Sécurité applicative

Whois

---

https://www.linkedin.com/in/fimbault/

N’hésitez pas à me contacter en cas de question.

Ce qu’on traitera dans ce module

---

1. Panorama de la cybersécurité [Rappels / self-paced]
2. Sécurité applicative / web
    a. OWASP
    b. AuthN/AuthZ
3. Bas niveau (intro rust)

L’objectif est de vous donner les bases pour réaliser du dév sécurisé.

Pré-requis

Expérience en programmation : on utilisera principalement js / rust dans les exemples (pour des raisons pédagogiques).

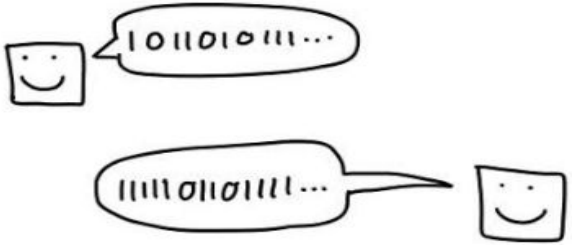
Connaissances de base en architecture des ordinateurs, réseaux, cryptographie.

Julia Evans
@b0rk

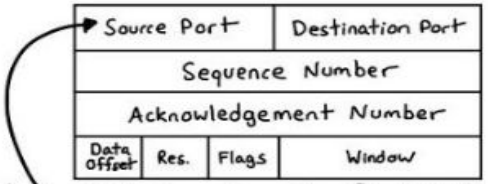
network protocols

computers communicate a lot

internet communication is made of bytes

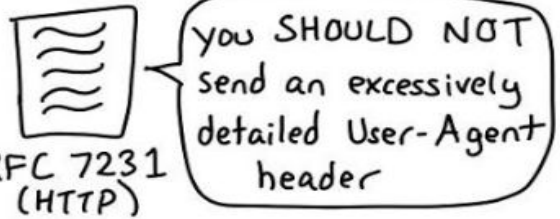


a protocol specifies what the bytes mean



in a TCP header, the first 2 bytes are the source port

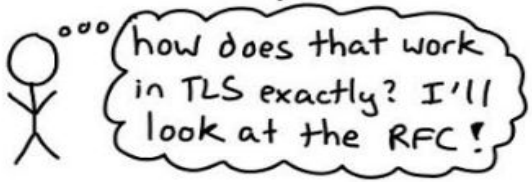
protocols also say which requests are allowed



Some network protocols

TCP UDP IMAP IP HTTP TLS DNS SSH ARP FTP

RFCs define internet protocols



The IETF publishes new RFCs

Ce qu’on ne traitera pas en détails dans ce module

Mais qu’il serait intéressant pour vous d’apprendre :

- bonnes connaissances en réseaux (physiques, virtuels) et de leur programmation (python)
- pentesting
- ransomware analysis (à faire dans une VM)
- forensics
- sécurité des OS
- devops
- CTF, exemple https://www.sstic.org/2020/challenge/

Mise en application (5 min)

à faire maintenant

Des exercices au fur et à mesure

> install **web refresh**

https://github.com/fimbault/webrefresh

[optionnel] si vous avez besoin de rappels sur le web

Projet honeypot

à faire plus tard

Fonctionnement

- équipe de 3 ou 4 étudiants
- tester avec l’autre équipe

***

Ethique et sécurité

Certaines techniques pourraient être utilisées à des fins offensives et malveillantes. Le piratage est puni par la loi.

Dans tous vos projets (pentest, bug bounty, etc.), faites attention à respecter le cadre légal et avec un objectif de défense.

-> notion de “ethical hacking”

Dans le cadre de ce cours, il s’agit de sécurité défensive.

Mise à disposition des supports

Pour les étudiants qui ont suivi le cours.

Si vous réutilisez le contenu, merci de citer l’origine (licence CC-BY-NC).

Références et autres ressources

Les références utilisées sont publiques et indiquées dans les slides (à leur première utilisation).

En cas d'oubli, merci de le signaler.

Dernier update : novembre 2020

Autres ressources complémentaires : https://github.com/fimbault/awesome_infosec

D'autres cours complémentaires pourront être indiquées dans les parties dédiées

Votre avis sur le cours

Ce cours est régulièrement amélioré.

Votre avis m’intéresse, sur ce qui va et ce qu’il faut améliorer pour vos successeurs. Vos remarques (positives comme négatives) seront prises en compte.

Panorama

Cybersécurité

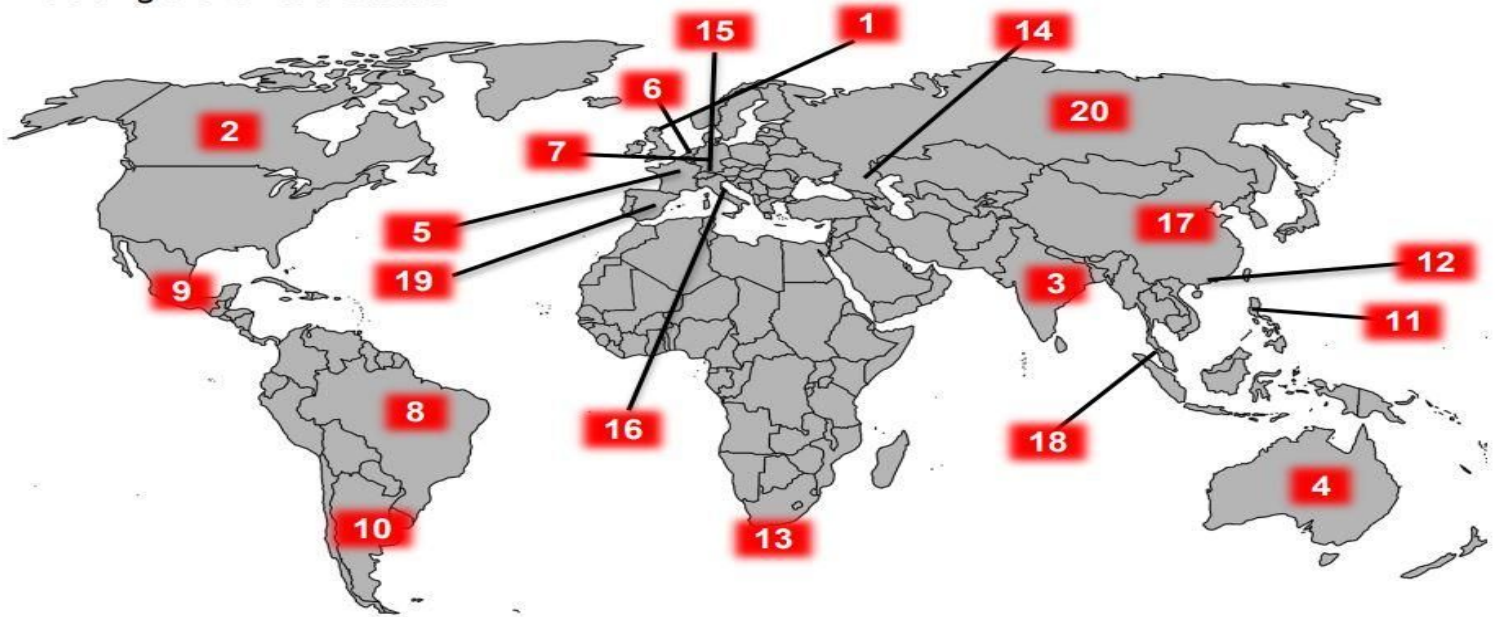
Géopolitique du cloud

- Les géants du cloud sont américains (AWS, Microsoft, Google) et bientôt chinois (Alibaba)
  - Rivalité US - Chine, certains parlent même de nouvelle guerre froide https://www.youtube.com/watch?v=qcVBHQa88xQ
  - Cas de la 5G / Huawei

- Exemple du RGPD (règlement européen sur la protection des données) : extra-territorialité US

2019 - TOP 20 INTERNATIONAL VICTIM COUNTRIES

Excluding the United States[7]



1. United Kingdom	93,796	6. Belgium	1,031	11. Philippines	561	16. Italy	428
2. Canada	3,721	7. Germany	850	12. Hong Kong	535	17. China	403
3. India	2,901	8. Brazil	628	13. South Africa	465	18. Malaysia	362
4. Australia	1,298	9. Mexico	605	14. Georgia	454	19. Spain	358
5. France	1,243	10. Argentina	578	15. Switzerland	438	20. Russian Federation	349

Source : FBI https://pdf.ic3.gov/2019_IC3Report.pdf (carte excluant les US)

Enjeux nationaux et internationaux

- Etats : US (+five eyes), Israël, Russie, Chine
  - Agences : NIST (US), ANSSI (FR) : les seules (en théorie) à pouvoir faire de l'attribution et éventuellement du hackback (illégal sinon)
  - Les états se dotent de nouvelles capacités

L'armée française délocalise son QG cyber à Rennes

La ministre Florence Parly inaugure jeudi à Rennes un centre pour le commandement cyber qui devrait doubler ses effectifs en cinq ans.

- Organisations internationales
  - https://cyberpeaceinstitute.org/

Les acteurs de la menace cyber

Concurrent

Threat Community (TCom)	Definition
Nation States	State sponsored professional groups that are engaged in espionage and either clandestine or overt action.
Cyber Criminals	A generic term for any group of criminal enterprises or loosely organized criminals. They are reasonably well-funded but not as well as a nation state.
Privileged Insiders (Malicious)	People inside your organization with specific access levels, knowledge, or some other privilege for which they do not need to overcome any controls to cause harm. Also people in which the organization has placed trust such that if they wanted to do some harm, they could. • **Malicious** – Those whom intend their actions to cause harm • **Error** – Those who make mistakes that affect security
Privileged Insiders (Errors)	
Non-Privileged Insiders (Malicious)	Everyone inside the organization who isn't privileged. These are the people who have to overcome some form of resistive control in order to affect harm.
Hacktivists/Eco-Terrorists	Generic term for those that are interested in embarrassing and making moral, disciplined, or some other conscientious argument expressed through some cyber means.

Exemple : la Corée du Nord

Les cyberattaques auraient rapporté 2 milliards de dollars à la Corée du Nord

Le mardi 06 Août 2019 à 15:10 par Jérôme G. | 9 commentaire(s)

D'après un rapport des Nations unies, la Corée du Nord a financé ses programmes d'armement via des cyberattaques ayant visé des banques et des plateformes de cryptomonnaies.

Exemples d'attaques célèbres

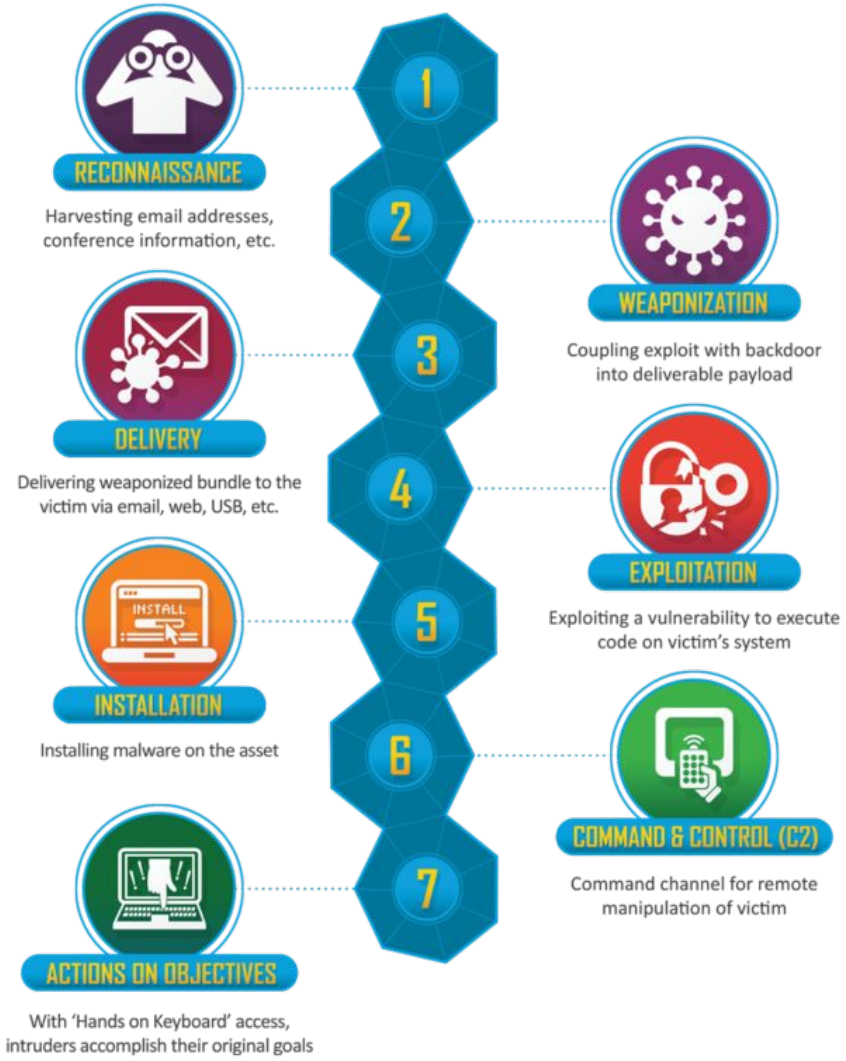
- Cuckoo's egg (1987) : https://www.youtube.com/watch?v=qubEamdc4Ng
- Stuxnet (2010) : attaque des centrifugeuses nucléaires iraniennes par les américains et israéliens
- TV5 (2015) : reportage sur france2
- Mirai (2016) : attaque par DDoS via des botnets
- Wannacry (2016) : https://www.youtube.com/watch?v=vveLaA-z3-o
- NotPetya (2017) : attaque attribuée à la Russie contre l'Ukraine https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Pour une liste exhaustive, voir :
https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

Déroulé d'une attaque

Temps moyen d'identification
~ 200 jours

(source : Ponemon)



Les paramètres

---

1) Taux de retour = à quelle fréquence les adversaires reviennent-ils ?

2) Taux de changement = à quelle fréquence les adversaires changent-ils de tactique ?

3) Coût de la correction = dans quelle mesure l'adversaire est-il confiant ?

4) Temps moyen d'identification = combien de temps ont-ils avant d’être identifiés ?

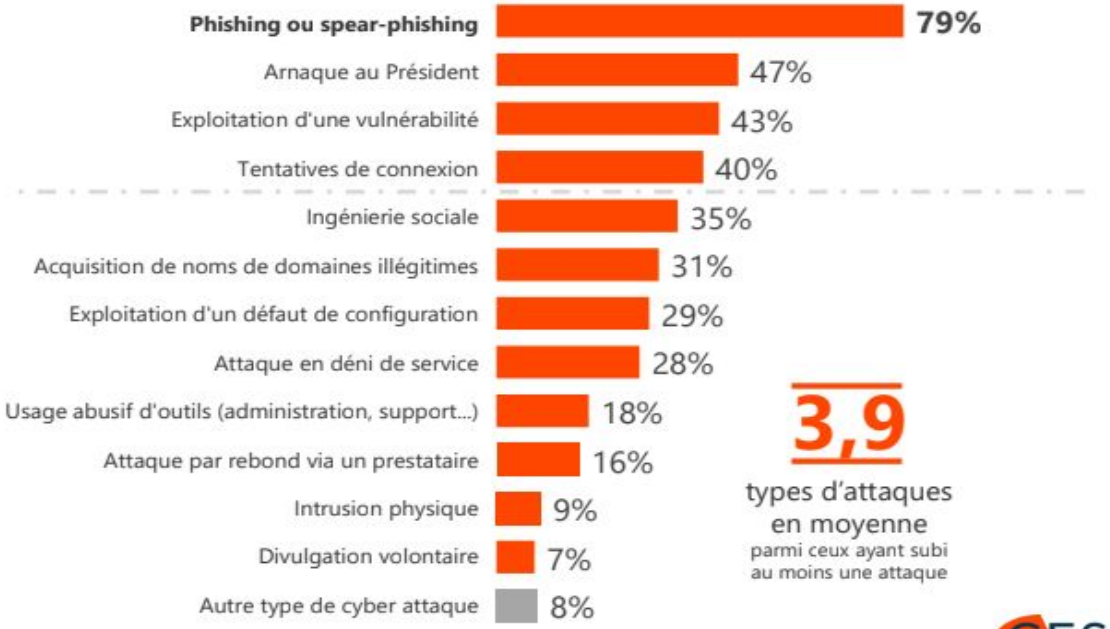
Typologie des attaques

- Différents vecteurs
  - Accès privilégié (ex: root, user impersonation, etc.)
  - Vulnérabilités (ex : OS, IOT, etc.)
- Attaque ciblée ou non
- Mitre (US https://attack.mitre.org) référence les techniques utilisées par les attaquants
  - Mapping des TTP (Tactics, Techniques and Procedures)
- OpenCTI (FR https://www.opencti.io/fr) permet de visualiser les cybermenaces

Typologie des attaques

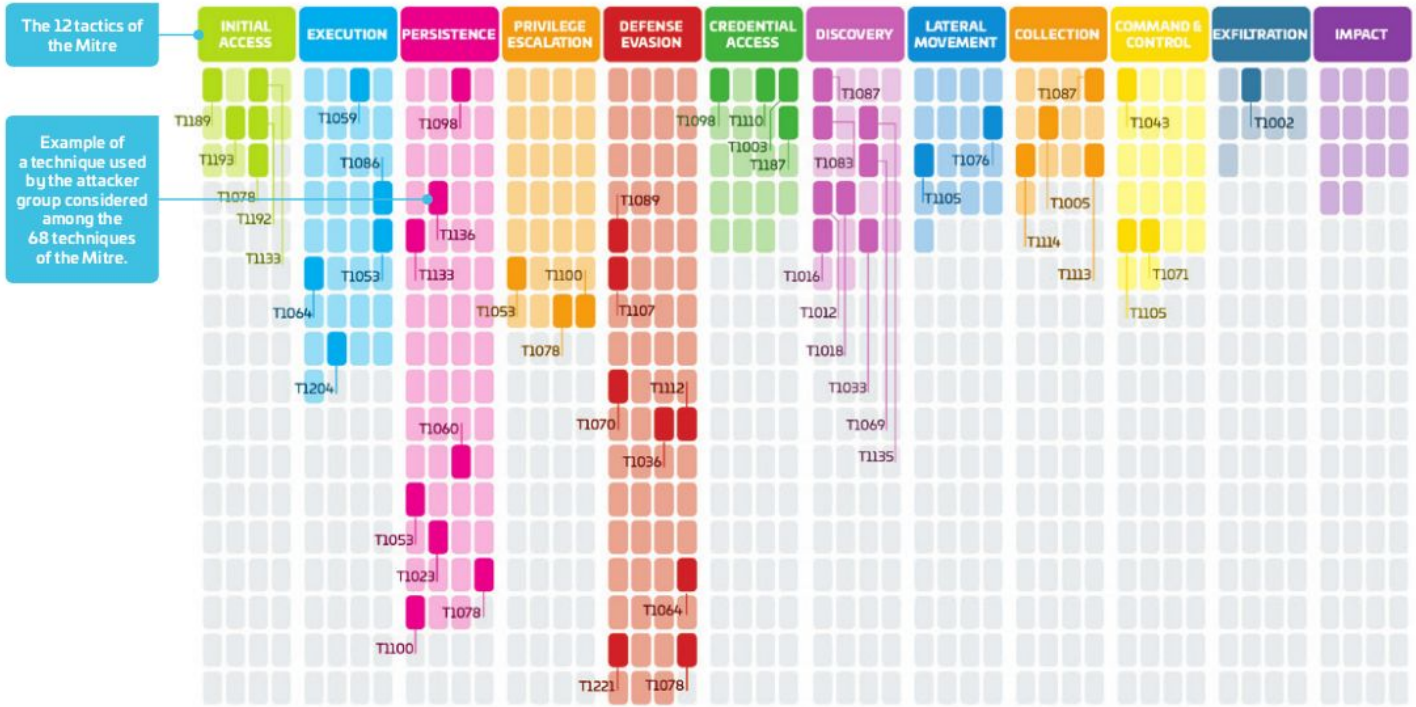
Q6C. Parmi les vecteurs d'attaques suivants, lesquels ont impactés votre entreprise au cours des 12 derniers mois ?

Base : ont constaté une attaque (163 répondants) / Plusieurs réponses possibles



CESIN

TTP

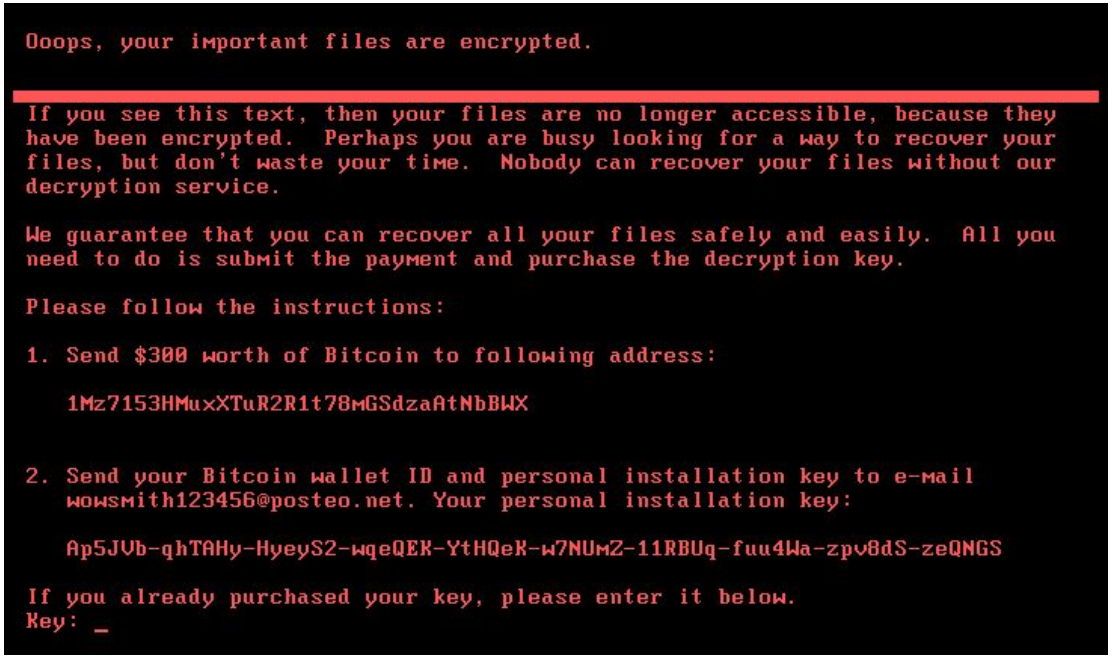


On this example the attacker group uses 11 tactics among the 12 of the Mitre and 44 techniques.

Source : Thales

Exemple : ransomware

“Why didn’t we detect the hacker? Because he ran somewhere.”

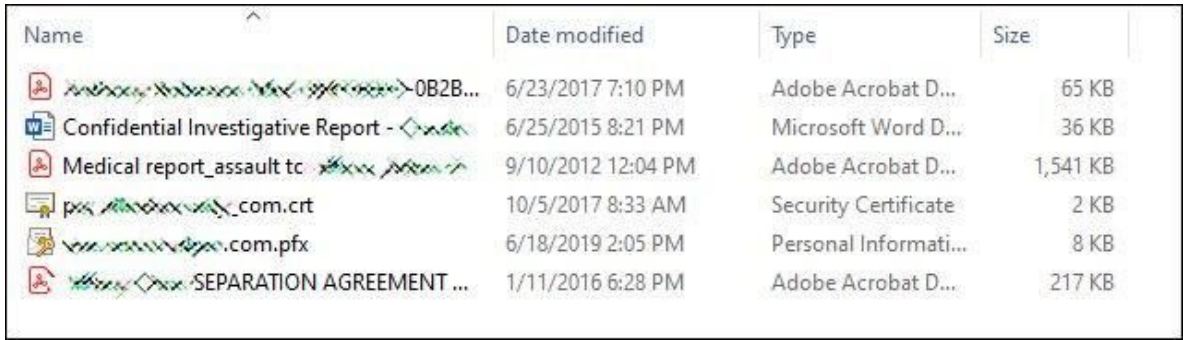


Faut-il payer la rançon ?

Idéalement non :

- aucune garantie que la clé de décryptage soit fournie ou fonctionne
- finance le ‘dark web’

De nouvelles menaces : publication des données sensibles



Name	Date modified	Type	Size
[redacted]-0B2B...	6/23/2017 7:10 PM	Adobe Acrobat D...	65 KB
Confidential Investigative Report - [redacted]	6/25/2015 8:21 PM	Microsoft Word D...	36 KB
Medical report_assault tc [redacted]	9/10/2012 12:04 PM	Adobe Acrobat D...	1,541 KB
[redacted]_com.crt	10/5/2017 8:33 AM	Security Certificate	2 KB
[redacted].com.pfx	6/18/2019 2:05 PM	Personal Informati...	8 KB
[redacted] SEPARATION AGREEMENT ...	1/11/2016 6:28 PM	Adobe Acrobat D...	217 KB

Les backups

- “Security is always seen as too much until the day it’s not enough.”
- Stratégie 3-2-1
  - 3 copies, 2 en local mais avec des supports différents, 1 offline/airgap
  - tester que la reprise fonctionne bien (associé à la notion de disaster recovery)
  - attention à la corruption possible si des synchronisations sont mises en oeuvre
  - s’assurer que les données sont encryptées ‘at rest’
- Outils pratiques
  - https://restic.net/ + solution de stockage (ex: https://www.backblaze.com)
  - Outils payants (ex: rubrik)

Quels sont les coûts d’une attaque ?

Fréquence : 2 à 5% - Ratio de 1/25 entre le coût de la rançon et le coût total.

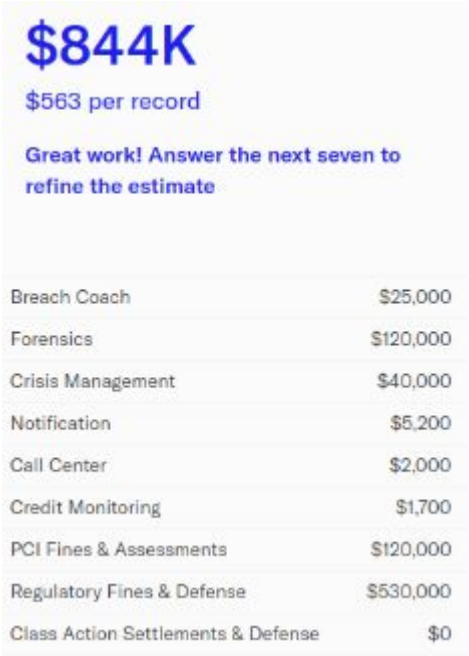
Pour les grandes organisations, les coûts peuvent être très importants, en centaines de millions d’euros (voir l’étude IBM, ‘cost of data breach report’).

Les coûts restent faibles pour les PME (étude SystemX ~ 10k euros). Les grands groupes sont de plus exigeants envers leur supply chain.

Evaluation des coûts par la cyber-assurance

Ex de simulation :

- Personal information
- Credit card
- Santé



Le secteur bancaire

Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis

Number 909
January 2020

JEL classification:

Authors: Thomas M. Eisenbach, Anna Kovner, and Michael Junho Lee

We model how a cyber attack may be amplified through the U.S. financial system, focusing on the wholesale payments network. We estimate that the impairment of any of the five most active U.S. banks will result in significant spillovers to other banks, with 38 percent of the network affected on average. The impact varies and can be larger on particular days and in geographies with concentrated banking markets. When banks respond to uncertainty by liquidity hoarding, the potential impact in forgone payment activity is dramatic, reaching more than 2.5 times daily GDP. In a reverse stress test, interruptions originating from banks with less than $10 billion in assets are sufficient to impair a significant amount of the system. Additional risk emerges from third-party providers, which connect otherwise unrelated banks.

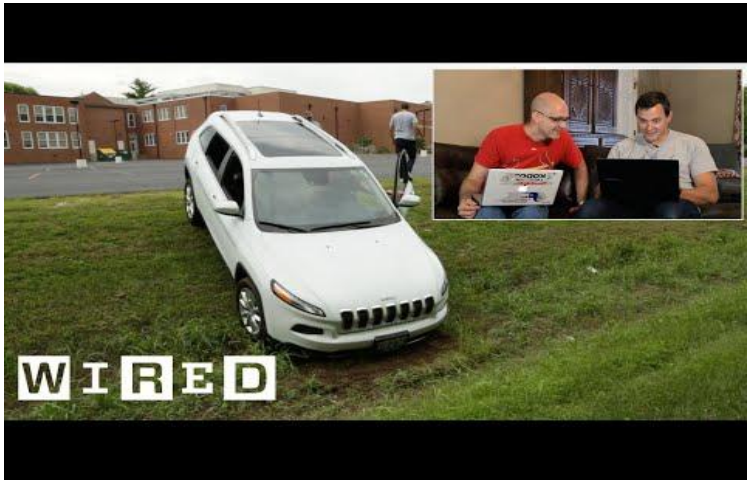
https://www.newyorkfed.org/research/staff_reports/sr909

IOT (Internet Of ~~Things~~ Too many sockets)

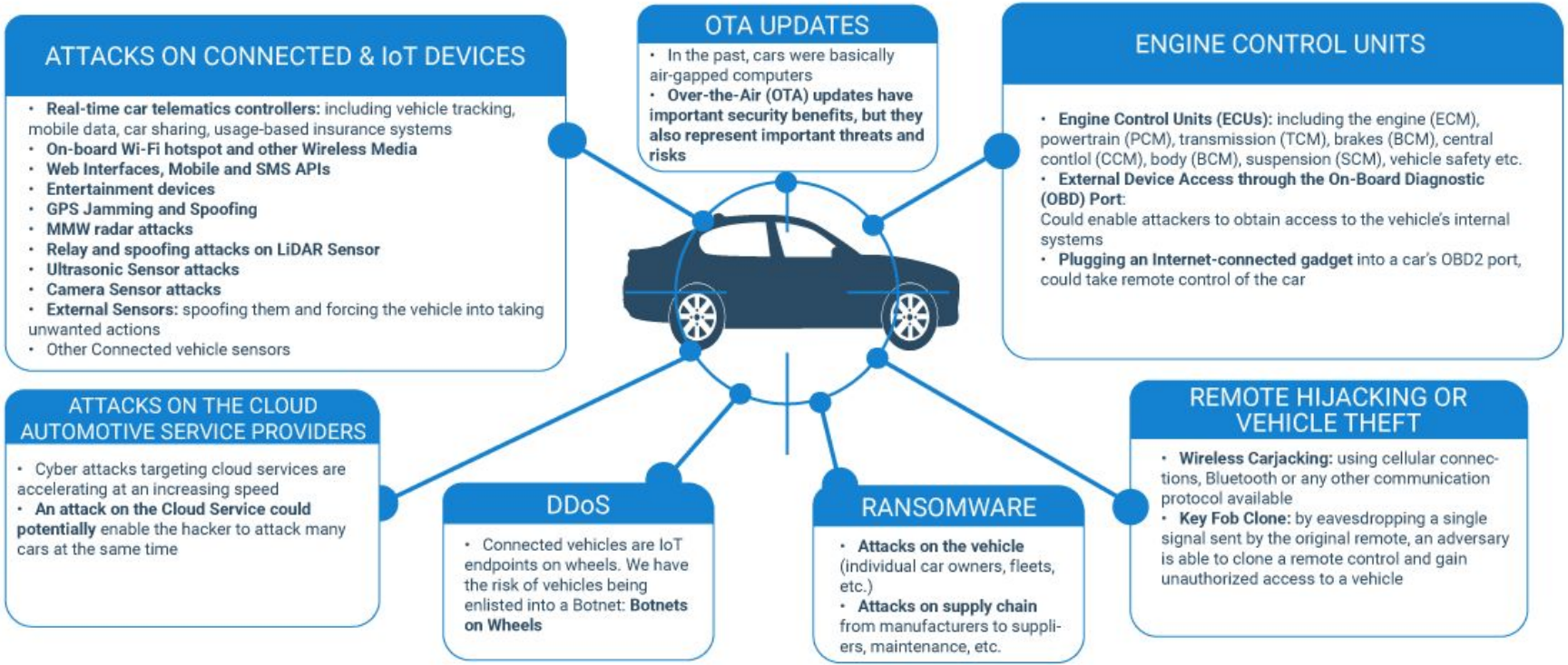
Est-ce ‘smart’ d’ouvrir tous nos objets sur internet ?

Ma voiture ? https://duo.com/decipher/hacker-history-time-charlie-chris-hacked-jeep-cherokee

https://www.youtube.com/watch?v=MK0SrxBC1xs



IOT (Internet Of ~~Things~~ Too many sockets)



La santé

- Wh0 K1ll3d D@vy M00r3? https://www.youtube.com/watch?v=e92YcLaL7bg
- Les hôpitaux deviennent des cibles, avec un coût moyen de 6.5M$ par attaque réussie
- Impact potentiel de 0,36% de morts supplémentaires (cas d'attaques cardiaques) https://onlinelibrary.wiley.com/doi/pdf/10.1111/1475-6773.13203
- Exemple détaillé d'une attaque : cas singHealth

L’énergie

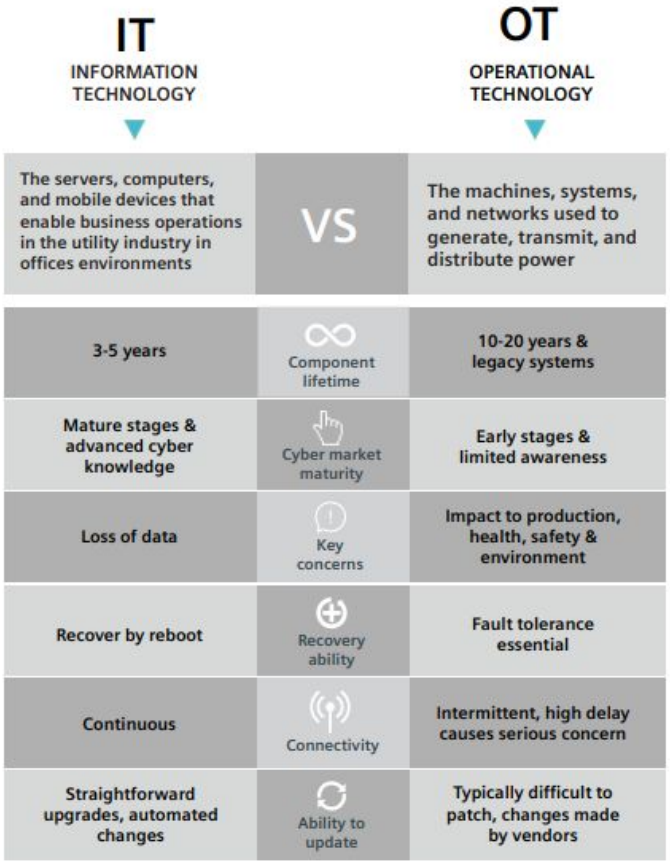
- Diverses attaques, par ex https://www.eenews.net/stories/1060281821
  https://www.forbes.com/sites/daveywinder/2020/05/15/cyber-attack-on-uk-electricity-market-confirmed-national-grid-investigates/#80516b5712a7


BRIEF

Senate passes cybersecurity bill to decrease grid digitization, move toward manual control

https://www.utilitydive.com/news/senate-passes-cybersecurity-bill-to-decrease-grid-digitization-move-toward/557959

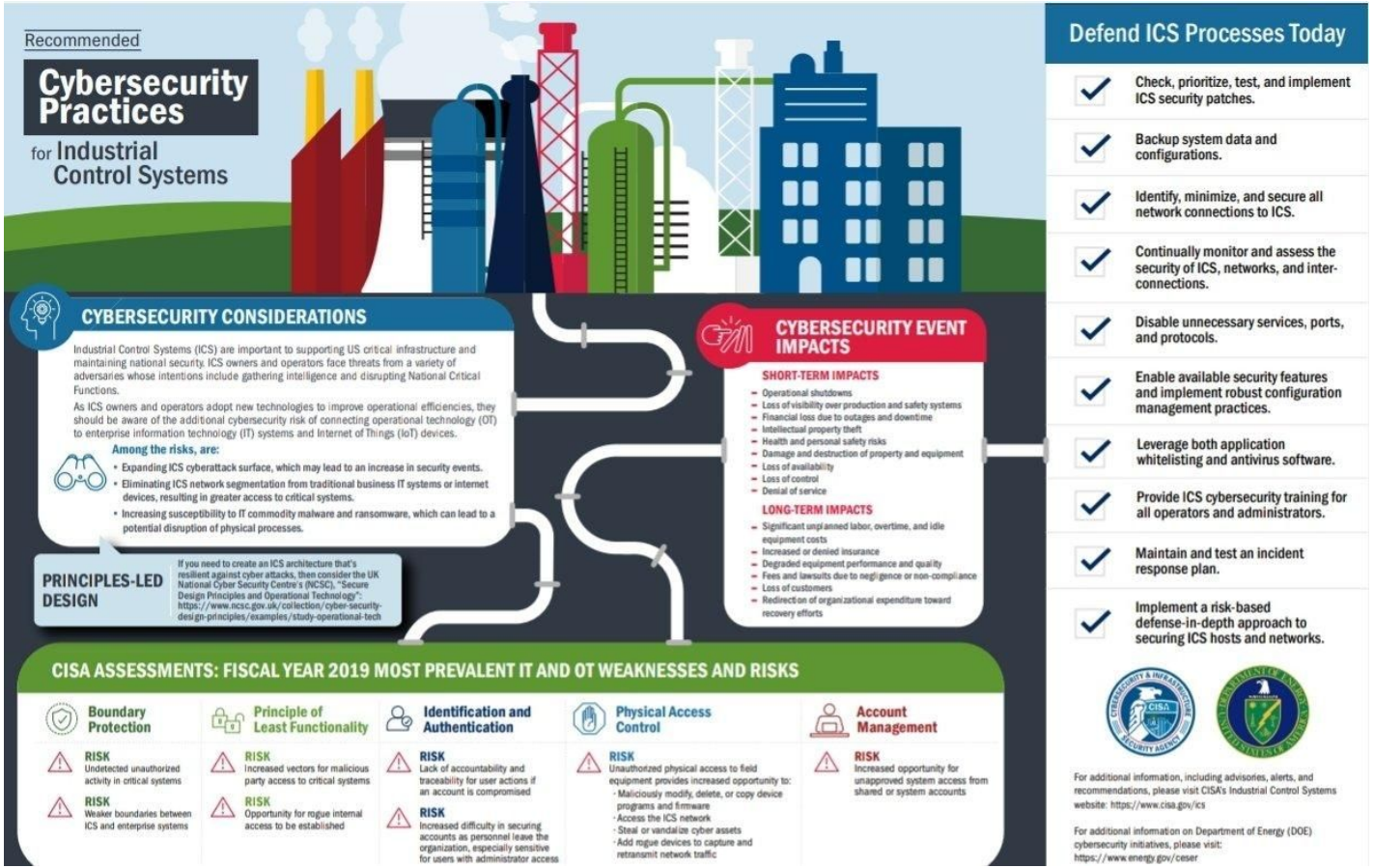
IT vs OT



IT INFORMATION TECHNOLOGY		OT OPERATIONAL TECHNOLOGY
The servers, computers, and mobile devices that enable business operations in the utility industry in offices environments	VS	The machines, systems, and networks used to generate, transmit, and distribute power
3-5 years	Component lifetime	10-20 years & legacy systems
Mature stages & advanced cyber knowledge	Cyber market maturity	Early stages & limited awareness
Loss of data	Key concerns	Impact to production, health, safety & environment
Recover by reboot	Recovery ability	Fault tolerance essential
Continuous	Connectivity	Intermittent, high delay causes serious concern
Straightforward upgrades, automated changes	Ability to update	Typically difficult to patch, changes made by vendors

https://www.tripwire.com/state-of-security/ics-security/electric-grid-ready-increased-cyber-threats/

IT vs OT


Recommended
Cybersecurity Practices
for Industrial Control Systems
CYBERSECURITY CONSIDERATIONS
Industrial Control Systems (ICS) are important to supporting US critical infrastructure and maintaining national security. ICS owners and operators face threats from a variety of adversaries whose intentions include gathering intelligence and disrupting National Critical Functions.
As ICS owners and operators adopt new technologies to improve operational efficiencies, they should be aware of the additional cybersecurity risk of connecting operational technology (OT) to enterprise information technology (IT) systems and Internet of Things (IoT) devices.
Among the risks, are:
• Expanding ICS cyberattack surface, which may lead to an increase in security events.
• Eliminating ICS network segmentation from traditional business IT systems or internet devices, resulting in greater access to critical systems.
• Increasing susceptibility to IT commodity malware and ransomware, which can lead to a potential disruption of physical processes.
PRINCIPLES-LED DESIGN
If you need to create an ICS architecture that's resilient against cyber attacks, then consider the UK National Cyber Security Centre's (NCSC), "Secure Design Principles and Operational Technology": https://www.ncsc.gov.uk/collection/cyber-security-design-principles/examples/study-operational-tech
CYBERSECURITY EVENT IMPACTS
SHORT-TERM IMPACTS
→ Operational shutdowns
→ Loss of visibility over production and safety systems
→ Financial loss due to outages and downtime
→ Intellectual property theft
→ Health and personal safety risks
→ Damage and destruction of property and equipment
→ Loss of availability
→ Loss of control
→ Denial of service
LONG-TERM IMPACTS
→ Significant unplanned labor, overtime, and idle equipment costs
→ Increased or denied insurance
→ Degraded equipment performance and quality
→ Fees and lawsuits due to negligence or non-compliance
→ Loss of customers
→ Redirection of organizational expenditure toward recovery efforts
CISA ASSESSMENTS: FISCAL YEAR 2019 MOST PREVALENT IT AND OT WEAKNESSES AND RISKS
Boundary Protection
RISK Undetected unauthorized activity in critical systems
RISK Weaker boundaries between ICS and enterprise systems
Principle of Least Functionality
RISK Increased vectors for malicious party access to critical systems
RISK Opportunity for rogue internal access to be established
Identification and Authentication
RISK Lack of accountability and traceability for user actions if an account is compromised
RISK Increased difficulty in securing accounts as personnel leave the organization, especially sensitive for users with administrator access
Physical Access Control
RISK Unauthorized physical access to field equipment provides increased opportunity to:
- Maliciously modify, delete, or copy device programs and firmware
- Access the ICS network
- Steal or vandalize cyber assets
- Add rogue devices to capture and retransmit network traffic
Account Management
RISK Increased opportunity for unapproved system access from shared or system accounts
Defend ICS Processes Today
Check, prioritize, test, and implement ICS security patches.
Backup system data and configurations.
Identify, minimize, and secure all network connections to ICS.
Continually monitor and assess the security of ICS, networks, and inter-connections.
Disable unnecessary services, ports, and protocols.
Enable available security features and implement robust configuration management practices.
Leverage both application whitelisting and antivirus software.
Provide ICS cybersecurity training for all operators and administrators.
Maintain and test an incident response plan.
Implement a risk-based defense-in-depth approach to securing ICS hosts and networks.
For additional information, including advisories, alerts, and recommendations, please visit CISA's Industrial Control Systems website: https://www.cisa.gov/ics
For additional information on Department of Energy (DOE) cybersecurity initiatives, please visit: https://www.energy.gov/ceser

Et dans le cloud ?

48% of AWS S3 buckets do not have server-side encryption enabled

41% of AWS Relational Database Service (RDS) instances do not have encryption enabled

55% of cloud user-configured S3 buckets do not have logging enabled

66% of cloud user-configured S3 buckets do not have logging enabled

26% of cloud user-configured AWS EC2 instances have SSH (port 22) exposed to the internet

17% of cloud user-configured AWS Security Groups allow ALL inbound traffic (0.0.0.0/0)

https://unit42.paloaltonetworks.com/cloud-threat-report-intro/

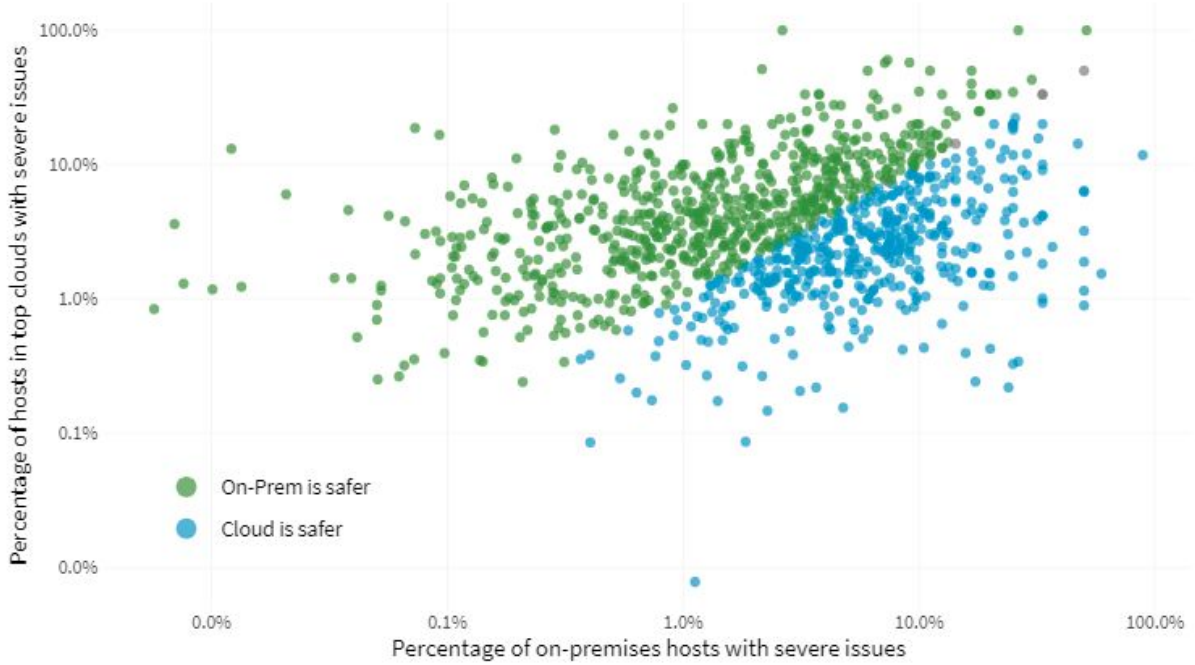
Sécurité : cloud vs on-prem

Report Overview

The Cloud Risk Surface Report is a new research study between RiskRecon and the Cyentia Institute, seeking to answer the question: Are organizations more secure in the cloud?

While the study found that 60% of organizations face higher-severity risk exposures in their cloud infrastructure, the study reveals various dynamics at play in cloud computing that influence an organization's cloud success.

Figure 1: Comparison of hosts with severe findings in on-prem vs. cloud environments



Cyber résilience : comment se remettre ?

> *“There are only two types of companies—those that know they've been compromised, and those that don't know. If you have anything that may be valuable to a competitor, you will be targeted, and almost certainly compromised.”*
> - Dmitri Alperovitch

> *“The mistake is in asking, ‘How can we prevent attacks?’ when we should be asking, ‘How can we limit the damage that can be done when an attack succeeds?’*" - Alan Karp

Gestion de crise

- Importance de la communication
  https://www.microsoft.com/security/blog/2019/12/17/norsk-hydro-ransomware-attack-transparency/
- Procédure en cas de crise
  - Quels experts peut-on mobiliser ?
  - Comment travailler en mode dégradé ? (PCA)
  - Comment reconstruire l'infra ? (PRA)
  - Comment communique-t-on en interne et en externe ?
- Besoin de s'entraîner à gérer des crises
  - Exemples : plateforme de simulation 'cyber range'
  - https://la1ere.francetvinfo.fr/polynesie/tahiti/exercice-cyberfenua-2018-entreprises-face-scenario-catastrophe-634304.html
  - https://github.com/secdevops-cuse/CyberRange

Occurrence des crises

Q5. Combien de cyber-attaques ont été constatées dans votre entreprise au cours des 12 derniers mois ?
Base : ensemble (253 répondants)

Définition donnée pour cette vague 5 : *« La cyber-attaque est le fait de subir un acte malveillant envers un dispositif informatique portant atteinte de manière significative à la confidentialité et/ou à l'intégrité de l'information de l'entreprise ou encore à la disponibilité du système d'information entrainant des pertes financières significatives et/ou une atteinte à l'image de l'entreprise. »*

65%
des entreprises ont constaté au moins une cyber-attaque

CESIN

Un frein majeur au coeur de la crise ...

- Difficultés à récupérer les données sauvegardées
  - indisponibilité du serveur de sauvegarde (destruction ou perte du catalogue des sauvegardes)
  - perte d'intégrité des sauvegardes (infection antérieure à la sauvegarde la plus ancienne)
- Le serveur de sauvegarde est-il sauvegardé ?

Une crise maîtrisée en 48h

Timeline of attack

Important Points

- The attacker connected to an internet facing system with Remote Desktop Protocol (RDP) open to the internet
- The attacker found data on one or more internal file shares, and exfiltrated a subset of those files
  - The attacker claims to have exfiltrated a total of 32 Gb of data from the City of Pensacola internal network
- The attacker then distributed and executed ransomware on 27 systems
- Shortly after being alerted, City of Pensacola IT personnel began restoration of affected systems and took initial steps to mitigate further damage to the environment
- Although it is clear that the attacker had potential access to database systems containing City of Pensacola client data, no evidence was found that indicates that data was actually accessed by the attackers

Une crise maîtrisée en 48h

On December 7, 2019, the City of Pensacola experienced a ransomware attack (the "Incident") that impacted the City of Pensacola's Information Technology environment.

The City of Pensacola engaged Deloitte & Touche LLP ("Deloitte & Touche") to assist with the investigation of the Incident, and to determine, to the extent possible, the initial compromise vector, the extent of the attack, and what internal data was exposed or stolen by the attackers. We were also asked to provide security observations and recommendations with the intent of improving the overall security of the environment and mitigating the risk of further cyber attacks.

Objectives	Findings
Determine initial attack vector	The initial attack vector was very likely two systems with RDP (Remote Desktop Protocol) exposed to the internet. Once compromised, this allowed full access to the internal environment due to lax firewall rules between the DMZ[1] and the internal network.
Determine overall extent of the attack	We confirmed ransomware activity on at least 27 systems, but it is possible that additional systems were impacted by the ransomware. The attacker also claimed to have exfiltrated approx. 32GB of data. We were able to confirm approximately 6GB of compressed data had left the environment.
Determine what internal data was exposed or stolen	The attacker claimed to have exfiltrated approx. 32GB of data. We were able to confirm approximately 6GB of compressed data had left the environment. We also confirmed that the attacker had full access to internal systems, and had knowledge of the primary network shares containing a variety of internal data. No evidence was available to allow confirmation of whether the attacker directly or indirectly accessed confidential client data due to inadvertent evidence destruction during the recovery efforts.

Areas of Strength

- **Backups -** Backups for major systems were readily available promptly following the attack
- **Proactive Communication -** City of Pensacola proactively communicated with the public, rather than failing to acknowledge the attack
- **Proactive Protection -** Out of an abundance of caution, the City of Pensacola chose to provide identity theft services to clients to protect them in the event of a potential damage as a result of the attack

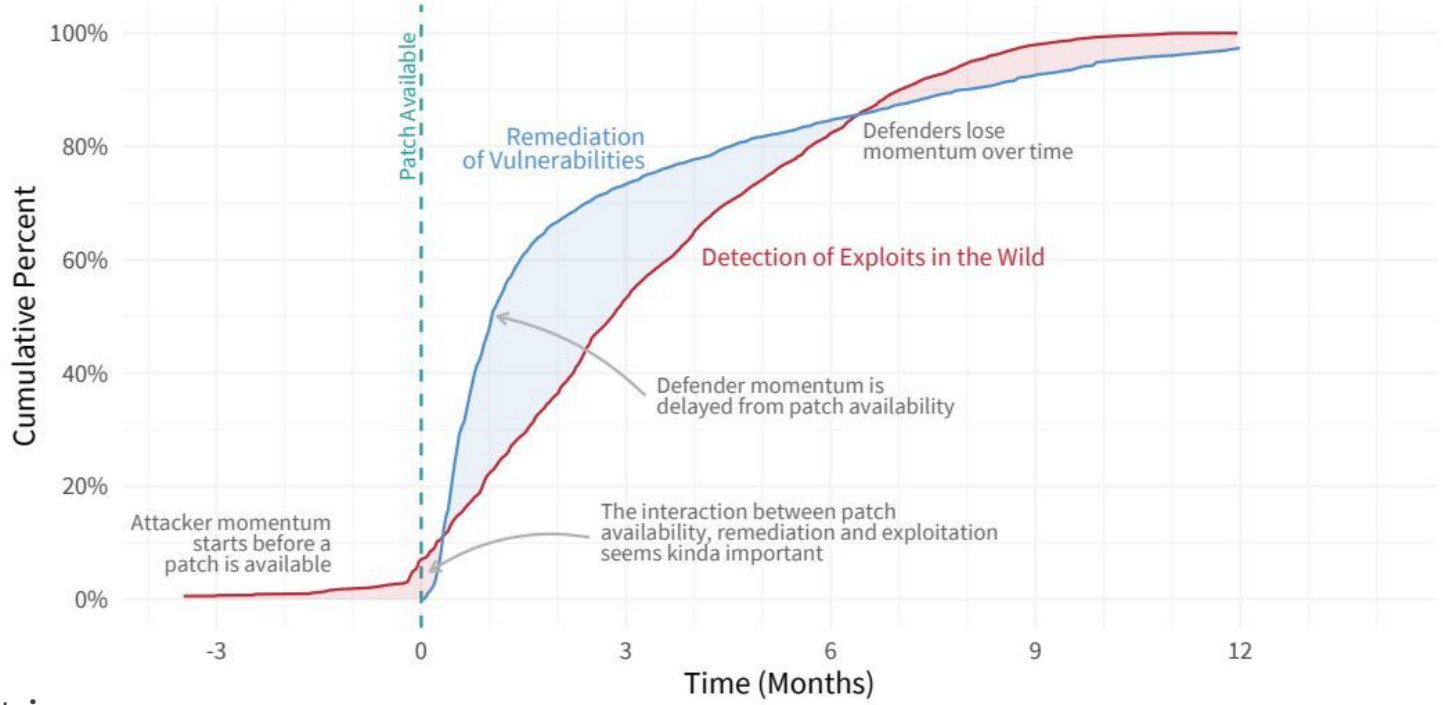
Opportunities for Improvement

- **Staffing -** Consider dedicated security staff
- **Incident Response Plan -** Consider developing a more robust Incident Response plan
- **Security Assessments -** Consider conducting regular assessments of the security posture of the City and addressing issues as they are discovered

[1] DMZ, or "Demilitarized Zone" is a separate subnet within an environment. Systems inside the DMZ are generally exposed and available to the outside world (the internet) and as a result are more at risk than standard systems. Access between the DMZ and the internal environment is restricted to mitigate the risk to the entire environment should a successful compromise of a DMZ system occur.

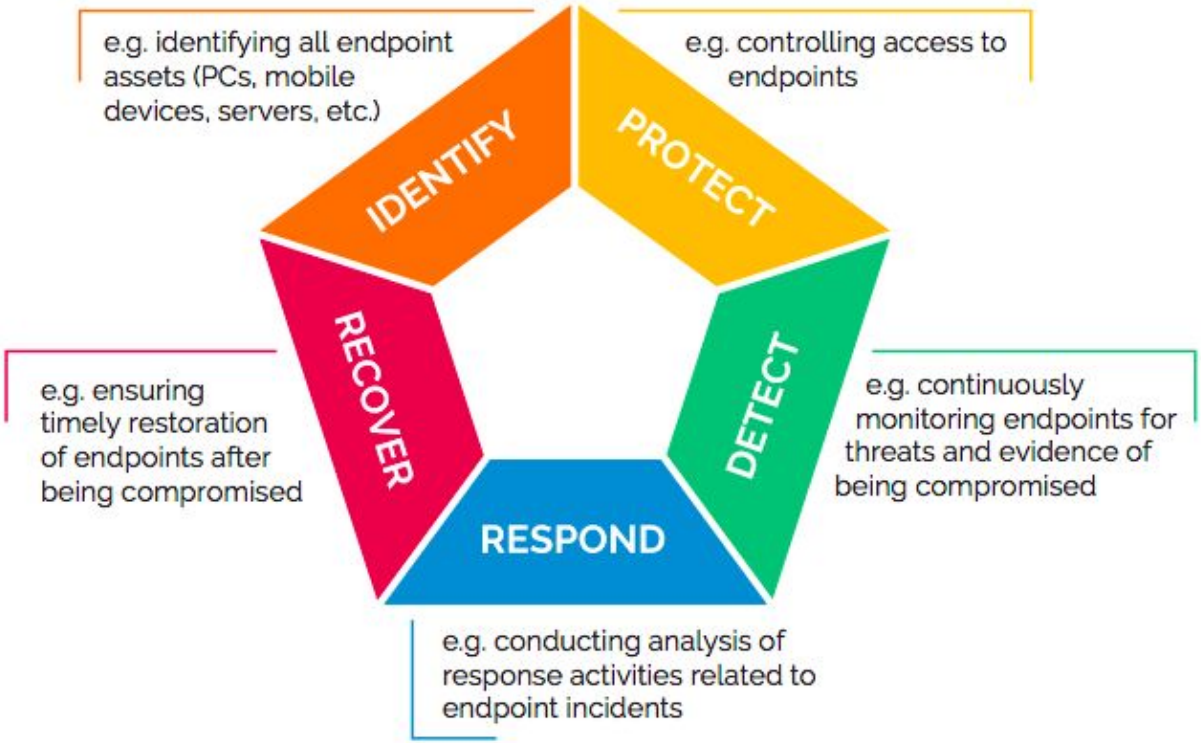
Une question de timing

Figure 20: Comparison of vulnerability remediation and exploitation timelines with momentum shifts highlighted

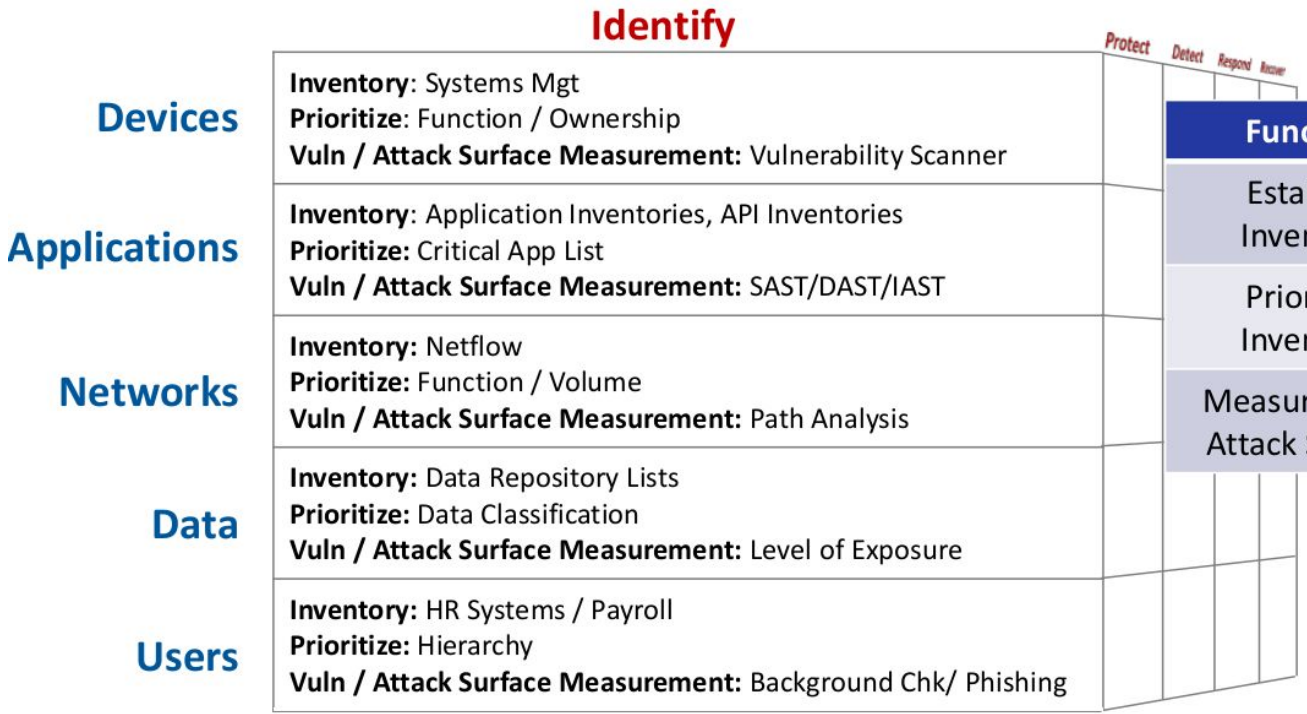


Source : cyentia

Un modèle opérationnel de défense (NIST)



Matrice RACI



Function	RACI
Establish Inventory	RA – Owner I – Security
Prioritize Inventory	R – Owner I – Security
Measure Vuln/ Attack Surface	R – Security ACI – Owner

Prise en compte des enjeux de sécurité

- EU cybersecurity act : https://www.ssi.gouv.fr/administration/reglementation/cybersecurity-act/
- Directive NIS : https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
- Pour les opérateurs d'intérêts vitaux (OIV) : https://www.ssi.gouv.fr/entreprise/protection-des-oiv/protection-des-oiv-en-france/

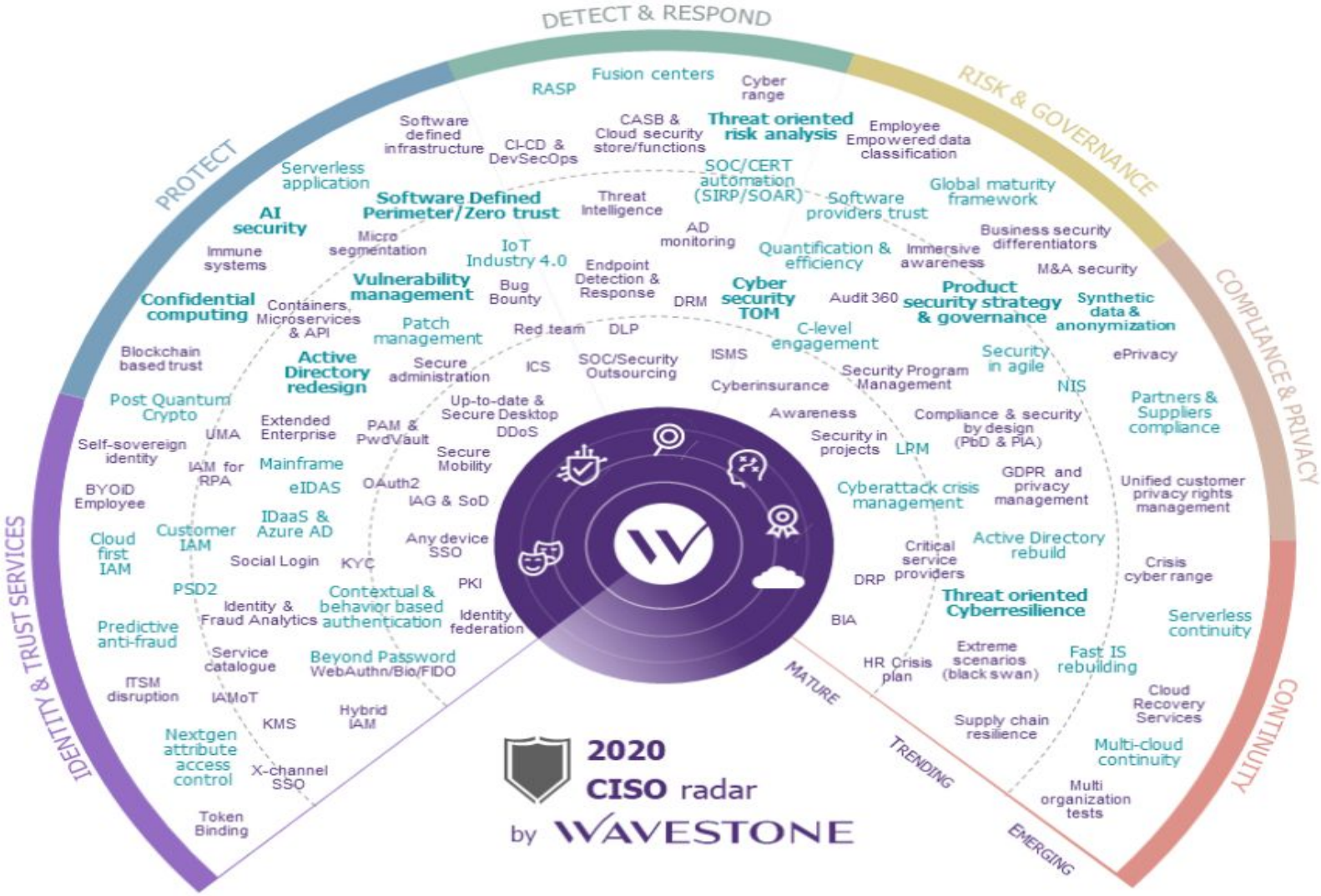
Critique : "*The move away from prescriptive standards towards a focus on outcomes under the NIS Regulations was welcomed because: standards are soon rendered out-of-date by fast-changing threats and the frequent discovery of previously unknown vulnerabilities" [so we rather should] "anticipate fast-changing threats instead of slipping into a 'tick-box compliance' with static standards.*" - Cyber Security of the UK's Critical National Infrastructure (Nov. 2018)

Conformité du SI

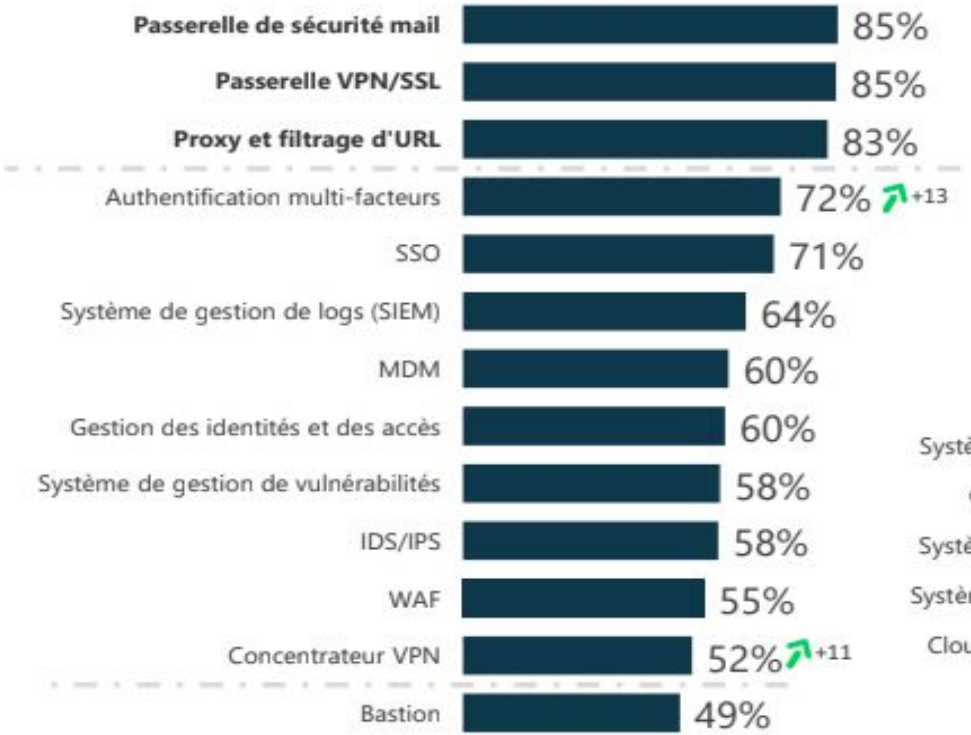
- ISO 27000 (et série)
- OWASP Top 10 / CSC Top 20 / CIS 20 / CWE Top 25
- GDPR / CCPA (Californie)
- Par type d’activité :
  - PCI DSS / GLBA (finance)
  - HDS / Hop’EN (santé)

Exemples d'outils

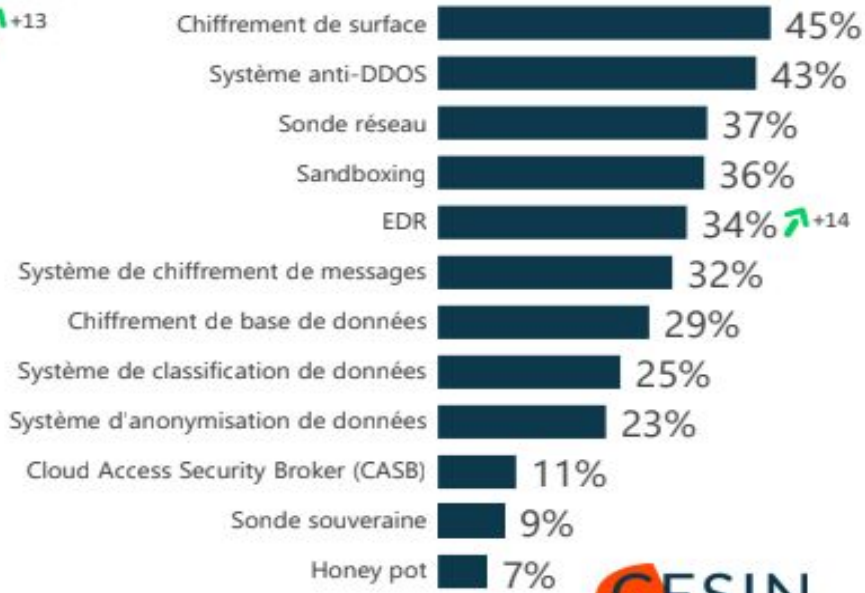
- Gestion des accès (ex: suppression automatique)
- SIEM (security and information event management)
  - Exemple : https://www.elastic.co/fr/siem, https://wazuh.com, https://punchplatform.com (thales, pas oss mais documentation intéressante)
- IDS (intrusion detection system) / IPS (intrusion prevention system)
  - Exemple : les firewalls, Deep Packet Inspection, mécanismes de rupture de protocole, etc.


DETECT & RESPOND
RISK & GOVERNANCE
COMPLIANCE & PRIVACY
CONTINUITY
IDENTITY & TRUST SERVICES
PROTECT
RASP
Fusion centers
Cyber range
Software defined infrastructure
CI-CD & DevSecOps
CASB & Cloud security store/functions
Threat oriented risk analysis
Employee Empowered data classification
Serverless application
SOC/CERT automation (SIRP/SOAR)
Global maturity framework
Software providers trust
Threat Intelligence
Software Defined Perimeter/Zero trust
AI security
Immune systems
Micro segmentation
AD monitoring
Business security differentiators
IoT Industry 4.0
Quantification & efficiency
Immersive awareness
M&A security
Endpoint Detection & Response
Vulnerability management
Bug Bounty
Cyber security TOM
Audit 360
Product security strategy & governance
Synthetic data & anonymization
Confidential computing
Containers, Microservices & API
DRM
Patch management
Red team
DLP
C-level engagement
Blockchain based trust
Active Directory redesign
Secure administration
ICS
SOC/Security Outsourcing
ISMS
Security in agile
ePrivacy
Security Program Management
Cyberinsurance
NIS
Post Quantum Crypto
Up-to-date & Secure Desktop
Awareness
Partners & Suppliers compliance
Extended Enterprise
PAM & PwdVault
DDoS
Compliance & security by design (PbD & PIA)
UMA
Self-sovereign identity
Secure Mobility
Security in projects
LRM
IAM for RPA
Mainframe
GDPR and privacy management
Unified customer privacy rights management
BYOiD Employee
eIDAS
OAuth2
IAG & SoD
Cyberattack crisis management
IDaaS & Azure AD
Customer IAM
Cloud first IAM
Any device SSO
Active Directory rebuild
Critical service providers
Social Login
KYC
DRP
Crisis cyber range
PSD2
PKI
Threat oriented Cyberresilience
Contextual & behavior based authentication
Identity & Fraud Analytics
Identity federation
BIA
Serverless continuity
Predictive anti-fraud
Service catalogue
Beyond Password
WebAuthn/Bio/FIDO
HR Crisis plan
Extreme scenarios (black swan)
Fast IS rebuilding
ITSM disruption
IAMoT
Hybrid IAM
Cloud Recovery Services
KMS
Supply chain resilience
Nextgen attribute access control
Multi-cloud continuity
X-channel SSO
Multi organization tests
Token Binding
MATURE
TRENDING
EMERGING
2020
CISO radar
by WAVESTONE

Q8. Parmi les solutions de protection suivantes, quelles sont celles qui ont été mises en place dans votre entreprise, en plus des antivirus et pare-feu ? *Base : ensemble (253 répondants) / Plusieurs réponses possibles*



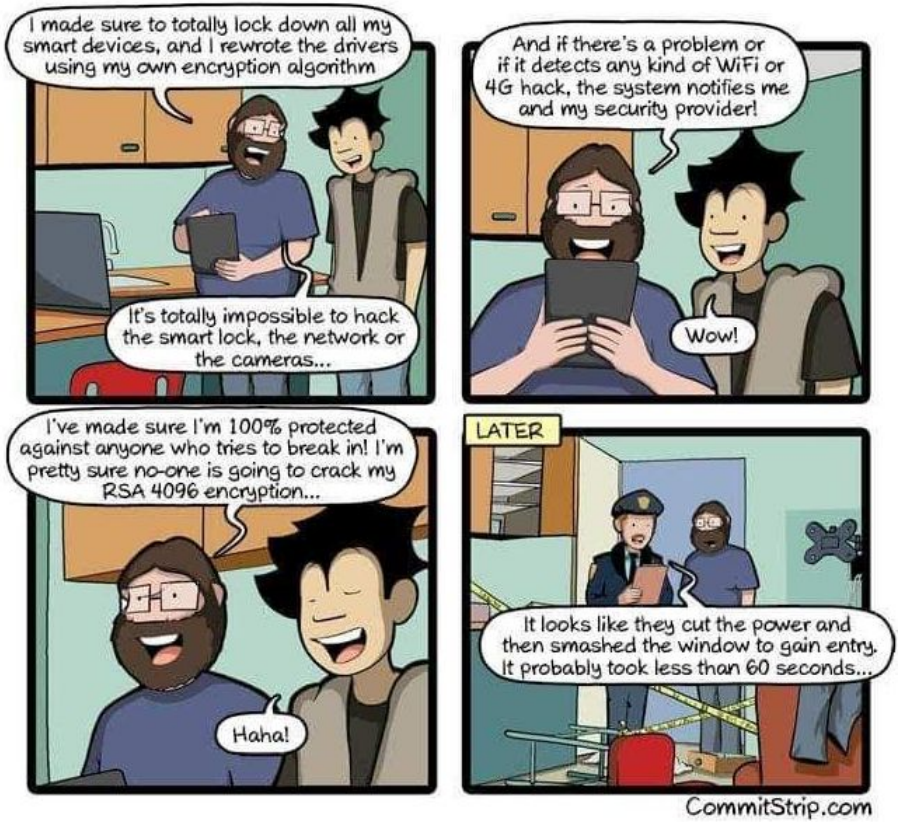
11,9 solutions en moyenne



Évolution statistiquement significative vs. 01/2019

CESIN

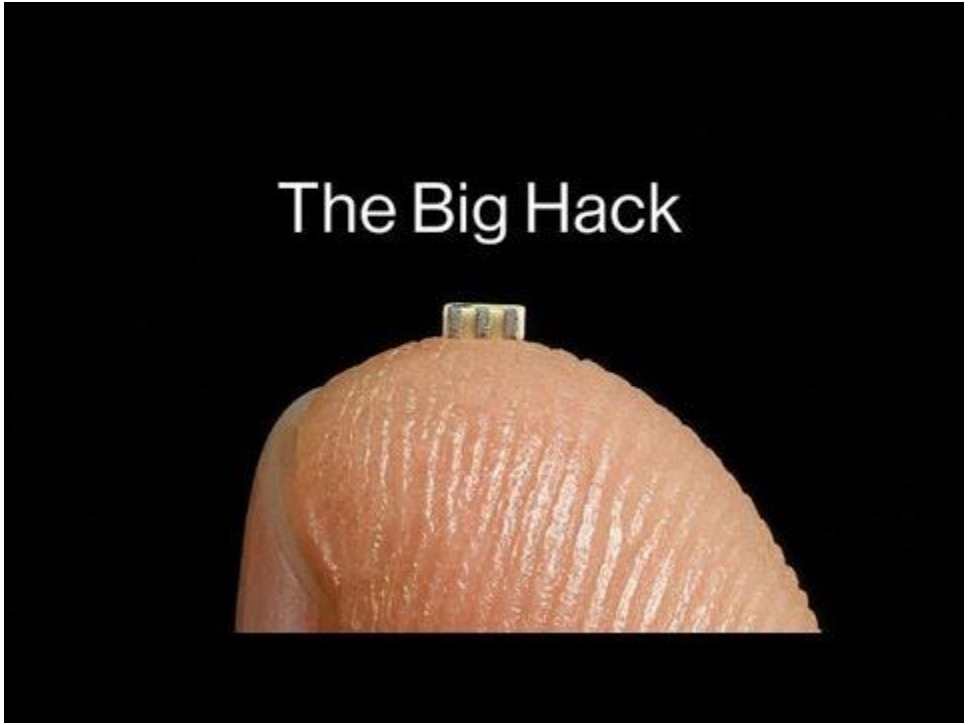
Pas seulement un enjeu logiciel



Pas seulement un enjeu logiciel

- Social engineering (lire le livre de Mitnick)
- Protection des accès physiques
  - réinitialiser son PC après une conférence (chromebook powerwash)
  - accès au datacenter
- Cryptage des disques durs (ex: vol)
- Multi-factor authentication (ex : yubikey)
- Marquage des composants électroniques
  - Exemple : https://www.securityweek.com/dust-identity-emerges-stealth-protect-device-supply-chain
- Protection hardware (TEE) :
  - Exemples : Intel SGX, https://asylo.dev/, https://keystone-enclave.org/

Hardware

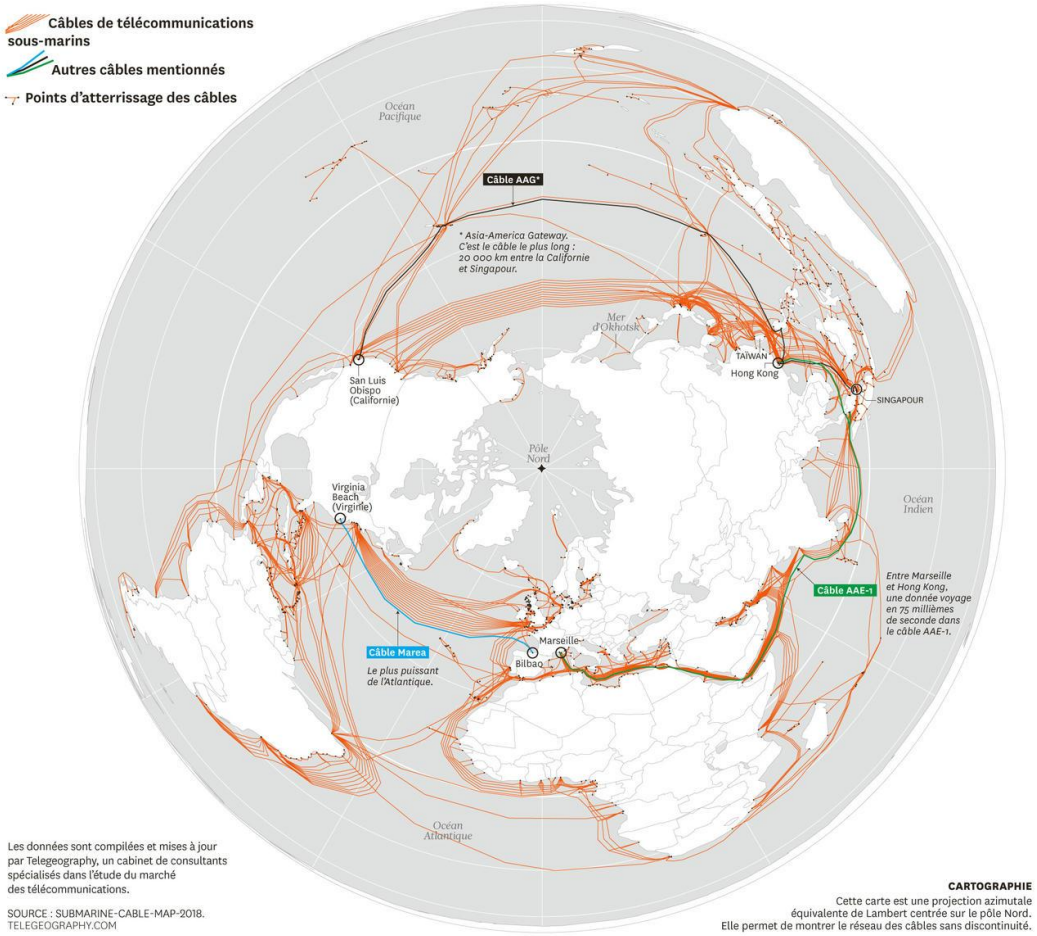


https://www.youtube.com/watch?v=ZQpI22MtTlQ

Fibre optique

Des espions russes s'intéressent de près aux câbles sous-marins d'internet

https://www.thetimes.co.uk/article/russian-agents-plunge-to-new-ocean-depths-in-ireland-to-crack-transatlantic-cables-fnqsmgncz



Carte interactive :
https://www.submarinecablemap.com

Data = new oil ?

- Utile pour le deep learning
- Certaines données nécessitent une attention particulière
  - Régulation PCI (Payment Card Industry Data Security Standard)
  - https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security
- Data = new CO2 ?
  - https://luminategroup.com/posts/blog/data-isnt-the-new-oil-its-the-new-co2

Le cryptage des données, un enjeu politique

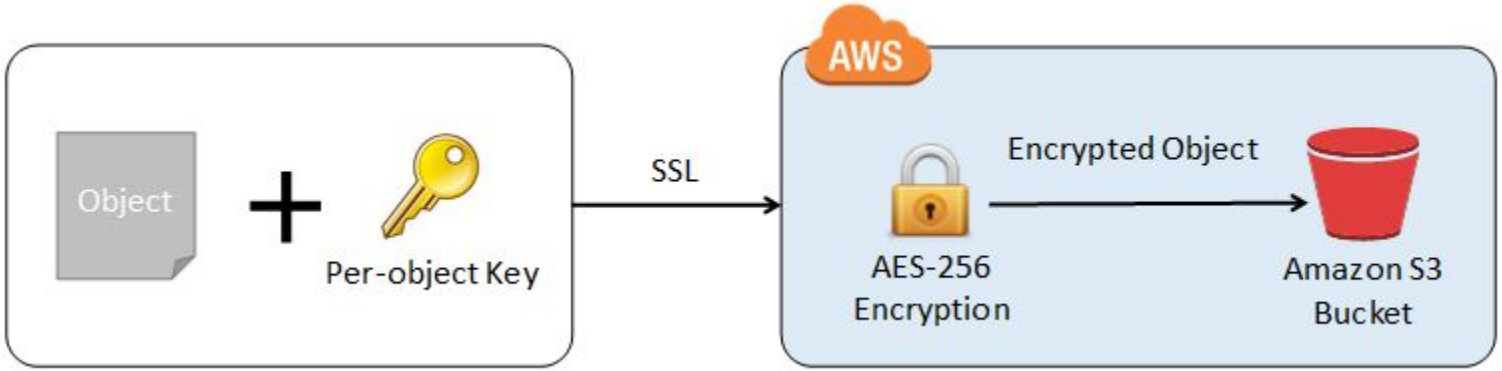
TECHNOLOGY NEWS JANUARY 21, 2020 / 1:07 PM / 8 DAYS AGO

Exclusive: Apple dropped plan for encrypting backups after FBI complained

https://www.reuters.com/article/us-apple-fbi-icloud-exclusive/exclusive-apple-dropped-plan-for-encrypting-backups-after-fbi-complained-sources-idUSKBN1ZK1CT

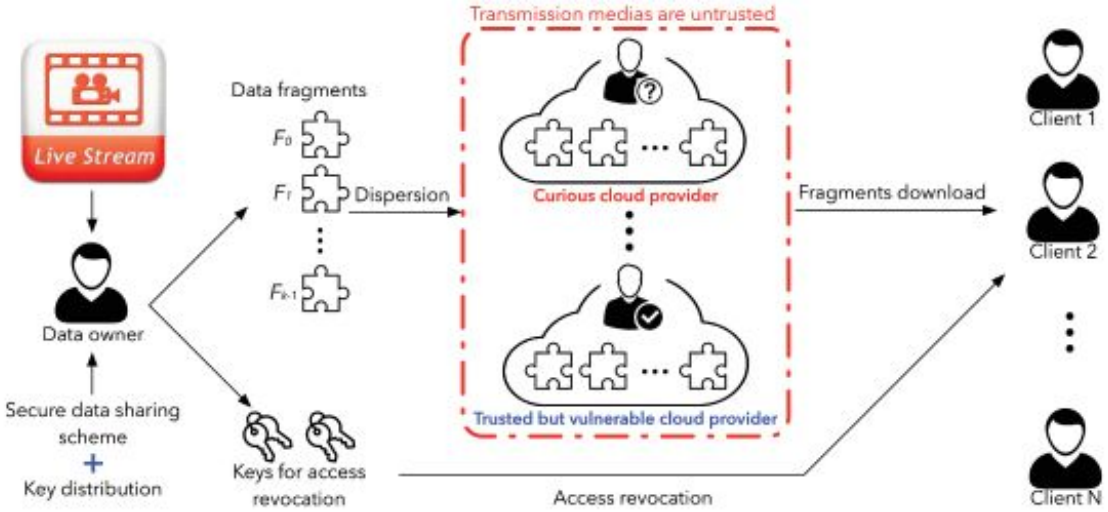
Protéger ses données dans le cloud public (minimum)

- Utiliser un gestion de clés (ex : AWS KMS ou https://github.com/google/tink/blob/master/docs/KEY-MANAGEMENT.md)
- Encryption at rest
- End to end encryption

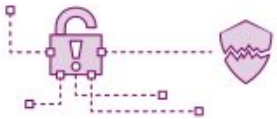


Protéger ses données dans le cloud public (avancé)

- Password vault séparé (ex https://www.vaultproject.io)
- Fragmentation (ex: https://www.parsec.cloud)

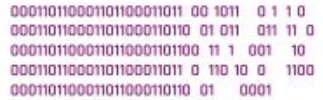


Cryptographie



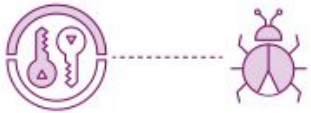
COMPROMISE OR BREACH OF ROOT

When a Root of Trust (RoT) is compromised, all trust is lost. In the case of a Certificate Authority (CA) issuing certificates, a breach renders all of your public and private keypairs moot, or even dangerous, as they can be issued and used maliciously. The immediate replacement of that RoT is required, along with the updating of all certificates and keys used by devices.



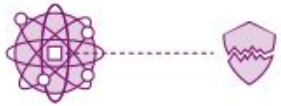
ALGORITHM DEPRECATION

Discovery of weaknesses and flaws in cryptographic algorithms — like SHA-1 and MD5 — routinely challenge security teams' ability to adapt and respond effectively. Any keys using the affected algorithm are rendered insecure or untrusted. Similar to a compromised RoT, a complete replacement is required.



CRYPTO LIBRARY BUG

Discovery of a bug in crypto libraries may result in the need to generate new keys and re-issue certificates according to the technology used in patching or replacing it. A TPM flaw, known as ROCA[1], left millions of devices vulnerable, requiring end users to install firmware updates and replace of weak encryption keys.



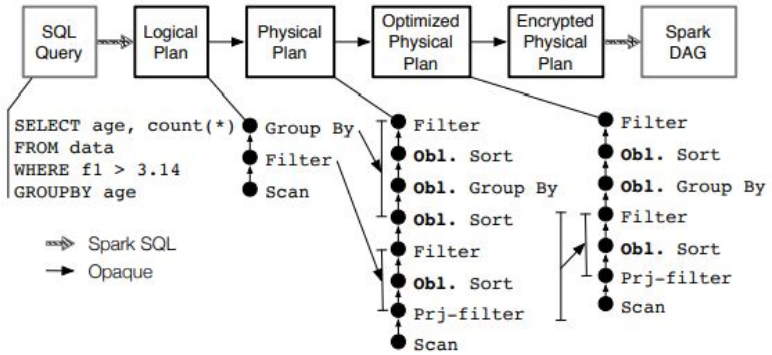
QUANTUM COMPUTING

NIST predicts[2] that large-scale quantum computing will break public key cryptography in use today. This leap forward will disrupt key components of cryptography, as we know it, forcing organizations to pivot to new strategies, cryptographic standards and technologies.

Source : KeyFactor

Confidential computing (complexe)

- Techniques d’anonymisation
  - https://en.wikipedia.org/wiki/K-anonymity et variantes
- Homomorphic encryption
- Trusted execution environment (TEE)



https://people.eecs.berkeley.edu/~wzheng/opaque.pdf

Machine learning

The use of AI in hacking. One submission mentions the threat from deep fakes. Interestingly, 2019 saw a **the first documented fraud case** in the UK where an AI programme mimicked the voice of a CEO to successfully convince a senior manager of a subsidiary to transfer EUR 200k[5]

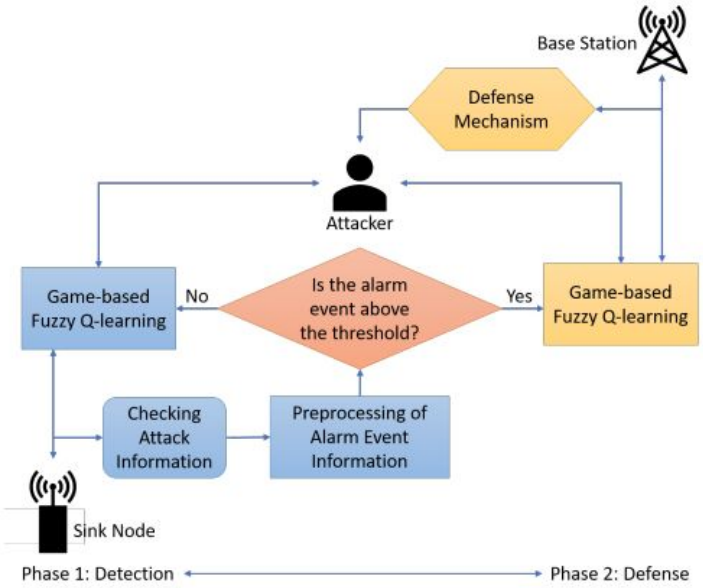
https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

Machine learning

- Les attaquants peuvent créer des leurres
- La protection avec des signatures fixes ne fonctionnera plus

Voir le rapport de CMU

https://resources.sei.cmu.edu/asset_files/TechnicalReport/2019_005_001_633597.pdf



Exercice : gestion des clés (30 min)

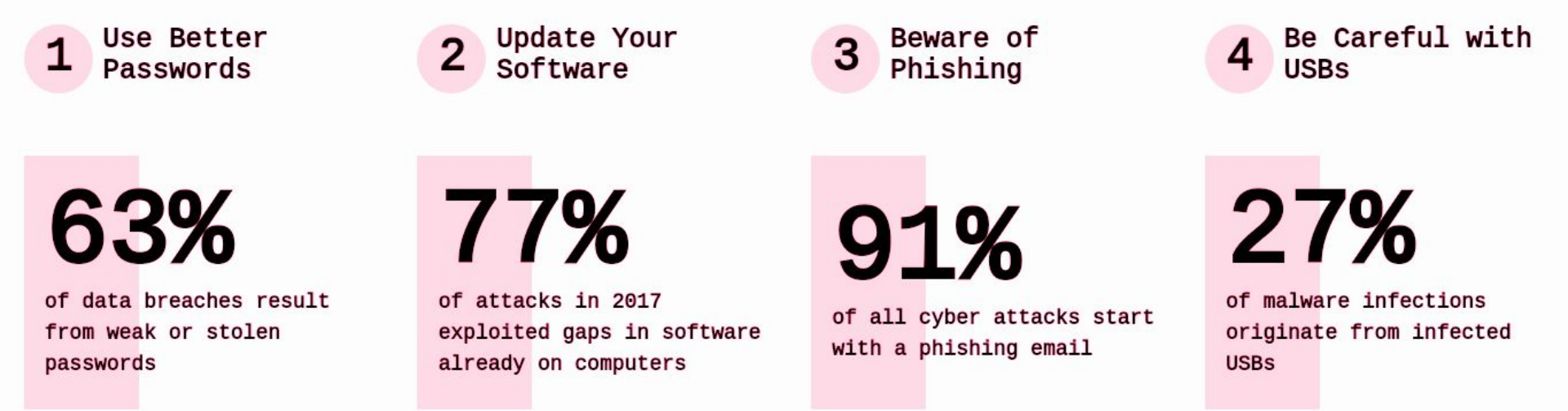
---

https://github.com/we45/AWS-KMS-Tour

en adaptant si besoin le script, ex : région AWS

nécessite un accès à AWS (https://aws.amazon.com/fr/niveau-gratuit)

Hygiène informatique minimale



Source : https://www.cyberreadinessinstitute.org/cyber-readiness-starter-kit

Compléter avec https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

Exemple sidérant (et courant)

- dé-commissioner ce qui n'est plus supporté

Le service informatique du GHT a réagi le jour-même: "on arrête les PC, on les débranche du réseau et on passe l'antivirus. Le rançongiciel Emotet a bien été détecté, les PC ont été nettoyés mais dès qu'on les rebranche sur le réseau, le virus revient et recommence à se propager", a poursuivi Jalal Soujad.

Le virus contenait une demande de rançon de 8.000 euros par poste infecté, ont précisé les dirigeants hospitaliers à TICsanté.

Face à la menace, le CH a alerté l'ARS et demandé l'aide de l'Agence du numérique en santé (ANS, ex-Asip santé) et de l'Agence nationale de sécurité des systèmes d'information (Anssi). L'Anssi lui a apporté "un soutien méthodique, presque journalier, par téléphone".

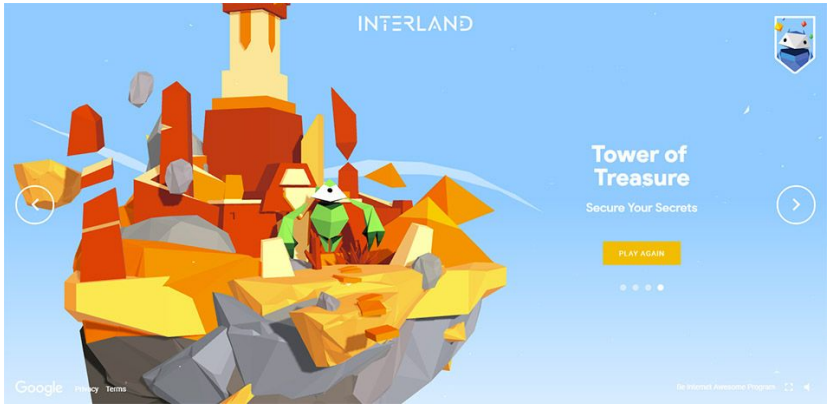
Parallèlement, le CH a fait appel à trois prestataires: Palo Alto, Orange cyberdéfense et Sophos.

Le 28 octobre 2019, "l'Anssi et les prestataires nous disent que c'est trop tard", a relaté Jalal Soujad. "Ils nous expliquent qu'il faut tout formater car le virus s'est propagé dans tout le SI et que les machines sont obsolètes. Elles tournaient sous Windows XP." Il n'y a plus d'antivirus qui permette un nettoyage car ce système d'exploitation est trop vieux, a-t-il indiqué.

https://www.ticsante.com/story/4985/le-centre-hospitalier-de-la-bassee-(nord)-perturbe-par-un-rancongiciel.html

Rester simple (et rappeler souvent)

- Possible d'expliquer la sécurité numérique à des enfants
  - Interland : https://beinternetawesome.withgoogle.com/en_us/interland
  - https://www.securitytuesday.com/wp-content/uploads/2018/10/ISSA.Cahier.SecNum777.pdf
  - 1-2-3 cyber https://github.com/wavestone-cdt/1-2-3-Cyber
- Formation pour les adultes : https://www.secnumacademie.gouv.fr



Faire comprendre la menace

Threat	Ex-girlfriend/boyfriend breaking into your email account and publicly releasing your correspondence with the My Little Pony fan club	Organized criminals breaking into your email account and sending spam using your identity	The Mossad doing Mossad things with your email account
Solution	Strong passwords	Strong passwords + common sense (don't click on unsolicited herbal Viagra ads that result in keyloggers and sorrow)	◆ Magical amulets? ◆ Fake your own death, move into a submarine? ◆ YOU'RE STILL GONNA BE MOSSAD'ED UPON

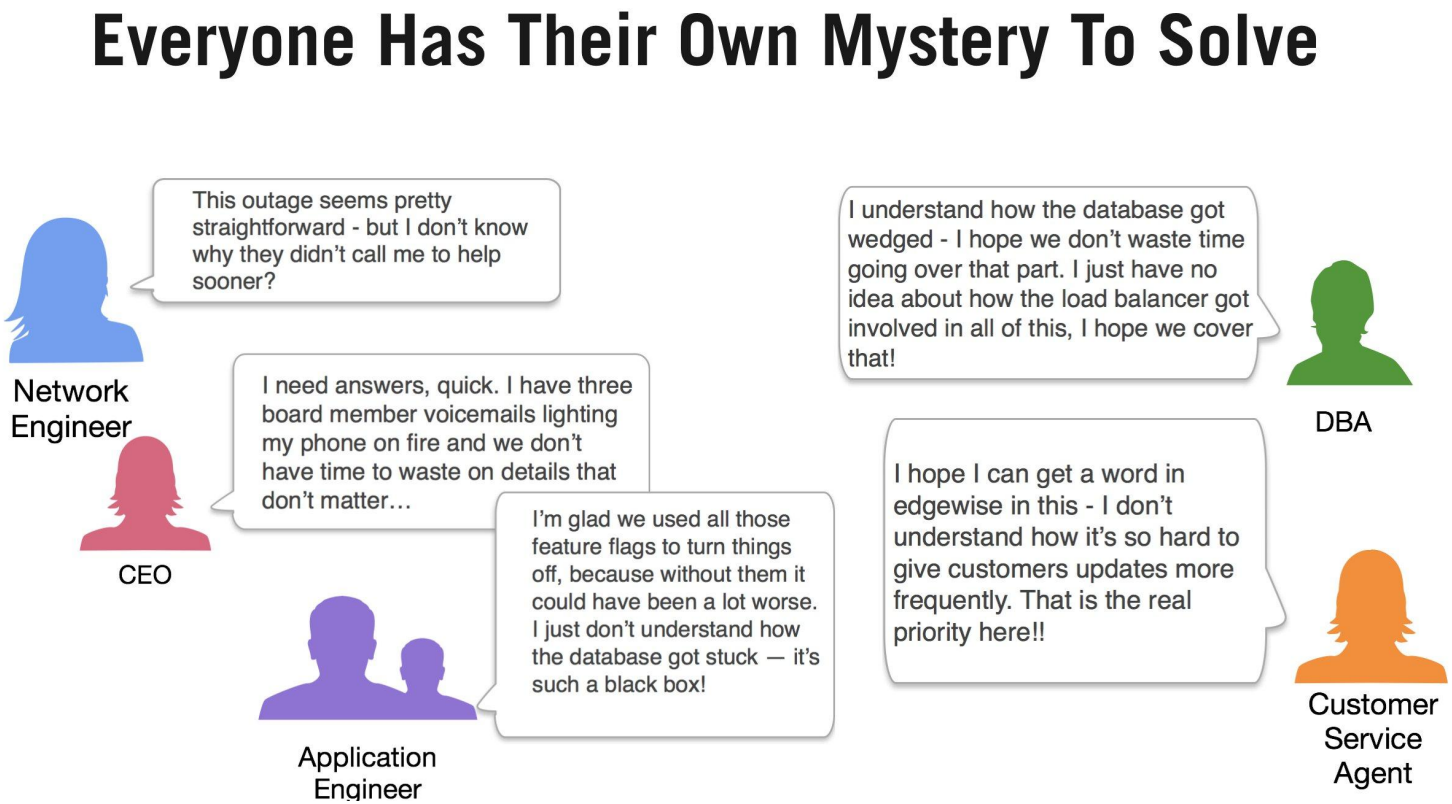
Figure 1: Threat models

https://www.usenix.org/system/files/1401_08-12_mickens.pdf

Exemple de concepts simples mais à rappeler souvent

Auth = AuthN + AuthZ

Gestion d'incident : importance de la communication



Former les décideurs

- Enjeux :
  - continuité d'activité
  - protection des données (interne et clients)
  - rendre la difficulté de l'attaque plus importante que le gain espéré
- La communication est très importante en infosec
- Eviter le jargon

  https://www.rsa.com/content/dam/en/analyst-report/gartner-how-to-talk-digital-risk-to-the-board.pdf
- Comprendre la notion de risque
- Mettre en place une stratégie de gestion des incidents

  https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents

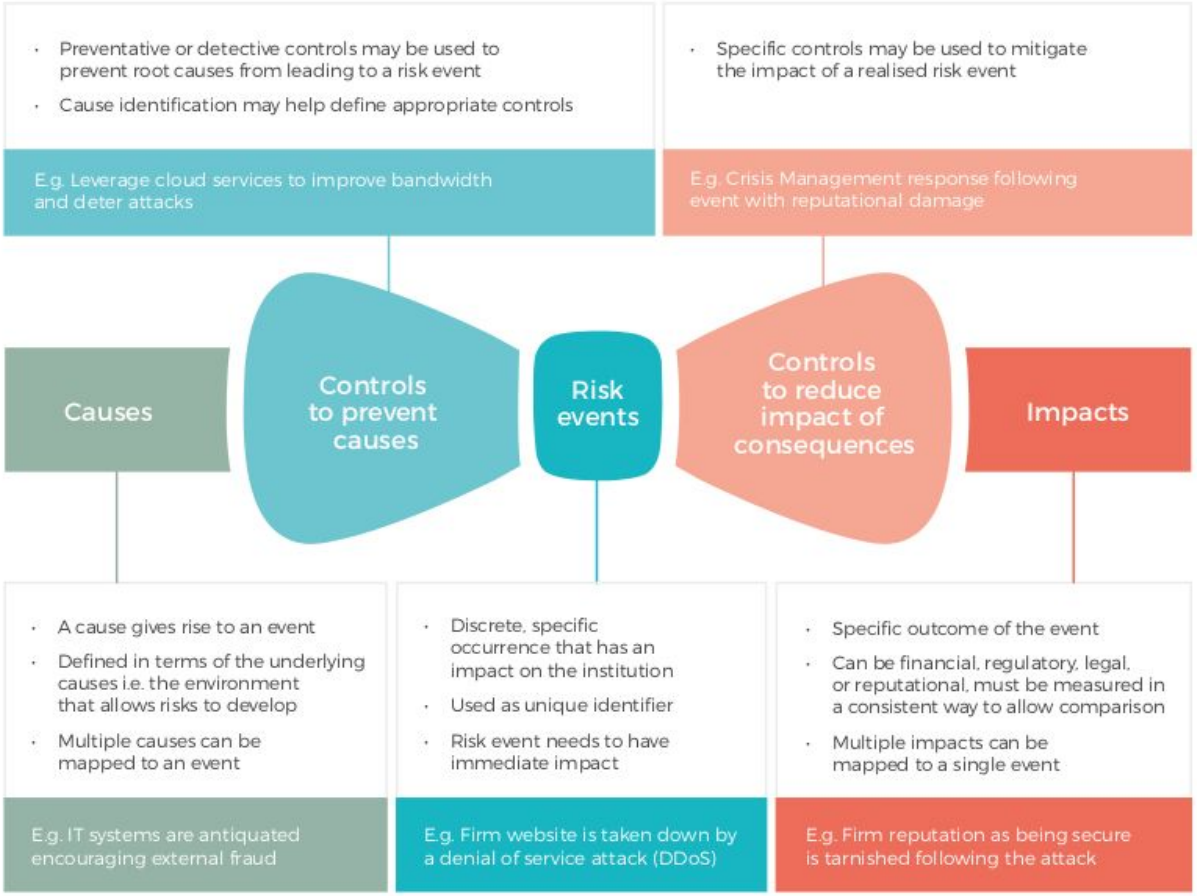
Notion de risque

Source : ORX

Reference taxonomy

Figure 1. Bow Tie Method

The "bow tie" method is used to ensure that only such events are captured by the taxonomy which plausibly lead to a direct impact.



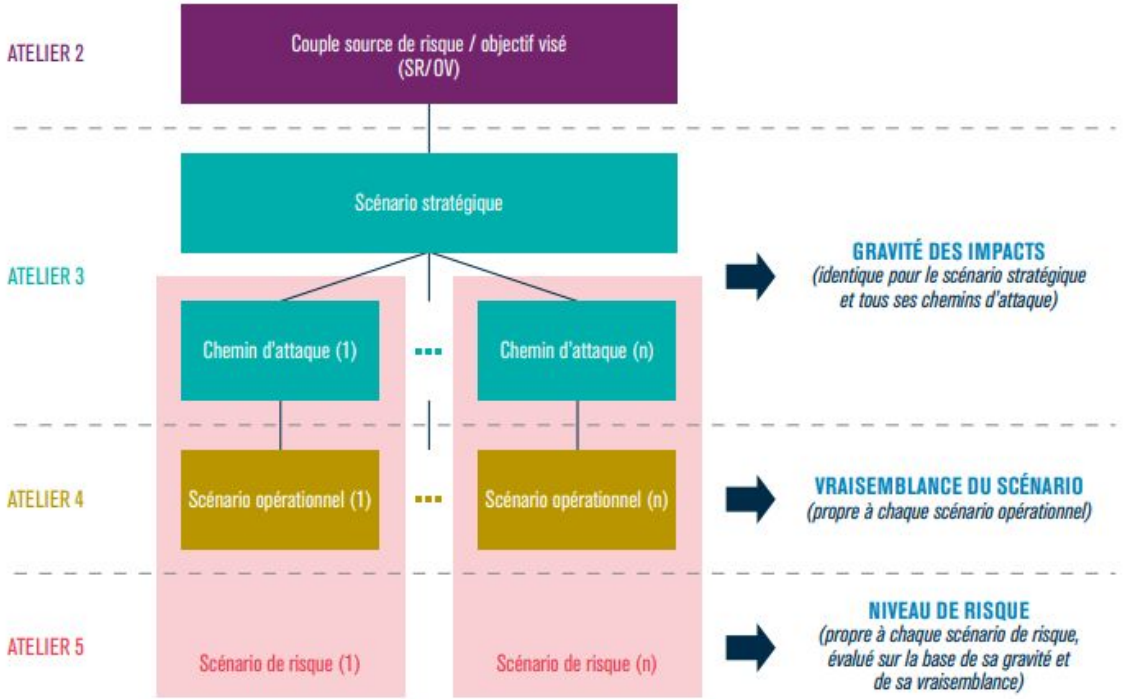
Niveau de risque

Table 1 – The most critical risks for a company
(1 being the most critical hazard in the respective year)

Risk	2013	2014	2015	2016	2017	2018	2019
Business interruption	1	1	1	1	1	1	1
Cyber risks		8	5	3	3	2	2
Natural catastrophes	2	2	2	4	4	3	3
Market trend	8	5	7	2	2	4	5
Regulation	4	4	4	5	5	5	4
Fire/Explosion	3	3	3	8	7	6	6
New technologies					10	7	7
Reputation/ market value	10	6	6	7	9	8	9
Political risks			9	9	8	9	11
Macroeconomics				6	6	0	13
Climate change/ weather fluctuations						10	8
Shortage of skilled workforce							10

Source: Allianz Risk Barometer, Allianz Global Corporate & Speciality SE, 2018 and earlier

EBIOS risk manager



https://www.ssi.gouv.fr/uploads/2018/10/guide-methode-ebios-risk-manager.pdf

Threat modeling / NO DIRT

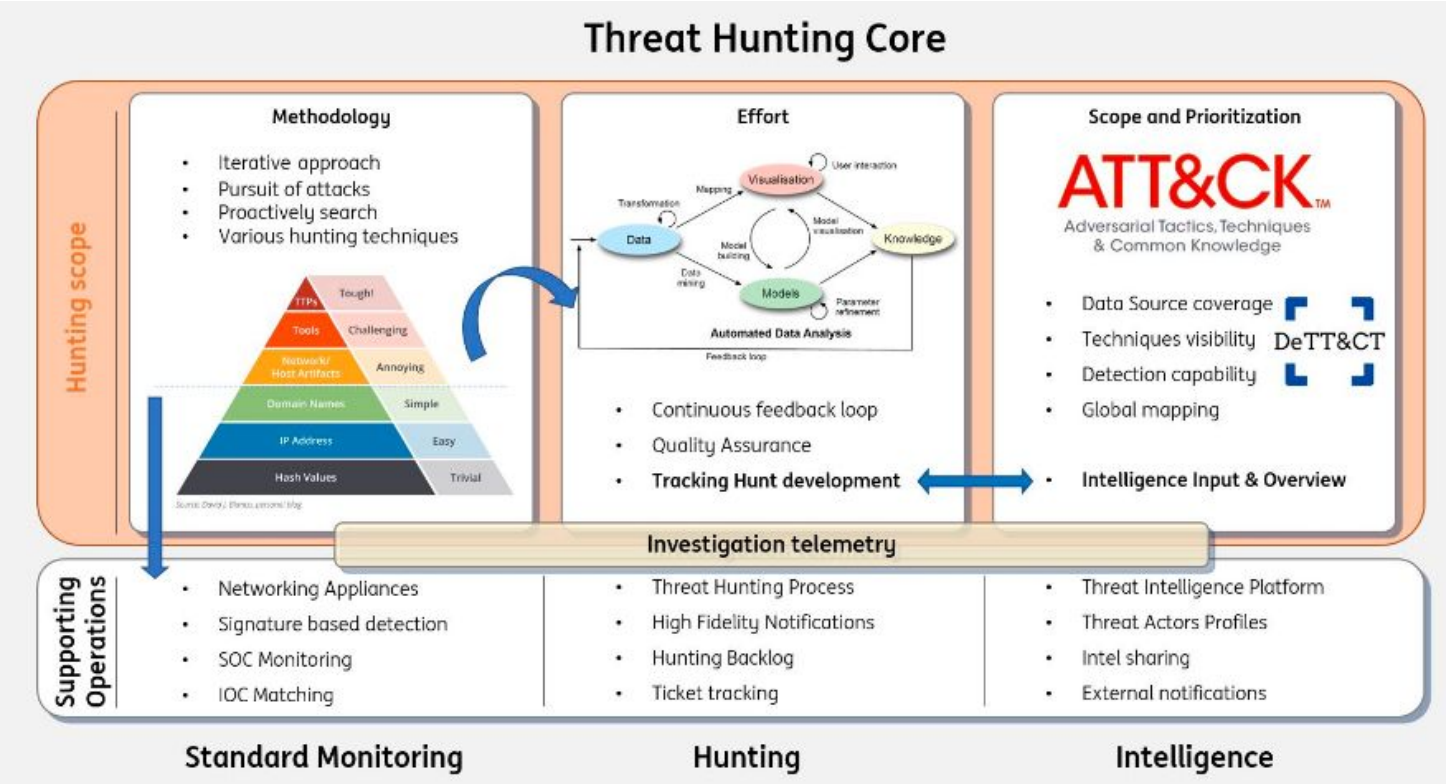
“privacy and security are often viewed in conflict, but in a wellrun program, these conflicts are resolved through collaboration and judgement.”

D’autres modèles existent, ex: STRIDE

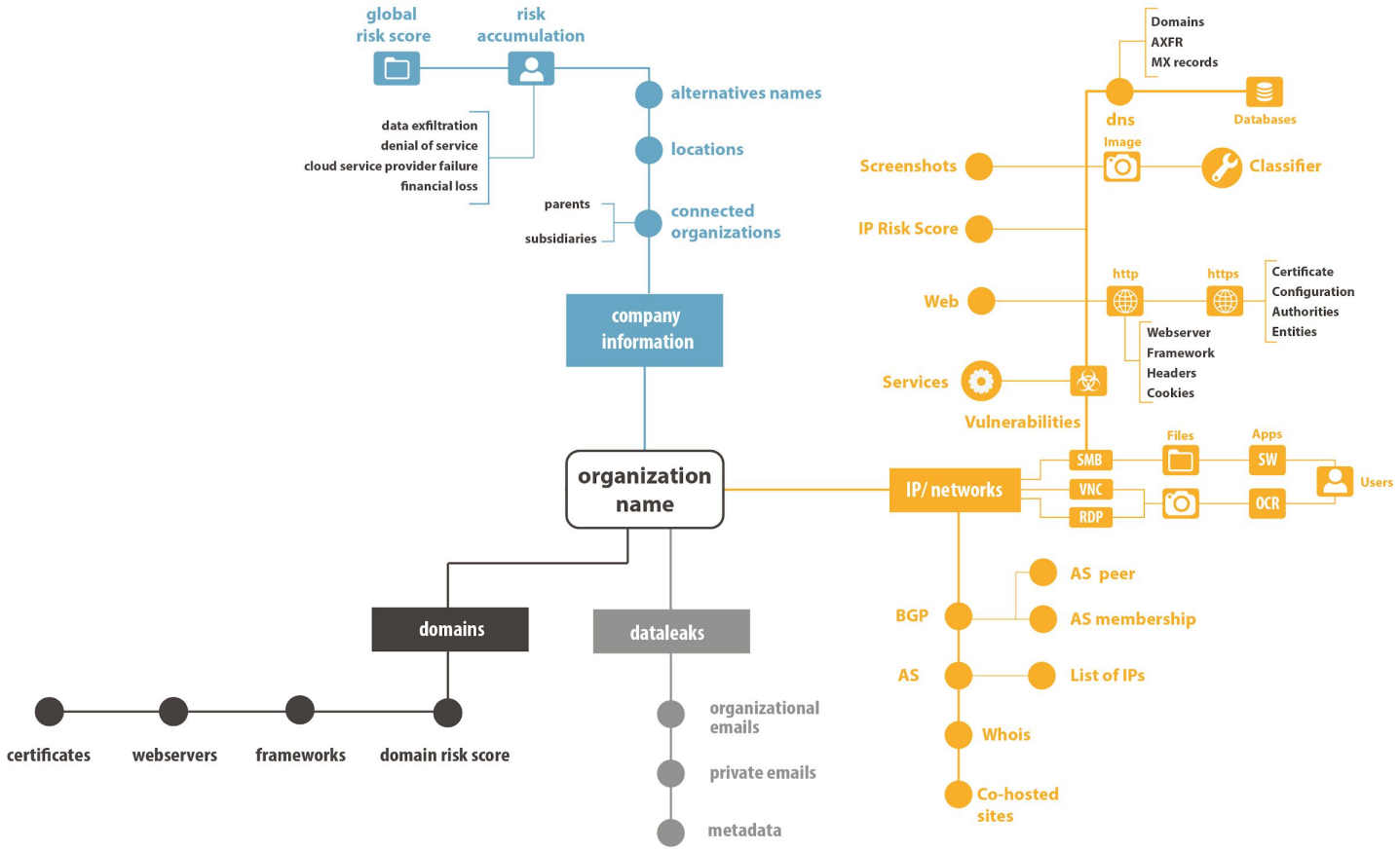
	RISK	PROPERTY/GOAL	REALM
I	IDENTIFIABILITY	Anonymity	Privacy
N	NON-REPUDIATION	Plausible Deniability	Privacy
C	CLINICAL ERROR	Correct Application of Clinical Standards	Compliance
L	LINKABILITY	Unlinkability	Privacy
U	UNLICENSED ACTIVITY	Proper Credentials or Licensure	Compliance
D	DENIAL OF SERVICE	Availability	Security
E	ELEVATION OF PRIVILEGE	Authorization	Security
S	SPOOFING	Authentication	Security
N	NON-COMPLIANT TO POLICY OR OBLIGATIONS	Policy or Contractual Adherence	Compliance
O	OVERUSE	Minimum Necessary	Compliance
D	DATA ERROR	Integrity	Security
I	INFORMATION DISCLOSURE	Confidentiality	Security
R	REPUDIATION	Non-Repudiation	Security
T	TAMPERING	Integrity	Security

https://www.omadahealth.com/hubfs/nodirt.pdf

Threat hunting



Cybermap


global risk score
risk accumulation
alternatives names
locations
connected organizations
data exfiltration
denial of service
cloud service provider failure
financial loss
parents
subsidiaries
company information
organization name
domains
dataleaks
certificates
webservers
frameworks
domain risk score
organizational emails
private emails
metadata
Domains
AXFR
MX records
dns
Databases
Image
Screenshots
Classifier
IP Risk Score
Web
http
https
Certificate
Configuration
Authorities
Entities
Webserver
Framework
Headers
Cookies
Services
Vulnerabilities
Files
Apps
SMB
SW
IP/ networks
VNC
OCR
Users
RDP
AS peer
BGP
AS membership
AS
List of IPs
Whois
Co-hosted sites

Former les utilisateurs

- User focused security :
  - https://blog.kolide.com/ufs-spotlight-jesse-kriss-of-netflix-b5c22923f53e
  - https://osquery.io/ (pour les endpoints)
- Passwords :
  - gestionnaire de mots de passe + multi-factor authentication
  - on commence à voir des solutions sans mots de passe (ex: https://webauthn.io) mais est-ce que cela se diffusera ?
- Confidentialité
  - Expliquer l'importance de la confidentialité
  - Filtre de confidentialité (dans les transports)
- Phishing
  - faire des tests avec https://getgophish.com (avec l'accord de l'entreprise, sinon c'est illégal)

Vocabulaire

Spear phishing

Spear phishing is an increasingly popular attack technique and is essentially a highly targeted phishing email.[26] Attackers will aim to establish credibility and trust and will have a specific outcome in mind, such as getting the target to trigger a malware link or enter credentials. The spear phishing exchanges will often include elements of informational power or referent power to persuade the target that their requests are legitimate and will try to exploit cognitive biases related to emotion, such as the affect heuristic.

Whaling

Whaling is a type of phishing email targeting a single high-value target, typically senior executives or those with privileged access. Attackers will typically play the 'long game', using methods of social power over a long period of time, often using expert power to establish credibility, attempting to trigger herd behaviour or using coercive power in the form of blackmail in return for privileged information.

Baiting

Baiting is in many ways similar to phishing attacks. However, what distinguishes baiting from other types of social engineering is the promise of an item that hackers use to entice targets. Baiters may offer users free music or movie downloads if they surrender their login credentials to a certain site. This type of attack uses reward power to draw targets in, before triggering the affect heuristic.

Tailgating

Tailgating is a more opportunistic form of attack, also known as 'piggybacking'. These types of attacks involve someone who lacks the proper authentication following an employee into a restricted area. Attackers can also leverage legitimate power to persuade the target to let them into restricted areas, wearing official uniforms or creating branded logos and fake passes. The availability heuristic tends to be triggered during tailgating as targets make a judgement on the likelihood of the attacker causing a security incident.

Smishing

Smishing is social engineering via text message,[27] and will likely become more popular as users have become more aware of traditional email-based phishing attacks, but less aware of text message attacks.[28] Usage of mobile phones has increased exponentially worldwide, providing another means for attackers to use coercive power or reward power, potentially triggering optimism bias. Smishing attacks are currently less common and targets are unlikely to perceive this type of attack technique as a real threat.

Vishing

Vishing is social engineering using voice, and increased 350% between 2014 and 2018.[29] Attackers can apply any number of social power techniques using their voices to build rapport and trust instead of using email or text message, triggering the affect heuristic or bounded rationality biases, through the intimacy of a direct phone call. As the capabilities of artificial intelligence grow more complex, AI chatbots will become increasingly believable.[30] This means that artificially intelligent vishing attacks are likely to be on the horizon.

Ca peut arriver à tout le monde

How a college student tricked 17k coders into running his sketchy script

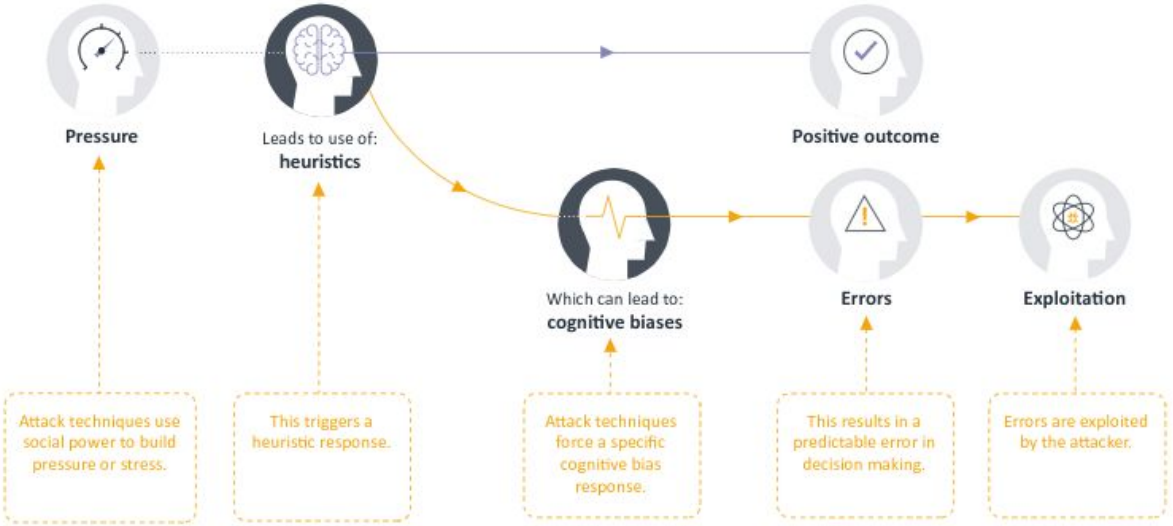
Infecting military and government software engineers is easier than you may think.

DAN GOODIN - 6/14/2016, 4:10 PM

Aspects humains de la cyber

"The whole idea is why invest hundreds of thousands of dollars to build your own malware when you can just convince someone to do something stupid?" [18] – Adam Meyers, Crowdstrike

Figure 5: The subconscious decision-making process and how attackers can influence and exploit it



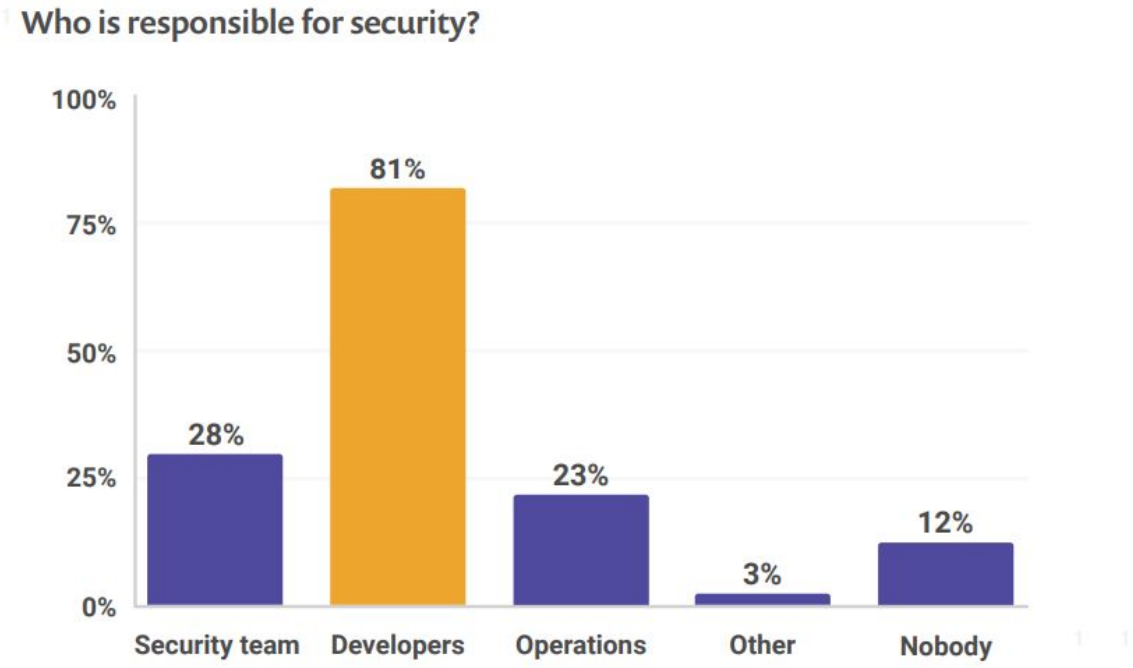
Source : ISF

Démarche DevSecOps

`Ratio DEV:OPS:SEC = 100:10:1`

Avant	Après
La sécurité s'occupe de sécurité	Tout le monde s'occupe de sécurité, vision orientée métier
Revue manuelle basée sur des checklists uniquement	Collaboratif, "trust but verify"
Peu d'instrumentation	Collection de métriques, de logs et corrélation avec la threat intel
Vérifications de sécurité juste avant la mise en production	Security by design, déploiement continu (quand c'est possible)

Qui est responsable de la sécurité ?



https://snyk.io/blog/devsecops-insights-2020/

Architecture (ex)

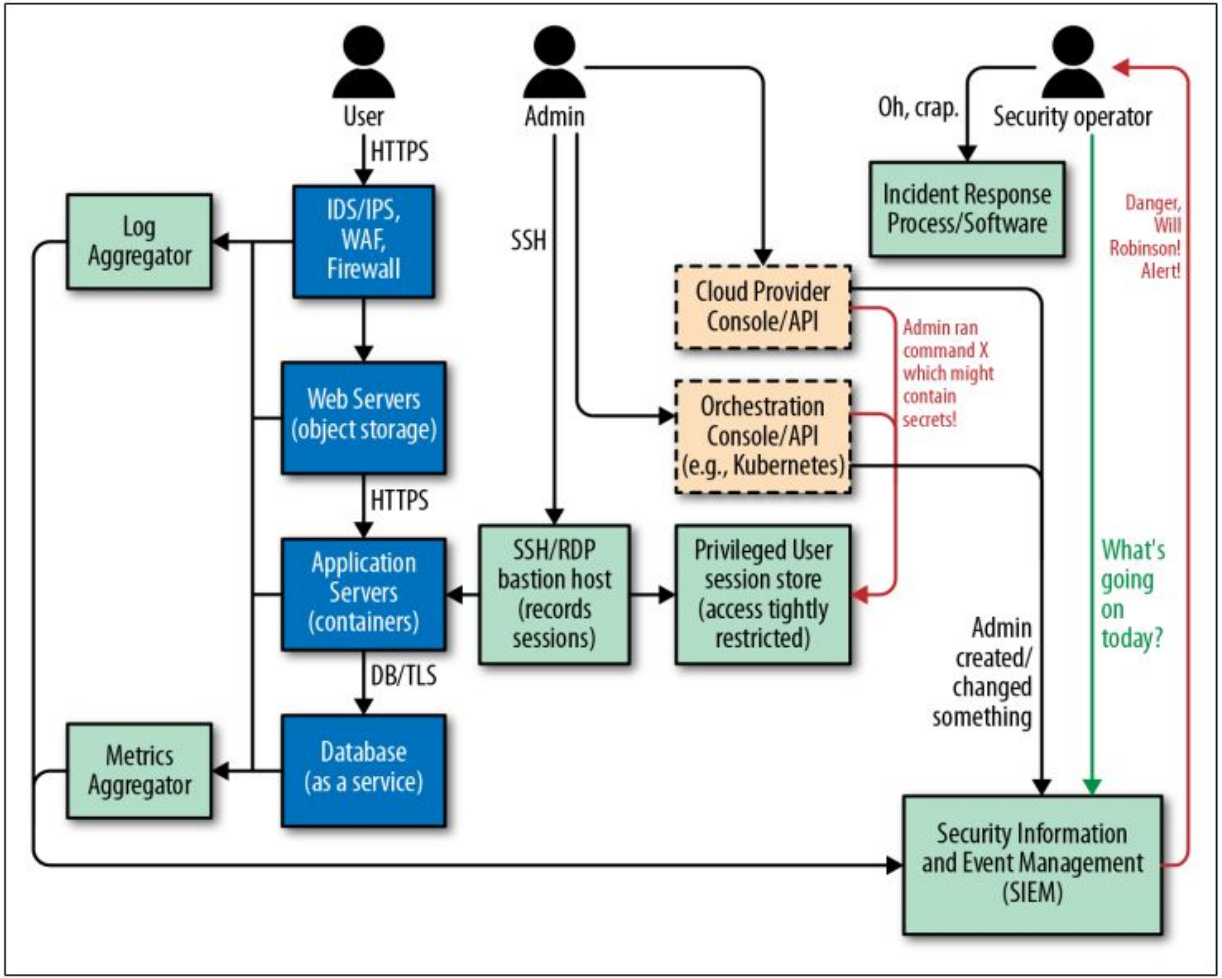
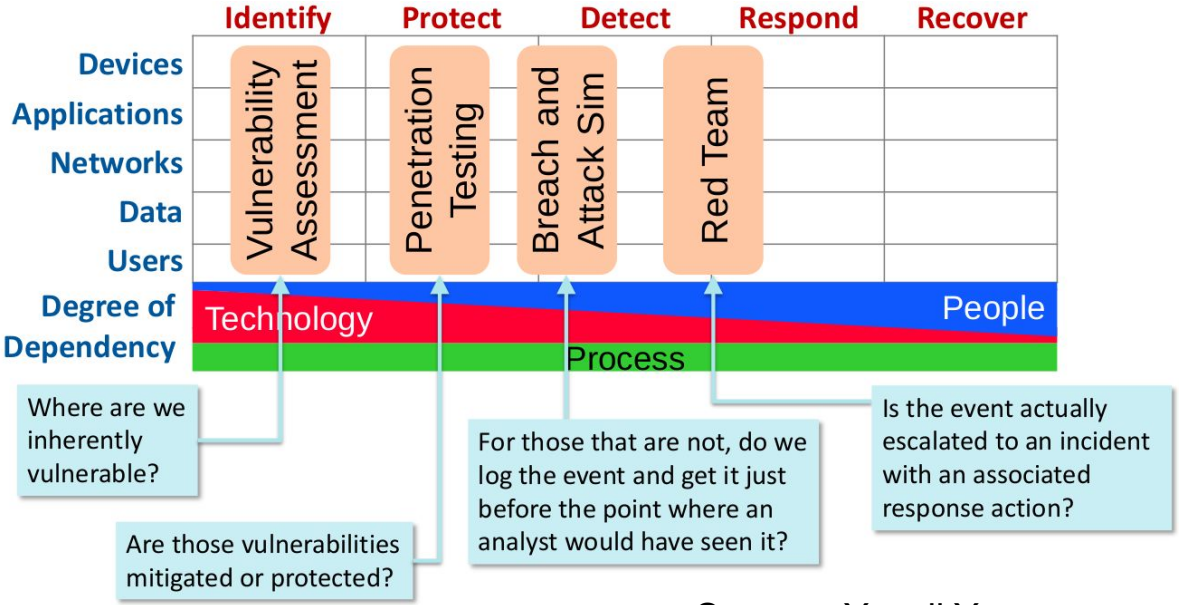


Figure 3-2. Sample application with detection capabilities

Source : Practical Cloud Security, p72

Nouveaux métiers : des opportunités

Voir les métiers de la SSI (ANSSI)



Source : Younil Yu

Ce que vous avez appris

- La cyber sécurité est un domaine vaste et complexe
- C’est l’affaire de tous
- Vous serez victime d’une attaque un jour ou l’autre ; il est possible de limiter les risques et de s’assurer qu’on survivra

Pour la suite, on se concentre sur un sous-domaine : la sécurité applicative (à l’usage de devs).