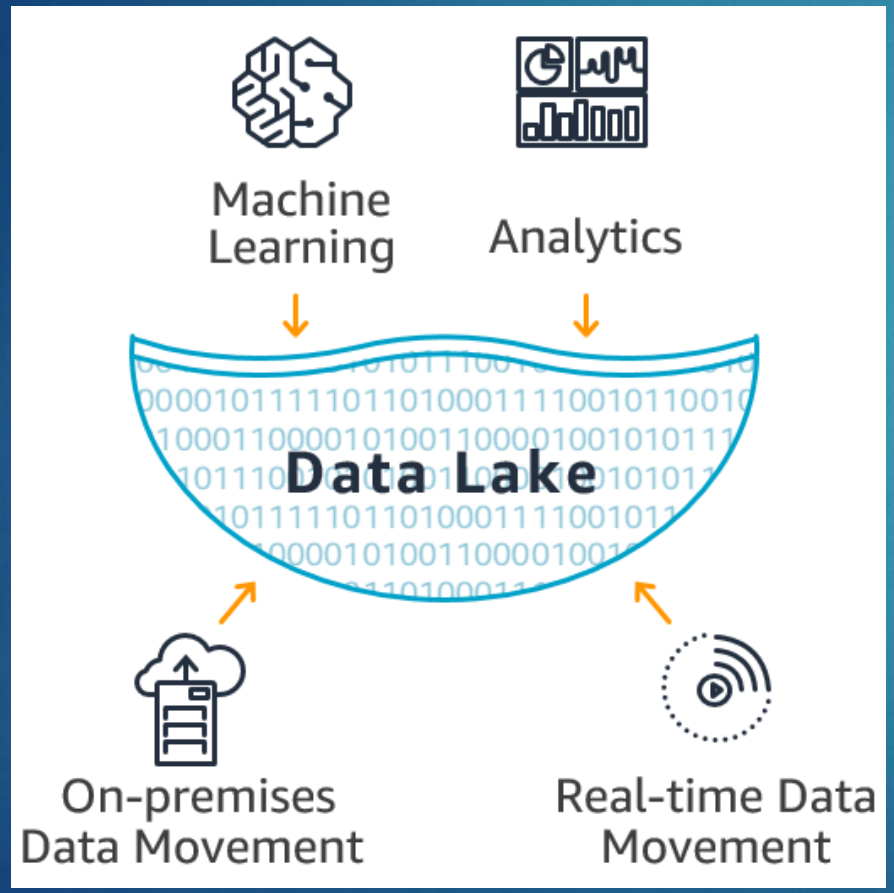
https://www.usinenouvelle.com/article/l-ia-un-allie-pour-detecter-les-intrusions-en-cybersecurite.N1816877
05/10/2022

SOC : Security Operations Center Analyse Comportementale

- D'une détection centrée sur l'équipement à une détection centrée sur l'attaque
  - L'EDR agit donc en complément de l'antivirus classique avec son approche comportementale et l'utilisation d'intelligence artificielle pour détecter des menaces inconnues ou fortement évolutives comme les ransomwares. Cette technologie offre également à une meilleure visibilité sur la sécurité informatique. Il suffit d'installer l'agent sur chaque endpoint de façon automatique ou grâce à un outil de déploiement pour qu'il alimente le SOC et les analystes cyber. Vous disposez ainsi d'informations capitales sur les agissements de l'attaquant.

https://www.servicenow.com/fr/products/security-operations/what-is-soc.html
05/10/2022

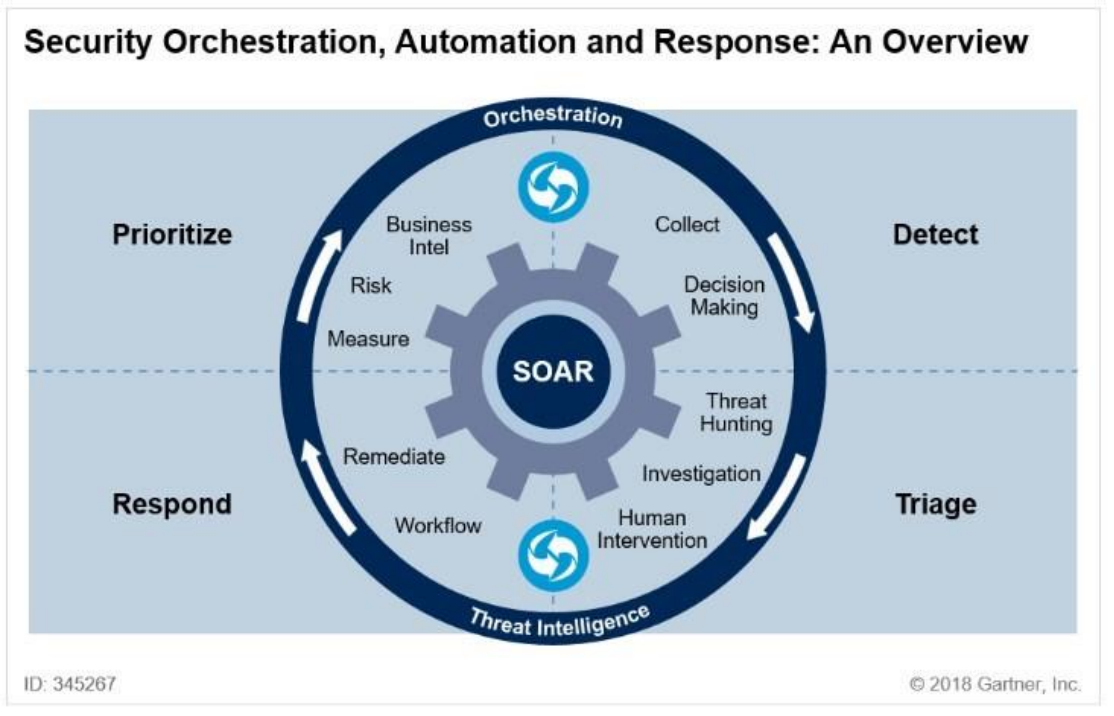
Le puit de données, une composante principale du SIEM



- Les analystes d'un SOC partent typiquement d'une alerte émanant d'un SIEM ou d'un autre outil pour ensuite en déterminer la criticité, l'étendue, l'urgence ainsi que les éléments techniques permettant de stopper les attaques et d'y remédier. Ils accèdent pour cela à un puits de données (data lake) où sont stockés les logs, des métadonnées de trafic ou autres informations. De plus ce puits de données peut être exploité pour rechercher des traces d'autres attaques qui n'auraient pas été détectées en temps réel.

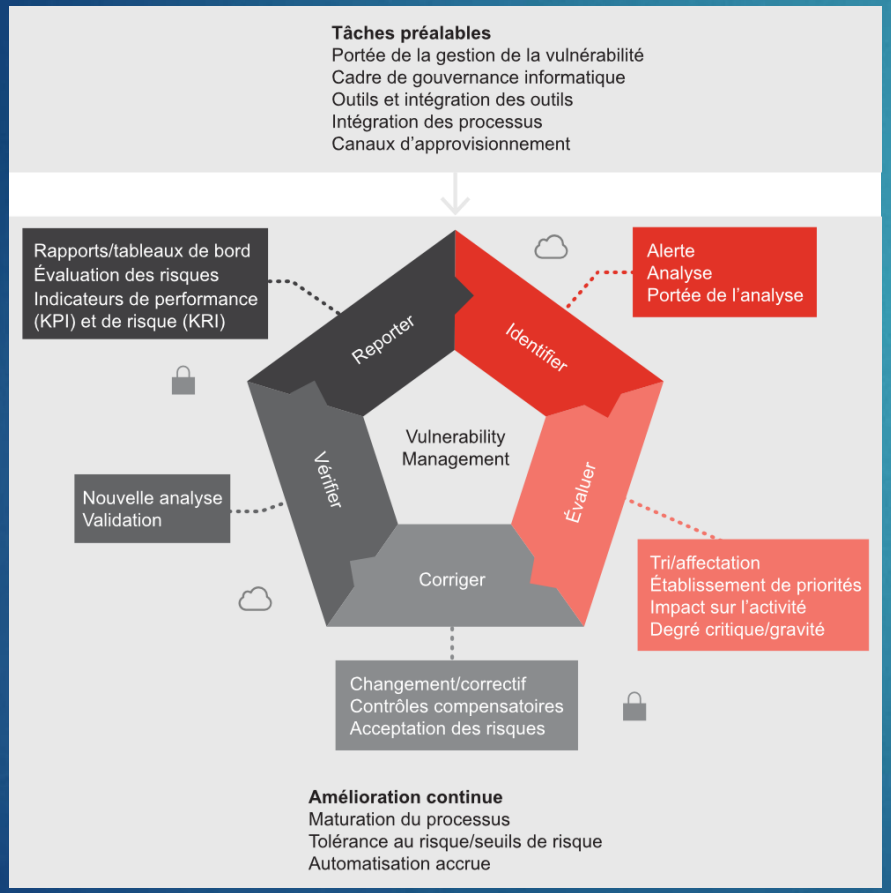
https://aws.amazon.com/big-data/what-is-a-data-lake/
05/10/2022

Proposition de scénarios de réponse par l'IA.



- Le SOAR fait référence à trois capacités logicielles clés qu'utilisent les équipes de sécurité : la gestion des cas et des workflows, l'automatisation des tâches et la centralisation de l'accès, de l'interrogation et du partage des renseignements sur les menaces. C'est le cabinet d'études Gartner qui a employé ce sigle pour la première fois. Les analystes de la sécurité désignent le même concept avec des signes différents : AIRO (Security Analytics, Intelligence, Response, and Orchestration) pour IDC et SAO (Security Automation and Orchestration) pour Forrester.

La gestion des vulnérabilités

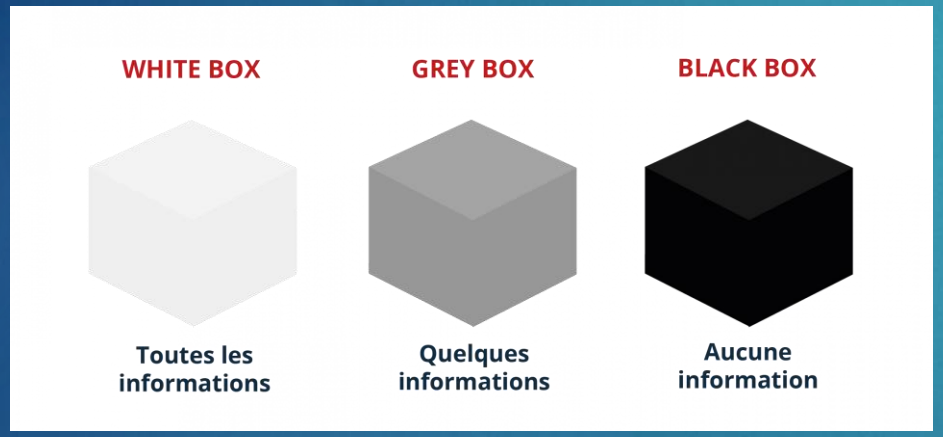


- La **gestion des vulnérabilités basée sur le risque** est un processus de cybersécurité qui vise à identifier les vulnérabilités et à les corriger. Celles-ci constituent en effet un risque majeur pour une entreprise.

https://www.crowdstrike.fr/cybersecurity-101/risk-based-vulnerability-management/
05/10/2022

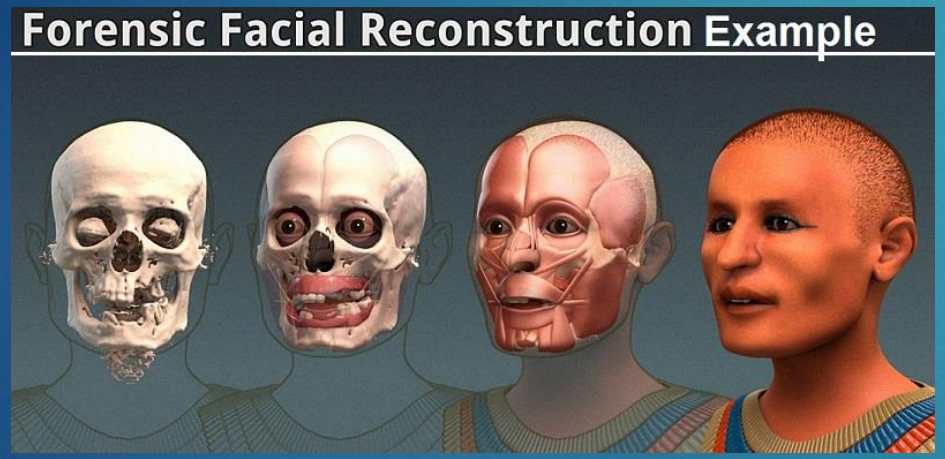
Pentest et IA, pour se prémunir d'une attaque, ou la subir…

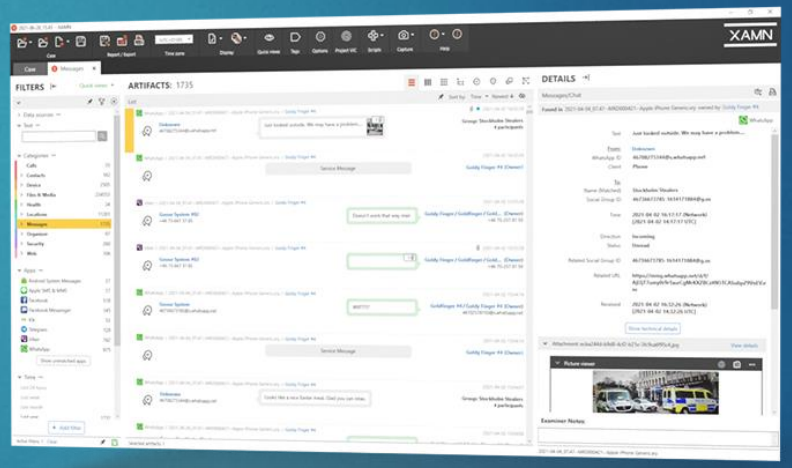
- La partie la plus délicate à aborder du fait que non seulement elle concerne aussi bien la défense que l'attaque.



https://www.login-securite.com/2019/02/22/le-pentest-de-a-a-z-methodologie-et-bonnes-pratiques-pour-securiser-son-si/

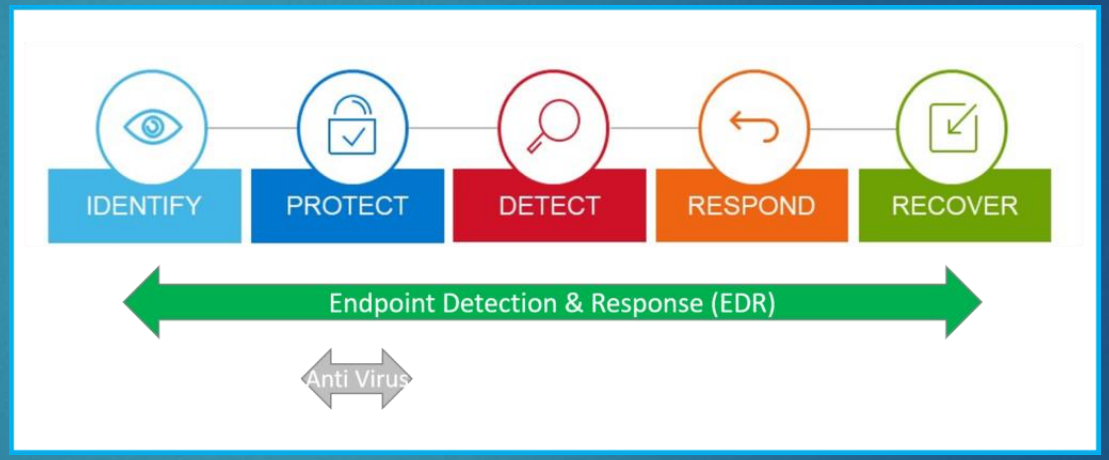
Enfin, l'analyse forensic





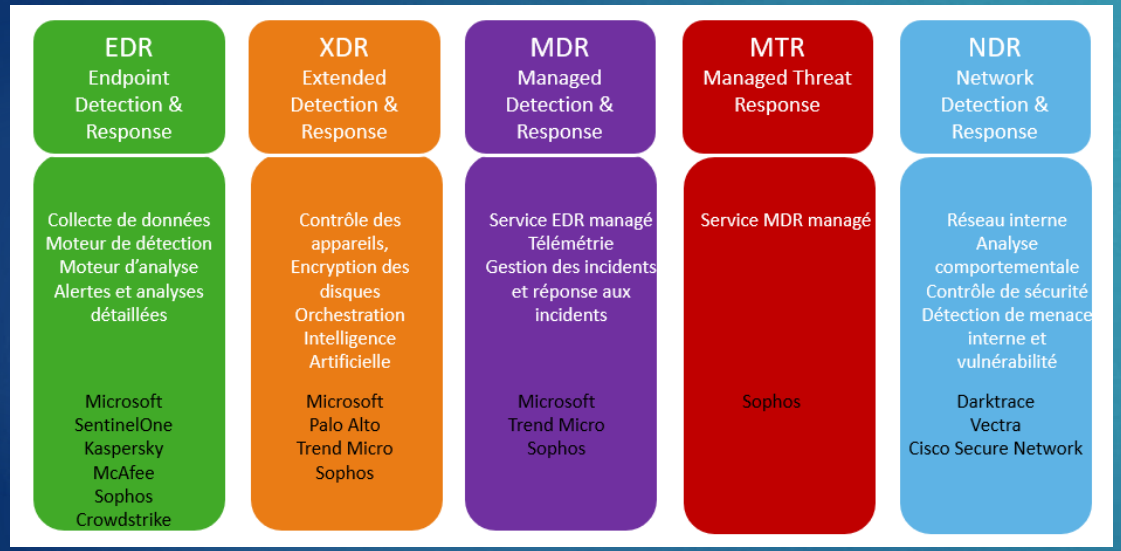
EDR Endpoint Detection and Response

- Nous venons de définir pour partie certaine brique qui compose un EDR.
- Un EDR est une solution de sécurité des terminaux qui inclut la surveillance en temps réel et la collecte des données de sécurité des terminaux avec un mécanisme de réponse automatisée aux menaces.
- Il s'agit d'une technologie de poste de travail qui permet un processus de
  - Analyse détaillée des attaques,
  - Détection d'évènements et d'incidents,
  - Recherche de menaces pour mettre en lumière des éléments suspects,
  - Réponse à des incidents.



https://gestion-services-info.com/cest-quoi-un-edr/
05/10/2022

Et ses évolutions : solutions du marché existante



- Selon Gartner : « XDR est une technologie fournie par le cloud comprenant des solutions multipoints et des analyses avancées pour corréler les alertes provenant de plusieurs sources en incidents provenant de signaux individuels plus faibles afin de créer des détections plus précises. Il vise à réduire l'étalement des produits, la fatigue des alertes, les défis d'intégration et les dépenses opérationnelles, et séduira en particulier les équipes d'opérations de sécurité qui ont des difficultés à gérer un portefeuille de solutions de pointe ou à tirer parti d'une solution SIEM ou SOAR. »

https://www.rcarre.com/blog/lintelligence-artificielle-associee-a-lintelligence-humaine-en-matiere-de-cybersecurite/
05/10/2022

Agenda

- Introduction
- Des risques Cyber réels
- L'IA au service de la cybersécurité
- Quelques outils
- Conclusion

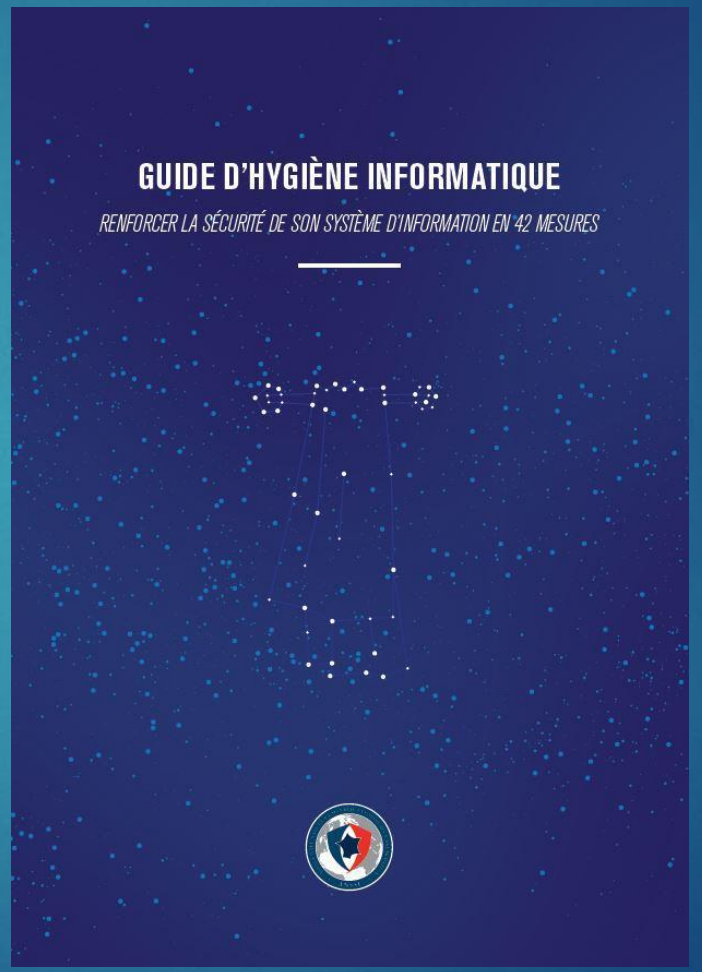
LA CYBERSÉCURITÉ POUR LES TPE/PME EN DOUZE QUESTIONS

L'ANSSI publie, en partenariat avec la direction générale des entreprises (DGE), un nouveau guide destiné aux TPE et aux PME. Réalisée avec le soutien du dispositif Cybermalveillance.gouv.fr, cette publication propose des réponses accessibles à 12 questions essentielles pour la sécurité de ces entreprises.

https://www.ssi.gouv.fr/guide/la-cybersecurite-pour-les-tpepme-en-douze-questions/
05/10/2022

Guide d'hygiène informatique - v.2

Les enjeux de sécurité numérique doivent se rapprocher des préoccupations économiques, stratégiques ou encore d'image qui sont celles des décideurs. En contextualisant le besoin, en rappelant l'objectif poursuivi et en y répondant par la mesure concrète correspondante, ce guide d'hygiène informatique est une feuille de route qui épouse les intérêts de toute entité consciente de la valeur de ses données.



https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

ISO/IEC 27000

ISO/IEC 27001 est la norme la plus connue de cette famille qui n'en compte pas moins d'une douzaine. Elle spécifie les exigences relatives aux systèmes de management de la sécurité des informations (SMSI). La mise en œuvre des normes de cette famille par tout type d'organisation facilite le management de la sécurité d'actifs sensibles tels que les données financières, les documents de propriété intellectuelle, les données relatives au personnel ou les informations confiées par des tiers.

https://www.iso.org/fr/isoiec-27001-information-security.html
05/10/2022

CyberEdu : Sécurité par l'enseignement supérieur des NTIC

Projet initié par l'ANSSI à la suite de la publication du Livre blanc sur la Défense et la sécurité nationale en 2013, le projet CyberEdu a pour objectif d'**introduire les notions de sécurité dans l'ensemble des formations dans le domaine du numérique en France**. En effet, la sécurité du numérique ne peut pas reposer uniquement sur des experts : chaque acteur de la chaîne des systèmes d'information (administrateurs, développeurs, chefs de projet, etc.) doit se sentir concerné et être impliqué.

SecNumacadémie : Formez-vous à la sécurité du numérique

Vous y trouverez l'ensemble des informations pour vous initier à la cybersécurité, approfondir vos connaissances, et ainsi agir efficacement sur la protection de vos outils numériques. Ce dispositif est accessible gratuitement. Le suivi intégral de ce dispositif vous fera bénéficier d'une attestation de réussite.

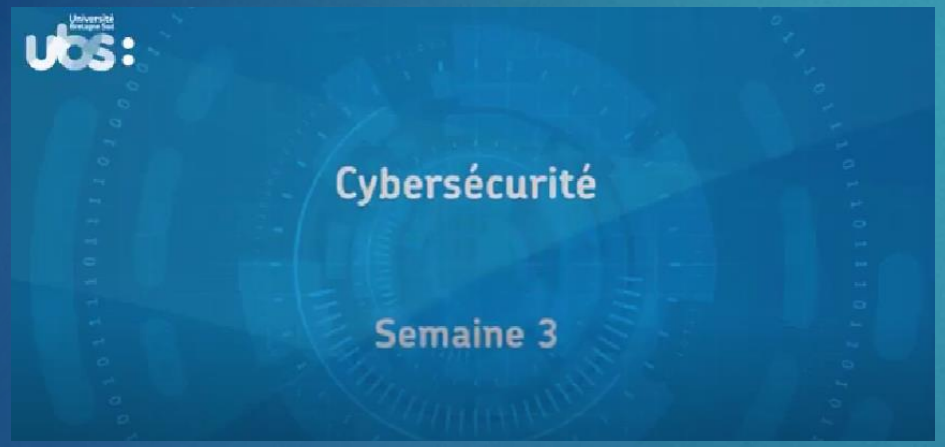
https://secnumacademie.gouv.fr/auth/login
05/10/2022

Guide d'Audit GSI

Lien de téléchargement :

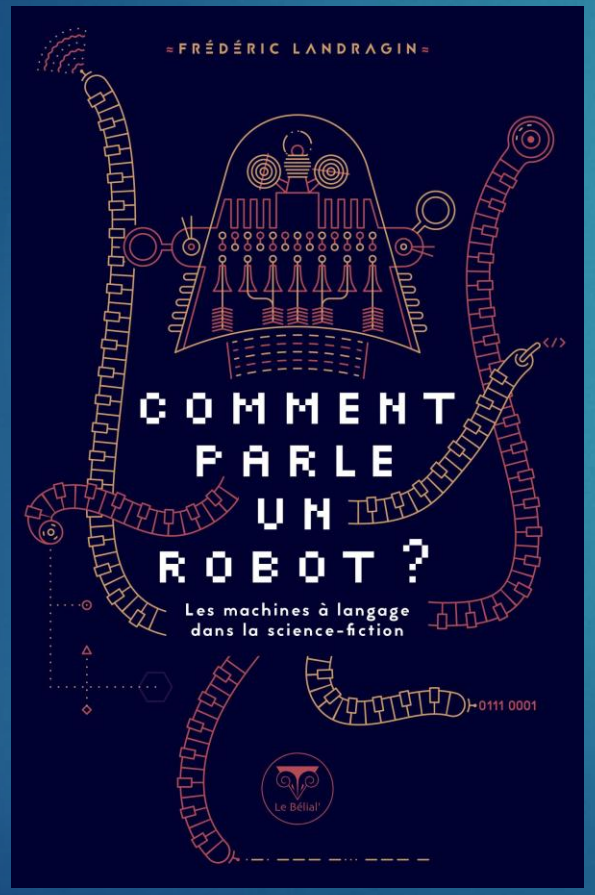
https://www.cigref.fr/wp/wp-content/uploads/2019/03/2019-Guide-Audit-Gouvernance-Systeme-Information-Entreprise-Numerique-2eme-edition-Cigref-Afai-Ifaci.pdf

IA & Cybersécurité
Université de Bretagne Sud



- Partie 1 : Introduction
  - https://www.youtube.com/watch?v=AB512D6knWQ
- Partie 2 : Lien IA & Cyber
  - https://www.youtube.com/watch?v=JZq6ZBDBX0k
- Partie 3 : Attaques et Défenses 1
  - https://www.youtube.com/watch?v=xJpu278D7hs
- Partie 4: Attaques et Défenses 2
  - https://www.youtube.com/watch?v=QgW8GKKG97E

Comment parle un robot ? (2020) de Frédéric LANDRAGIN et Cedric BUCAILLE



- « I'm sorry Dave, I'm afraid I can't do that », nous dit HAL dans 2001, l'odyssée de l'espace. Certes. Mais comment nous le dit-il ? Les machines parlantes sont partout, dans la science-fiction – de Metropolis jusqu'à WALL-E en passant par le T-800 de Terminator – ou dans la vie de tous les jours, avec les androïdes Pepper ou Nao, les assistants vocaux que sont Siri ou Cortana. Dans leurs entrailles de silicium, que se passe-t-il ? Comment s'en faire comprendre ? Et comment, elles, nous comprennent-elles ? Que penser des IA et des robots de la SF capables, à l'image de C-3PO, de parler six millions de langages ? La machine qui comprend tout et le traducteur automatique universel sont-ils à portée de main ?

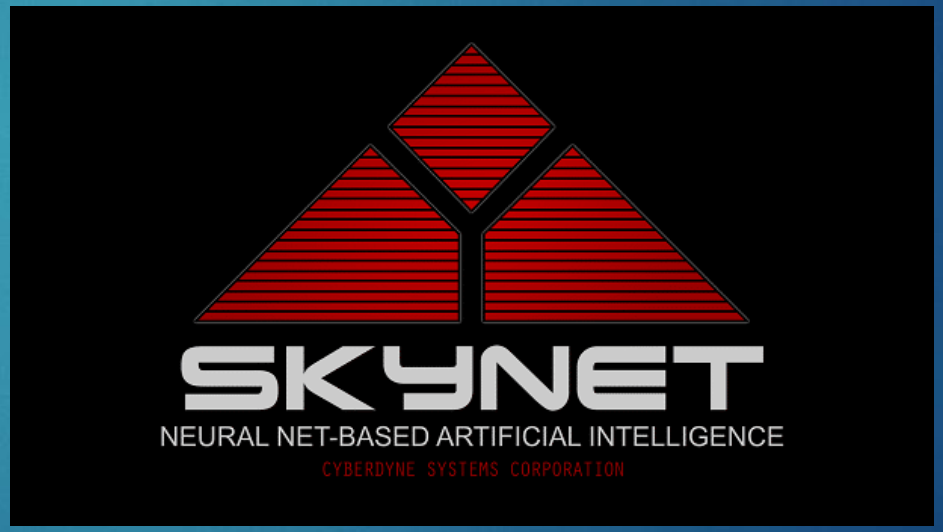
https://www.belial.fr/frederic-landragin/comment-parle-un-robot
05/10/2022

Agenda

- Introduction
- Des risques Cyber réels
- L'IA au service de la cybersécurité
- Quelques outils
- Conclusion

L'intelligence artificielle au service de la cybersécurité

- Le marché de l'intelligence artificielle dans la cybersécurité devrait atteindre 38,2 milliards de dollars d'ici 2026, contre 8,8 milliards de dollars en 2019.
- Au même titre que nous cherchons à utiliser l'IA pour nous protéger, les pirates ont aussi saisi cette opportunité pour améliorer leur démarche d'attaques sous toutes leurs formes.
- Loin de la dystopie, décrite dont de nombreux films de SF, il est possible aujourd'hui d'utiliser ces technologies à bon escient.



https://www.lebigdata.fr/intelligence-artificielle-cybersecurite#:~:text=Le%20march%C3%A9%20de%20l'intelligence,milliards%20de%20dollars%20en%202019

05/10/2022

Conclusion

- Selon l'ANSSI :
  - En l'absence de préparation, lorsque l'incident survient, il est déjà trop tard. N'attendons pas que le pire arrive. Protégeons-nous !

- En résumé :
  - le préventif > le curatif,
  - Ainsi, appréhender le risque cyber permet d'envisager la pérennité de votre activité,
  - Mieux, en fonction de l'évolution de votre activité, il peut devenir un avantage concurrentiel.

Des question ?!

Y COMPRIS LES MOINS INTÉRESSANTES !!!

Merci à vous !

CONTACT@NISTIN.NET

IIBA Geneva Chapter

IA et Cybersécurité

10:50 – 11:35

Yannis Martin
contact@nistin.net

Laissez-nous votre avis !

SWORD UPGRADE YOUR BUSINESS

IIL EMEA

Qim info

SMP Société suisse de management de projet

REDSEN CONSULTING