LES GRANDS ENJEUX

LE SCORING CYBER

Avril 2024

CLUSIF

Table des matières

Remerciements

Le Clusif tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Les responsables du groupe de travail :

Gerulf	**KINKELIN**	CETRAC.io
Luc	**PAPADOPOULOS**	GPMSE / Crédit Agricole Protection et Sécurité

Les contributeurs :

Frédéric	**JESUPRET**	ALLIANZ
Vivian	**FROIDEVAUX**	BATIGERE
Etienne	**BUSNEL**	BESSE
Luc	**DECLERCK**	BOARD OF CYBER
Alain	**DETELDER**	BOUYGUES TELECOM
Sébastien	**VAIVRE**	CNP ASSURANCES
Nicolas	**ANDREU**	COFACE
Marek	**KUREK**	CREDIT MUTUEL
François	**SAMARCQ**	CYBER COVER
Thibaut	**LAPEDAGNE**	CYBERVADIS
Sheldon	**FRESNE**	DANONE
Hervé	**SCHAUER**	HS2
Eric	**MELKI**	INFOCLIP
Eric	**EGEA**	NTT
François	**ZAMORA**	ORANGE
Emmanuel	**MEYRIEUX**	OVHCLOUD
Pierrik	**CHAIGNAUD**	REDSIFT
Frank	**VAN CAENEGEM**	SCHNEIDER ELECTRIC
Thomas	**GAYET**	SCOVERY
Stéphane	**DEPLAT**	SDIS 77
Gilles	**RAGUY**	COVEA
Aïmad	**BERADY**	YESWEHACK

1 Introduction

La notation (cyber scoring) et l'évaluation (cyber rating) de la cybersécurité des organisations sont devenues en quelques années des incontournables de la vie des RSSI et des équipes de cybersécurité.

Les clients ou utilisateurs de ces notations et évaluations peuvent être des directions des achats qui qualifient leurs sous-traitants critiques, les assureurs qui évaluent les risques à assurer, les banques, les fonds d'investissement, et bien sûr les organisations elles-mêmes dans leur poursuite d'une maîtrise et d'une amélioration de leur cybersécurité.

Les évaluations de cybersécurité sont le résultat de questionnaires pouvant être qualifiés par des preuves, mais aussi d'audits conduits par des experts, auxquels peuvent se rajouter les notations en cybersécurité.

Les notations en cybersécurité elles-mêmes sont en général émises par des sociétés qui rassemblent le résultat de sondages systématiques, via internet, des failles des systèmes d'information des organisations et les transforment en notation par la mise en œuvre d'algorithmes qui leur sont propres. Ces notations sont parfois appelées « scoring externe ».

Si cette approche systématique peut revêtir un caractère d'objectivité, elle contribue néanmoins à plusieurs situations problématiques : note dégradée en raison de la prise en compte d'éléments non pertinents (anciennes filières, sociétés homonymes), mauvaise qualification des risques de sécurité qui dégradent l'appréciation ou encore une notation, pour une société d'hébergement, des pratiques risquées sur le plan cyber de ses clients hébergés.

Pour éviter toute confusion, nous ferons un détour initial par le cyberscore du gouvernement français, qui n'est ni une évaluation ni une notation en cybersécurité, puisqu'il considère aussi des exigences de protection des données personnelles et de souveraineté sur les données. Nous aborderons ensuite une clarification des concepts entre notation et évaluation et proposerons des pistes d'amélioration des pratiques dans le domaine de la notation cyber. Enfin, une charte de bonne conduite des acteurs sera présentée.

1.1 Le cyberscore de la loi n° 2022-309

Le cyberscore est issu de la loi française n°2022-309 du 3 mars 2022 (dite loi Lafon) et devait entrer en application au 1er octobre 2023.

Toutefois, le décret et l'arrêté d'application, pour lesquels le groupe de travail a coordonné la réponse du Clusif à la consultation publique du gouvernement en avril 2023, n'ont pas encore été promulgués à la date de février 2024. Cette loi, en s'inspirant du Nutri-Score pour l'alimentaire, a pour objectif de présenter au consommateur une certification de cybersécurité des plateformes numériques destinées au grand public. L'audit annuel permettant le calcul du cyberscore et qui porte sur « la sécurisation et la localisation des données » est pris en charge par des prestataires qualifiés auprès de l'ANSSI.

Cette certification s'applique spécifiquement à des opérateurs de plateformes en ligne et des personnes qui fournissent des services de communications interpersonnelles non fondés sur la numérotation, selon un seuil de fréquentation qui sera fixé par décret. À ce jour, une proposition de critères d'audit est en cours d'étude, et les méthodes d'audit associées n'ont pas encore été publiquement évoquées.

1.2 Notation en cybersécurité et évaluation en cybersécurité

1.2.1 Distinguer notation et évaluation

Il est essentiel de clarifier les différences entre notation et évaluation en cybersécurité, deux approches distinctes et complémentaires pour évaluer les risques en cybersécurité, comparable aux pratiques en vigueur dans le domaine de la notation financière.

La notation en cybersécurité s'appuie sur un modèle de calcul automatique et statistique pour mesurer le niveau de risque. Cette méthode repose sur un algorithme qui analyse et traite les données recueillies sans intervention humaine. La notation en cybersécurité évalue le risque en se fondant sur plusieurs paramètres, tels que la présence de vulnérabilités, la configuration des systèmes ou encore les incidents de sécurité antérieurs.

L'évaluation en cybersécurité résulte quant à elle d'une analyse menée par un expert en cybersécurité qui prend en compte des données quantitatives et qualitatives, dont notamment la notation en cybersécurité. Cette méthode requiert l'intervention humaine et permet une évaluation plus contextualisée des risques selon l'orientation recherchée, par exemple la sensibilité d'une organisation à un risque donné. L'analyste examine divers facteurs, tels que les politiques de sécurité, les processus internes, la sensibilisation des employés ou encore les résultats des audits externes. L'évaluation en cybersécurité implique généralement l'utilisation de questionnaires de sécurité, la réalisation d'audits et l'analyse de leurs résultats.

La notation en cybersécurité se veut ainsi d'offrir une notation en continu, rapide et automatisée, du risque en cybersécurité, tandis que l'évaluation en cybersécurité se propose de réaliser une analyse ponctuelle, plus approfondie et personnalisée, en tenant compte des aspects qualitatifs et contextuels tels que les risques spécifiques à une organisation et produisant une évaluation sur plusieurs axes.

1.2.2 Diversité des besoins et des acteurs

Bien que distinctes, les différentes méthodes utilisées par la notation en cybersécurité et l'évaluation en cybersécurité peuvent donc se compléter selon les besoins, afin de fournir une vision adaptée du niveau de risque en cybersécurité pour une entreprise.
L'évaluation en cybersécurité répond donc à des besoins divers, de la part de différents acteurs :

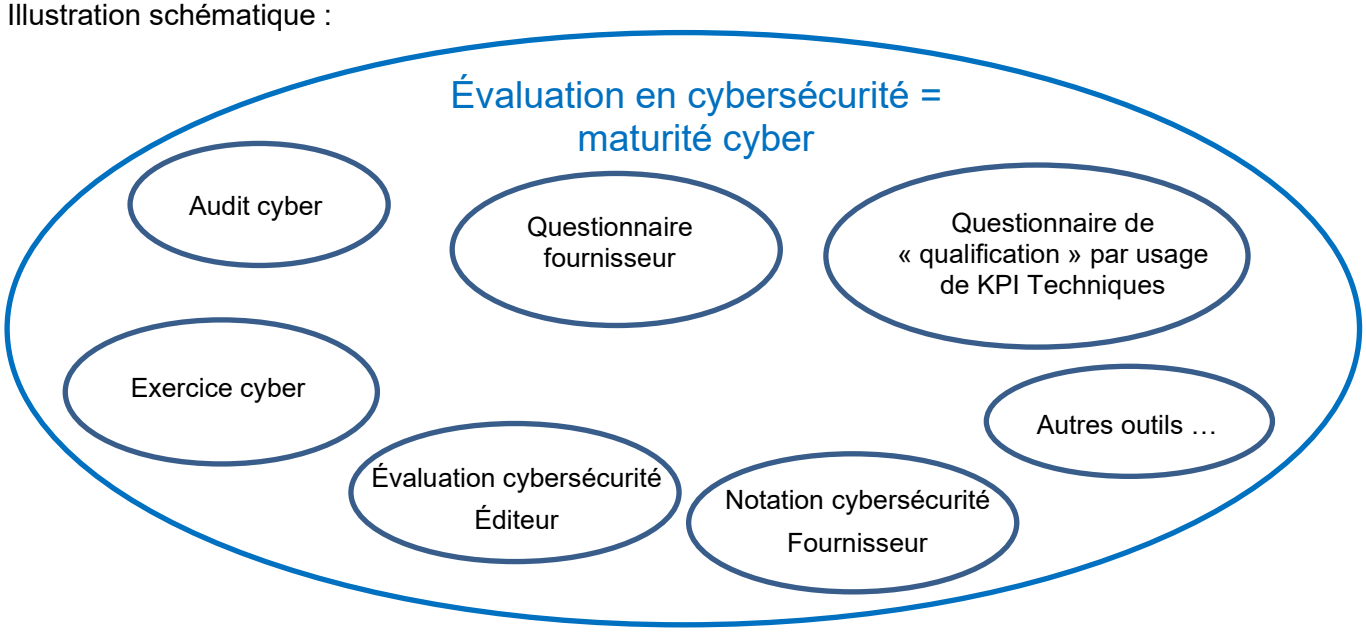
- Autoévaluation : connaître la solidité de mes défenses et rendre compte des évolutions (pour le RSSI, DSI et DG), protéger de manière proactive mon SI, mais aussi mon image.
- Évaluation des tiers partenaires et fournisseurs :
    - Même si le SI de l'organisation est correctement protégé, il est connecté à des centaines, des milliers ou dizaines de milliers de fournisseurs, partenaires, etc., tous potentiels vecteurs d'attaque (60% des piratages passent par un tiers). Les tiers partagent également des données de l'entreprise, dont des données personnelles.
    - Les tiers non connectés peuvent également, à travers des incidents IT à leur niveau, avoir un fort impact opérationnel, en répercussion des perturbations de leurs propres opérations sur la *supply chain*.
- Inversement, la note issue de la notation en cybersécurité et sa stabilité peuvent être un facteur différenciant sur le marché.
- Assurance cyber : un marché porteur au risque mal maîtrisé car trop récent. Les assureurs utilisent des outils de notation en cybersécurité et des questionnaires déclaratifs pour évaluer le risque à couvrir.

- Fusions-acquisitions : à performances commerciales, financières, technologiques égales, une entreprise mieux protégée a une plus grande valeur. La cybersécurité a aussi un impact direct sur la valeur du capital immatériel de l'entreprise.

L'évaluation en cybersécurité correspond à la terminologie « maturité cyber » qui est utilisée dans le document de référence « EBIOS Risk Manager » édité par l'Agence nationale de la sécurité des systèmes d'information[1]. La maturité cyber d'une organisation est l'appréciation de sa capacité à anticiper, éviter et surmonter une attaque cyber. Elle est évaluée par l'utilisation de différents outils, du plus simple au plus sophistiqué.

Associée aux trois autres critères de la méthode EBIOS qui sont « dépendance », « pénétration » et « confiance », la maturité cyber permet de déterminer une valorisation du « niveau de menace » que représente une organisation.

Illustration schématique :



1.2.3 Les différentes façons d'évaluer la maturité en cybersécurité

Quelles sont les différentes méthodes pour évaluer une maturité en cybersécurité ?

- Audit : la méthode la plus exhaustive est bien sûr un audit sur site avec contrôle de l'ensemble des outils, méthodologies, implémentations. Il s'agit d'une démarche limitée à de grandes entreprises opérant dans des secteurs critiques, car longue et très onéreuse.
- Questionnaires : l'entreprise développe un questionnaire qui lui est souvent propre mais peut reposer sur certains standards (NIST, par exemple) et le soumet au tiers qu'elle souhaite évaluer :
  - Gestion généralement manuelle (échanges de fichiers Excel).
  - Beaucoup de temps à investir pour les deux parties (dépouillements pour les uns, réponse à des questionnaires multiples pour les autres).
  - Déclaratif (la fiabilité des réponses est limitée) ou avec collecte de preuves.

[1] Ebios Risk Manager, version 1.1 – Janvier 2019 / Le Supplément / Fiche Méthode 5 / Page 28

- Questionnaires éditeur avec revue de preuve : l'éditeur de la solution développe son questionnaire générique pour tous ses clients, se charge des contacts avec l'entreprise interrogée et vérifie les preuves qui sont exigées face à chaque réponse :
    - Meilleure fiabilité que le questionnaire simple.
    - Gain de temps dans le cas où le questionnaire repose sur un standard éditeur de fait.
    - Démarche favorisant une standardisation du questionnaire, car les entreprises notées peuvent partager leurs notes avec d'autres clients/partenaires.
- Outils de notation externe, qui reposent tous sur le même principe :
    - Établissement de l'inventaire IP de l'entreprise (manuel ou par algorithme).
    - Déploiement de capteurs sur le Net qui capturent les informations relatives aux adresses IP.
    - Classement, remédiation, pondération pour obtenir une note par type de vulnérabilité (santé DNS, fréquences de mise à jour…).
    - Ajout éventuel d'informations externes (scan du dark web, ingénierie sociale…).
    - Calcul d'une note globale par algorithme éditeur propriétaire.

1.2.4 Spécificités et enjeux de la notation externe

Les spécificités identifiées de la notation externe (souvent au cœur de la notation cyber) sont les suivantes :

- Notation automatique et continue (par opposition aux questionnaires et audits).
- Non intrusif : sans autorisation préalable de l'entreprise notée et a priori sans risque d'impact technique sur l'organisation auditée.
- Un grand nombre d'entreprises notées (près de 20 millions).
- Un bon coefficient de corrélation entre les notes obtenues et la fréquence des attaques.
- Ne rend compte que de la partie externe du SI, aucunement de la sécurité du SI interne ou de la gouvernance, par exemple.
- L'inventaire IP est d'autant moins précis que la structure notée est complexe (faux positifs et faux négatifs) et qu'il n'a pas été mis fréquemment à jour.
- Les algorithmes de notation peuvent être opaques, sans transparence et évolutifs : le score ne peut pas toujours être expliqué facilement.
- Pas d'approche unifiée : les scores des différents acteurs sont indépendants et ne peuvent donc être comparés.
- Le score repose sur la collecte d'informations de toute nature, les attributions aux organisations peuvent être erronées ou arbitraires.
- Ces sociétés sont presque toutes américaines : des questions peuvent se poser sur les enjeux de confidentialité et de souveraineté.
- Le modèle en place peut contraindre les organisations à payer pour reconfigurer leur périmètre et améliorer leur score.

1.2.5 Les points d'amélioration à apporter à l'évaluation cyber et à la notation cyber

Plusieurs points problématiques ont été relevés chez les grands acteurs du domaine de la notation cyber. Pour chacun, nous proposons une piste d'amélioration :

- Métriques opaques sans transparence => besoin d'un score explicable.
- Approche opérationnelle de collecte d'informations techniques de toutes natures et attributions parfois hasardeuses à des organisations => besoin d'une procédure de correction rapide et gratuite.
- Business model contraignant les organisations avec des scores faibles à payer pour configurer plus précisément leurs périmètres et donc jouir d'un meilleur score.

En résumé, les problèmes posés par l'évaluation cyber (qui inclut la notation cyber) telle que pratiquée aujourd'hui sont pour l'essentiel de deux natures :

- Questionnaires d'évaluation demandés par les assureurs, les donneurs d'ordre… Ces

questionnaires sont de plus en plus longs et complexes, de plus, chaque acteur a tendance à développer le sien. Ceci occasionne une perte de temps et d'énergie importante pour un certain nombre d'acteurs, en particulier les RSSI.

- Évaluations par l'extérieur de la surface d'attaque par Internet, proposés par un certain nombre d'acteurs du marché : si ces opérateurs peuvent communiquer sur certaines des vulnérabilités rencontrées, leur algorithme de notation est en général secret et peut varier plusieurs fois par an. En outre, ces évaluations dépendent fortement de l'attribution retenue (par exemple, des fournisseurs de cloud qui se voient attribuer le périmètre de leurs clients). Il en résulte des biais à différents niveaux qui peuvent être très préjudiciables (notamment pour les RSSI qui sont amenés à rendre des comptes sur les notes émises), ainsi qu'un modèle d'affaires qui ressemble à un péage imposé qui n'est pas forcément ni légitime ni souhaitable, modèle qui risque d'être de plus en plus pénalisant à l'avenir, dans la mesure où le recours à la notation cyber des tiers est une pratique en voie de généralisation.

L'objectif d'une standardisation partielle ou totale des pratiques de l'évaluation cyber pourra être de mieux maîtriser les effets pervers tels qu'évoqués ci-dessus :

- Dans le cas des listes : en les simplifiant et en les standardisant pour permettre leur réutilisation.
- Dans le cas de la notation cyber : en édictant des règles de fonctionnement telles que des critères de transparence, de confidentialité, de pratiques commerciales… Aspects qui seront développés dans la charte proposée ci-dessous.

En l'état actuel, les questionnaires peuvent comporter un millier de questions et différent grandement les uns des autres. Ils portent sur l'organisation, les process, les pratiques, les architectures et technologies déployées. Le besoin d'un standard d'évaluation cyber vise donc à rendre les évaluations comparables entre elles et explicables, tout en évitant de devoir perdre des ressources à satisfaire des formats différents.

Le besoin qui croît aujourd'hui est celui de l'évaluation de parties tierces (third party assessement) que les grandes organisations déploient pour mieux maîtriser le risque provenant de la supply chain.

2 État des lieux mondial des acteurs

Le tableau ci-dessous représente un inventaire non exhaustif des acteurs de l'évaluation et de la notation en cybersécurité, il permet de constater en un coup d'œil que les acteurs européens et français ne sont pas les plus nombreux sur le sujet.

Nom	Pays d'origine
Allgress	US
Aravo	US
Archer	US
Bitsight	US
Black Kite	US
BoardOfCyber	FR
Certa	US
Coupa	US
Cyber Cube	UK
Cyber Essentials	US
CyberGRX	US

CyberVadis	FR
CyRating	FR
Diligent	US
Graphite Systems	US
Logic Gate	US
Logic Manager	US
OneTrust	US / UK
Panorays	US / IL
Prevalent	US
ProcessBolt	US
Scovery	FR
SecurityScoreCard	US
ServiceNow	US
SIG	US
SureCloud	UK
ThirdPartyTrust	US
Upguard	AU
Venminder	US
Whistic	US

3 Amélioration des pratiques des acteurs de la notation cyber

Le GT s'est inspiré des pratiques qui se sont développées dès les années 2000 pour les agences de notation financières (des chartes à des réglementations contraignantes) puis des actions plus récentes de la Commission européenne pour mieux maîtriser les activités des agences de notation ESG (environnement, social, gouvernance) censées refléter le niveau de responsabilité sociétale des organisations.

La vocation de cette charte n'est pas d'être contraignante mais de viser à servir de canal d'expression pour la filière, selon un principe de libre adhésion.

Elle vise plus largement à promouvoir un cercle vertueux autour de plusieurs principes : confiance entre les acteurs de la notation, dynamique d'amélioration des pratiques, recherche d'une méthodologie transparente et explicable, capacité des RSSI à s'approprier les résultats de la notation…

4 Charte de bonne conduite des acteurs de la notation

- La typologie des actifs traités (adresses IP, noms de domaines…) par chaque agence de notation doit être décrite et accessible aux utilisateurs de la notation et aux organisations notées.
- Le référentiel de notation (points de contrôle…) doit être accessible aux utilisateurs de la notation et aux organisations notées.
- L'interaction entre l'acteur de la notation et l'organisation notée ne doit pas être conditionnée à une relation commerciale.
- L'organisation doit pouvoir :
    - accéder à la cartographie des actifs inclus dans la notation avec les explications associées aux défaillances ;
    - demander la modification de la cartographie / du périmètre, si nécessaire, avec une correction effectuée dans un délai objectif de 10 jours.
- Un acteur qui émet une notation sur une organisation doit préciser si le périmètre pris en compte est reconnu comme représentatif par l'organisation notée et à quelle date (ce qui augmente l'indice de confiance).
- La logique de l'algorithme de notation et la pondération doivent être identiques, quelles que soient les organisations notées.
- Le système d'information mise en œuvre par l'agence de notation doit faire l'objet d'une certification en cybersécurité par un tiers.
- La référence de l'algorithme de notation utilisé pour établir une note doit accompagner la note émise.
- Tout changement majeur du système de notation (modification de l'algorithme, référentiel de notation…) devrait être communiqué et accessible a minima aux clients et aux organisations surveillées 3 mois à l'avance (un préavis plus faible pouvant être justifié par la prise en compte d'une menace nouvelle), avec si possible une phase de superposition des notations initiales et nouvelles pendant une période de 6 mois.
- Les agences de notation s'engagent à répondre de manière appropriée aux sollicitations techniques des organisations scrutées, en particulier pour les levées de doute (adresses IP utilisées).

Campus Cyber
5 rue Bellini
92821 Puteaux cedex
France
✆ +33 1 53 25 08 80
clusif@clusif.fr

clusif.fr