La cybersécurité à l'ère cognitive

Préparer votre système immunitaire numérique

IBM Institute for Business Value

Que peut apporter IBM ?

La cybercriminalité est une menace insidieuse qui a atteint des niveaux de crise. Bien qu'ils soient difficiles à quantifier avec précision, les coûts de la cybercriminalité pour l'économie mondiale se situent entre 375 et 575 milliards USD par an. Aucun pays et aucun secteur d'activité n'est à l'abri. IBM® dispose d'un large portefeuille d'offres intégrées de solutions et de services de sécurité qui traitent de la prévention, la détection, la réponse ainsi que la résolution des incidents pour aider les organisations à prévoir et à prendre des mesures par anticipation pour réduire l'impact des risques de cybersécurité. IBM Security aide les clients à mettre en œuvre un système immunitaire de sécurité, renforcé par des analyses et des défenses en temps réel et avec l'intervention d'experts accrédités. Pour savoir comment IBM collabore avec des entreprises afin de sécuriser leurs infrastructures numériques, veuillez visiter **ibm.com**/security.

De nouvelles capacités pour une ère de challenges

Les responsables de la sécurité s'efforcent de combler trois lacunes identifiées dans leurs capacités actuelles à savoir : renseignement, rapidité et précision. Certaines organisations commencent à explorer des solutions de sécurité cognitive potentielles pour éliminer ces lacunes et anticiper les risques et les menaces. Cette technologie répond à des attentes importantes. 57 % des responsables de la sécurité qui ont répondu à notre enquête ont affirmé qu'elle peut considérablement ralentir les efforts des cybercriminels. 22 % des répondants (que nous appelons "Initiateurs") sont déjà concrètement engagés dans l'ère cognitive de la cybersécurité. Ils estiment avoir les connaissances, la maturité et les ressources requises. Pour être prêt, il est important d'explorer vos faiblesses, de déterminer comment vous souhaitez augmenter vos capacités et solutions cognitives, définir des plans de formation et d'investissement pour l'ensemble des personnes concernées.

Résumé

La situation de la sécurité est proche d'un point d'inflexion. Le nombre de risques et d'événements progresse de manière exponentielle et les équipes de sécurité ont des difficultés à faire face aux volumes. Le paysage des menaces évolue rapidement. La sophistication et le nombre des variables et agressions dépassent les capacités basées sur des approches traditionnelles. Les répercussions des incidents et violations s'aggravent. Les risques et les coûts financiers augmentent rapidement. De nombreuses entreprises sont confrontées à une pénurie d'experts ayant les bonnes compétences en sécurité. Avec toutes ces contraintes, les entreprises rencontrent de grandes difficultés pour maintenir un système immunitaire sain qui leur apporte une protection suffisante.

Pour créer ce rapport, nous avons contacté 700 directeurs de la sécurité des informations (CISO) et d'autres responsables de la sécurité dans 35 pays, représentant 18 secteurs d'activité. Notre objectif consistait à identifier leurs difficultés, les insuffisances et les efforts qu'ils doivent fournir pour progresser. Nous souhaitions aussi comprendre leur opinion sur les solutions de sécurité cognitive : comment ils perçoivent l'utilité de telles solutions, leur niveau de préparation pour les mettre en œuvre, et les obstacles potentiels.

Nous avons constaté que la complexité des menaces et la rapidité des réponses nécessaires sont des difficultés majeures pour les responsables de la sécurité. L'impact des incidents sur leurs opérations actuelles et sur leur réputation future est une préoccupation importante. Ils estiment qu'ils ne sont pas assez efficaces qu'ils pourraient l'être pour assurer la protection des réseaux et des données, avec des réponses rapides mieux adaptées aux menaces. Cependant, ils se préparent à pallier à ces insuffisances pendant les prochaines années. L'acquisition des ressources appropriées pour résoudre de tels problèmes pose des difficultés. Confrontés à l'augmentation des coûts et à la pénurie des ressources qualifiées en sécurité, les responsables recherchent des moyens pour mieux justifier leurs investissements auprès de leurs directions.

Le **principal challenge de la cybersécurité,** aujourd'hui et demain, **est de réduire les délais moyens de réponses et de résolutions des incidents**.

57 % des responsables de la sécurité affirment que **les solutions de sécurité cognitive** peuvent considérablement **ralentir les efforts des cybercriminels**.

Les prévisions indiquent que le nombre de professionnels engagés dans la mise en œuvre **de solutions de sécurité sera** multiplié par trois **pendant** les deux ou trois prochaines années.

Avec l'explosion des volumes de données collectées sur la sécurité et le déploiement de capacités analytiques supplémentaires, les charges de travail atteignent les limites de ce que peuvent supporter des opérations manuelles. Certaines entreprises souhaitent utiliser des solutions cognitives pour gérer cette situation et éliminer les écarts dans les connaissances, la rapidité et la précision. Bien que les technologies cognitives appliquées à la sécurité soient encore très jeunes, elles offrent un potentiel qui justifie un fort optimisme et d'immenses espoirs. Les répondants à notre enquête ont déclaré que les principaux avantages qu'ils attendent des solutions de sécurité cognitive incluent de meilleures capacités de détection et de prise de décision, une accélération importante dans la réponse aux incidents, une distinction plus fiable entre événements et réels incidents. En dépit de ce remarquable potentiel, il y a encore du chemin à faire dans l'éducation et la préparation avant d'aboutir à une adoption généralisée.

Heureusement, nous avons identifié un groupe qui est « prêt pour l'ère cognitive » des solutions de sécurité. Grâce à nos questions sur l'efficacité de la sécurité, la préparation et les connaissances cognitives, nous avons identifié des responsables enthousiastes qui s'estiment prêts à entrer dans l'ère cognitive des solutions de sécurité. En général, ces responsables ont tendance à avoir de meilleures connaissances des solutions cognitives, une plus grande confiance dans leurs compétences en sécurité et sont généralement peu confrontés aux problèmes d'accès aux ressources.

Au fur et à mesure de l'adoption généralisée des solutions de sécurité cognitive, toutes les entreprises pourront tirer profit de ces avantages. Si vous vous sentez prêts, et que vous décidez de suivre la voie cognitive, la première étape consiste à identifier les lacunes que vous espérez combler à l'aide des solutions de sécurité cognitive. Vous devrez ensuite connaître les cas d'application potentiels et les aligner sur vos insuffisances identifiées. Dans un environnement où la justification des investissements est incontournable, prenez le temps de communiquer à vos dirigeants sur les avantages des solutions de sécurité cognitive. Dans un langage compréhensible par vos dirigeants, insistez sur le fait que ces solutions peuvent améliorer la situation générale de votre système de sécurité. Ces premières étapes prépareront votre organisation à faire son entrée dans l'ère cognitive de la cybersécurité.

Le contexte actuel

Au premier regard, les responsables sondés pendant notre enquête peuvent donner l'impression que la situation générale est maitrisable. En fait, ces professionnels ont confiance dans leurs capacités organisationnelles et technologiques qui est, par ailleurs, en progression. La majorité – 77 % – de ceux qui ont répondu aux questions sur la préparation à la cybersécurité estiment qu'ils sont à égalité avec leurs pairs de l'industrie. Les répondants sont aussi très optimistes concernant leur évolution au cours des deux ou trois prochaines années. 86 % ont déclaré qu'ils seront *mieux* positionnés que leurs pairs dans leur secteur d'activité.

Si ces réponses peuvent ne pas surprendre, elles méritent d'être examinées : les responsables de la sécurité estiment qu'ils font au moins aussi bien que d'autres et sont sûrs de progresser et de continuer à le faire. Près des trois-quarts pensent que leur approche pour fonder les bases de leur organisation de sécurité est efficace. 72 % jugent que leur hygiène informatique est efficace. Et 71 % ont déclaré que leurs méthodes de sensibilisation aux risques dans l'entreprise portent leurs fruits. Mais creusons un peu pour en savoir plus sur les difficultés, les conséquences, les capacités, les financements et les retours sur les investissements consacrés à la sécurité.

Le besoin de rapidité

Réduire les délais moyens de réponses et de résolutions des incidents est actuellement le challenge numéro un pour les responsables de la sécurité. 45 % des répondants ont identifié cette question comme étant le principal défi de la cybersécurité actuelle. Les entreprises prévoient que ce challenge restera inchangé au cours des deux ou trois prochaines années. À plus long terme, 53 % des répondants pensent que l'amélioration de la réactivité restera un challenge prioritaire pour la cybersécurité (voir Figure 1).

« Vous vous retrouvez littéralement dans la situation d'un navire marchand à la belle époque des pirates et des corsaires : vous êtes seul en mer, exposé à tous les dangers, sans police ou marine militaire pour vous protéger. En plus, bien des capitaines ne savent pas naviguer dans de telles eaux et ne peuvent pas tirer sur les agresseurs (la loi actuelle l'interdit). Vous devez survivre dans un monde hostile en ayant les deux mains attachées dans le dos. Néanmoins, vous disposez de quelques outils sophistiqués et très utiles qui vous permettent d'identifier vos menaces ».

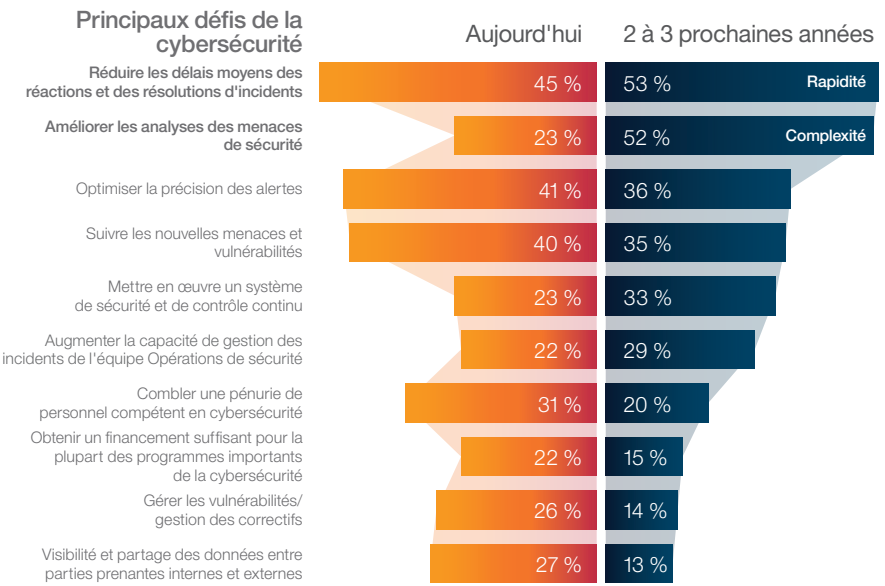
David Shipley, Director of Strategic Initiatives, Information Technology Services, University of New Brunswick

Le temps augmente le risque

Dans une étude réalisée en 2016, le « Ponemon Institute » a découvert que le temps nécessaire pour identifier une violation de sécurité est en moyenne de 201 jours, et de 70 jours pour la bloquer. L'Institut a aussi déterminé que disposer d'une équipe dédiée aux incidents de sécurité constituait le facteur le plus important pour réduire les coûts de chaque violation.[1]

Figure 1

Les responsables de la sécurité ont identifié les principaux challenges actuels de la cybersécurité et partagé leur opinion sur les difficultés à moyen terme.



Ces préoccupations persistent même si 80 % des organisations contactées ont indiqué que leur réponse aux incidents est déjà beaucoup plus rapide que deux ans plus tôt (16 % plus rapide). 86 % souhaitent progresser encore plus au cours des deux ou trois prochaines années et atteindre un objectif d'amélioration moyenne de 24 % de la réactivité.

Cet objectif est extrêmement important pour les organisations. Plus une organisation a besoin de temps pour réagir à un incident, plus les dégâts encourus seront importants et plus les coûts engendrés par la résolution de la crise seront élevés. Le temps est un facteur certain de l'augmentation des pertes.

L'amélioration des analyses des menaces est un autre challenge qui prend de plus en plus d'importance aux yeux des responsables de la sécurité. 22 % des participants à notre enquête le considèrent actuellement comme un challenge prioritaire. mais 52 % prévoient que l'amélioration des ressources analytiques sera le principal défi de la cybersécurité pendant les deux ou trois prochaines années. Les analystes de sécurité ont besoin de recueillir les connaissances, définir les menaces prioritaires, identifier les modèles et les écarts d'activité. Les responsables recherchent toutes les solutions capables d'améliorer leur réactivité et leur gestion de la complexité des menaces.

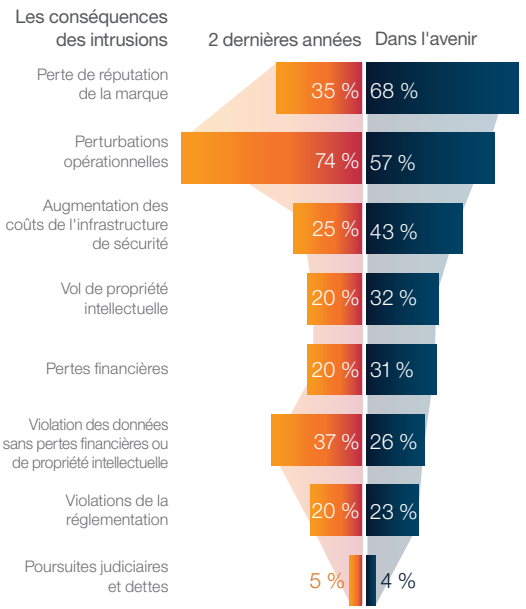
Des préoccupations croissantes

Près des trois-quarts des répondants ont déclaré que les intrusions ont provoqué des perturbations opérationnelles importantes au cours des deux dernières années. En revanche, leurs prévisions pour les prochaines années sont totalement différentes.

Pour les entreprises, l'impact des intrusions sur la réputation de la marque est une préoccupation de plus en plus forte, voire même supérieure aux perturbations opérationnelles. À l'avenir, la crainte d'un impact sur la réputation sera multipliée par deux, pour 35 % des répondants au cours des deux dernières années contre 68 % pendant les prochaines années (voir Figure 2). Cette évolution démontre que pour de nombreux responsables l'importance des dégâts engendrés par les intrusions est une préoccupation majeure. De plus en plus, les conséquences concernent non seulement les opérations, mais aussi la réputation de l'entreprise. Une réputation ternie peut impacter à la baisse les revenus, car la confiance des clients diminue et peut les inciter à aller voir ailleurs.

Figure 2

Si au cours des deux dernières années, les entreprises ont signalé diverses ramifications des intrusions, elles prévoient maintenant une évolution dans ls conséquences.



L'augmentation des coûts de l'infrastructure de cybersécurité sera un problème à long terme et présente déjà une progression spectaculaire aujourd'hui. Comme le risque d'une intrusion réussie persiste, les entreprises doivent consacrer plus de budget pour trouver des solutions appropriées. Pour les responsables de la sécurité, toute intrusion est révélatrice d'une faille. Par conséquent, ils doivent chercher à faire monter en compétence les ressources, à améliorer l'efficacité des solutions et de l'infrastructure pour que leur système de sécurité soit le plus fiable possible.

Faiblesses de la sécurité

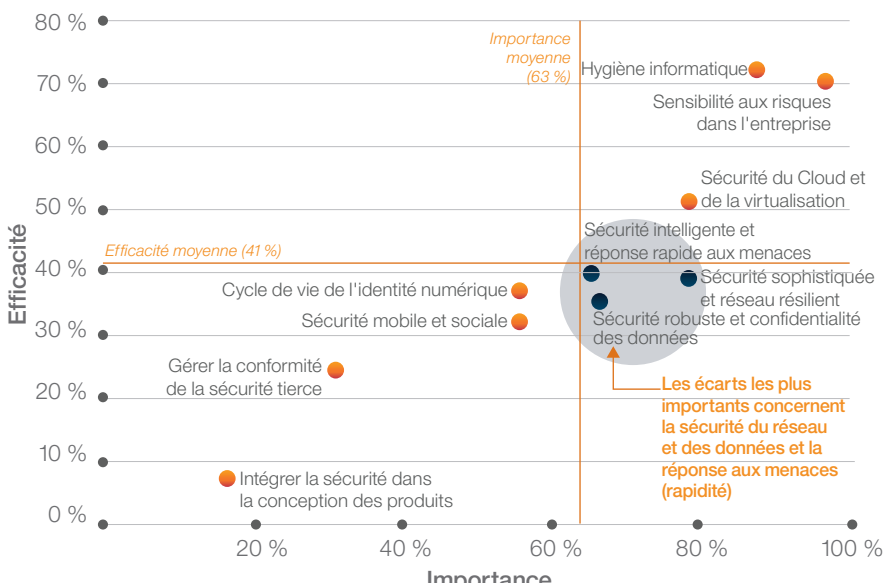
Nous avons demandé aux personnes sondées qui occupent différentes fonctions dans la sécurité d'identifier pour nous les facteurs clés pour leur système de sécurité et quels seraient selon eux ceux qui auront un meilleur rendement en terme d'efficacité.
En général, les responsables de sécurité estiment que tout doit être traité avec une importance égale, pour que rien ne puisse passer au travers des mailles du filet.
Or compte tenu des ressources limitées disponibles, il est impossible d'assurer une protection maximale partout et constamment, surtout lorsque de nouvelles technologies, approches et difficultés émergent sans cesse.

La plupart des répondants ont indiqué qu'ils sont satisfaits de la gestion de l'hygiène informatique et de la sensibilisation aux risques dans leur entreprise, aussi bien du point de vue organisationnel que technologique. Les domaines que les répondants ont identifié comme importants mais dans lesquels ils manquent d'efficacité sont pour nous les plus intéressants (voir Figure 3). Nous trouvons dans cette catégorie la protection du réseau et des données ainsi que la réponse aux menaces.

Les répondants ont déclaré qu'ils ne sont pas aussi efficaces qu'ils devraient l'être en termes de réactivité aux menaces, de gestion des événements et information sur la sécurité (SIEM), de détection des activités sur le réseau, de filtrage et classification des données, et de prévention des pertes. Bien sûr, il est essentiel que les organisations continuent à faire face à la croissance à la fois du volume et de la complexité des incidents de sécurité. Pour ce faire, elles doivent se concentrer sur leurs niveaux de réactivité, grâce à de meilleures analyses des menaces et pourront ainsi renforcer considérablement leurs défenses.

Figure 3

Importance contre efficacité des capacités de sécurité



« Nous avons découvert dans l'entreprise de réelles réductions de coûts générés par nos analyses et notre contrôle de la sécurité. Nous avons réduit les coûts de la bande passante, désengagés des ressources à faible utilisation, augmenté la productivité du personnel en réduisant considérablement les spams, pour n'en citer que quelques exemples ».

Un leader canadien de la protection financière, de la gestion des biens

Gérer le bilan

Les responsables de la sécurité doivent concentrer leurs efforts sur une multitude d'éléments. Ils prévoient ainsi d'importantes augmentations des budgets nécessaires pour que leur système de cybersécurité soit le plus efficace possible, mais ne savent pas dire quand les coûts finiraient par se stabiliser. 78 % des répondants ont constaté une augmentation des coûts de la sécurité au cours des deux dernières années et 84 % prévoient qu'ils continueront d'augmenter pendant les deux à trois prochaines années. Plus de 70 % des répondants consacrent plus de 10 % de leur budget informatique à la cybersécurité (la majorité dépensant entre 10 et 15 %). Ces dépenses sont principalement dédiées à la prévention et la détection. À tel point que certaines institutions financières consacrent plus de 500 millions de dollars par an à la cybersécurité. [2] Comme l'augmentation des dépenses ne garantit pas nécessairement une meilleure protection, une telle escalade des coûts devient insoutenable à long terme. — Les responsables de la sécurité seront confrontés à des contraintes de plus en plus lourdes pour justifier leurs investissements.

92 % des répondants ont indiqué que leurs demandes de financement pour des programmes de cybersécurité doivent démontrer un retour sur investissement (ROI) pour être autorisées. Les deux facteurs clés pour justifier de tels investissements incluent à la fois une communication claire sur l'exposition actuelle de l'entreprise aux risques (pour 65 % des répondants) ainsi que le soutien des principaux décideurs qui sont les responsables Finances, Risques et Opérations (pour 51 % des répondants). Les≈responsables de la sécurité doivent communiquer sur leurs besoins dans la langue de l'entreprise et s'assurer du soutien d'autres décideurs clés.[3] A l'avenir, ils doivent identifier de nouvelles approches pour justifier les investissements en cybersécurité et démontrer leur importance. L'idée que la sécurité est une police d'assurance ou un centre de coût doit être éradiquée.

Gérer les insuffisances

La bonne nouvelle est que les responsables de la sécurité, qui ont répondu à notre enquête, semblent connaître leurs points faibles et planifient des projets d'amélioration à court terme. Les entreprises utilisent actuellement plusieurs programmes pour améliorer leur niveau de préparation aux risques de la cybersécurité (voir Figure 4). Les efforts actuels sont principalement centrés sur l'amélioration du comportement des employés grâce à des activités de sensibilisation et d'éducation (67 % des organisations ont fait ce choix). 40 % des répondants ont aussi mis en place un outil de contrôle des identités. Ces options sont généralement considérées comme fondamentales.

Figure 4

Les responsables des programmes de sécurité souhaitent améliorer la préparation aux risques de la cybersécurité.

Classement aujourd'hui		Classement dans 2 ou 3 ans	Initiatives
1	▼-30 %	5	Améliorer les comportements des employés par l'éducation et la formation
2	▼-25 %	7	Mettre en œuvre un logiciel de contrôle d'identité (activités des utilisateurs)
3	▲+8 %	4	Suivre les mesures de sécurité stratégiques/ opérationnelles avec de nouveaux outils analytiques
4	▲+28 %	1	**Améliorer le contrôle de la sécurité du réseau, des applications et des données**
5	▲+17 %	3	**Améliorer la méthodologie, les processus et la rapidité de la réponse aux incidents**
6	▼-9 %	8	Recruter et former plus d'analystes de la sécurité
7	▼-16 %	10	Tester la sécurité des applications (incluant les applis mobiles, API)
8	▲+36 %	2	**Développer ou perfectionner les capacités SOC**
9	▲+14 %	6	Mettre en œuvre des solutions de sécurité basée sur la technologie cognitive
10	▲+1 %	9	Incorporer des capacités criminalistiques dans les opérations de sécurité

« Les responsables se lassent de voir la sécurité absorber des sommes importantes, sans aucun retour positif confirmant que toutes les dépenses antérieures ont amélioré sensiblement leur sécurité. Les responsables de la sécurité n'ont pas besoin de chercher plus loin les justifications de leurs investissements. Ne faites pas seulement une évaluation, identifiez les écarts et demandez des fonds pour éliminer les écarts ».

Chad Holmes, Principal and Cyber-Strategy, Technology and Growth Leader (CTO) pour Ernst & Young LLP

Au cours des deux à trois années, ces programmes d'amélioration connaîtront une transformation notable. En effet, les répondants ont indiqué que les trois principales initiatives seront alors totalement différentes que celles d'aujourd'hui. L'initiative prioritaire sera l'amélioration de la sécurité du réseau, des applications et des données d'après 57 % des réponses. Le développement ou le perfectionnement des capacités du SOC sera la deuxième priorité. Et l'amélioration de la réponse aux incidents sera en troisième position. Tous ces domaines correspondent aux points faibles identifiés précédemment.

Combler ses lacunes est considérée comme une avancée, mais des changements importants peuvent créer de nouveaux écarts, ou aggraver les manquements existants. Dans tous les cas, les responsables de la sécurité doivent traiter en priorité les éléments les plus pertinents pour leur entreprise. La véritable question est de savoir si ces efforts suffiront à l'avenir.

Reconnaître les écarts

Tous ces challenges, points faibles, efforts et pressions sont révélateurs de trois lacunes critiques : connaissances, rapidité et précision. Les responsables de la sécurité doivent éliminer ces lacunes et gérer simultanément les coûts et les contraintes liées au ROI.

Écart de connaissances

- Pour 65 % des répondants, l'analyse des menaces est le point faible le plus difficile à traiter, du fait du manque de ressources.
- 40 % des répondants ont déclaré que le suivi des menaces et des vulnérabilités constitue un défi très important pour la cybersécurité.

Écart de réactivité

- En dépit du fait que 80 % des répondants ont déclaré que leur niveau de réactivité aux incidents est largement supérieur à ce qu'il était deux ans plus tôt, réduire les délais moyens des réactions et des résolutions aux incidents restera un challenge prioritaire pour les équipes de sécurité.
- Les répondants prévoient d'augmenter leurs efforts dans ce domaine dans les prochaines années. Seulement 27 % ont mis en place des programmes pour améliorer leur réactivité aux incidents, mais ce chiffre passera à 43 % dans les deux à trois prochaines années.

Écart de précision

- D'après nos répondants, l'optimisation de la précision des remontée d'alertes est le deuxième challenge à faire face (le nombre de faux positifs est actuellement excessif).
- Pour 61 % des répondants, l'identification, l'évaluation des menaces et la sélection des incidents potentiels à remonter constituent un autre challenge du fait du manque de ressources.

Les avantages les plus souvent cités et attendus d'une solution de solution cognitive

1. Intelligence

Améliorer les capacités de prise de décision en matière de détection et de réponse aux incidents

2. Rapidité

Amélioration importante des délais de réponse aux incidents

3. Précision

Augmenter la confiance dans la différenciation des événements et des incidents réels

Multiplication par trois

Adoption planifiée de solutions de sécurité cognitive pendant les 2-3 prochaines années

Comment la sécurité cognitive sera-t-elle utilisée ?
Les systèmes cognitifs serviront à analyser des tendances de sécurité et à distiller d'énormes volumes de données structurées et non-structurées en connaissances exploitables. Les analystes et les responsables de la sécurité ne peuvent pas absorber toutes les connaissances d'origine humaine sur la sécurité, incluant des documents d'études, des publications industrielles, des rapports d'analystes, et des blogs. Les systèmes cognitifs visent à combiner ces informations avec des données de sécurité traditionnelles. Les solutions de sécurité cognitive seront utilisées en combinaison avec des technologies, des techniques et des processus de sécurité automatisés, pilotés par des données, pour obtenir les plus hauts niveaux de précision en fonction de différents contextes

Les solutions de sécurité cognitive peuvent contribuer à augmenter les capacités des analystes SOC, pour les aider à augmenter leur réactivité, mieux identifier les menaces, renforcer la sécurité des applications et à réduire le niveau de risque pour l'entreprise. L'objectif est de libérer les analystes des tâches de sécurité répétitives et ordinaires, pour qu'ils se consacrent à des travaux intellectuellement plus difficiles et plus valorisants.

Les solutions de sécurité cognitive

Des technologies et des approches différentes sont nécessaires pour éliminer ces écarts. À long terme, augmenter les dépenses et recruter indéfiniment n'est pas une solution durable pour atteindre les objectifs. Au fil des ans, les technologies de sécurité ont évolué, allant des simples contrôles périmétriques (par exemple des défenses statiques) aux capacités de sécurité avancée basées sur les renseignements (par exemple en mettant l'accent sur les informations en temps réel et les déviations de comportement).

Aujourd'hui, nous entrons dans l'ère cognitive de la sécurité, avec des solutions capables de comprendre le contexte, le comportement et l'importance des événements grâce à l'analyse de données de sécurité structurées et non-structurées. La sécurité cognitive vise à créer un nouveau partenariat entre les analystes de la sécurité et les technologies qu'ils utilisent. Ces solutions peuvent interpréter et organiser les informations et offrir des explications sur leur importance, leur signification, tout en proposant une logique capable de justifier les conclusions et les prises de décision. Elles apprennent également de façon continue à mesure que les données s'accumulent et les renseignements remontent des interactions

Les avantages des solutions de sécurité cognitive
Imaginez une panoplie de solutions supportées par des technologies cognitives, qui vous permettent de :

- Renforcer les capacités des nouveaux analystes SOC en leur donnant accès aux meilleures pratiques et connaissances qui nécessitaient auparavant des années d'expérience.
- Améliorer votre réactivité en exploitant les informations externes extraites de blogs et autres sources, pour prendre les mesures nécessaires avant la disponibilité des nouvelles signatures.
- Identifier rapidement les menaces et accélérer la détection des comportements à risques, l'exfiltration des données, les infections par malware, grâce à des méthodes d'analyse sophistiquées.
- Acquérir une meilleure connaissance du contexte spécifique aux incidents de sécurité grâce à l'automatisation de la collecte et de l'exploitation des données externes et locales.

La promesse et les défis

Nombre de nos répondants estiment que les avantages des solutions de sécurité cognitive permettent d'éliminer les écarts qu'ils ont identifiés. Bien que la sécurité cognitive soit une technologie émergente, 57 % des répondants déclarent que ses solutions peuvent considérablement ralentir les efforts des cybercriminels. Ils comprennent les avantages potentiels.

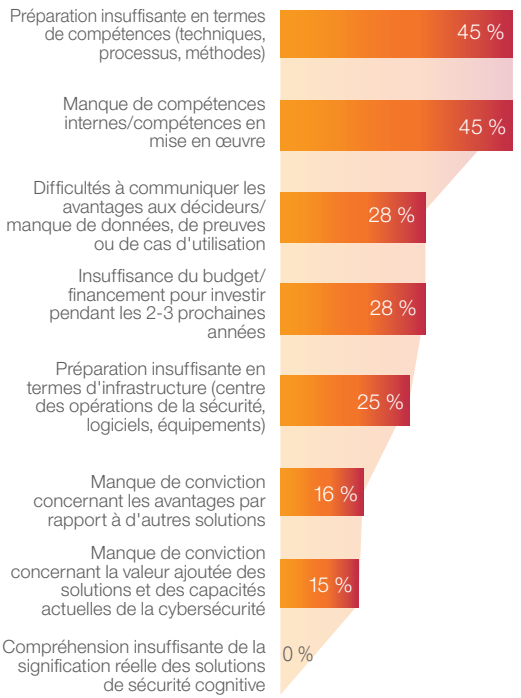
Lorsque nous avons demandé aux responsables de la sécurité de sélectionner les avantages des solutions de sécurité cognitive, 40 % ont indiqué l'amélioration des capacités de détection et de prise de décision, 37 % ont coché l'accélération importante de la réactivité en cas d'incident, et 36 % la discrimination plus fiable des événements et des incidents réels. Les répondants attendent des solutions de sécurité cognitive qu'elles puissent combler les principaux écarts qu'ils ont identifiés. Ils ont besoin de ces solutions pour améliorer leurs connaissances, leur réactivité et leur précision.

Actuellement, seulement 7 % des personnes sondées se sont engagées dans la mise en œuvre de solutions cognitives pour améliorer leur capacité de réponse aux risques de cybersécurité. Cette situation est normale compte tenu de la jeunesse de cette technologie. À court terme, ce nombre sera multiplié par trois, pour atteindre 21 %. Pendant les prochaines années, son adoption s'accélérera puisque les responsables de la sécurité l'ajouteront à leurs ressources pour renforcer leurs systèmes numériques immunisés.

Cependant, les répondants perçoivent des difficultés potentielles pour adopter des solutions de sécurité cognitive. Ce n'est pas que les responsables de la sécurité ne comprennent pas le concept de cette technologie, ou qu'ils ne sont pas convaincus par les avantages ou la valeur qu'elle apporte par rapport aux autres technologies. Les difficultés perçues sont liées aux compétences, aux processus et aux méthodes. Pour 45 % des répondants, les principales difficultés de l'adoption proviennent du manque de préparation en termes de compétences et du manque de connaissances techniques internes nécessaires à leur mise en œuvre (voir Figure 5). Par conséquent, il faut prévoir des activités d'éducation et de préparation pour répondre à ces besoins.

Figure 5

Les responsables de la sécurité ont identifié les principaux défis pour la mise en œuvre des solutions de sécurité cognitive.



« Nous sommes prêts pour la prochaine étape des solutions cognitives et intelligentes qui assimileront, organiseront et donneront avec efficacité des contextes appropriés à de vastes quantités de connaissances et d'informations de sécurité et qui consomment actuellement une grande partie de notre temps et de nos ressources ».

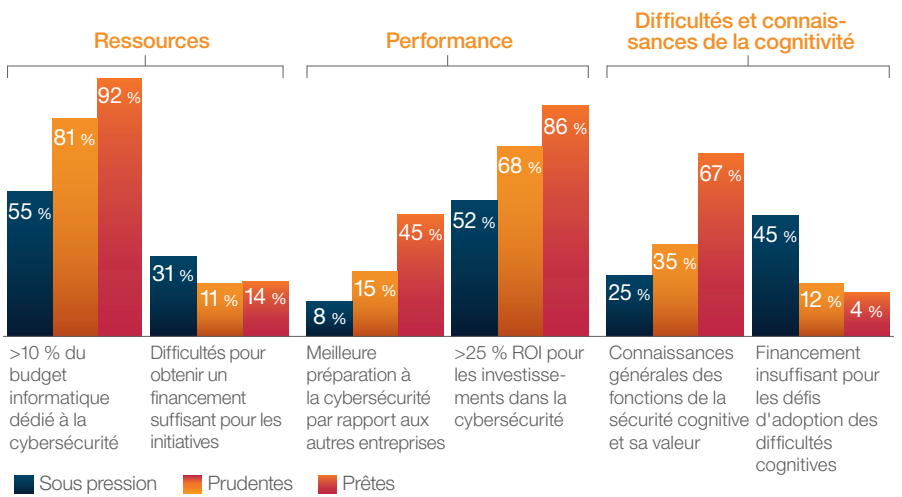
Un leader canadien de la protection financière, de la gestion des biens

Prêts pour l'ère cognitive

Pour savoir qui est prêt aujourd'hui pour l'ère cognitive de la sécurité du future, nous avons créé des profils de répondants basés sur les niveaux d'efficacité, de préparation et de connaissance cognitive qu'ils ont eux-mêmes définis. Une analyse de leurs réponses a révélé trois groupes distincts (voir Figure 6).

Figure 6

Trois niveaux de préparation : Sous-pression, Prudentes et Prêtes



Les entreprises *Sous-pression*, qui représentent 52 % de notre sondage, sont caractérisées par des difficultés de financement et de recrutement, un niveau de connaissance générale inférieur concernant les fonctions et la valeur de la sécurité cognitive. En général, leur budget informatique alloue un pourcentage plus faible à la cybersécurité. Il est plus probable qu'elles aient plus de difficultés à obtenir des financements suffisants et les ressources nécessaires. Elles ont aussi indiqué l'insuffisance de financement parmi les obstacles à l'adoption de solutions cognitives.

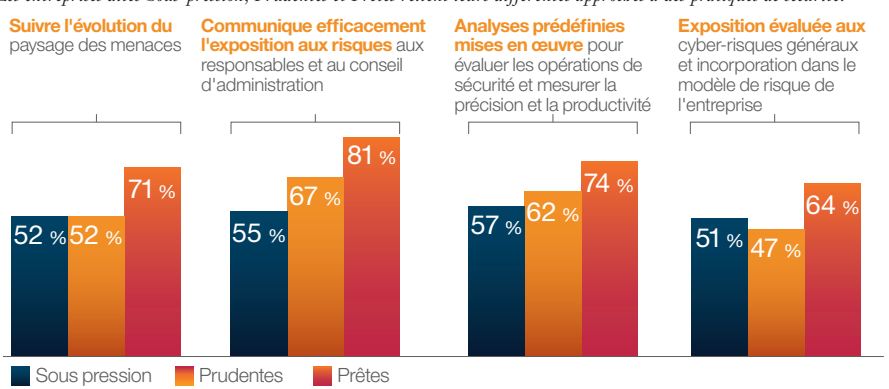
(Pour plus d'informations sur la création et la définition de ces groupes, voir la section Données démographiques et méthodologies, à la page 20.)

Les entreprises *Prudentes*, qui constituent 27 % du sondage, n'ont pas les mêmes difficultés de ressources que celles appartenant au groupe Sous-pression. Mais elles ne sont pas actuellement prêtes à mettre en œuvre une sécurité cognitive de prochaine génération.

Les entreprises *Prêtes*, soit 22 % du sondage, ont le plus haut niveau de connaissances et de motivations pour adopter des solutions de sécurité cognitive. Les entreprises Prêtes connaissent mieux la sécurité cognitive et ont une plus grande confiance, un budget plus élevé et un meilleur ROI que les autres. Elles pensent qu'elles appliquent une approche plus mature à leurs pratiques de sécurité. Elles sont plus nombreuses à déclarer que leur équipe est capable de suivre les changements affectant le paysage des menaces. Elles communiquent efficacement aux responsables et au conseil d'administration le niveau d'exposition au risque et elles intègrent l'exposition au cyber-risque dans le modèle de risque de leur entreprise (voir Figure 7).

Figure 7

Les entreprises dites Sous-pression, Prudentes et Prêtes relient leurs différentes approches à des pratiques de sécurité.



« Mais cette masse de données contient aussi une bonne part de bruit. Et le cerveau humain ne peut pas tout traiter au quotidien ». Nous avons besoin de quelque chose pour nous aider, quelque chose comme l'intelligence artificielle, ou des technologies cognitives ».

Chad Holmes, Principal and Cyber-Strategy, Technology and Growth Leader (CTO) pour Ernst & Young LLP

« La nature quotidienne et incessante des opérations de sécurité constitue un challenge de recrutement coûteux pour la plupart des entreprises. Et c'est bien là qu'intervient tout l'intérêt de la sécurité cognitive : elle ne se fatigue pas, elle ne dort jamais ».

Michael Pinch, Chief Information Security Officer, University of Rochester

Qu'attendent les responsables de sécurité des solutions de sécurité cognitive pendant la première étape ? Pendant nos conversations avec les entreprises Prêtes, nous avons constaté qu'elles recherchent des solutions de sécurité cognitive répondant aux besoins suivants :

- Constamment opérationnelles et fournissant un support continu.
- Réduire les faux positifs et identifier les anomalies comportementales.
- Mieux comprendre le paysage des menaces et décrire le contexte des incidents.
- Supporter la gouvernance, la gestion des risques, la conformité, en fonction des exigences uniques en termes d'industrie, de géographie et de réglementation.
- Changer la nature des opérations de sécurité, aider les analystes à travailler mieux, plus intelligemment, fournir un plus haut niveau de valeur.

On peut s'attendre à ce que les responsables de sécurité qui estiment qu'ils sont plus matures, qui ont moins de contraintes en termes de ressources, seraient les premiers à explorer une technologie émergeante comme la sécurité cognitive. Mais, il est important de réaliser que toutes les personnes qui ont des connaissances supérieures et une expérience plus grande peuvent appliquer des technologies cognitives pour réduire leurs écarts et repousser les limites de leurs analystes afin d'améliorer les opérations de sécurité.

Recommandations

Nous avons exploré le paysage de la sécurité actuel pour comprendre les pressions, les difficultés et les priorités de nos répondants. Basé sur nos observations, nous avons compilé des recommandations pour vous aider, ainsi que votre organisation, à devenir Prêts pour l'ère cognitive de la cybersécurité.

Reconnaître vos points faibles
Les responsables de sécurité cherchent à augmenter leur réactivité et à réduire la complexité. Ils sont de plus en plus préoccupés par l'impact sur la réputation engendré par les incidents. Examiner les principaux points faibles et vulnérabilités au sein de votre organisation. Comment se font les connexions ? Qu'est-ce qu'une priorité ?

- Manquez-vous d'informations et d'études pertinentes sur les menaces ?
- Vos délais de réactivité et de résolution d'incidents sont-ils assez rapides pour vos opérations ?
- Avez-vous des difficultés à faire la différence entre des événements et des incidents réels, ou pour replacer les choses dans leur contexte ?

Bien connaître les capacités de la sécurité cognitive
Adopter une approche formelle et holistique pour connaître les solutions de sécurité cognitive. Dans une perspective de capacité, de coût et de mise en œuvre, il peut y avoir un grand nombre d'idées reçues dans votre organisation.

- Comprendre les cas d'utilisation potentiels des solutions de sécurité cognitive et les aligner sur vos points faibles. Voulez-vous connaître le contexte général des incidents de sécurité, avoir de meilleures évidences pour améliorer les prises de décision, ou de nouvelles approches pour évaluer pro-activement les risques ?

« La sécurité cognitive a un potentiel impressionnant. Vous pouvez identifier vos manques de compétences, réduire votre profil de risque, augmenter l'efficacité de votre processus de réponse. Elle peut vous aider à comprendre le narratif. Les histoires sont des objets de consommation. Les gens se disent il s'est passé cela, ceci est arrivé, cela a eu tel impact, avec telle personne. En outre, la sécurité cognitive peut abaisser le niveau de compétence requis pour participer à des activités de cybersécurité. Elle vous permet d'intégrer de nouvelles perspectives provenant de contextes non informatiques pour résoudre des problèmes ».

David Shipley, Director of Strategic Initiatives, Information Technology Services, University of New Brunswick

- Planifier comment communiquer sur les avantages des solutions de sécurité cognitive aux responsables techniques et métiers ; développer un plan de formation pour votre équipe et vos responsables.
- Identifier et adresser les écarts de compétences qui peuvent freiner l'adoption de la technologie dans votre propre organisation.

Définir un plan d'investissement

Il est difficile de construire un plan d'investissement lorsqu'une technologie est nouvelle et n'a pas encore fait ses preuves sur le marché : vous n'avez pas beaucoup d'exemples à présenter et obtenir l'adhésion peut être difficile. Comme la grande majorité de nos répondants ont indiqué que leurs demandes de financement exigent un ROI ou d'autres analyses financières, il est impératif que les responsables adoptent une approche différente des solutions de sécurité cognitive.

- Traitez les solutions de sécurité cognitive comme des outils distincts. Ne vous préoccupez pas seulement des justifications traditionnelles des investissements dans la sécurité. Concentrez-vous plutôt sur le fait que la sécurité cognitive est une technologie qui peut améliorer l'efficacité générale des opérations de sécurité.
- Utilisez votre plan de formation pour obtenir l'adhésion totale des autres responsables de l'entreprise, pour qu'ils vous aident à construire votre plan d'investissement et ses justifications.
- Appliquer une approche créative et recherchez de nouveaux moyens d'investissement dans la sécurité cognitive pour votre entreprise, en plus du ROI.

Voyez comment augmenter vos capacités, quelle que soit votre maturité.
Les entreprises que nous avons identifiées comme Prêtes ont tendance à disposer de plus de ressources, ont plus confiance dans leurs capacités et une grande volonté pour mettre en œuvre aujourd'hui des solutions de sécurité cognitive. Mais cela ne signifie pas que ce type de technologie est réservé à un groupe privilégié. Les solutions de sécurité cognitive font partie des technologies émergentes et leurs caractéristiques uniques peuvent être bénéfiques aux organisations de toutes tailles.

- *Si votre entreprise est dite Sous-pression :* Identifiez des mesures spécifiques et des manques de compétences auxquelles les solutions de sécurité cognitive pourraient pallier, et ensuite montez votre dossier d'investissement.
- *Si votre entreprise est dite Prudente :* Adoptez une communication claire pour réduire l'anxiété liée aux manques de compétence.
- *Si votre entreprise est dite Prête :* Maîtrisez votre empressement, choisissez un cas d'utilisation très spécifique pour mettre en œuvre un pilote cognitif, assurez-vous qu'il n'est pas isolé de vos opérations générales de sécurité.

Pour plus d'information :
Pour en savoir plus sur cette étude de l'IBM Institute for Business Value, veuillez nous contacter à l'adresse iibv@us.ibm.com. Suivez @IBMIBV sur Twitter et, pour obtenir la liste complète de nos études ou vous abonner à notre bulletin d'information mensuel, consultez : **ibm.com**/iibv.

Vous pouvez accéder aux rapports de l'IBM Institute for Business Value sur votre appareil mobile en téléchargeant l'application gratuite « IBM IBV » pour iPad ou Android depuis votre App Store.

Le bon partenaire dans un monde en constante évolution
Chez IBM, nous collaborons avec nos clients en assemblant les informations commerciales avec les recherches avancées et la technologie afin de leur donner un avantage concurrentiel dans un environnement en forte évolution.

IBM Institute for Business Value
Rattaché à IBM Global Business Services, IBM Institute for Business Value apporte aux cadres dirigeants un éclairage stratégique fondé sur des faits autour de thèmes spécifiques ou critiques pour les secteurs publics et privés.

Participants
Lisa van Deth, Directrice de programme de marketing, Campaign & Thought Leadership Strategy, IBM Security ; Christophe Veltsos, Professeur associé, Department of Computer Information Science de la Minnesota State University, Mankato.

Remerciements
Caleb Barlow, Vice-président, WW Portfolio Marketing, IBM Security ; Maria Battaglia, CMO, Resilient, IBM Security ; Wangui McKelvey, Directeur, Portfolio Marketing - Security Services & Web Fraud, IBM Security ; Kevin Skapinetz, Directeur de la stratégie, IBM Security ; Oxford Economics, pour son assistance dans l'administration des données de l'enquête.

Notes et sources

1 Étude sur le coût des failles de sécurité 2016 : Analyse globale. Ponemon Institute. Juin 2016. http://www-03.ibm.com/security/data-breach/

2 Friedman, Gabe. JPMorgan Chase Atty : Les banques dépenseront 500M$ en cybersécurité. 29 janvier 2016. https://bol.bna.com/jpmorgan-chase-atty-bank-will-spend-500m-on-cyber-security/. Accédé le 21 septembre 2016

3 Kelley, Diana et Carl Nordman. "Securing the C-suite : Cybersecurity perspectives from the boardroom and C-suite." IBM Institute for Business Value. 2016. ibm.biz/csuitesecurity

Données démographiques et méthodologie
Pour mieux comprendre les défis de la sécurité auxquels votre entreprise est confrontée, comment ils peuvent être abordés et comment sont perçus les solutions de sécurité cognitive et leur potentiel, IBM Institute for Business Value et Oxford Economics à enquêté de mai à juillet 2016 sur un échantillon de 700 RSSI et autres professionnels de la sécurité dans 35 pays, représentant 18 industries.

Pour déterminer nos groupes (Prêtes, Prudentes, Sous-pression), nous avons appliqué un algorithme de quantification vectorielle des k-moyennes qui a révélé trois types de comportements. Ces trois comportements sont basés sur des questions liées à l'efficacité de la sécurité, à la compréhension cognitive, et à la préparation cognitive.

À propos des auteurs
Diana Kelley est Executive Security Advisor (ESA) pour IBM Security et directrice d'IBM Security Newsroom. En tant qu'ESA, elle a plus de 25 ans d'expérience en sécurité informatique, dans le conseil et l'orientation des RSSI et des professionnels de la sécurité. Elle a participé au rapport IBM X-Force et publie fréquemment des articles de recherches et d'analyses sur le blog Security Intelligence. Elle est actuellement membre de la faculté IANS Research et siège au conseil consultatif d'InfoSec World et du Comité des contenus pour l'Executive Women's Forum. Diana intervient fréquemment dans diverses conférences sur la sécurité. Elle a collaboré comme experte de la sécurité avec *The New York Times, TIME*, MSNBC.com, *la revue Information Security* et *The Wall Street Journal*. Elle est le co-auteur du livre *Cryptographic Libraries for Developers*. Vous pouvez la contacter à l'adresse : drkelley@us.ibm.com.

Vijay Dheap est Directeur des programmes pour la division IBM Security, spécialiste des technologies émergentes intégrées dans des offres commerciales. Il gère actuellement un portefeuille d'offres de Security Intelligence, couvrant Advanced Analytics, Cognitive et SaaS. Antérieurement, il a dirigé des entreprises de sécurité mobile et de cybercriminalistique. Vijay est un véritable scientifique qui a reçu le titre d'IBM Master Inventor. Son portefeuille de brevets couvre des innovations dans les domaines de la sécurité, de la collaboration professionnelle et des mobiles. Il a un MBA international de la Duke Fuqua School of Business et une maîtrise en génie informatique de l'University of Waterloo, Canada. Vous pouvez le contacter à l'adresse : vdheap@us.ibm.com.

David Jarvis est le directeur de la sécurité et CIO pour IBM Institute for Business Value. Il est responsable du développement et de l'exécution d'un programme qui explore des thèmes d'ordre commercial et technologique émergents dans ces domaines. David est un expert passionné du développement et de la gestion des points de vue du marché, de projets de prévisibilité stratégique et de réflexion avancée. Il a occupé plusieurs postes chez IBM dans ces domaines. Il est l'auteur de nombreux rapports d'expertise sur la cybersécurité, incluant les évaluations d'IBM pour les RSSI de 2012 – 2014. Outre ses responsabilités de chercheur, David enseigne la prévisibilité commerciale et la résolution créative des problèmes. Vous pouvez le contacter à l'adresse : djarvis@us.ibm.com.

Carl Nordman est Directeur du C-suite Study Program et dirigeant de CFO Research pour IBM Institute for Business Value. Il est responsable de la recherche principale dans ces deux domaines. Il dirige des études sur l'identification des tendances et des perspectives sur les questions stratégiques actuelles. Carl a plus de 25 ans d'expérience dans le domaine du risque financier et de la fraude. Il a précédemment occupé des postes chez IBM Consulting Services, réalisé des missions pour des CFO d'entreprises des « Fortune 1000 », géré des services « Finance and Accounting BPO » en tant que responsable de comptes pour plusieurs clients. Vous pouvez le contacter à l'adresse : carl.nordman@us.ibm.com.

Compagnie IBM France
17, avenue de l'Europe
92275 BOIS COLOMBES CEDEX

IBM Ireland enregistré en Irlande en tant que société numéro 16226

Pensez à recycler

SEL03111-FRFR-00