Réflexions des établissements financiers du

Forum des Compétences

Cyber-rating

Une étude menée avec

THALES

I. Introduction

A. De l'intérêt du cyber rating

Le cyber rating est fréquemment présenté comme étant le Graal permettant d'évaluer le niveau de maturité cyber de n'importe quelle organisation, indépendamment de sa taille, du marché sur lequel elle opère, et de son industrie.

De nombreux acteurs se sont emparés du sujet parmi lesquels figurent à la fois des acteurs historiques de la notation, comme les agences de notation financière (*Moody's, Fitch* ou encore *Standards & Poors*) mais aussi de nouveaux acteurs (*Bitsight*, *Security Scorecard, Trusight, etc.*). Tous se disputent un marché en très forte croissance alimenté à la fois par des cyber attaques de plus en plus fréquentes, une réglementation renforcée et une volonté de la part des *top management* d'avoir des rapports clairs et visuels sur leur niveau d'exposition face à la menace.

En plus de ces 3 éléments qui favorisent l'essor du cyber rating, de nombreux cas d'usages peuvent être évoqués lorsque l'on parle d'évaluation cyber au sens large :

- Une boite à outils pour le RSSI :
  - Permet à un RSSI qui prendrait son poste d'avoir rapidement un premier avis sur le niveau de maturité cyber du système d'information dont il a la charge.
  - Favorise également la comparaison avec d'autres acteurs du même secteur.
  - Enfin, permet de suivre les progrès de son système d'information dans le temps et ainsi informer ou rassurer des parties prenantes (régulateurs, partenaires, clients, actionnaires, etc.).
- La cyber assurance :
  - Permet de définir le montant d'une police d'assurance basé sur une évaluation du risque cyber encouru par l'entité à assurer.
- La cyber due diligence :
  - Permet d'identifier le niveau de risque encouru d'un point de vue cyber sécurité lors d'une opération de fusion ou d'acquisition.
- Le raccordement de nouveaux systèmes d'information :
  - Permet d'identifier les faiblesses avant « l'ouverture des vannes ».

Pour beaucoup aujourd'hui le terme cyber rating se limite à ce qui pourrait s'apparenter à de l'OSINT (Open Source Intelligence) ou la recherche d'informations sur sources ouvertes en français.

Cependant, il existe d'autres moyens de déterminer le niveau de maturité cyber. Quelles sont ces approches ? Comment fonctionnent-elles ? Quels sont leurs avantages, leurs inconvénients et surtout sont-elles toutes réellement pertinentes ?

Ce livre blanc a trois objectifs :

- Alerter sur les limites du cyber rating lorsqu'il se limite à de l'OSINT.
- Apporter un éclairage sur d'autres approches permettant d'évaluer le niveau de maturité cyber d'une organisation.
- Et surtout alimenter la réflexion sur le cyber rating tel qu'il existe.

II. Les différentes approches d'une évaluation cyber

A. Analyse de sources ouvertes (OSINT en anglais)

Fonctionnement

Le cyber rating basé sur l'OSINT consiste à collecter des informations à partir de sources ouvertes (Internet, Deep Web, Dark Web). Cela permet, par exemple, de détecter les fuites de données ou de scanner rapidement de façon périmétrique l'état de sécurité d'un SI. C'est la méthode d'évaluation privilégiée par de nombreux nouveaux acteurs. En général, ces solutions cartographient l'ensemble des IP publiques d'une entreprise et scannent ensuite les actifs techniques associés à ces IP pour relever des traces de compromissions et d'activités malveillantes. La configuration de ces actifs est ensuite testée pour enfin agréger l'ensemble de ces résultats dans une seule et même note détaillée au travers d'un ensemble d'indicateurs.

Cependant, du fait de l'absence de mandat d'audit, les données observées ne proposent la plupart du temps qu'une vue parcellaire du SI, la note ainsi obtenue est donc souvent loin de la réalité. De plus, cette note dépend grandement de l'exposition d'une entreprise sur Internet. En effet, une startup qui n'a qu'une adresse IP publique aura plus de facilité à avoir une bonne note alors que des grands groupes très exposés sur Internet auront un périmètre beaucoup plus vaste à couvrir, et donc plus de chances d'avoir une mauvaise note.

Avantages

- Pas de mandat d'audit nécessaire.
- Rapide.
- Automatisé.
- Relativement bon marché pour la vision « big picture ».
- Capacité à dégager des tendances dans le temps.
- Possibilité de se comparer par rapport à d'autres acteurs de l'industrie.
- Résultats visuels et synthétiques.

Inconvénients

- Opacité des critères de notation.
- Vue « iceberg » uniquement.
- Contrainte pour l'audité de définir le périmètre d'analyse.
- Fiabilité de la notation très dépendante de l'exposition sur internet.

Cette approche parait-elle pertinente pour évaluer de manière représentative le niveau de maturité cyber d'une organisation ?

Les solutions présentes sur le marché qui reposent sur cette approche produisent une note quantifiable à l'issue de leurs analyses qu'elles restituent au travers de rapports clairs et intelligibles. L'agrégation des résultats en une seule note et la présence de rapports clairs constituent les points forts de ces solutions et expliquent en partie leur succès.

Pour autant, la communauté cyber est relativement unanime sur les défauts de ce type de solution : la vue n'est que parcellaire, les indicateurs utilisés ne sont pas toujours les plus pertinents, et les algorithmes de notation parfois opaques…

Pour ces raisons, **l'OSINT, à elle seule ne suffit pas pour dresser un portrait cyber complet d'une organisation.**

B. Les questionnaires d'auto-évaluation

Le moyen le plus répandu actuellement pour évaluer le niveau de maturité cyber d'une organisation ou d'une entité repose sur l'envoi d'un questionnaire.

Fonctionnement

Ces questionnaires reposent la plupart du temps sur des référentiels connus tels que la norme ISO/CEI 27001, le NIST américain ou encore sur COBIT Security Framework. Ils couvrent en général de nombreux aspects de la sécurité (sécurité des infrastructures, sécurité physique et environnementale, contrôle d'accès logique, sécurité des tiers, etc.). Pour autant, aucun questionnaire n'a réussi à s'imposer comme référence ultime et la plupart des grosses organisations disposent de leur propre questionnaire.

Avantages

- Facile à mettre en œuvre.
- Pratique répandue.
- Peu couteux (en termes numéraire).
- Permet d'obtenir des informations internes à l'entreprise, tant d'un point de vue technique, qu'organisationnel (fonctionnement interne)

Inconvénients

- Chronophage à la fois pour le créateur et pour le répondant.
- Niveau de fiabilité discutable dans le cas des questionnaires uniquement déclaratifs (sans vérification de preuve).
- Pas de possibilité de se comparer (car les questionnaires ne sont pas identiques pour tous).
- Objectivité non garantie

Cette approche parait-elle pertinente pour évaluer de manière représentative le niveau de maturité cyber d'une organisation ?

L'approche, bien que facile à mettre en œuvre, montre de nombreuses limites :

- Les questionnaires doivent régulièrement être mis à jour pour intégrer nouveaux enjeux (technologiques, réglementaires, etc.).
- Un temps conséquent est nécessaire pour l'analyse des réponses :
    - Le temps à allouer au remplissage des différents questionnaires est également conséquent pour les organisations : certains questionnaires regroupent plus d'une centaine de questions. A titre d'exemple, si un questionnaire comporte environ 100 questions et que 3 minutes sont nécessaires pour répondre à chacune des questions, il faut 300 minutes soit 5 heures pour répondre à un questionnaire. En partant du principe qu'un RSSI reçoive 1 questionnaire par semaine sur 44 semaines, il faut allouer en une année de travail 220 heures soit un peu plus de **31 jours travaillés par an** (calculé pour une journée de travail de 7h) !

Par ailleurs, le questionnaire revêt par nature un aspect déclaratif et il apparait fondamental de mettre en place une vérification des preuves et des contrôles pour s'assurer de la véracité des réponses.
Enfin, dans une logique de rating, et donc d'évaluation, il apparait compliqué de mettre en place un système de notation basé sur des questionnaires, dans la mesure où chaque questionnaire est différent : la comparaison entre deux entités soumises à deux questionnaires différents est donc impossible.
À elle seule, **cette approche ne constitue donc pas un moyen suffisant pour juger du niveau de maturité cyber d'une organisation.**

Afin de capitaliser sur les forces de cette approche et d'en diminuer les limites, il pourrait être intéressant de définir un unique questionnaire d'évaluation cyber qui soit commun à la place bancaire et assurantielle. En effet, cela permettrait à la fois un gain de temps conséquent pour les répondants, et en même temps de s'assurer de disposer d'un outil puissant, car financé par plusieurs organisations.

Pour autant, il est parfois compliqué de disposer d'un unique questionnaire au sein d'une même organisation (chaque filiale ayant ses spécificités), il semble donc compliqué de réussir à ce que plusieurs banques ou assurances arrivent à se mettre d'accord pour établir un seul questionnaire.

Afin de remporter l'adhésion, l'outil devra au minimum :

- Etre disponible en mode *Saas*[1] et en même temps proposer la possibilité d'être *on-premise*[2]. (afin de garantir la confidentialité des données notamment).
- Etre basé sur les principaux référentiels de sécurité.
- Fonctionner sous forme de questionnaire à tiroirs, avec une version light et une version plus détaillée.
- Disposer d'une possibilité de télécharger (et faire valider) les preuves.

De plus, une adoption et un sponsoring par une ou plusieurs grandes organisations constitueraient un avantage conséquent.

[1] *Software As A Service : modèle d'exploitation commerciale des logiciels dans lequel ceux-ci sont installés sur des serveurs distants.*
[2] *On-premise : modèle d'exploitation commerciale des logiciels dans lequel ceux-ci sont installés sur des serveurs de l'utilisateur.*

C. Analyse basée sur des composants techniques

Fonctionnement

Cette méthode consiste à déployer un ou plusieurs composants techniques au sein du SI interne d'une organisation afin de surveiller les équipements (réseaux, serveurs et postes de travail notamment) et détecter des comportements anormaux et des potentielles compromissions. De tels composants sont généralement déployés sur les points critiques du réseau.

Avantages

- Délivre une vue factuelle quant à la gestion des évènements de sécurité.
- Permet de traiter des périmètres à très grande échelle.
- Est automatisé.

Inconvénients

- N'explicite pas forcément les pratiques et les comportements humains.
- L'efficacité est fortement corrélée au paramétrage (qui est, par ailleurs, chronophage).
- Nécessite de tourner un certain temps pour fournir des résultats pertinents.
- Nécessite l'intrusion dans le système de celui dont on veut connaitre le niveau de maturité

Cette approche parait-elle pertinente pour évaluer de manière représentative le niveau de maturité cyber d'une organisation ?

Dans le cadre d'un cyber rating, cette approche est pertinente grâce au vaste périmètre qu'elle couvre. De plus, c'est une analyse de l'intérieur contrairement au deux approches précédentes, les résultats sont donc factuels et justifiés.

Pour autant, les composants techniques utilisés tels que les sondes nécessitent d'être bien paramétrés et les résultats sont difficiles à synthétiser dans une note unique. Il est laborieux de produire une note avec cette approche seule car elle est basée sur la détection de compromission. Le résultat est binaire : si oui ou non, il y a une attaque en cours.

On peut alors imaginer que la présence de composants techniques bien configurés au sein du SI contribuerait à améliorer la maturité cyber d'une entreprise. Cependant, il reste encore à définir un moyen de quantifier une note à partir de cette approche.

Bien que cette approche semble être fiable, car basée sur une analyse factuelle, **elle ne se suffit pas à elle-même dans un cyber rating** car elle ne prend que partiellement en compte le facteur humain.

Cependant, le développement de cette approche semble inéluctable, la Loi de Programmation Militaire pousse ainsi les organismes d'importance vitale (OIV) à se doter de sondes pour surveiller leurs réseaux.

D. Les audits indépendants

Fonctionnement

Il existe une multitude de types d'audit pour évaluer la sécurité d'un SI :

- Test d'intrusion.
- Audit de code.
- Audit de configuration.
- Audit organisationnel et physique.
- Etc.

Ces audits peuvent être soit réalisés dans une logique d'autocontrôle, soit réalisés par des tiers (qu'ils soient internes à l'organisation ou non, comme ce peut être le cas avec les Inspections Générales des banques).

Ces audits ont pour but d'évaluer la sécurité, la résilience ou encore l'organisation d'un SI.

Avantages

- Font l'objet de constats étayés par des preuves.
- Indépendance

Inconvénients

- Un même périmètre audité par deux auditeurs différents ne fera pas forcément l'objet des mêmes constats.
- Couteux car nécessitent d'être réalisés par des auditeurs.
- Ne peuvent être réalisés sur des périmètres trop vastes.

Cette approche parait-elle pertinente pour évaluer de manière représentative le niveau de maturité cyber d'une organisation ?

Une analyse via un audit sur un périmètre donné est un bon moyen de déterminer la maturité de celui-ci. Les résultats sont étayés de preuves et sont factuels cependant une telle approche est couteuse car elle nécessite l'intervention d'auditeurs.

Il est compliqué de produire une note à partir d'un audit car le périmètre entier d'une organisation est généralement trop grand. De plus, deux auditeurs différents peuvent produire deux notes différentes. Il est pertinent d'incorporer cette approche dans un cyber rating, mais il est **difficile de déterminer le niveau de maturité cyber d'une organisation avec des audits seuls car le périmètre analysé serait trop vaste**.

En conclusion, il existe de nombreux moyens de réaliser des diagnostics sur le niveau de maturité cyber d'une organisation. Pour autant, **aucune d'entre elles n'apparait comme suffisante si elle est considérée de façon exclusive.**

Dès lors, ne serait-il pas possible de mixer ces différentes approches afin d'obtenir un rating qui soit pertinent en compensant les forces et les faiblesses de chacune d'entre elles ?

III. Comment combiner plusieurs approches pour obtenir un cyber rating pertinent?

A. Indicateur de la maturité cyber

Il parait difficile d'avoir la possibilité, dans chaque cas, de déployer toutes les approches ; A titre d'exemple, il parait peu probable qu'une organisation, en phase de due diligence, autorise la mise en place de sondes sur son réseau. Au-delà des difficultés sur la capacité à dérouler systématiquement l'ensemble de ces approches, le principal obstacle dans la construction d'un cyber rating basé sur plusieurs méthodes réside dans la difficulté de combiner des notes provenant de sources différentes et qui sont assez difficilement comparables.

Comment choisir et déterminer une agrégation des différentes approches utilisées pour avoir, en fin de compte, une note qui représenterait fidèlement le niveau de maturité d'une organisation ?

La première étape consiste à s'assurer que chacune des approches puisse produire une note. Dans le cas des solutions cyber rating se basant sur de l'analyse de sources ouvertes, il en ressort systématiquement un rapport contenant une note claire et intelligible. Ce qui n'est pas forcément toujours le cas lorsque l'on manipule d'autres approches (ex : analyse basée sur des composants techniques, audits …) qui se concentrent plutôt sur la mise en avant de vulnérabilités ou de signes de compromissions ou bien encore sur une évaluation du niveau de conformité.

Chaque auditeur s'appuyant sur ses expériences et sa perception du risque, deux audits effectués par deux organismes différents ne fourniront pas nécessairement la même note. Dans le cas hypothétique où une note serait obtenue pour chacune des approches déployées, il resterait encore à réaliser un travail de consolidation de ces notes. Ceci parait difficilement faisable dans la mesure où il semble difficile de s'accorder sur une formule d'agrégation de ces notes :

- La formule d'agrégation sera-t-elle identique dans chaque cas ?
- Quels seront les éléments pris en compte dans le calcul (comme par exemple la taille de l'organisation, le secteur d'activité ou autre) ?
- En agrégeant les notes, devrons-nous accorder plus de poids à une approche qu'a une autre ? Et en fonction de quel(s) critère(s) ?
- Etc…

Avec toutes ces interrogations à prendre en compte, il sera compliqué pour la communauté cyber de s'aligner sur un seul et unique moyen de calculer un indicateur de la maturité cyber.

Le schéma ci-dessous résume cette idée :

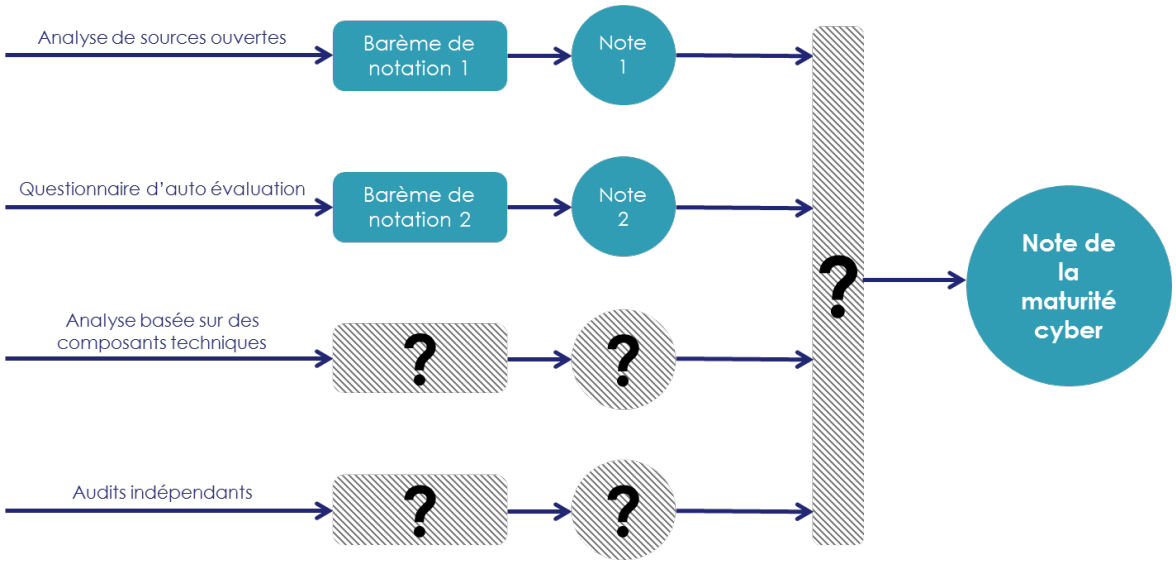

Figure 1. Formule de calcul de l'indicateur de la maturité cyber

Il est déjà compliqué de trouver un barème de notation pour chacune de ces approches et, dans l'hypothèse où ce serait fait, la consolidation de ces approches pour former une note indiquant la maturité cyber représente un obstacle encore plus grand.

Cependant, la communauté pourra sans doute s'accorder sur le fait que ces différentes approches ont toutes des particularités propres et que ces particularités définissent un certain niveau de fiabilité pour chacune d'elles.

La fiabilité d'une approche ajoutant une nouvelle dimension au cyber rating, la notion d'indice de confiance peut être introduite afin de mieux expliciter cette dimension.

B. L'indice de confiance

Chaque approche produit un résultat avec un niveau de fiabilité qui lui est propre. Par exemple, le résultat d'un audit indépendant (qu'il soit réalisé par un tiers ou par une direction de l'Inspection Générale par exemple) sera plus fiable que celui d'une analyse de sources ouvertes qui ne voit que la partie émergée de « l'iceberg ». On peut alors se demander s'il est possible d'associer un indice de confiance avec une note de la maturité cyber.

Premièrement, il faut définir le niveau de fiabilité pour chacune des approches. Il semble alors possible de trouver un consensus sur le classement des fiabilités des différents types d'approches. Un exemple de barème de notation de la fiabilité de chaque approche est décrit ci-dessous :

Les approches	Fiabilité	Justifications
Analyse de sources ouvertes	10	Périmètre couvert très faible
Questionnaires d'auto-évaluation (sans preuves)	10	Pas de contrôles pour vérifier la véracité
Questionnaires d'auto-évaluation (avec preuves)	30	Plus fiable que le questionnaire seul, mais pas forcément indépendant
Audits indépendants	40	Plus fiable que le questionnaire seul car indépendant
Analyse basée sur des composants techniques	40	Ne prends que partiellement en compte les comportements humains

Tableau 1 Proposition d'un barème de notation de l'indice de confiance

Dès lors, on peut s'intéresser aux différentes combinaisons possibles afin de maximiser la fiabilité de la note et donc de l'évaluation cyber. Remarquons tout de même que certaines combinaisons ne sont pas possibles, voici la liste de ces combinaisons :

- Questionnaire d'auto-évaluation avec preuve + Questionnaire d'auto-évaluation sans preuves : n'a pas lieu d'être puisque les périmètres se recoupent dans ces cas.
- Audit indépendant + Questionnaire avec preuve

Indice de confiance	Combinaisons
10	(Analyse de source ouverte) **OU** (Questionnaire sans preuve)
20	Questionnaire sans preuve **+** Analyse de source ouverte
30	Questionnaire avec preuves
40	(Questionnaire avec preuves **+** Analyse de source ouverte) **OU** (Audit indépendant) **OU** (Analyse technique)
50	(Audit indépendant **OU** Analyse basée sur des composants techniques) + Analyse de source ouverte
60	(Audit indépendant **OU** Analyse basée sur des composants techniques) **+** Questionnaire sans preuve **+** Analyse de source ouverte
70	(Analyse basée sur des composants techniques **+** Questionnaire avec preuves)
80	(Analyse basée sur des composants techniques **+** audit indépendant) **OU** (Analyse basée sur des composants techniques + Analyse de sources ouvertes + Questionnaire avec preuves)
90	Analyse technique + Audit indépendant + Analyse de sources ouvertes

Tableau 2 Liste des combinaisons d'indices de confiances possibles

Avec cet exemple de barème, les combinaisons possibles permettent d'obtenir un indice de confiance sur un cyber rating ayant des valeurs comprises entre 10 et 90 sur une échelle de 0 à 100. La valeur maximale atteignable est 90 car il y aura toujours un doute présent, quoique minime, sur le résultat d'une évaluation cyber.

Comment choisir l'indice de confiance souhaité ?

Un cyber rating sera donc composé d'un ensemble de notes (dépendant du nombre d'approches retenues) mis en perspective par l'indice de confiance que l'on peut légitimement accorder à chaque approche.

Dans un souci d'optimisation des coûts et des moyens, toute la collection d'approches ne peut être déployée pour chaque cas de figure. En effet, lorsqu'il s'agit d'évaluer le niveau de maturité cyber d'un prestataire n'ayant pas accès à des données sensibles de l'organisation, cela ne vaut peut-être pas la peine de lui imposer des audits sur site tous les 3 mois.

Pour déterminer alors les approches à utiliser, une organisation qui souhaitera faire du cyber rating devra évaluer le risque encouru si le résultat du cyber rating n'est pas fiable. Si ce risque est trop grand, alors elle adoptera le maximum d'approches afin de maximiser l'indice de confiance. Par exemple, si une organisation « A » souhaite recourir aux services d'une organisation « B » sur une de ses activités critiques, alors l'organisation « A » exigera logiquement un indice de confiance fort pour son cyber rating. Chaque organisation doit donc établir le niveau d'indice de confiance à atteindre, pour chaque type d'activité (standard, critique, etc.).

Enfin, plusieurs illustrations d'un cyber rating ont été proposées pour clarifier l'idée. Elles sont présentes ci-dessous :

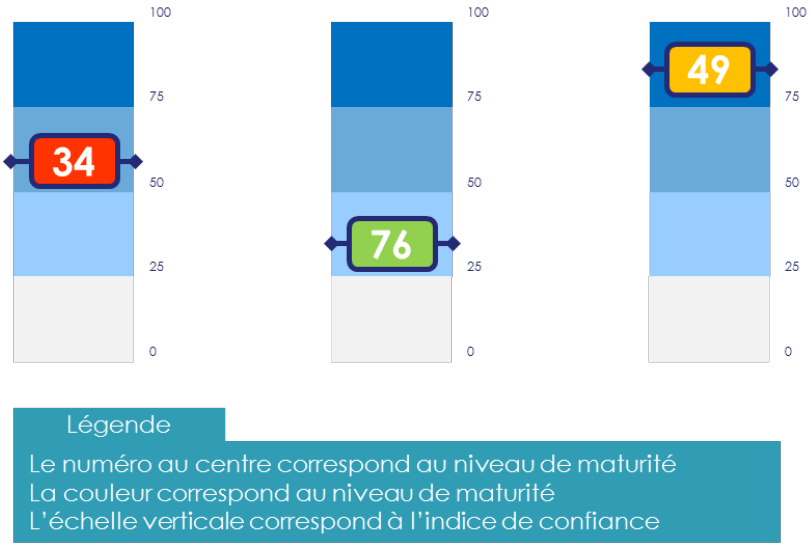

Figure 2 Proposition d'illustration du cyber rating

Figure 3 Proposition d'illustration du cyber rating

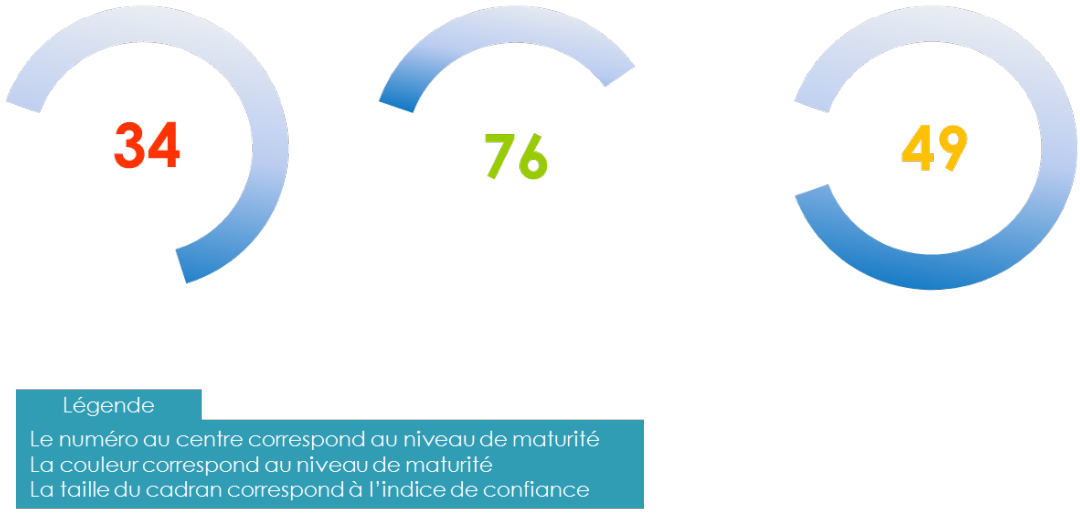

Figure 4 Proposition d'illustration du cyber rating

IV. Conclusion

Le cyber rating est souvent associé à des solutions qui utilisent exclusivement de l'analyse de sources ouvertes. Toutefois, ces solutions sont souvent décriées par la communauté cyber en raison de leur opacité, et de leur fonctionnement qui repose uniquement sur des données visibles.

En dehors de l'OSINT, il existe d'autres approches permettant d'évaluer le niveau de maturité cyber d'une organisation. Toutes ces approches ont leurs avantages et leurs inconvénients, mais aucune n'est auto suffisante pour établir un cyber rating pertinent et unanimement partagé. Une des étapes envisageables pourrait, dans un premier temps, consister à s'accorder sur un questionnaire d'évaluation commun qui pourrait être partagé par l'ensemble de la place bancaire et assurantielle de Paris. Ce qui permettrait un gain de temps, tant au niveau de la construction (et la mise à jour) du questionnaire, qu'au niveau des répondants, passant parfois plusieurs heures par semaine à répondre à ce type de questionnaire.

La combinaison de ses approches, ayant pour but de compenser les forces et les faiblesses de chacune d'entre elles, s'avère être une solution attrayante. Néanmoins, le bon « mix » de chacune d'entre elles semble lui aussi faire débat. Cependant, la proposition de la mise en place de la notion d'indice de confiance qui permettrait, entre autres, de doser l'effort en fonction des activités concernées devrait pouvoir être unanimement partagée.

Dans une logique d'optimisation des coûts, il faut mettre en adéquation le cas d'usage avec l'approche retenue et donc le niveau de confiance attendu. Les prestations critiques doivent faire l'objet d'un indice de confiance élevé là où certaines prestations jugées moins sensibles ne nécessitent pas forcément de déployer tout l'arsenal à la disposition du RSSI (analyse de sources ouvertes + analyse basée sur des composants techniques + audits indépendants + etc…). Il faut donc ajuster l'effort à fournir, en termes d'évaluation cyber, au cas d'usage.

De plus, le manque de maturité des outils OSINT et les défauts précédemment évoqués ne permettent pas de leur accorder un niveau de confiance suffisant. Pour autant, ils ont l'avantage de pouvoir permettre de monitorer les fluctuations (progrès ou régressions en termes de niveau cyber) dans le temps. De plus, ces outils évoluent rapidement et le nombre d'acteurs se développe, il faut donc continuer à les suivre de près.