LUNDI DE LA CYBERSÉCURITÉ

18 OCTOBRE 2021

CYBER RISK INDEX ET CYBER NOTATIONS

ARCSI
Association des Réservistes du Chiffre
et de la Sécurité de l'Information

Université
de Paris

PIERRE-LUC REFALO
VICE PRÉSIDENT – CAPGEMINI GROUP CYBERSECURITY

prefalo @plrefalo

Avertissement

CETTE PRÉSENTATION PROPOSE UN ÉTAT DE L'ART DES TENDANCES OU DES POINTS DE DISCUSSION BASES SUR L'EXPERIENCE DE L'INTERVENANT, EN AUCUN CAS DES POSITIONS DE SON ENTREPRISE (CAPGEMINI).

Plus de 30 ans d'engagement dans
La sécurité numérique
et la protection des données.

SFR

CISO CYBERSECURITY

1997 - 2002

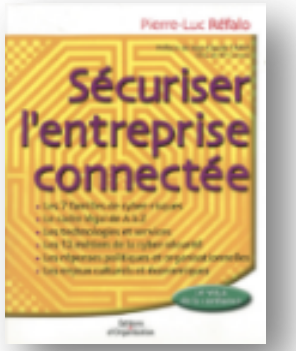
Capgemini

Depuis 2013

Certified Information Privacy Manager CIPM iapp

2018

Auteur



2002

2004 - 2011

2012

FIC 2013

Prix du Livre

Enseignant

utt université de technologie Troyes

ESIEE PARIS

TELECOM & Management SudParis

isep École d'ingénieurs du numérique

Conférencier

lesassises de la sécurité et des systèmes d'information

FIC 2013

FIC 2015

FIC 2024

NET FOCUS

CESIN

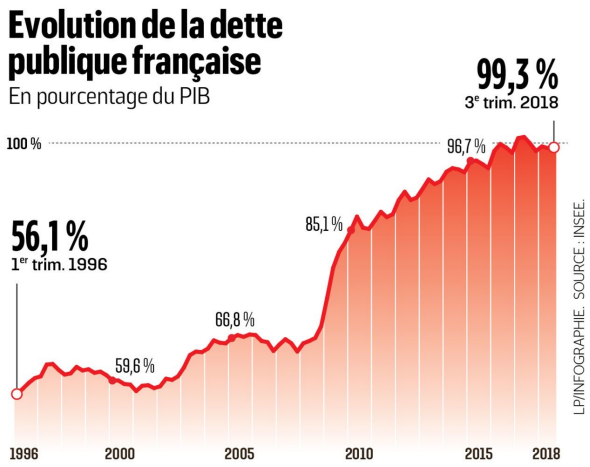
ISACA

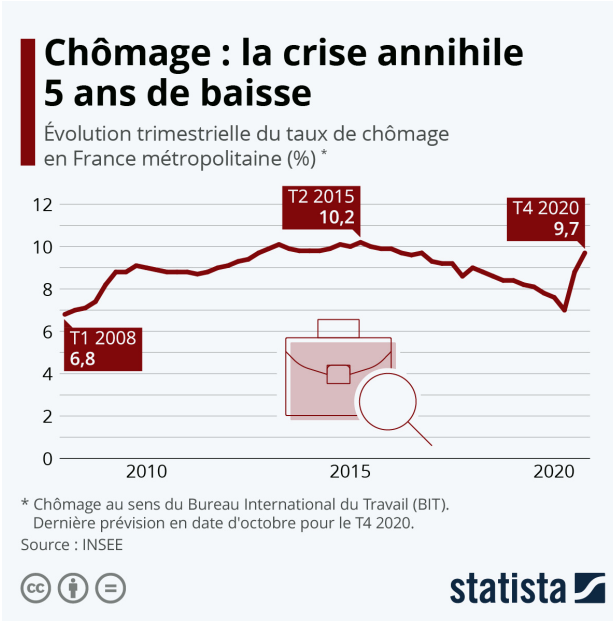
RSAConference2018 San Francisco | April 16 – 20 | Moscone Center

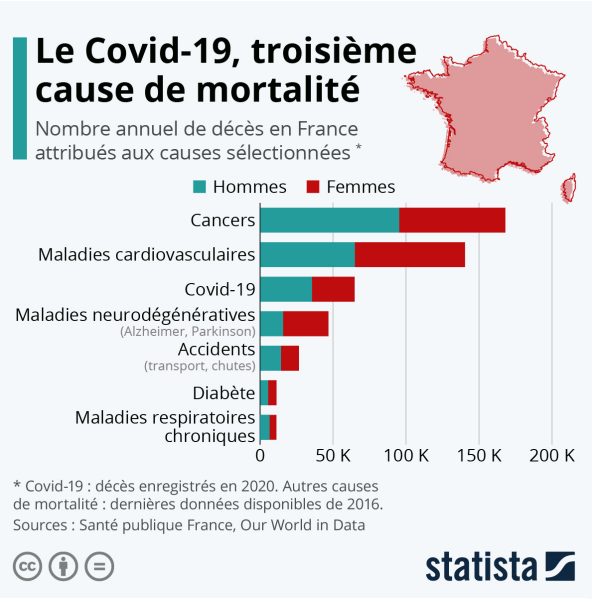
Gartner

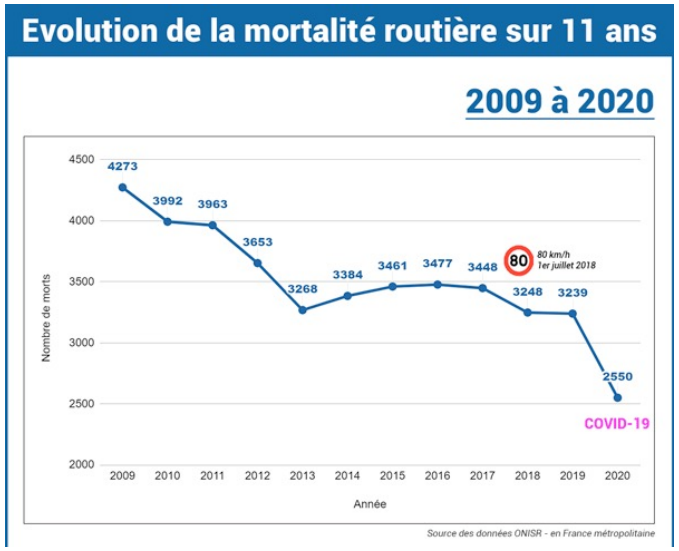
CSI COMPUTER SECURITY INSTITUTE

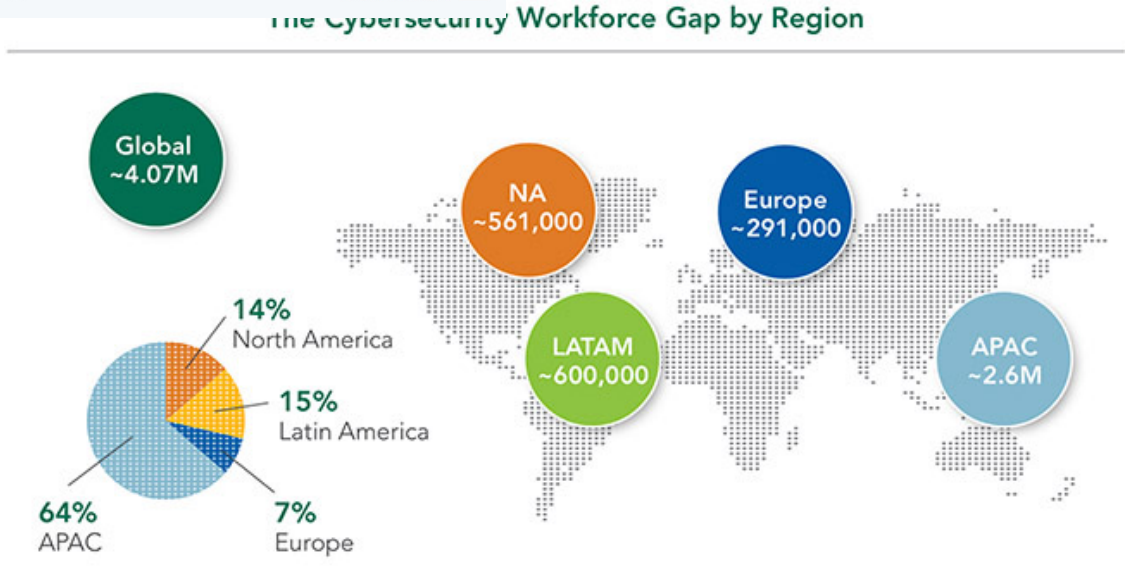
NASSCOM®
Bangalore – Oct 6-7 2018 | Leela Palace





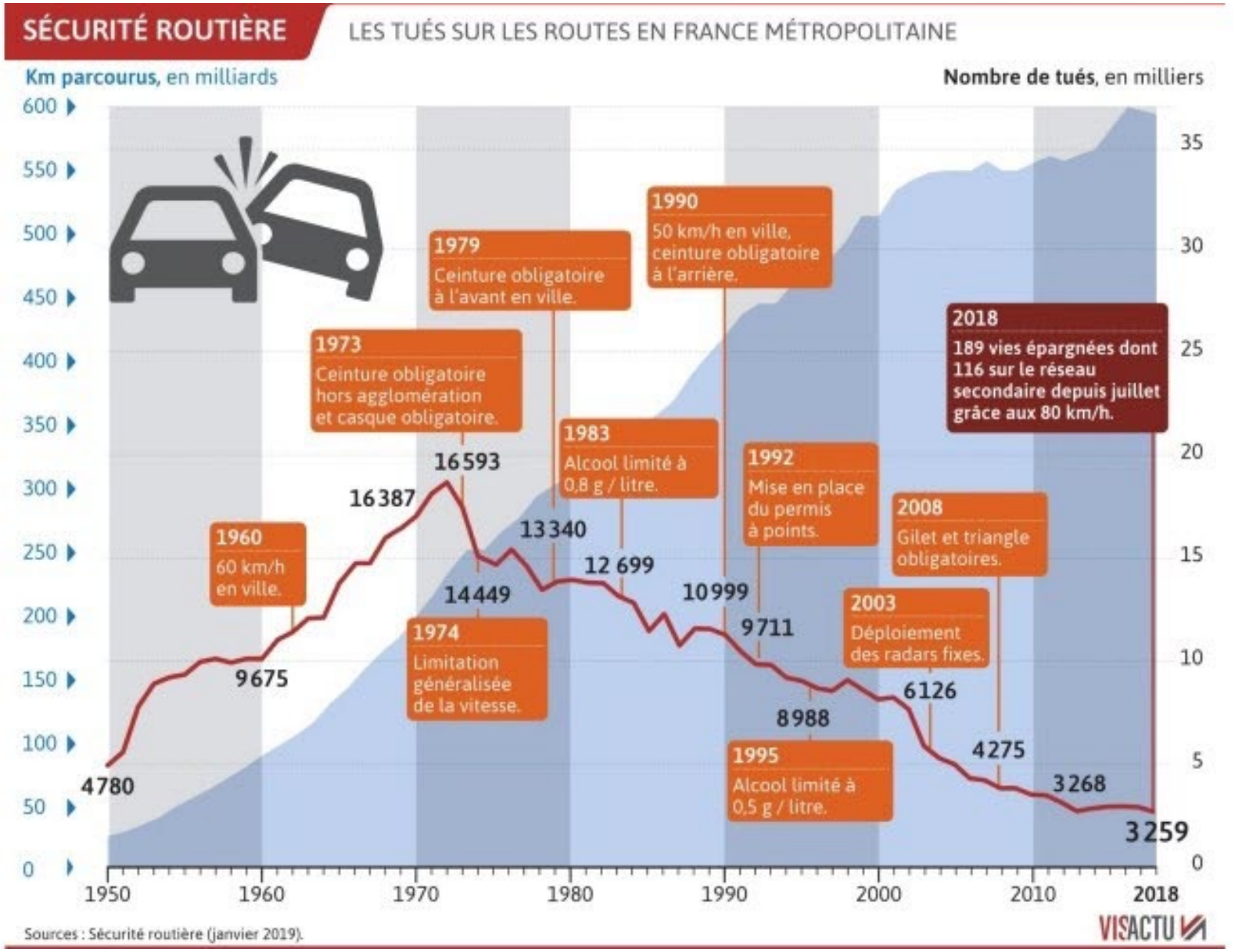






Le poids des nombres au quotidien …

INDICATEURS DE LA SECURITE ROUTIERE



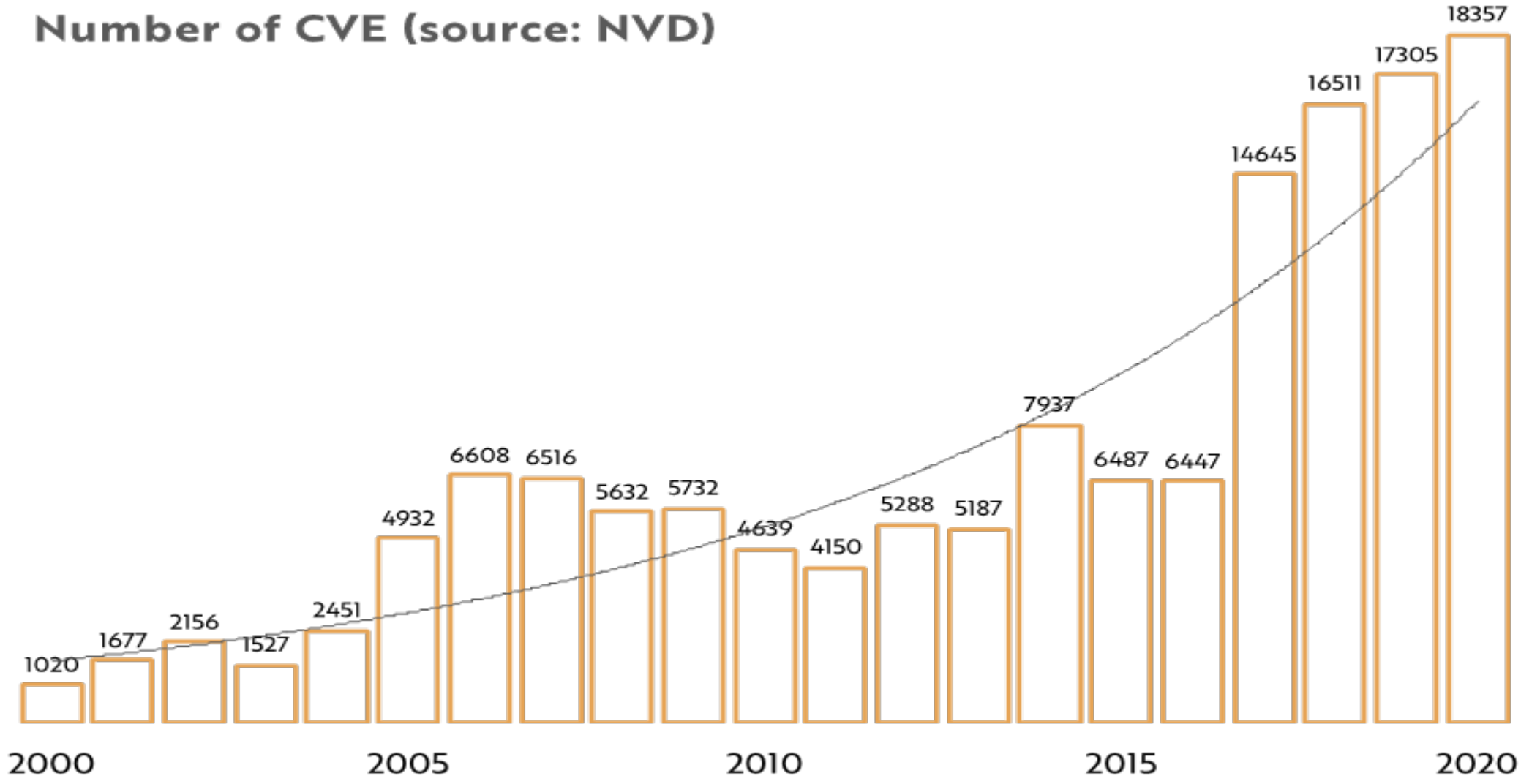
« J'ai appris qu'une vie ne vaut rien mais rien ne vaut une vie. »

André Malraux

INDICATEURS DE LA DIGITALISATION DE LA SOCIETE

« Our goal is to organize the world's information and to make it universally accessible and usefull. »

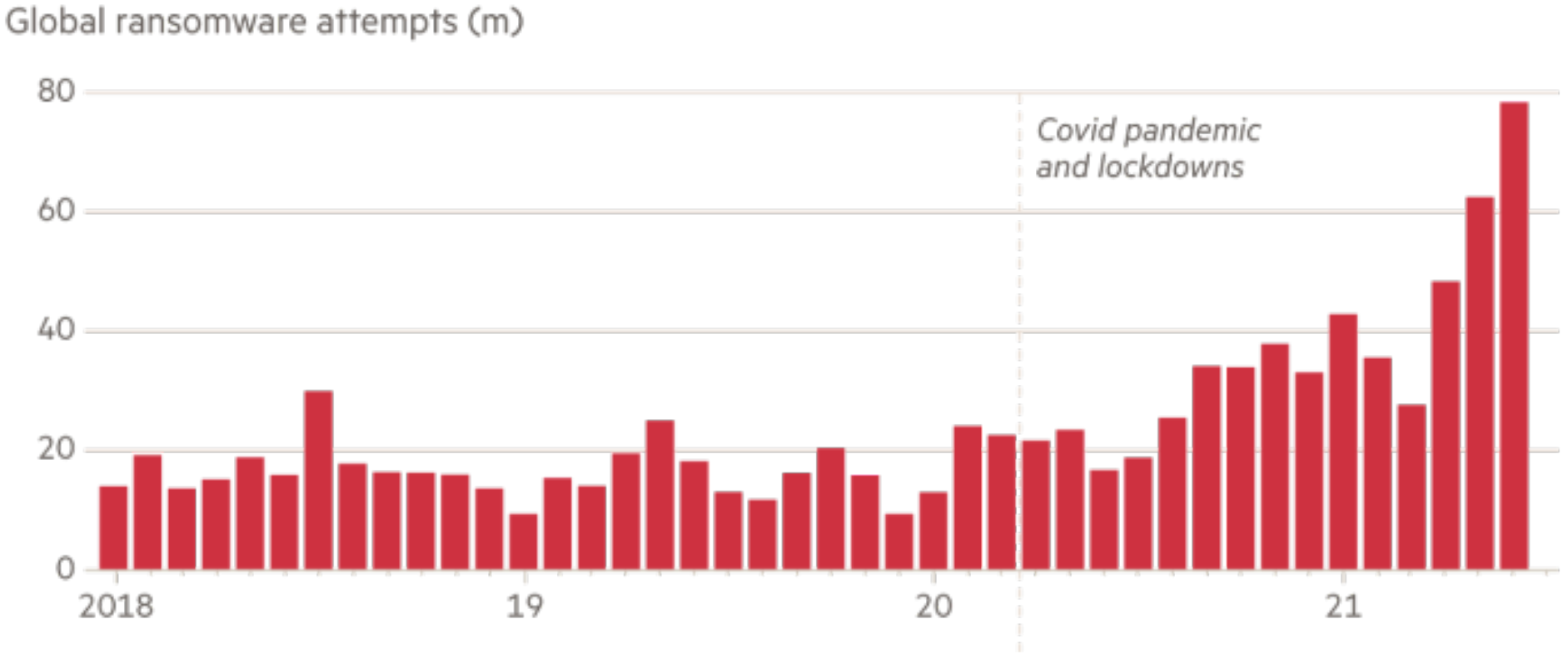
Larry Page



Nos faiblesses: Plus de 100 000 vulnérabilités en 20 ans !

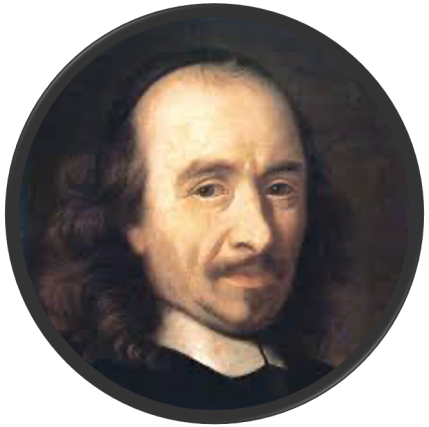
Les menaces: Plus de 100 millions de tentatives d'attaque par ransomware en 3 ans!

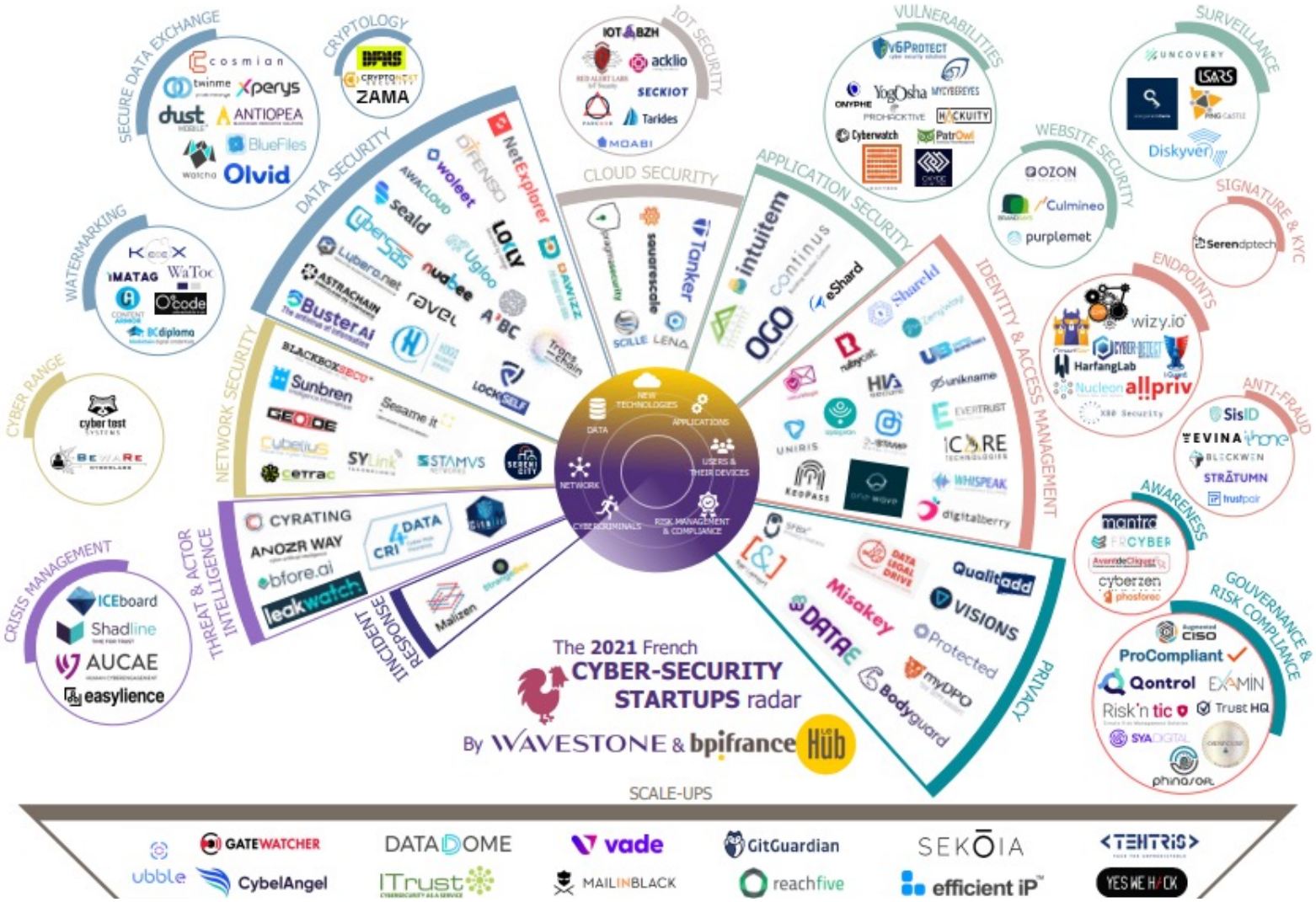
Ransomware attempts reached an unprecedented level in 2021...



« He who fears not death fears not a threat. »

Pierre Corneille





INDICATEURS DE L'INNOVATION EN CYBERSECURITE

INDICATEURS DE LA CROISSANCE DU MARCHE DE LA CYBERSECURITE

Market Segment	2017	2018	2019	2020	2021	Growth%
Application Security	2 434	2 742	3 003	3 333	3 738	12.2
Cloud Security	185	304	459	595	841	41.2
Data Security	2 563	3 063	3 524	2 981	3 505	17.5
Identity Access Management	8 823	9 768	10 578	12 036	13 917	15.6
Infrastructure Protection	12 583	14 106	15 337	20 462	23 903	16.8
Integrated Risk Management	3 949	4 347	4 712	4859	5 473	12.6
Other Information Security Software	1 832	2 079	2 285	2 306	2 527	9.6
Security Services	52 315	58 920	64 237	65 070	72 497	11.4
Consumer Security Software	5 948	6 395	6 661	6 507	6 990	7.4
Total	**101 544**	**114 152**	**124 116**	**133 776**	**150 409**	**12.4%**

WORLDWIDE SECURITY SPENDINGS BY SEGMENT, 2017-2021 (MILLIONS OF U.S DOLLARS)**

Source: Gartner

Les agences de notation ... Note de la France

STANDARD & POORS		MOODY'S		FITCH RATINGS		
LONG TERME	COURT TERME	LONG TERME	COURT TERME	LONG TERME	COURT TERME	
AAA	A-1+	AAA	P-1	AAA	F1+	Sécurité optimale
AA+		AA1		AA+		De bonne qualité à qualité moyenne inférieure
AA		AA2		AA		
AA-		AA3		AA-		
A+	A-1	A1		A+	F1	
A		A2		A		
A-	A-2	A3	P-2	A-	F2	
BBB+		BAA1		BBB+		
BBB	A-3	BAA2	P-3	BBB	F3	
BBB-		BAA3		BBB-		
BB+	B	BA1	NOT PRIME	BB+	B	Spéculatif
BB		BA2		BB		
BB-		BA3		BB-		
B+		B1		B+		
B		B2		B		
B-		B3		B-		
CCC+	C	CAA				Extrêmement spéculatif
CCC		CA		CCC	C	
CCC-		C				
SD	/	/		DDD		En défaut
D		/		DD	/	
		/		D		

La note correspond aux perspectives de remboursement de ses engagements envers ses créanciers

idé

Moody's

Fitch Ratings

S&P Global Ratings

LA NOTATION DES ENTREPRISES : Une santé financière sous surveillance

LA CYBERSECURITE S'INVITE DANS LA RESPONSABILITE SOCIALE ET ENVIRONEMENTALE

AGENCES DE NOTATION

Vue interne – RSE & Cybersecurity / Data Protection

- Deux approches: RSE et Evaluation des fournisseurs
- Plate-forme en ligne avec questionnaires thématiques (déclaratif) avec ou sans fourniture de preuves (analyse par consultant)
- Scoring valable un an accessible à tous clients de la plateforme
- Des questionnaires parfois très volumineux et évolutifs
- Une mise en valeur de la cybersécurité auprès des dirigeants
- Un usage important en termes de réputation et de maîtrise des risques intégrant les « fournisseurs »

Dow Jones Sustainability Indexes

ecovadis

ecodesk

cybervadis

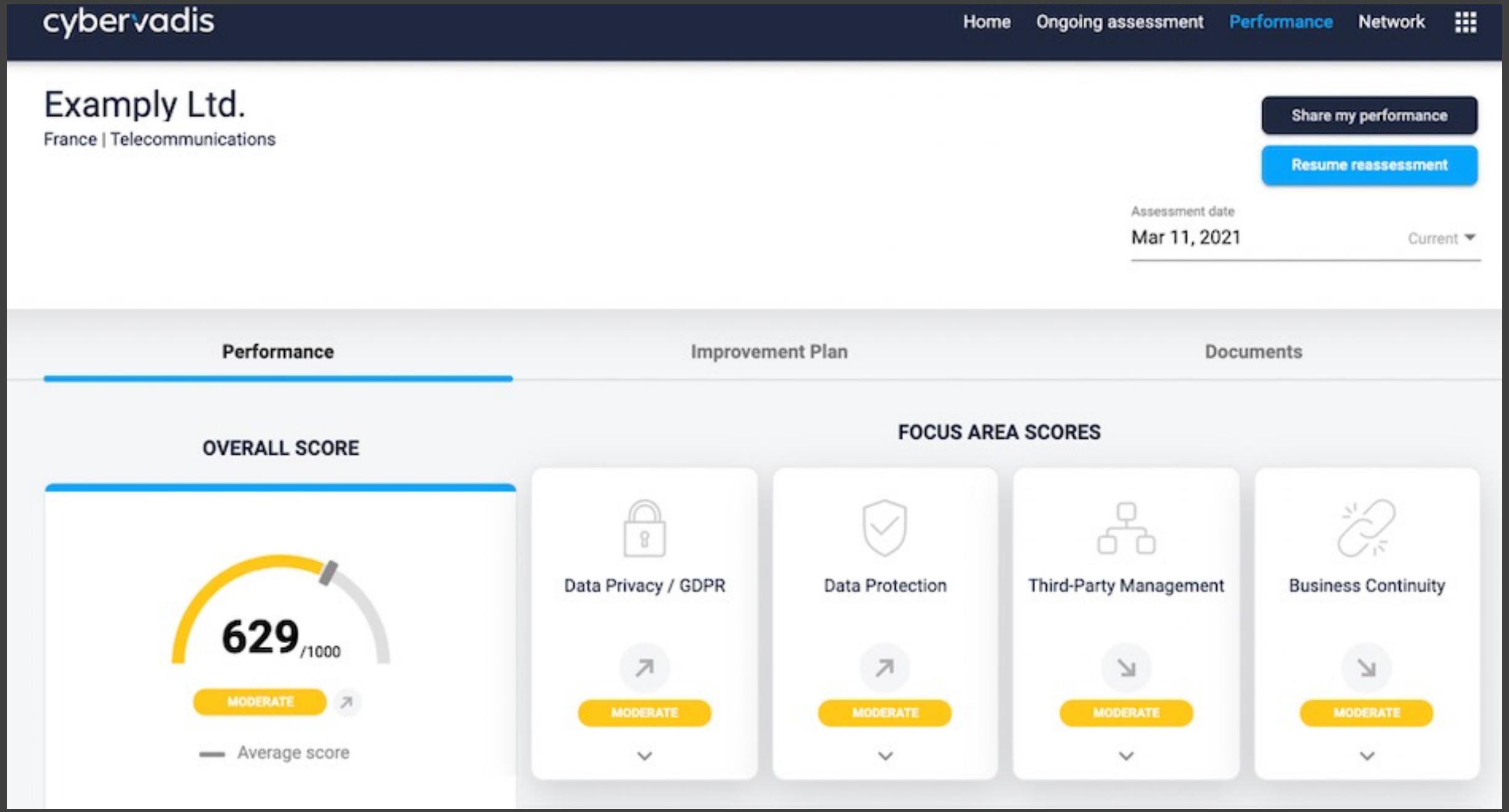
CyberGRX

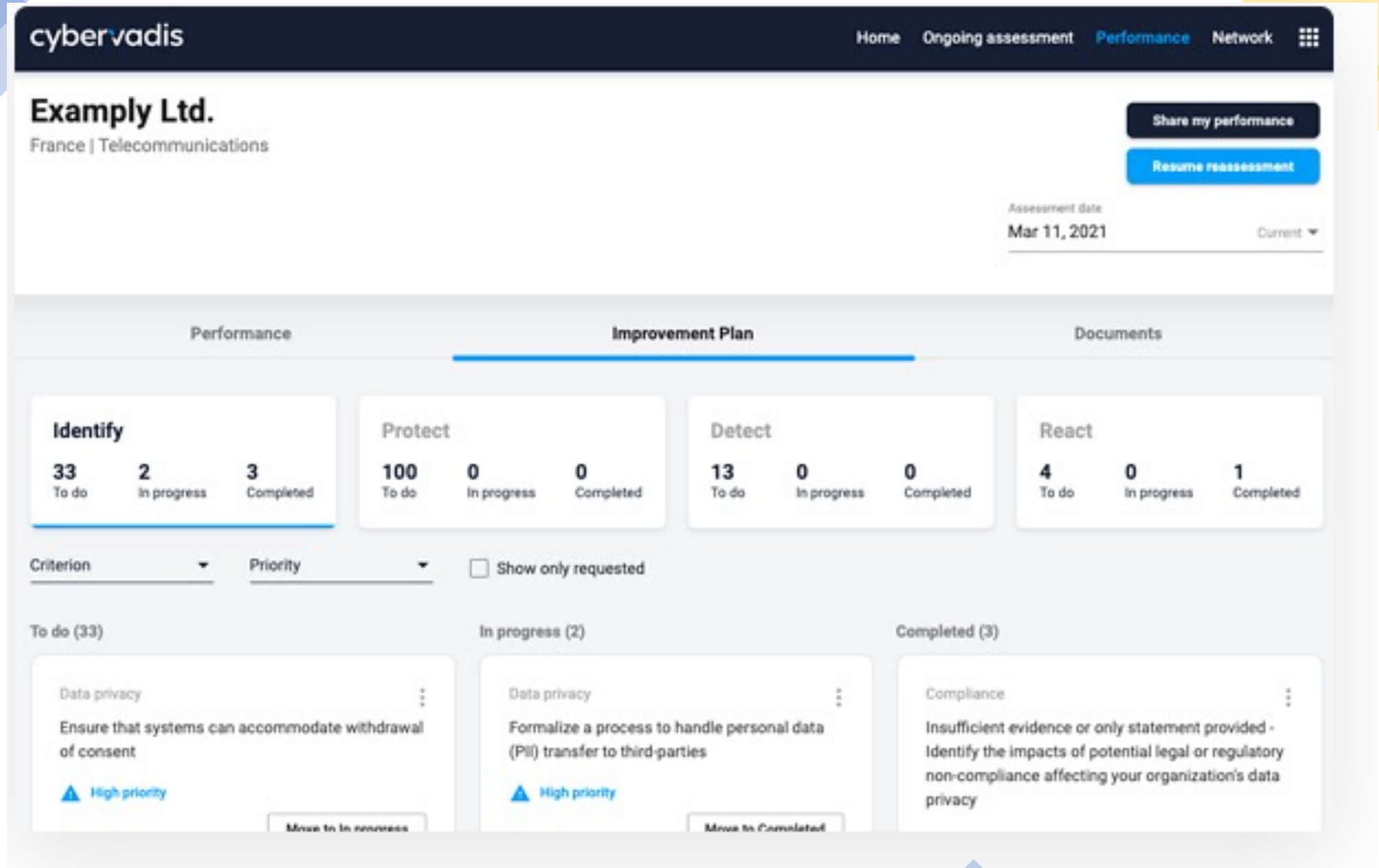
FRANCE

DIGITEMIS CYBERSECURITY & PRIVACY

CESIN

almond





AGENCES DE NOTATION

Vue externe – External Risk Rating

Un « scanning » des noms de domaines et IP avec de grands différences entre plateformes (scope, périodicité, qualification et faux positifs, suivi des remédiations).

Des algorithmes peu transparent et évolutifs.

Des méthodes de scoring non homogènes.

Des plateformes de management très complètes (monitoring permanent ou ponctuel, benchmark, etc.)

Une maturité naissante pour un marché en forte croissance.

Des usages variables : risques « fournisseurs » pour démarrer mais aussi risques / vulnérabilités et incidents en lien avec le SOC

Des scores minimum requis lors d'appels d'offres

Fort utile lors d'acquisitions

SecurityScorecard

BITSIGHT

riskrecon™

RISKIQ

Panorays

BlueVoyant

BITSIGHT: PILOTAGE DES SECURITY RATINGS DANS UNE ORGANIZATION DECENTRALISÉE

Compromised Systems

Botnet Infections	A
Spam Propagation	A
Malware Servers	A
Unsolicited Communications	A
Potentially Exploited	C

User Behavior

File Sharing	A
Exposed Credentials**	N/A

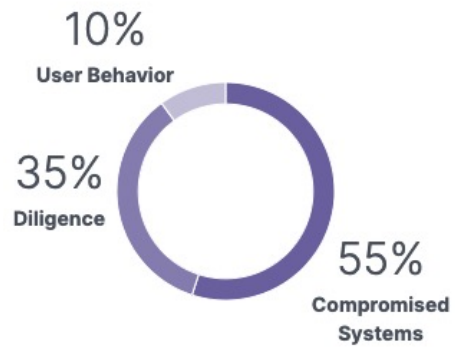
Public Disclosures

Security Incidents/Breaches	A
Other Disclosures*	N/A

Diligence

SPF Domains	A
DKIM Records	A
TLS/SSL Certificates	C
TLS/SSL Configurations	C
Open Ports	C
Web Application Headers	D
Patching Cadence	C
Insecure Systems	B
Server Software	B
Desktop Software	B
Mobile Software	
DNSSEC*	
Mobile *	

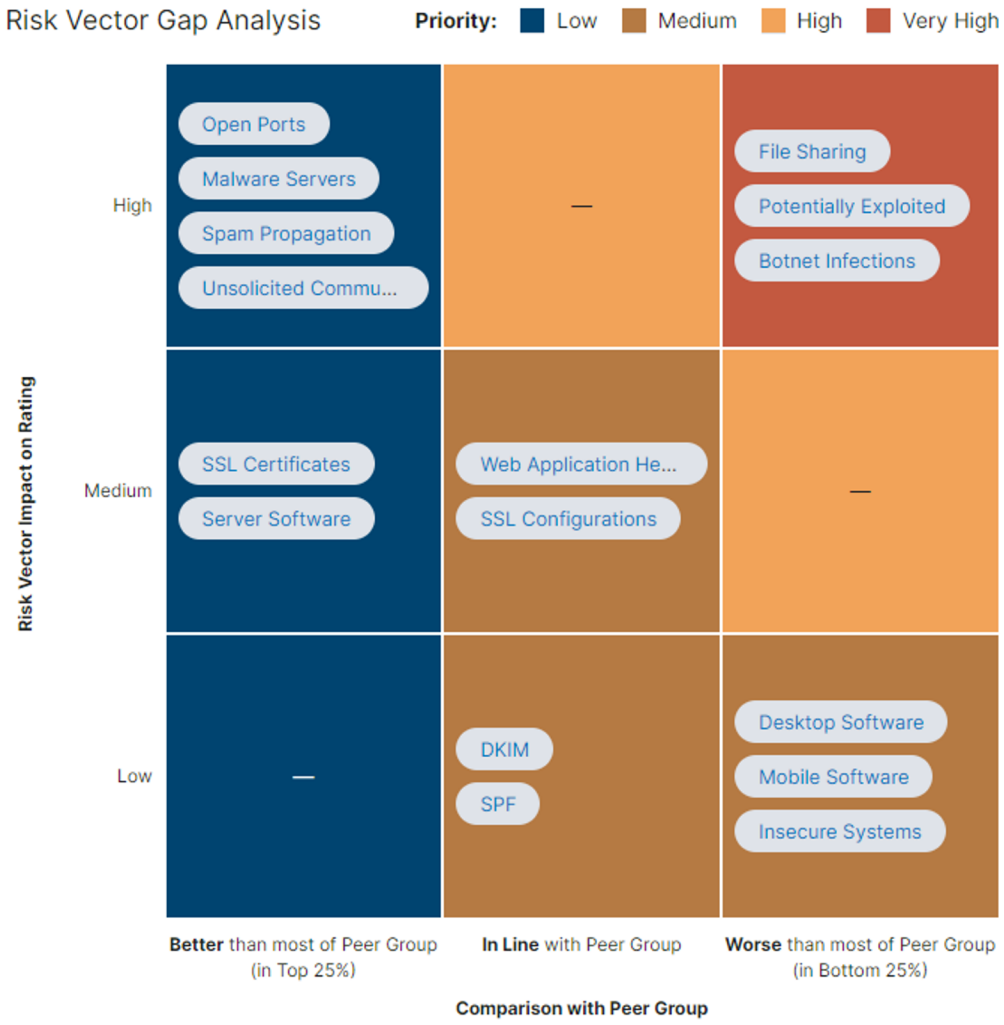
What Makes A Security Rating?

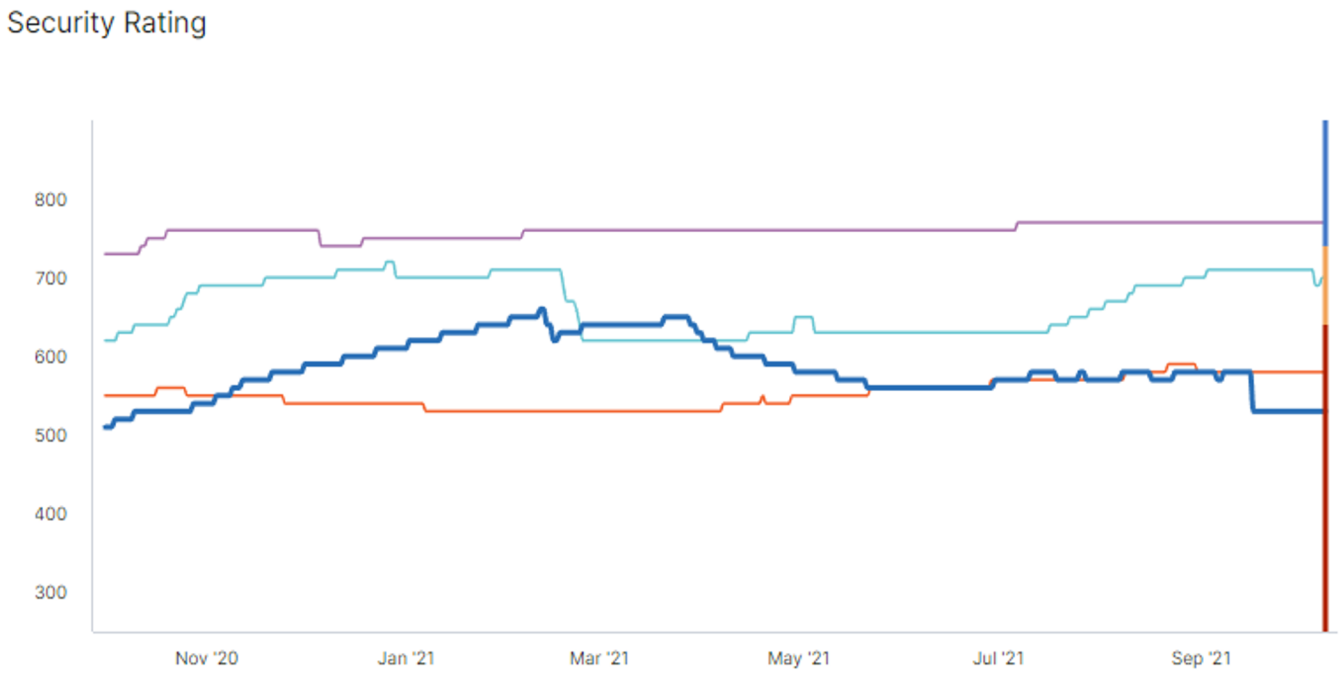


FAKE

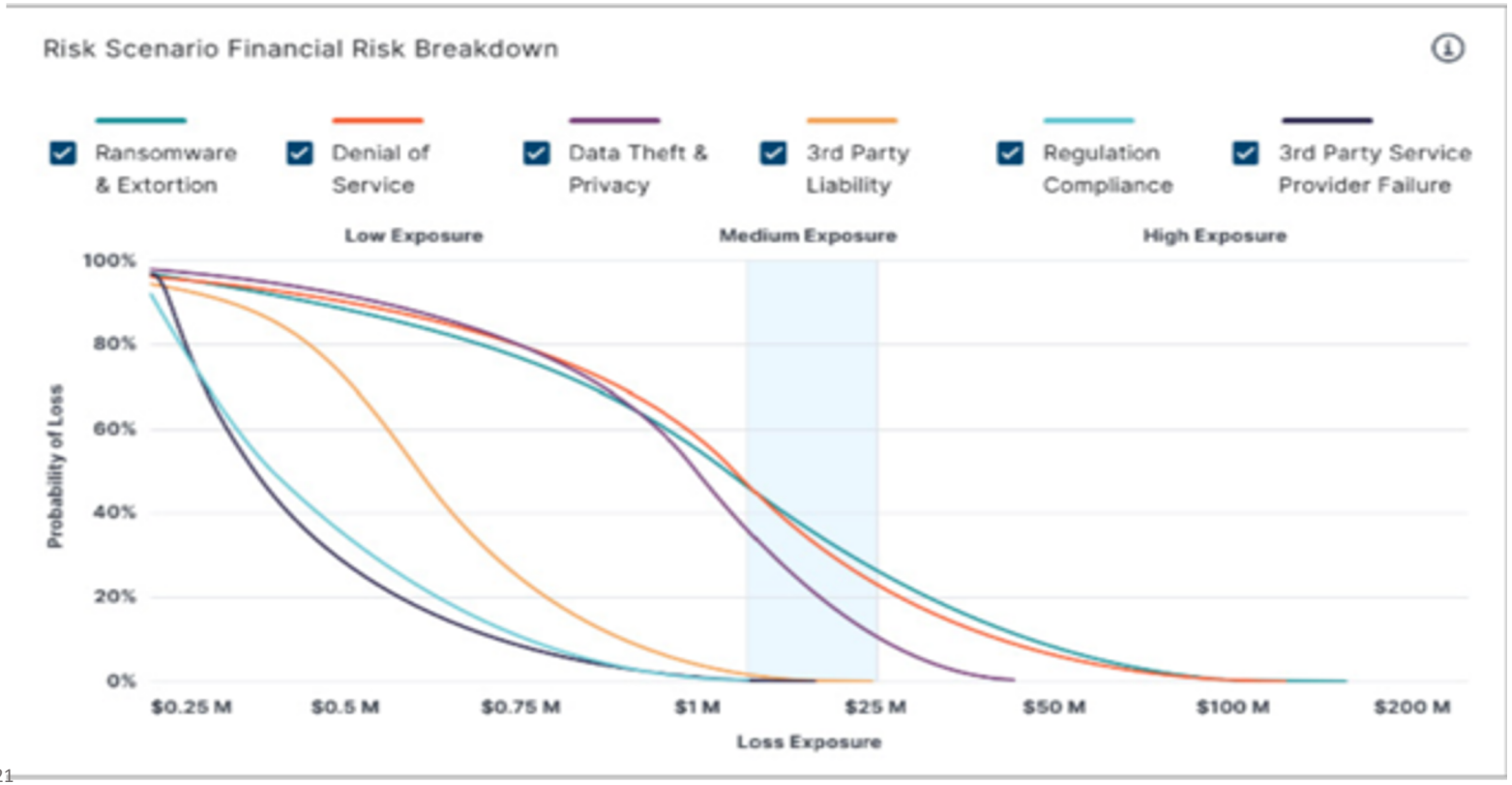
	Oct 2021	Sep 2021	Aug 2021	Jul 2021	Jun 2021	May 2021
	530	580	570	570	560	580
	630	630	630	630	630	630
Sa	670	670	670	670	670	660
Sape	710	710	710	710	720	720
Saperix - US Central	720	720	720	720	720	720
Saperix Hosting Service	720	720	720	720	720	720
Saperix Email Provider	720	720	720	690	700	720
Saperix Corporate - US East	730	730	730	730	730	730
Saperix Corporate - US West	750	750	750	750	750	750
Saperix Corporate	760	760	760	760	760	760

BITSIGHT: BENCHMARKING





BITSIGHT: QUANTIFICATION FINANCIÈRE DES CYBER-RISQUES



CYBER ASSURANCE

Cyber rating pour la cyber-assurance

Au delà des questionnaires, qui se multiplient et se complexifient, les assureurs ont besoin de mieux qualifier le risqué cyber de leurs clients.

Les assureurs s'appuient sur les agences de notation afin de déterminer l'assurabilité et évaluer les primes dans le cas de nouveaux contrats ou de renouvellements.

Agences de notation Cyber Rating

BENEFICES

OUTIL DE DECISION ET PRESSION POUR AGIR
COMPLEMENTARITÉ INTERNE / EXTERNE
EDUQUER (AU DELA DU SCORE)
VISIBILITE SUR LES ASSETS
AUTOMATISATION / API (EN COURS)

LIMITES

ABSENCE DE MODELE
FAUX POSITIFS (ASSETS, NIVEAU DE RISQUE)
CHANGEMENT DE L'ALGORITHME
PAS DE PLATEFORME UNIFIEE
ENVIRONNEMENTS « CLOUD »

CONFIDENTIALITE / SECURITE DES PLATEFORMES

CHARGE DE TRAVAIL IMPORTANTE DANS LES ENVIRONNEMENTS COMPLEXES ET ÉVOLUTIFS

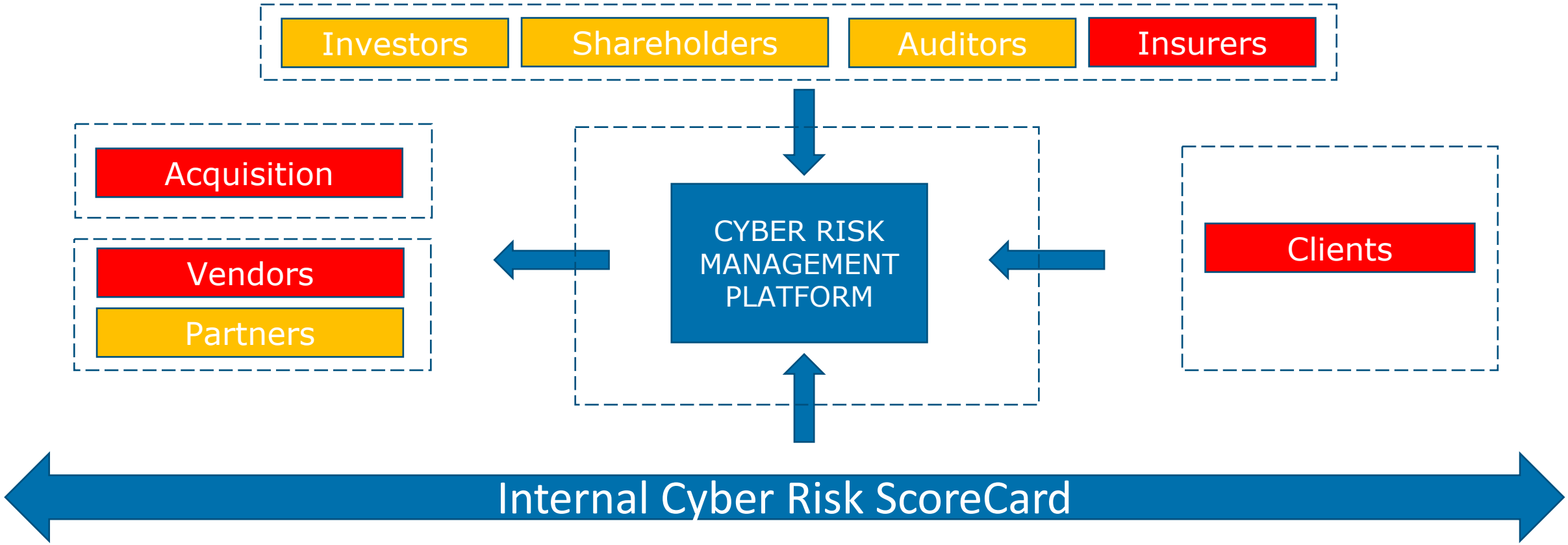
CYBER RISK INDEX

VALORISER DES INDICATEURS DE RISQUE

Face à la complexite du domaine, comment consolider des indicateurs de natures et sources variées pour caractériser un “niveau” de risqué “cyber”?

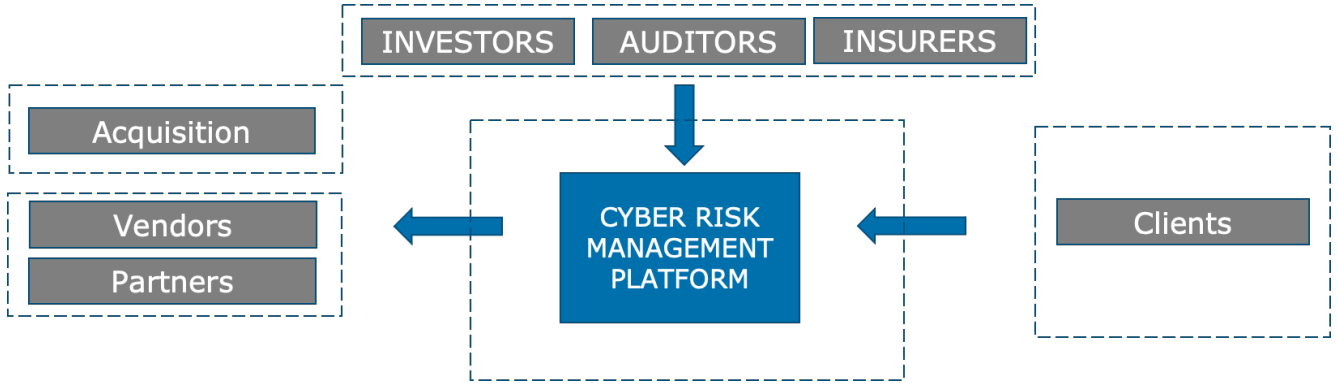
Peut-on créer un modèle qui nécessite des éléments externes et indépendants comme des éléments internes sous le contrôle de l’organisation (plus détaillés et moins transparents…) ?

UN CYBER RISK INDEX « COMPOSITE » QUI TRADUIT LA SECURITE DE L'ECOSYSTEME



Techno **H**uman Factor **E**xternal Risk **S**uppliers **Co**mpliance **P**olicy **E**nforcement

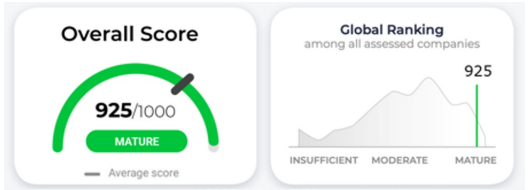
CAS 1 : FOCUS SUR LES SCORING EXTERNES (EXEMPLE)



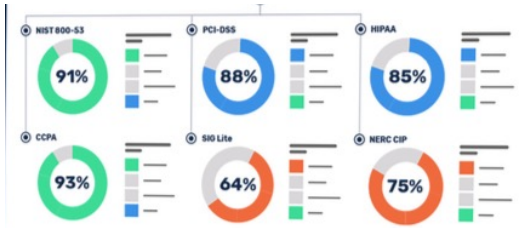
SecurityScorecard

BITSIGHT

cybervadis



CyberGRX



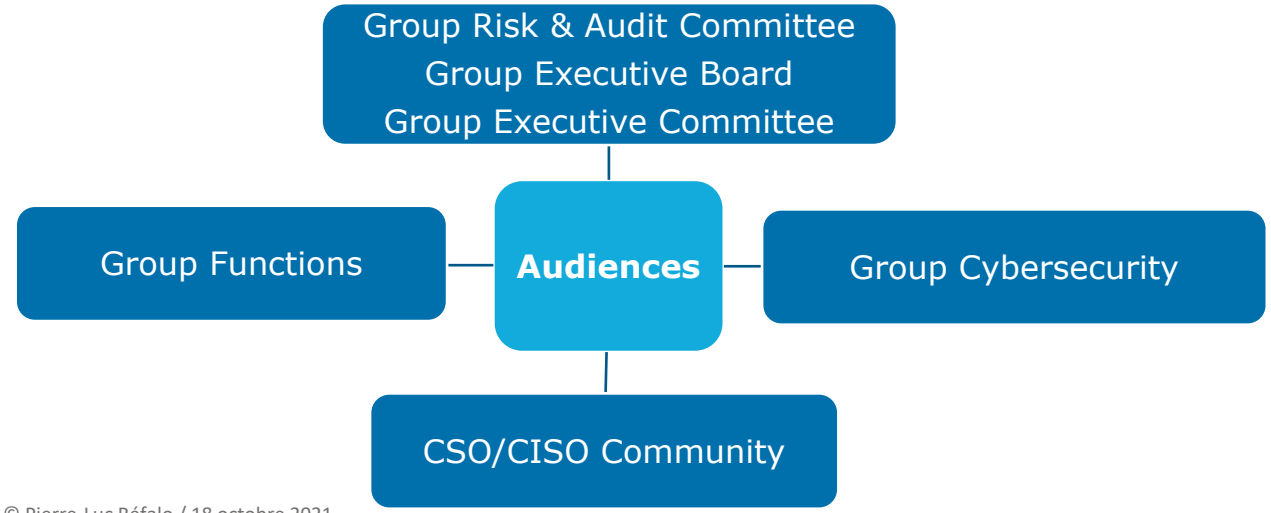
Créer son propre algorithme avec pondérations
Associer son évaluation et celle de ses fournisseurs / partenaires / acquisitions

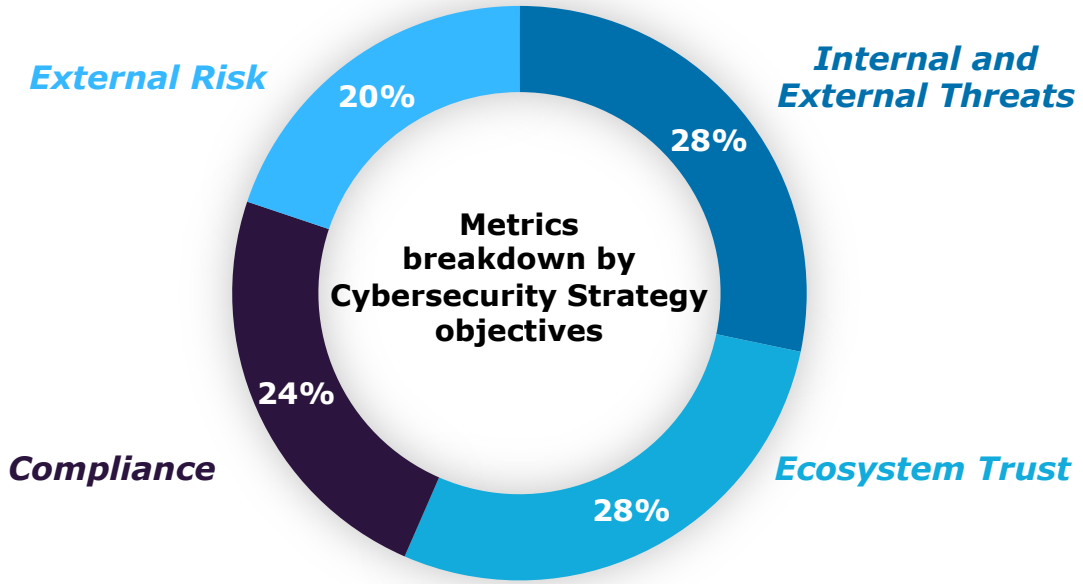
CAS 2 : CONSOLIDER DES METRIQUES DE « RISQUE » POUR REPORTING INTERNE

Internal Cyber Risk ScoreCard

Techno · Human Factor · External Risk · Suppliers · COmpliance · Policy Enforcement

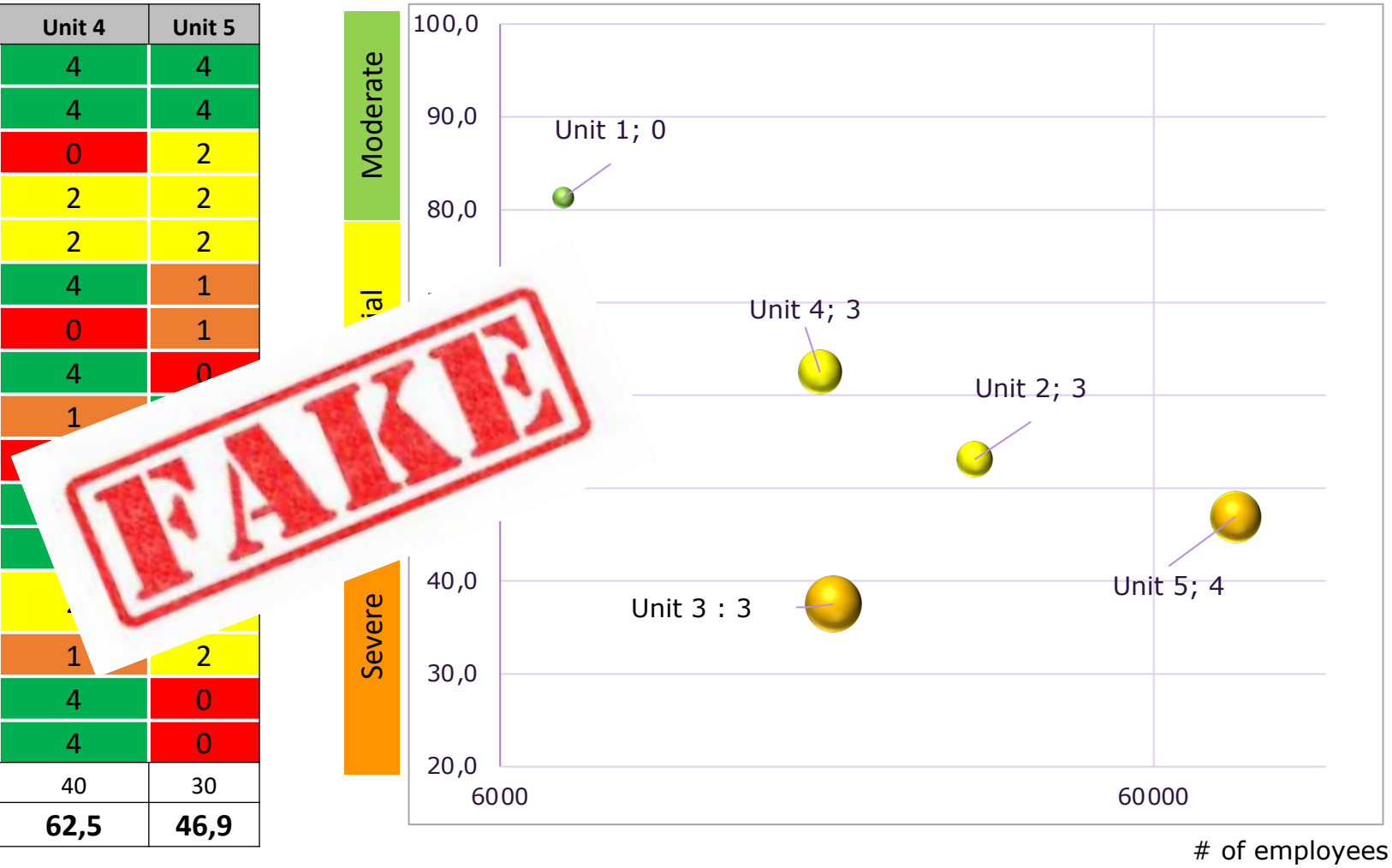
TECHNOLOGY	HUMAN FACTOR	EXTERNAL RISK	SUPPLIERS	COMPLIANCE	POLICY ENFORCEMENT
T1 Technical Debt (W2003) **T2** Technical Debt (W2008) **T3** Technical Debt (Linux)	**H1** New Joiners Awareness **H2** Phishing test (click rate) **H3** Phishing test (shared data) **H4** Local Awareness Campaigns	**E1** Platform 1 Score **E2** Platform 2 Score **E3** # of Critical issues	**S1** Third Party Security Plan **S2** # of T1 vendors at risk	**C1** Baseline score **C2** Baseline Findings **C3** Findings Duration **C4** CIS Benchmark score	**P1** Policy adoption **P2** Sites to be ISO27001 certified **P3** Contract management **P4** Projects Risk assessment



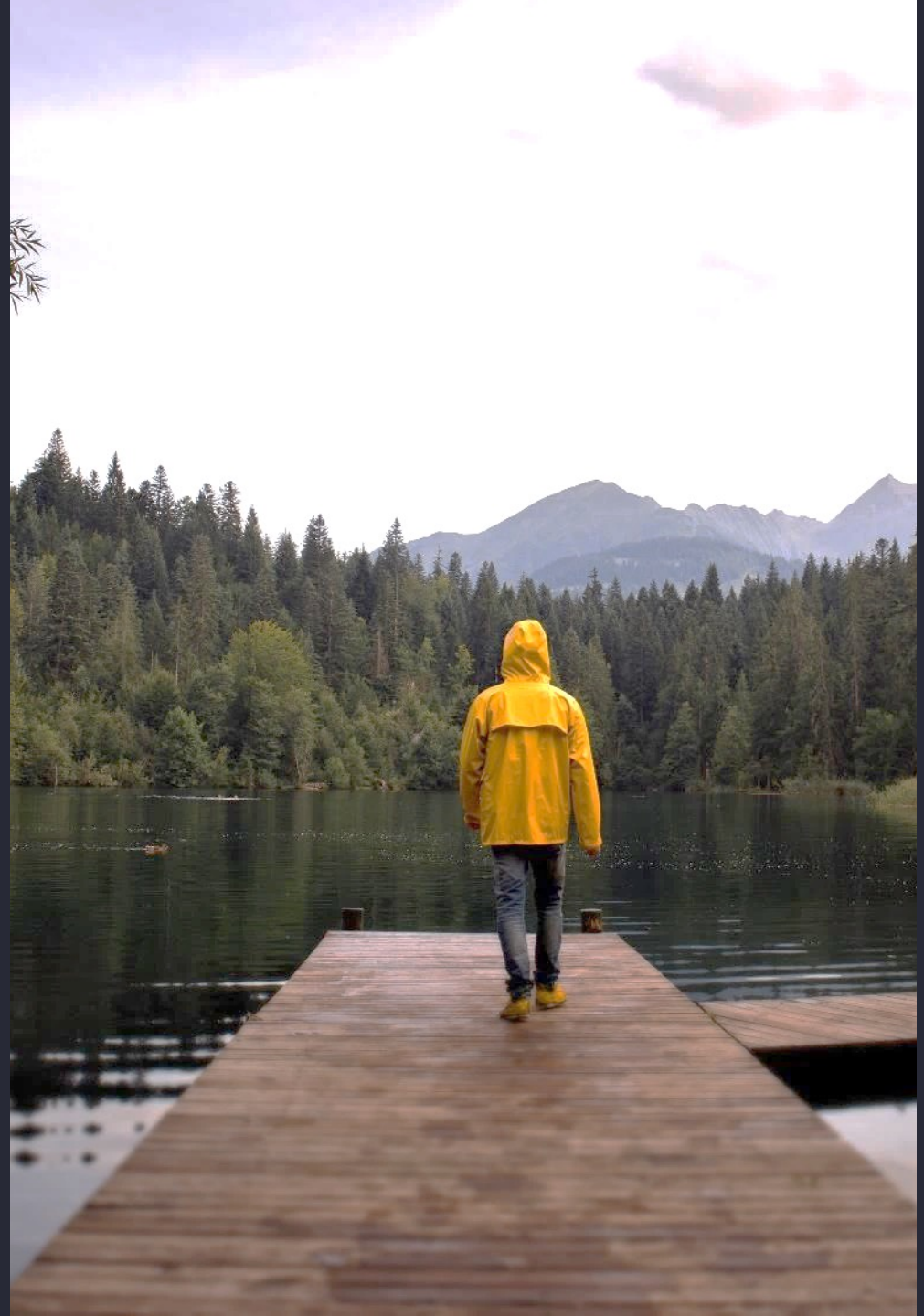


CYBER RISK INDEX INTERNE – REPORT (EXEMPLE)

Metric	Unit 1	Unit 2	Unit 3	Unit 4	Unit 5
Technical Debt W2003	4	4	1	4	4
Technical Debt W2008	4	4	4	4	4
New Joiners Awareness	4	1	1	0	2
Phishing test (click rate)	2	0	0	2	2
Phishing test (shared data)	2	1	0	2	2
Awareness campaings	4	2	0	4	1
RiskRecon P1/P2	1	2	2	0	1
RiskRecon P1-P4	2	4	2	4	0
Bitsight P1-P2	1	0	0	1	
Bitsight score	4	2	2		
Third-Party Security Plan	4	4	2		
Baseline Policy compliance score	4	2	1		
Baseline Policy compliance findings	4	2	0		
Days to remediate findings	4	1	1	1	2
Policy Adoption	4	1	4	4	0
Sites to be ISO 27001 certified	4	4	4	4	0
Total points	52	34	24	40	30
Score (%)	**81,3**	**53,1**	**37,5**	**62,5**	**46,9**



Réflexions pour 2022-2025



UN MODELE COMPOSITE

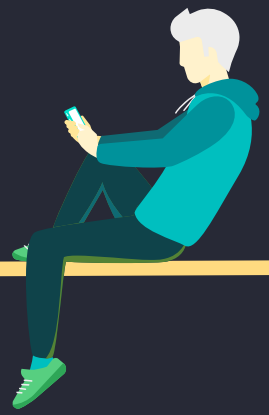
DES ACTEURS CLES

DE L'AUTOMATISATION

UN LIEN AVEC FINANCE

UN LEADER EUROPEEN ?

MERCI



prefalo

@plrefalo