FRANSEC
SECURING **FRANCE** FROM CYBER THREATS

ETUDE DE CAS

COMMENT SE PRÉPARER À UNE BRÈCHE : RÉUSSIR À MINIMISER LES RISQUES

Thomas Billaut, *Head of Cyber Operations*

FORVIA
Inspiring mobility

#FRANSEC | PARIS | 6 - 7 JUIN

#FRANSEC23

> ❝ **DATA IS THE NEW OIL**
>
> CLIVE HUMBY, 2006

> “ CHEZ NOUS, PAS D’INQUIÉTUDE. IL N’Y A RIEN À VOLER, NOUS N’AVONS PAS DE SECRETS OU DE DONNÉES TRÈS CONFIDENTIELLES
>
> UN CIO EN 2022

HOW TO PREPARE FOR A DATA BREACH:

HOW TO MINIMIZE THE RISKS?

THOMAS BILLAUT

FRANSEC 2023

WELCOME TO FRANSEC 2023

@tbillaut

https://fr.linkedin.com/in/thomasbillaut

AGENDA

- Le vol de données…
- Panorama de la menace
- Comment se préparer ?
- Où est la recette magique ?
- Faire de la conformité un allié
- Améliorer continuellement sa maturité

AGENDA

- Le vol de données…
- Panorama de la menace
- Comment se préparer ?
- Où est la recette magique ?
- Faire de la conformité un allié
- Améliorer continuellement sa maturité

> “ THE CHARACTER OF CYBERTHREATS HAS CHANGED. RESPONDENTS NOW BELIEVE THAT CYBERATTACKERS ARE MORE LIKELY TO FOCUS ON **BUSINESS DISRUPTION** AND **REPUTATIONAL DAMAGE**. THESE ARE THE TOP TWO CONCERNS AMONG RESPONDENTS

WORLD ECONOMIC FORUM 2023

HTTPS://WWW.WEFORUM.ORG/REPORTS/GLOBAL-CYBERSECURITY-OUTLOOK-2023/

LE VOL DE DONNÉES…

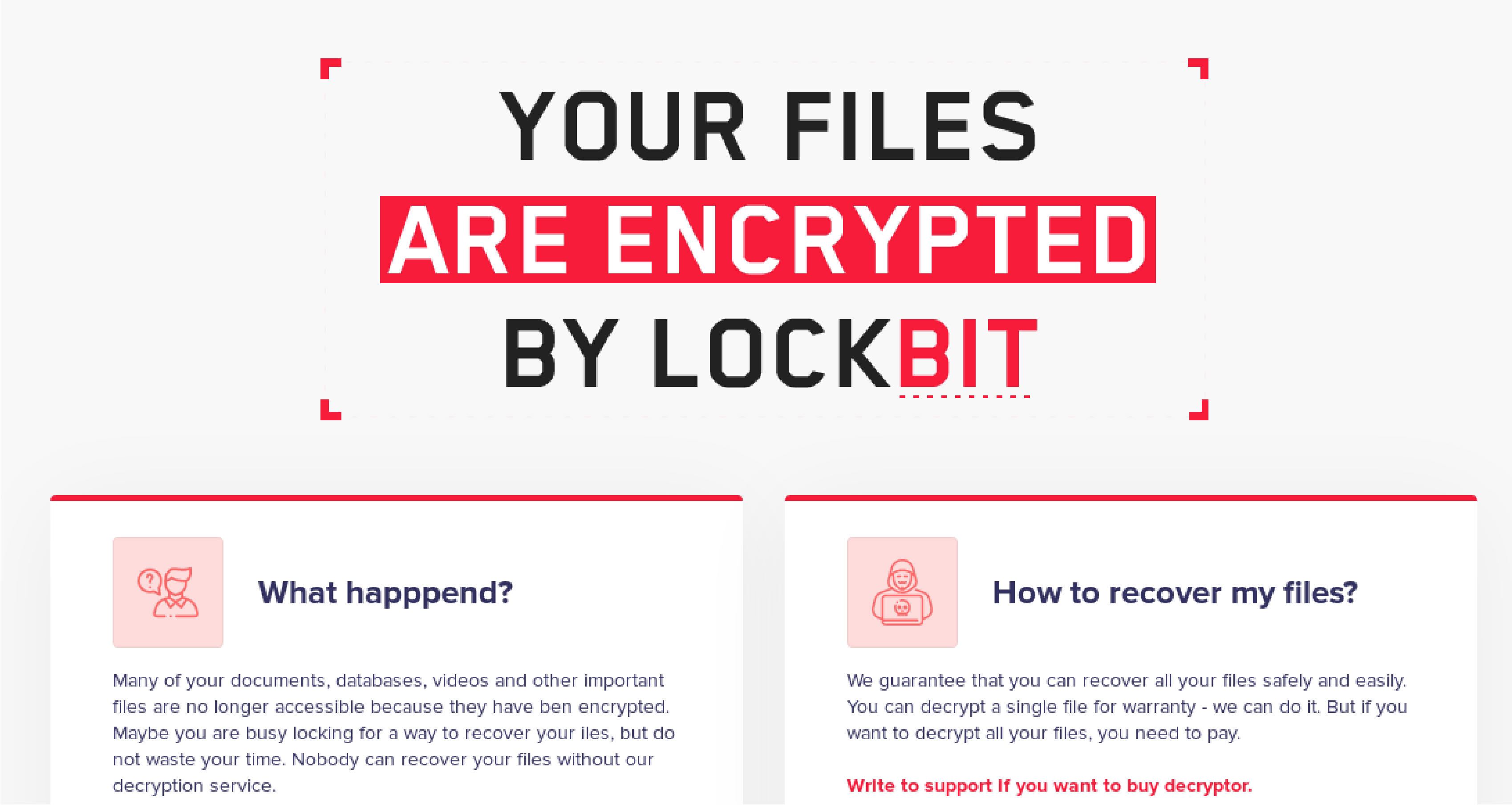
ET LA QUANTIFICATION DU RISQUE

RISQUE = VULNÉRABILITÉ x MENACE x IMPACT

AGENDA

- Le vol de données…
- Panorama de la menace
- Comment se préparer ?
- Où est la recette magique ?
- Faire de la conformité un allié
- Améliorer continuellement sa maturité

LE RANSOMWARE, MENACE #1 ?



YOUR FILES ARE ENCRYPTED BY LOCKBIT

What happpend?

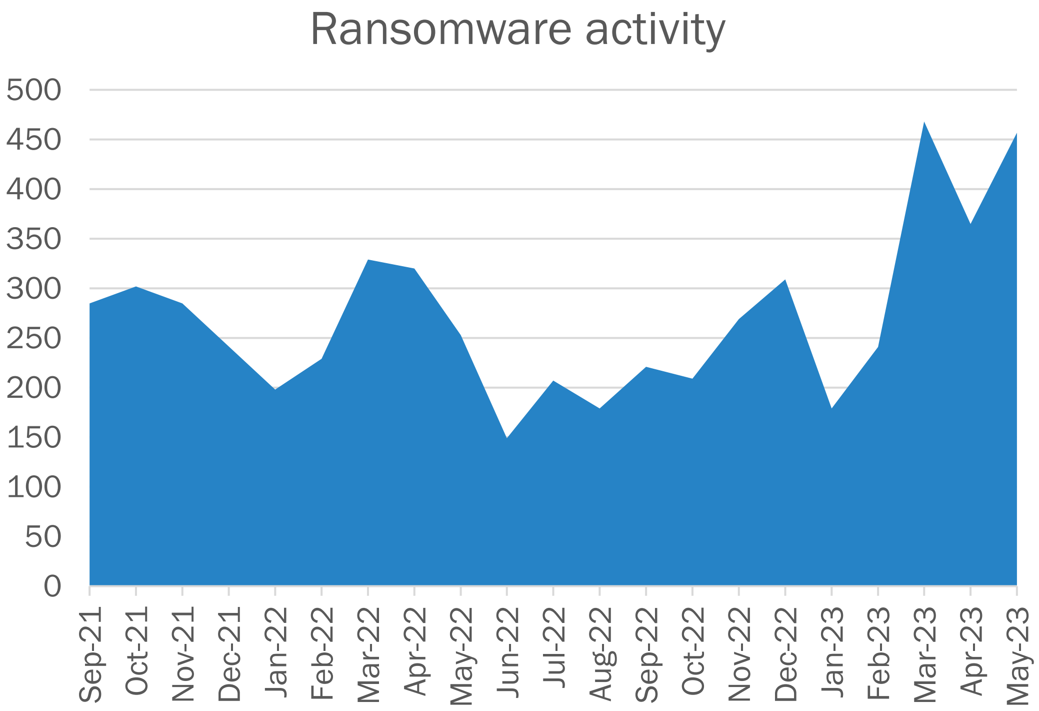
Many of your documents, databases, videos and other important files are no longer accessible because they have ben encrypted. Maybe you are busy locking for a way to recover your iles, but do not waste your time. Nobody can recover your files without our decryption service.

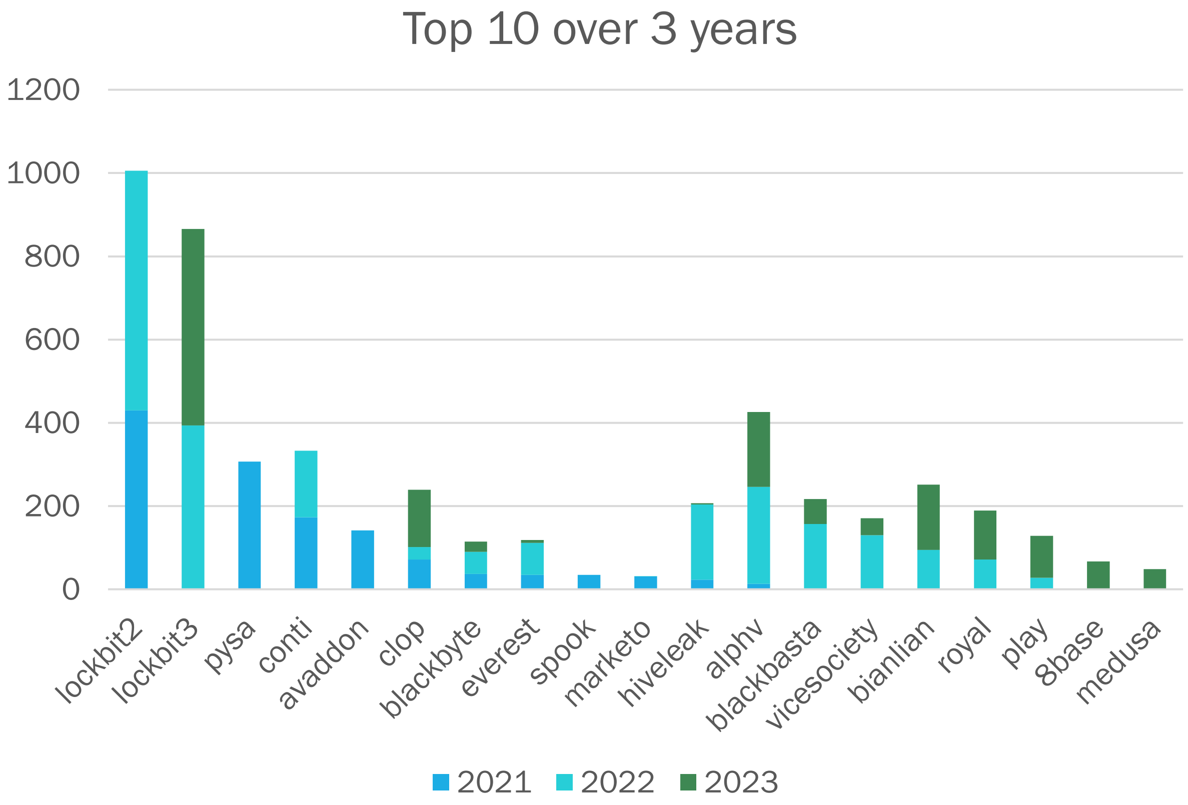
How to recover my files?

We guarantee that you can recover all your files safely and easily. You can decrypt a single file for warranty - we can do it. But if you want to decrypt all your files, you need to pay.

Write to support If you want to buy decryptor.

LE RANSOMWARE, MENACE #1 ?





EUH ? LE VOL DE DONNÉES, ÇA FAIT AUSSI PARTIE DU PLAN ?

Source : https://github.com/joshhighet/ransomwatch/blob/main/posts.json

BACK TO THE FUTURE

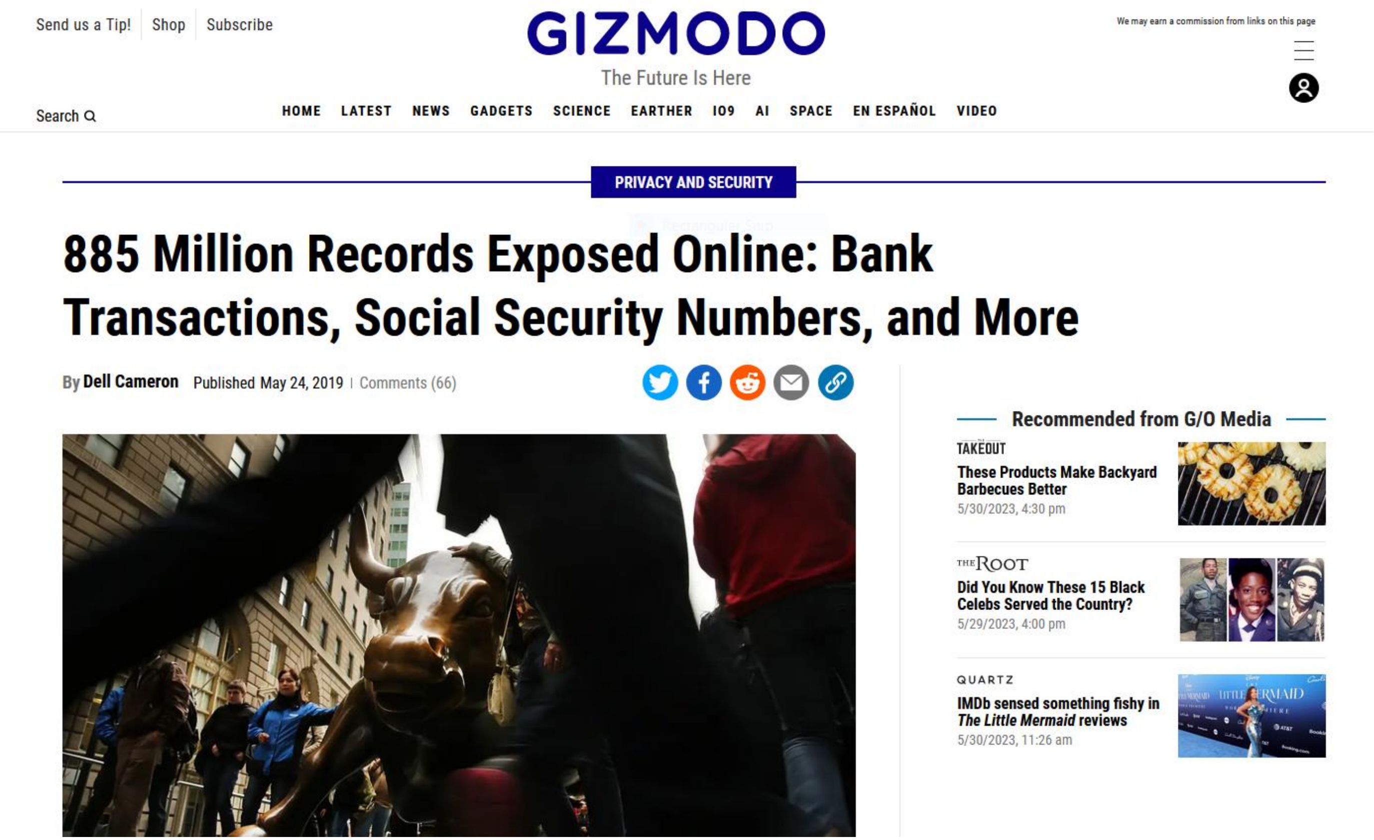
DATA BREACH RECAP'

YAHOO!	FIRST AMERICAN First American	facebook
3 000 M	885 M	540 M
(2013)	(2019)	(2019)
HACKED !	POOR SECURITY	POOR SECURITY

Source : https://en.wikipedia.org/wiki/List_of_data_breaches

BACK TO THE FUTURE

DATA BREACH RECAP' #2 – FIRST AMERICAN CORP



Send us a Tip! | Shop | Subscribe
GIZMODO
The Future Is Here
We may earn a commission from links on this page
Search
HOME LATEST NEWS GADGETS SCIENCE EARTHER IO9 AI SPACE EN ESPAÑOL VIDEO
PRIVACY AND SECURITY

885 Million Records Exposed Online: Bank Transactions, Social Security Numbers, and More

By Dell Cameron Published May 24, 2019 | Comments (66)

Recommended from G/O Media

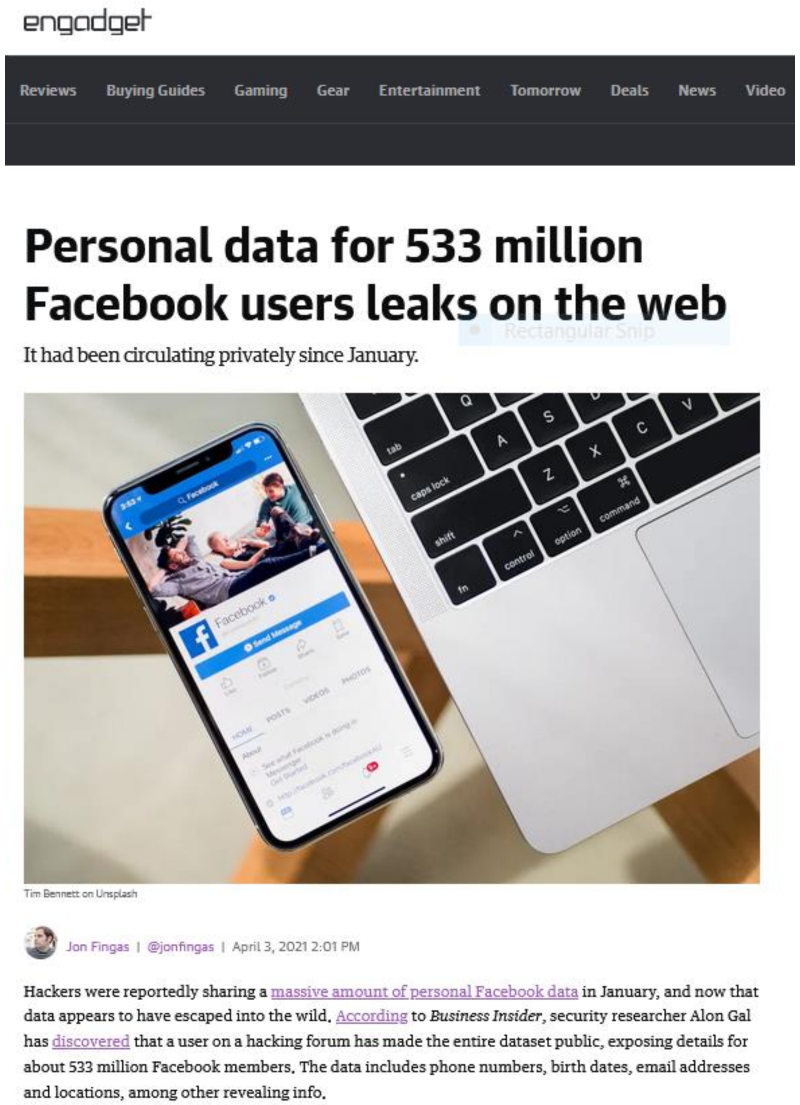
TAKEOUT
These Products Make Backyard Barbecues Better
5/30/2023, 4:30 pm

THE ROOT
Did You Know These 15 Black Celebs Served the Country?
5/29/2023, 4:00 pm

QUARTZ
IMDb sensed something fishy in *The Little Mermaid* reviews
5/30/2023, 11:26 am

BACK TO THE FUTURE

DATA BREACH RECAP' #2 – FACEBOOK



Personal data for 533 million Facebook users leaks on the web

It had been circulating privately since January.

Tim Bennett on Unsplash

Jon Fingas | @jonfingas | April 3, 2021 2:01 PM

Hackers were reportedly sharing a massive amount of personal Facebook data in January, and now that data appears to have escaped into the wild. According to *Business Insider*, security researcher Alon Gal has discovered that a user on a hacking forum has made the entire dataset public, exposing details for about 533 million Facebook members. The data includes phone numbers, birth dates, email addresses and locations, among other revealing info.

BACK TO THE FUTURE

DATA BREACH RECAP', POOR SECURITY ROOT CAUSES...

First American	facebook	EXACTIS	airtel	mongoDB
885 M	540 M	340 M	320 M	275 M
(2019)	(2019)	(2018)	(2019)	(2019)
POOR SECURITY	POOR SECURITY	POOR SECURITY	POOR SECURITY	POOR SECURITY

Source : https://en.wikipedia.org/wiki/List_of_data_breaches

AGENDA

- Le vol de données…
- Panorama de la menace
- Comment se préparer ?
- Help ! Où est la recette magique ?
- Faire de la conformité un allié
- Améliorer continuellement sa maturité

PDCA DE LA GESTION DE RISQUE

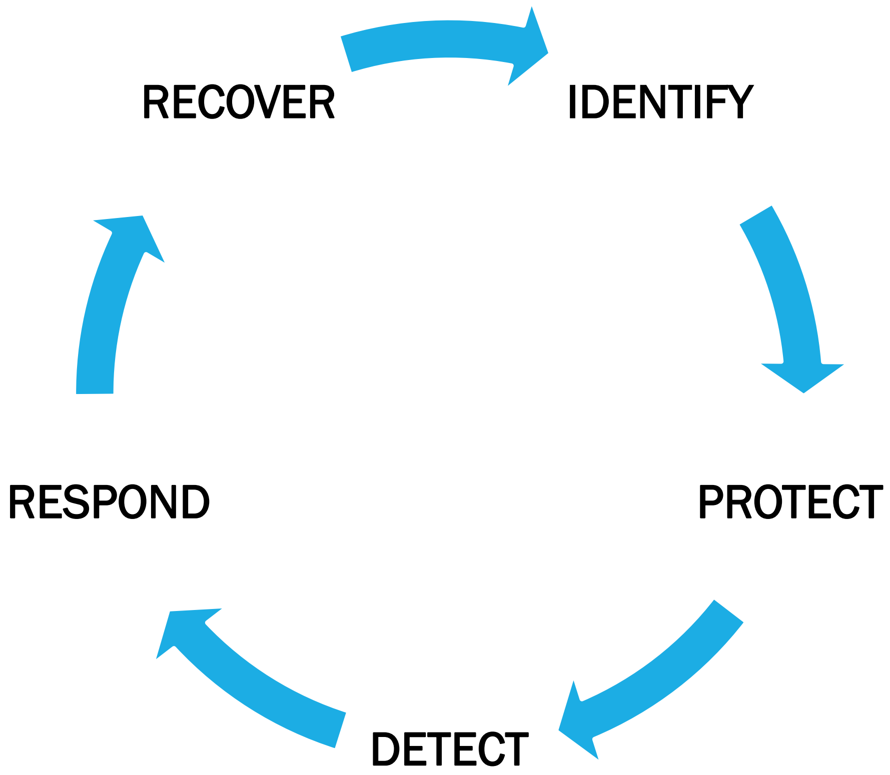
EN ROUTE POUR LE SMSI

- PDCA : Plan, Do, Check, Act
- Un SMSI est un **système de management permettant de définir des actions (techniques, organisationnelles) pour atteindre un objectif fixé**

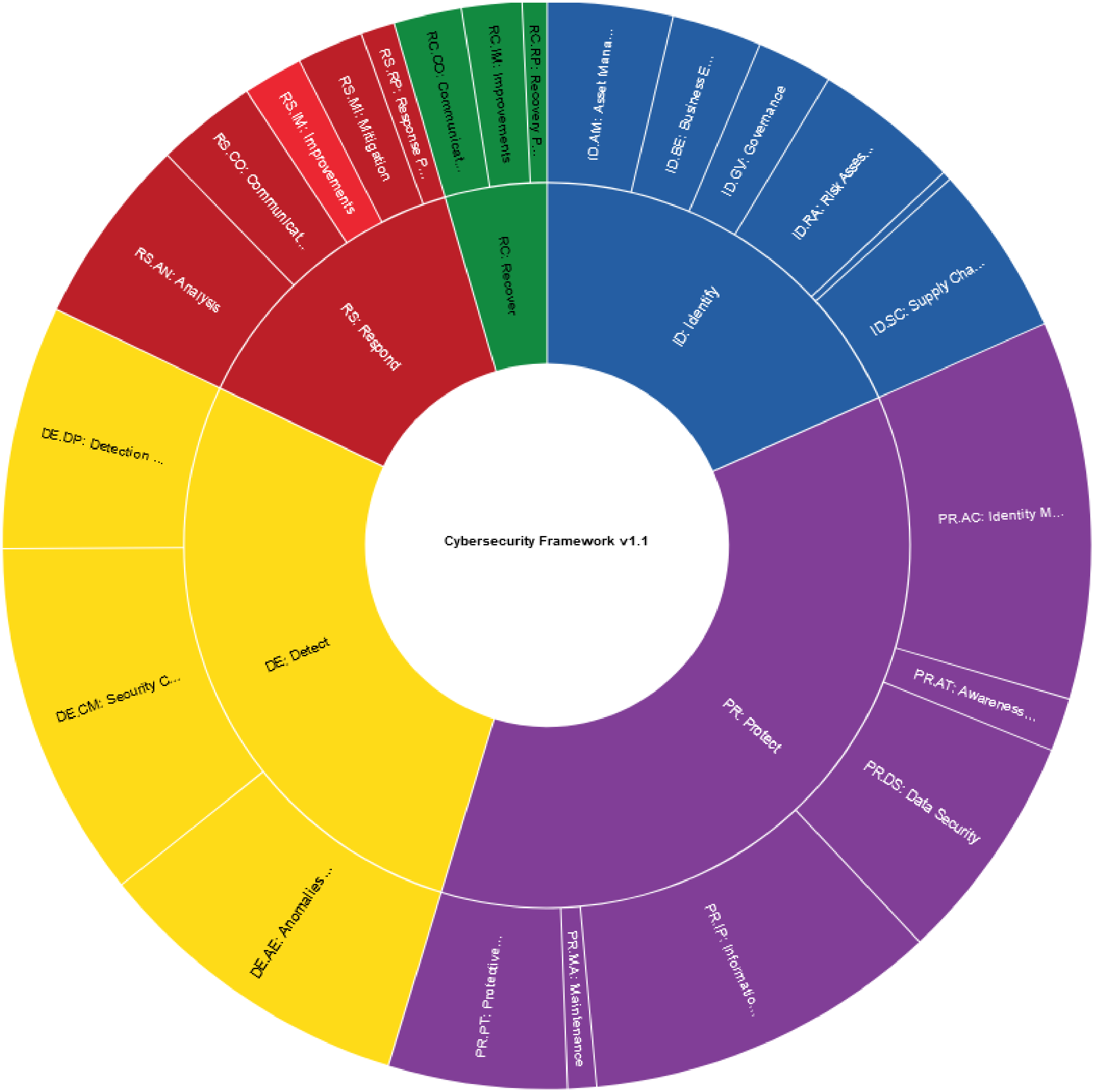
1. Etablir un cadre de gestion des risques
2. Identifier les risques
3. Analyser les risques
4. Evaluer les risques
5. Sélectionner les options de traitement des risques

UNE DECLINAISON PLUS OPERATIONNELLE, LE CPG DU CISA

CPGs = CYBERSECURITY PERFORMANCE GOALS



UNE DECLINAISON PLUS OPERATIONNELLE, LE CPG DU CISA
CPGS = CYBERSECURITY PERFORMANCE GOALS

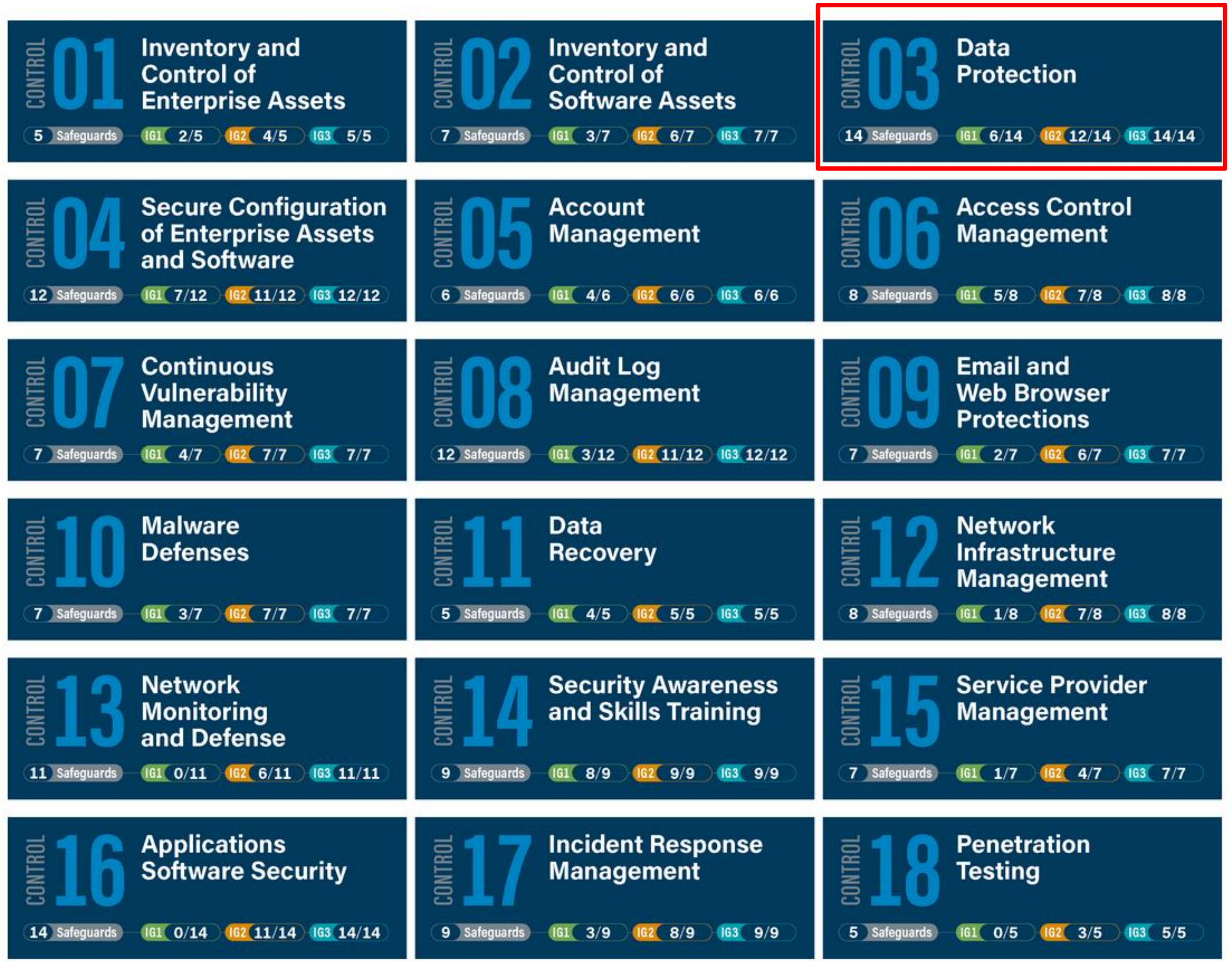


AGENDA

- Le vol de données…
- Panorama de la menace
- Comment se préparer ?
- Help ! Où est la recette magique ?
- Faire de la conformité un allié
- Améliorer continuellement sa maturité

CIS CRITICAL SECURITY CONTROL (V8)

DATA PROTECTION, NOW CONTROL 3 (CONTROL 13 IN V7)



CONTROL 01 Inventory and Control of Enterprise Assets — 5 Safeguards · IG1 2/5 · IG2 4/5 · IG3 5/5

CONTROL 02 Inventory and Control of Software Assets — 7 Safeguards · IG1 3/7 · IG2 6/7 · IG3 7/7

CONTROL 03 Data Protection — 14 Safeguards · IG1 6/14 · IG2 12/14 · IG3 14/14

CONTROL 04 Secure Configuration of Enterprise Assets and Software — 12 Safeguards · IG1 7/12 · IG2 11/12 · IG3 12/12

CONTROL 05 Account Management — 6 Safeguards · IG1 4/6 · IG2 6/6 · IG3 6/6

CONTROL 06 Access Control Management — 8 Safeguards · IG1 5/8 · IG2 7/8 · IG3 8/8

CONTROL 07 Continuous Vulnerability Management — 7 Safeguards · IG1 4/7 · IG2 7/7 · IG3 7/7

CONTROL 08 Audit Log Management — 12 Safeguards · IG1 3/12 · IG2 11/12 · IG3 12/12

CONTROL 09 Email and Web Browser Protections — 7 Safeguards · IG1 2/7 · IG2 6/7 · IG3 7/7

CONTROL 10 Malware Defenses — 7 Safeguards · IG1 3/7 · IG2 7/7 · IG3 7/7

CONTROL 11 Data Recovery — 5 Safeguards · IG1 4/5 · IG2 5/5 · IG3 5/5

CONTROL 12 Network Infrastructure Management — 8 Safeguards · IG1 1/8 · IG2 7/8 · IG3 8/8

CONTROL 13 Network Monitoring and Defense — 11 Safeguards · IG1 0/11 · IG2 6/11 · IG3 11/11

CONTROL 14 Security Awareness and Skills Training — 9 Safeguards · IG1 8/9 · IG2 9/9 · IG3 9/9

CONTROL 15 Service Provider Management — 7 Safeguards · IG1 1/7 · IG2 4/7 · IG3 7/7

CONTROL 16 Applications Software Security — 14 Safeguards · IG1 0/14 · IG2 11/14 · IG3 14/14

CONTROL 17 Incident Response Management — 9 Safeguards · IG1 3/9 · IG2 8/9 · IG3 9/9

CONTROL 18 Penetration Testing — 5 Safeguards · IG1 0/5 · IG2 3/5 · IG3 5/5

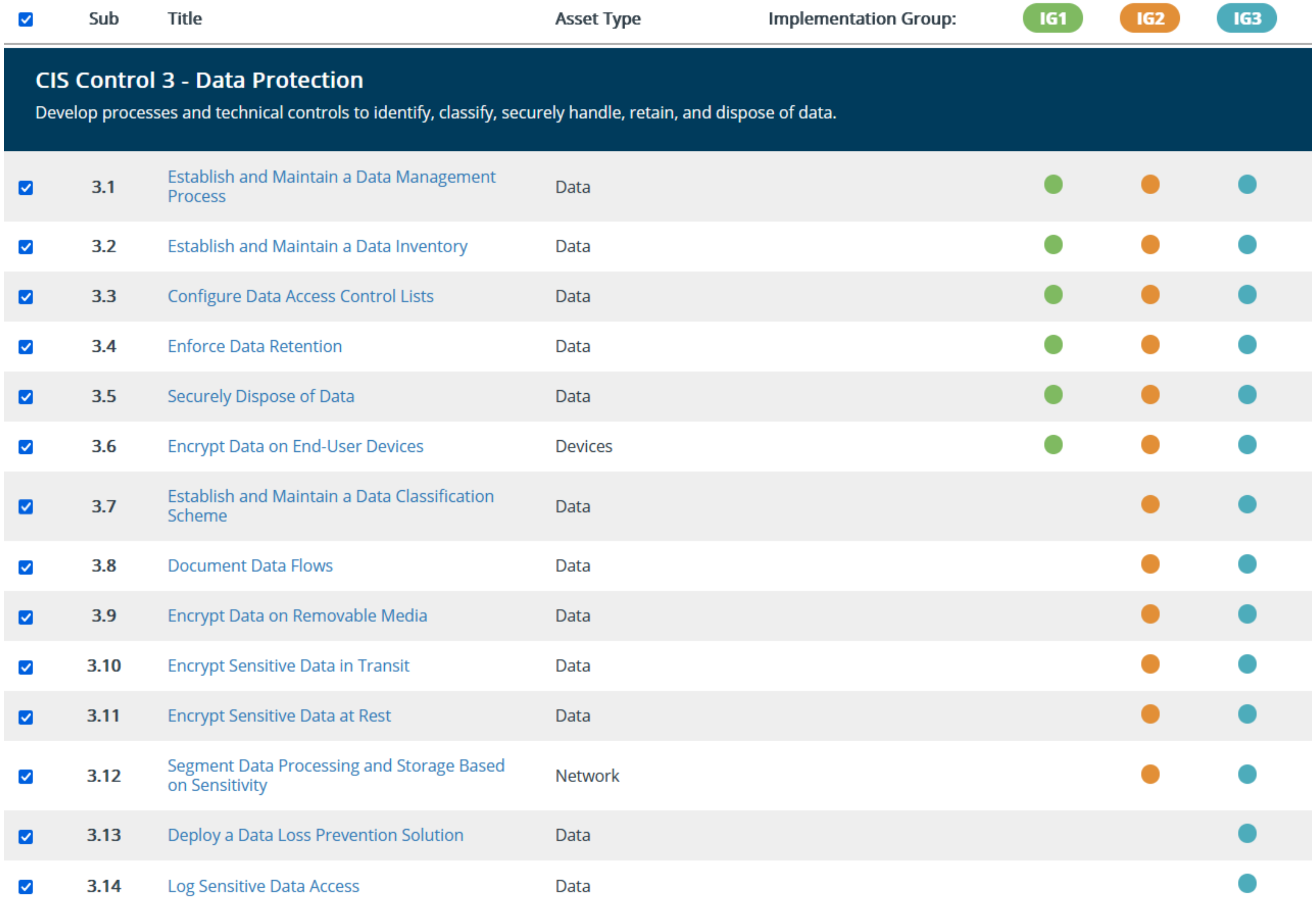
CIS CRITICAL SECURITY CONTROL

DATA PROTECTION / CIS SECURITY CONTROL 3

- Develop processes and technical controls to
  - Identify
  - Classify
  - securely handle
  - Retain
  - and dispose of data

CIS CRITICAL SECURITY CONTROL

DATA PROTECTION / CIS SECURITY CONTROL



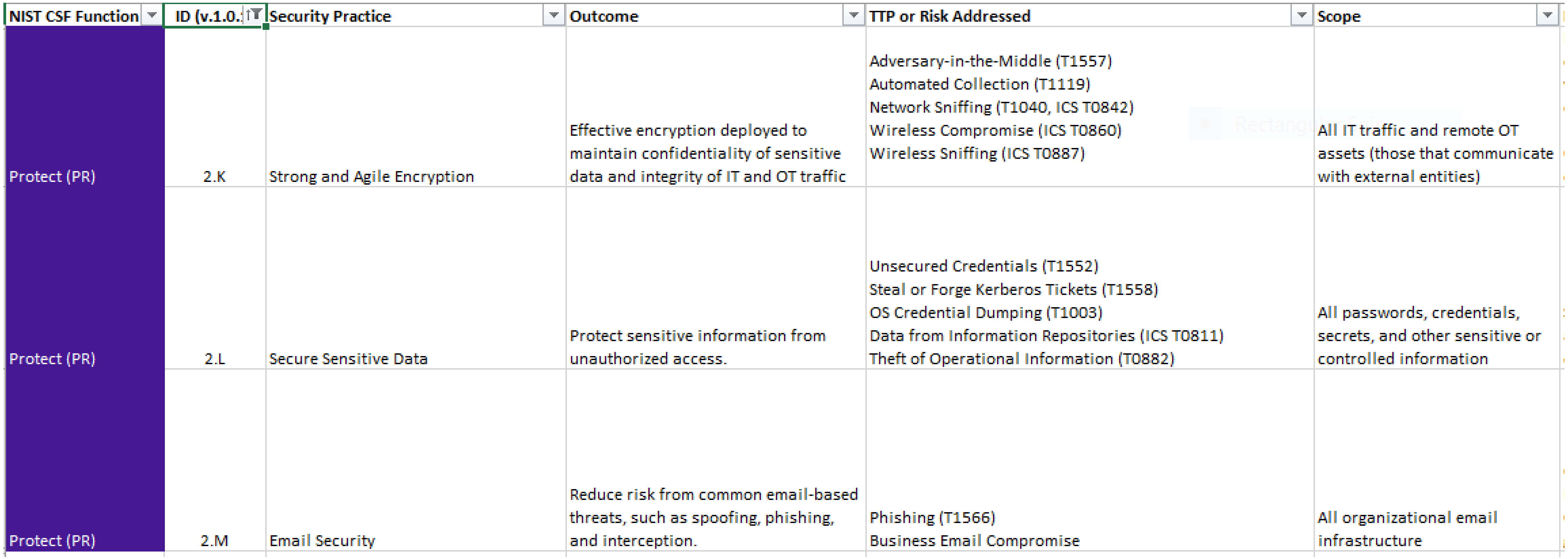
CIS Control 3 - Data Protection

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

☑	Sub	Title	Asset Type	Implementation Group:	IG1	IG2	IG3
☑	3.1	Establish and Maintain a Data Management Process	Data		●	●	●
☑	3.2	Establish and Maintain a Data Inventory	Data		●	●	●
☑	3.3	Configure Data Access Control Lists	Data		●	●	●
☑	3.4	Enforce Data Retention	Data		●	●	●
☑	3.5	Securely Dispose of Data	Data		●	●	●
☑	3.6	Encrypt Data on End-User Devices	Devices		●	●	●
☑	3.7	Establish and Maintain a Data Classification Scheme	Data			●	●
☑	3.8	Document Data Flows	Data			●	●
☑	3.9	Encrypt Data on Removable Media	Data			●	●
☑	3.10	Encrypt Sensitive Data in Transit	Data			●	●
☑	3.11	Encrypt Sensitive Data at Rest	Data			●	●
☑	3.12	Segment Data Processing and Storage Based on Sensitivity	Network			●	●
☑	3.13	Deploy a Data Loss Prevention Solution	Data				●
☑	3.14	Log Sensitive Data Access	Data				●

EN ADOPTANT LE CPG

CPGs = CYBERSECURITY PERFORMANCE GOALS



NIST CSF Function	ID (v.1.0.:	Security Practice	Outcome	TTP or Risk Addressed	Scope
Protect (PR)	2.K	Strong and Agile Encryption	Effective encryption deployed to maintain confidentiality of sensitive data and integrity of IT and OT traffic	Adversary-in-the-Middle (T1557) Automated Collection (T1119) Network Sniffing (T1040, ICS T0842) Wireless Compromise (ICS T0860) Wireless Sniffing (ICS T0887)	All IT traffic and remote OT assets (those that communicate with external entities)
Protect (PR)	2.L	Secure Sensitive Data	Protect sensitive information from unauthorized access.	Unsecured Credentials (T1552) Steal or Forge Kerberos Tickets (T1558) OS Credential Dumping (T1003) Data from Information Repositories (ICS T0811) Theft of Operational Information (T0882)	All passwords, credentials, secrets, and other sensitive or controlled information
Protect (PR)	2.M	Email Security	Reduce risk from common email-based threats, such as spoofing, phishing, and interception.	Phishing (T1566) Business Email Compromise	All organizational email infrastructure

AGENDA

- Le vol de données…
- Panorama de la menace
- Comment se préparer ?
- Help ! Où est la recette magique ?
- Faire de la conformité un allié
- Améliorer continuellement sa maturité

S’APPUYER SUR LA CONFORMITÉ POUR FAIRE LEVIER

GDPR, PCI DSS, HIPAA, TISAX,…À CHACUN D’IDENTIFIER CE QUI FAIT DU SENS

- Jouer sur la peur du gendarme …

« Concernant la procédure ordinaire, avec le RGPD (règlement général sur la protection des données), **le montant des sanctions pécuniaires peut s'élever jusqu'à 20 millions d'euros ou dans le cas d'une entreprise jusqu'à 4 % du chiffre d'affaires annuel mondial.** Ces sanctions peuvent être rendues publiques.”

- La volonté de montrer votre savoir faire (27k1, TISAX, …)
- Attention à ne pas tomber dans l’approche “check the box”
- Faire de la Conformité et de la Sécurité des alliés

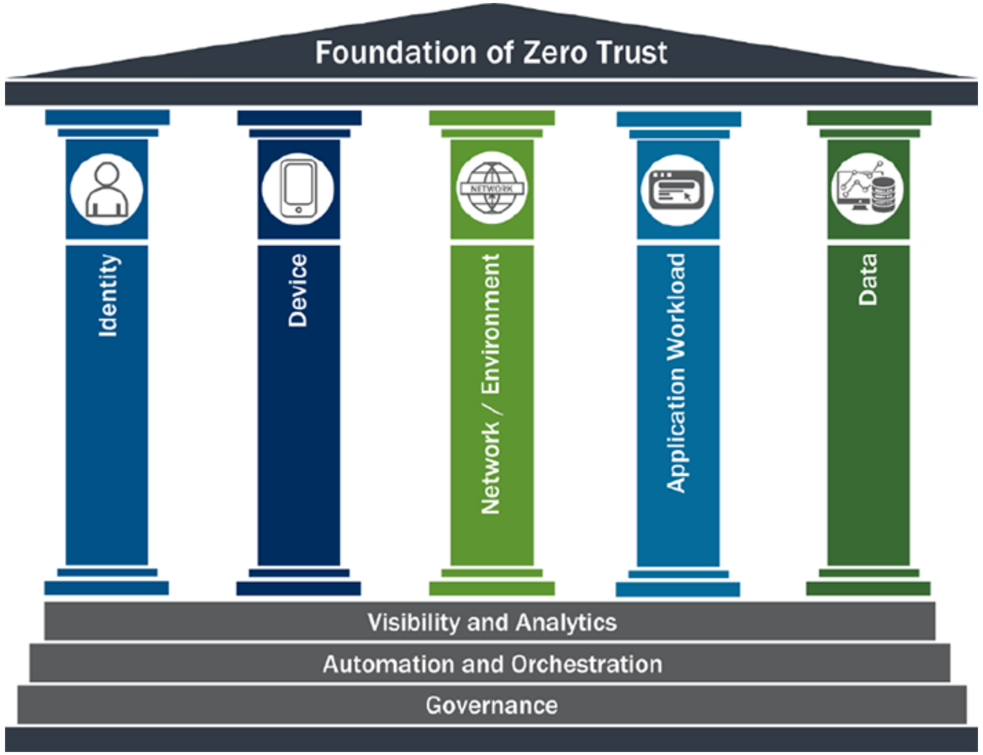
AGENDA

- Le vol de données…
- Panorama de la menace
- Comment se préparer ?
- Help ! Où est la recette magique ?
- Faire de la conformité un allié
- Améliorer continuellement sa maturité

ALLER VERS DES MODELES ZERO TRUST

VERS LE CONTINUOUS ASSUMED BREACHED APPROCHE ?

- “Nevers trust, always verify”
- Un des avantages du modèle ZT est de fortement limiter l’impact en cas d’incident (least privilege access for resource and data)
- Approche Assumed breach :
  - Évolution du what if
  - l’attaquant a déjà réussi à compromettre des ressources



CONCLUSION

- Revenir aux fondations, en repartant du risque
- Pas d’impact = pas de risque
- S’appuyer sur un framework est facilitant, à chacun de choisir
- Simple…et donc très complexe à exécuter et opérationnaliser à l’échelle
- Think big, start small…

> “AVEC UN TALENT ORDINAIRE ET UNE PERSÉVÉRANCE EXTRAORDINAIRE, ON PEUT TOUT OBTENIR
>
> THOMAS FOXWELL BUXTON

MERCI

@tbillaut

https://fr.linkedin.com/in/thomasbillaut

ANNEXES ET REFERENCE

- **Cross-Sector Cybersecurity Performance Goals**
  The CPGs are a prioritized subset of information technology (IT) and operational technology (OT) cybersecurity practices that critical infrastructure owners and operators can implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques.
  https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
- **CSF Tool**
  This site contains a number of helpful tools that will make the NIST Cybersecurity Framework (CSF) and Privacy Framework (PF) more understandable and accessible. Some of those tools are outlined below.
  https://csf.tools/
- **CIS control**
  Follow our prioritized set of actions to protect your organization and data from cyber-attack vectors.
  https://www.cisecurity.org/controls