Séparés par un language commun :

Les cadres dirigeants sont-ils en mesure de cerner les menaces pour mieux faire face aux cyberattaques ?

kaspersky

Sommaire

Introduction

> **“ Le langage est très puissant. Le langage ne se contente pas de décrire la réalité. Le langage crée la réalité qu'il décrit”** **Desmond Tutu**

Le langage est important. Sans lui, il n'y aurait pas… eh bien, de langage, et tout ce qui en dépend, que ce soit les livres, les archives, le code informatique ou encore les messages WhatsApp de vos amis et de vos proches. Le langage est le vecteur de transmission d'absolument tout, des normes sociales à la culture, en passant par l'histoire collective, les mythes, les religions et toutes les formes d'art, et la cybersécurité ne fait pas exception: elle aussi possède son propre langage.

On sait déjà depuis longtemps que les cybermenaces sont devenues un problème du quotidien, qu'elles prennent toutes les formes et toutes les tailles et qu'elles s'expriment dans des langages technologiques variés et des langues différentes. Les forums Internet, les publications sur les réseaux sociaux et les chaînes d'information du monde entier diffusent des informations sur les dernières attaques qui, sous forme écrite ou verbale, sont l'articulation d'un mélange d'acronymes, de jargon et d'expressions idiomatiques qui servent de raccourci à ceux qui maîtrisent les codes de la cybersécurité, mais qui peuvent être difficiles à interpréter pour quiconque n'a pas d'expérience préalable du secteur.

Les termes "deep web" et "dark web" sont souvent utilisés de manière interchangeable, évoquant des images de groupes criminels se réunissant pour acheter des numéros de cartes de crédit, des drogues, des armes, de la fausse monnaie et des données de comptes piratés qui peuvent être utilisés pour s'introduire dans les ordinateurs des victimes, voire pour voler leur identité. Dans les faits, il s'agit de deux choses différentes. Le "deep web" désigne simplement tout ce qui se trouve sur l'internet sans être indexé par des moteurs de recherche comme Google, et donc introuvable par ce biais.

Le "dark web" est un sous-ensemble du deep web qui est intentionnellement caché et nécessite un navigateur spécifique pour y accéder. Il existe des raisons légitimes pour lesquelles certaines personnes pourraient souhaiter mettre à disposition des informations qui ne peuvent pas être indexées comme elles le sont dans le web de surface. Cela joue par exemple un rôle important dans les luttes pour les droits de l'homme, pour les militants et les journalistes de pays opprimés, les gouvernements de leurs pays ne leur permettant pas de s'exprimer librement. Cependant, il faut bien admettre que le dark web est également employé pour mener des activités illégales.

Étant donné la nature ésotérique des transactions illégales qui s'y déroulent, il est impossible de les interpréter et de les comprendre sans maîtriser les codes langagiers de la cybercriminalité. Le côté le plus épineux du dark web, celui qui concerne les logiciels malveillants, les attaques DDoS, les botnets, les chevaux de Troie, les escroqueries par hameçonnage et les enregistreurs de frappe, est bien documenté, mais de quoi s'agit-il réellement et que doit connaître un dirigeant d'entreprise pour pouvoir protéger cette dernière au mieux?

Alors que les pratiques commerciales sont continuellement repensées à l'échelle globale dans un contexte de bouleversements géopolitiques, environnementaux et économiques, il n'a jamais été aussi essentiel de

connaître la nature des menaces de cybersécurité à tous les niveaux de l'entreprise. La numérisation croissante du monde signifie que presque toutes les décisions et transactions commerciales sont désormais concernées par la cybersécurité. Les priorités, qui portaient hier sur les pare-feux et la gestion des identités, se concentrent aujourd'hui sur des défis stratégiques tels que la confiance dans la marque, la sécurité des produits et la résilience.

Kaspersky est une entreprise internationale dont les experts en threat intelligence / renseignement sur le menace sont actifs partout dans le monde. L'entreprise a mis à profit son expérience unique pour mener des recherches approfondies sur la façon dont la nature évolutive des menaces de cybersécurité est interprétée par les responsables chargés de défendre les entreprises contre ces dernières.

Ces dirigeants se concentrent-ils sur les véritables menaces et en discutent-ils en réunion ? Ont-ils investi dans les bons outils pour se défendre ? Sont-ils seulement conscients des menaces les plus dangereuses pour leur entreprise ?

Notre étude exclusive révèle que les dirigeants sont généralement conscients de la fréquence des attaques contre leurs entreprises, mais que le langage et la terminologie utilisés pour décrire les menaces cyber sont tout simplement trop opaques pour être interprétés correctement et ne sont généralement pas compris. En d'autres termes, **les dirigeants d'entreprise se retrouvent souvent dans des situations où ils doivent prendre des décisions cruciales sans avoir une image claire du paysage des menaces et du risque qu'elles peuvent représenter pour leur organisation.**

Le rapport suivant met en évidence, d'une part, les progrès considérables réalisés en matière de sensibilisation à la cybersécurité au sein des conseils d'administration et, d'autre part, les points à améliorer. Les résultats révèlent que si les informations sur le sujet et les préoccupations des groupes dirigeants ne manquent pas, ils souffrent tout de même d'un manque évident de renseignements disponibles et exploitables.

Méthodologie

Un total de 1 800 entretiens avec des cadres supérieurs de grandes entreprises de plus de 1 000 employés ont été menés dans 12 pays en septembre 2022: en France (200), au Royaume-Uni (200), en Allemagne (100), en Autriche (50), en Suisse (50), aux Pays-Bas (100), en Belgique (100), en Espagne (200), au Portugal (200), en Italie (200), en Roumanie (200) et en Grèce (200). Les personnes consultées ont été interrogées sur la cybersécurité au sein de leur organisation, les mesures prises pour se protéger des menaces et les obstacles auxquels les équipes de direction sont confrontées.

Tout au long de ce rapport, les Directeurs généraux, les responsables d'exploitation, du marketing, des risques, des investissements, des finances, de la conformité et de l'information sont désignés par le terme "C-suite" (ou cadres supérieurs/dirigeants).

Principales conclusions

Les cadres dirigeants savent que les cyberattaques représentent la plus grande menace pour les activités de leur entreprise, pourtant, plus l'entreprise est grande, moins la menace est au cœur des préoccupations du conseil d'administration :

- Du point de vue des responsables, les plus grands risques auxquels les entreprises sont actuellement confrontées sont les cyberattaques (49 %), qui inquiètent plus que les aléas économiques tels que l'inflation et les taux d'intérêt (37 %).
- Dans cette optique, un peu plus de la moitié (51 %) des dirigeants interrogés, et 57 % des dirigeants français ont déclaré que **la cybersécurité est désormais systématiquement à l'ordre du jour** des réunions de leur conseil d'administration, tandis que 43% des répondants européens et 36,5 % des répondants français indiquent qu'elles sont à l'agenda de temps en temps.
- Pourtant, **plus l'entreprise est grande, moins ses cadres ne se préoccupent des cybermenaces** : seulement 35 % des entreprises de plus de 5 000 employés admettent être parfaitement au fait des attaques, contre 52 % des entreprises de 1 000 à 1 999 employés.

Bien que la cybersécurité soit une priorité incontestable pour les cadres dirigeants, le langage utilisé pour décrire les menaces a un impact important sur la capacité des agents à les comprendre et à agir :

- Malgré les inquiétudes des cadres dirigeants vis-à-vis de la cybersécurité, près de la moitié des responsables de la sécurité (48 %) interrogés ont déclaré que **le jargon spécialisé et les termes technologiques consacrés sont déroutants et constituent le principal obstacle à la compréhension de la cybersécurité** par les équipes de direction au sens large, et à la façon dont elles doivent s'y prendre pour faire face aux menaces.
- 38 % des dirigeants interrogés, et près de 45 % des dirigeants français ont déclaré que **le vocabulaire de base de la cybersécurité, des termes tels que "malware", "phishing" et "ransomware", prêtent à confusion.**
- En outre, les restrictions budgétaires (47 %, et 52 % en France) et le manque de formation (43 %, et 51.5 % en France) sont d'autres freins majeurs qui expliquent les lacunes des cadres supérieurs en matière de cybersécurité.

Bien qu'il y ait quelques spécificités régionales, les responsables dépendent très généralement des réseaux sociaux, des blogs et des sites d'informations pour recueillir des renseignements :

- Afin de mieux comprendre la cybersécurité, près de la moitié (47 %) des répondants et près de 6 décideurs français sur 10 ont déclaré **se fier aux médias sociaux, aux blogs sur la cybersécurité et aux sites d'informations accessibles au public** pour recueillir des renseignements sur les tendances en matière de cybersécurité afin d'en discuter au travail.
- Parmi tous les pays étudiés, ce sont les répondants espagnols (49 %) qui sont **les plus susceptibles de se tourner vers le dark web pour recueillir de la threat intelligence** afin d'en discuter en réunion. Quant aux répondants français, ils sont 42 % à avoir recours à ces sources d'information.

Oui, nous savons bien que la cybersécurité est notre plus gros problème… Pourtant, ce n'est généralement pas un sujet prioritaire lors des conseils d'administration.

Au cours des 12 derniers mois, les incidents relatifs à la cybersécurité n'ont pas cessé de faire la une des journaux partout dans le monde, avec des attaques très médiatisées entraînant perte d'argent, impact sur la réputation des entreprises et vulnérabilités au niveau humain. Il n'est donc pas surprenant que notre recherche révèle que presque tous (99 %) les cadres dirigeants interrogés sont désormais conscients de la fréquence à laquelle leurs entreprises sont prises pour cible par des acteurs de la menace.

Parmi ces répondants, 52 % des cadres dirigeants d'entreprises de 1 000 à 1 999 employés ont affirmé qu'ils étaient très conscients de la fréquence à laquelle leur entreprise était attaquée, tandis que seuls 35 % de leurs pairs travaillant dans des entreprises de plus de 5 000 employés ont fait le même constat. En outre, près de la moitié (49 %) des cadres dirigeants interrogés ont admis que la cybercriminalité est désormais la plus grande menace auquelle leur entreprise est confrontée, bien devant les principaux aléas économiques tels que la hausse de l'inflation (37 %), la réglementation et la conformité (35 %), et les concurrents (29%). Le classement est le même pour les dirigeants français avec les cyberattaques arrivant en tête des menaces (46%), suivies par les facteurs économiques (37%).

Malgré cette compréhension claire de la prévalence des risques liés à la cybersécurité, 43 % des répondants ont déclaré que cette dernière n'était à l'ordre du jour des réunions du conseil d'administration que de temps en temps. Parmi ceux-ci, 1 cadre dirigeant sur 7 (14%) travaillant dans une entreprise de plus de 5 000 employés a déclaré que la cybersécurité est rarement un point à l'ordre du jour lors des réunions de direction ou des conseils d'administration. A titre de comparaison, pour les entreprises de 1000 à 2999 employés, seuls 3% des cadres interrogés ont répondu de la sorte.

Ces résultats soulignent que plus l'organisation est grande, plus la déconnexion entre ceux qui ont des connaissances techniques et les décideurs est conséquente, ce qui suggère un échec à exprimer les enjeux relatifs à la cybersécurité dans la langue des affaires, de façon à ce qu'ils soient compréhensibles pour les dirigeants.

Les cadres dirigeants considèrent la cybersécurité comme le plus gros problème auquel sont confrontées leurs entreprises, avec près de la moitié d'entre eux la considérant comme un plus gros problème que les facteurs économiques comme l'inflation et son impact sur les coûts pour l'entreprise. Cependant, plus l'organisation est grande, moins il est probable que les cadres dirigeants aient une connaissance approfondie des principaux problèmes de cybersécurité et des conséquences qu'ils peuvent avoir sur l'entreprise, et que ces sujets soient régulièrement discutés en salle de conférence.

	UK	France	DACH	Benelux	Espagne	Portugal	Italie	Roumanie	Grèce
Cyberattaques	57.0%	46.0%	61.0%	52.0%	45.5%	51.5%	44.0%	45.0%	43.0%
Facteurs économiques	30.5%	37.0%	35.0%	44.0%	40.5%	33.0%	41.0%	45.5%	28.0%
Réglementation et conformité	27.0%	36.0%	35.0%	35.5%	38.5%	35.0%	34.5%	37.0%	34.0%
Catastrophes naturelles	26.0%	36.5%	29.0%	30.0%	40.5%	26.5%	31.0%	32.5%	26.0%
Concurrence	30.5%	30.0%	26.5%	30.0%	31.5%	30.5%	28.0%	25.0%	31.0%
Défis environnementaux	26.0%	31.5%	25.0%	32.0%	37.0%	20.0%	29.5%	29.0%	28.0%
Mouvement syndical	29.5%	30.0%	29.0%	23.0%	27.5%	29.5%	26.00%	26.0%	34.0%

Fig 1. Principaux risques/menaces pour la continuité des activités

Évidemment, plus une entreprise est grande et plus les vecteurs de menace y sont nombreux (car en toute logique, plus il y a d'employés, plus il y a de systèmes à protéger), mais ces chiffres suggèrent que les entreprises courent en permanence pour rattraper un retard généré par leur propre croissance. Les décideurs de toutes les entreprises doivent décider de leurs priorités, que celles-ci portent sur le recrutement, l'acquisition de clients, la maintenance de l'infrastructure, etc., mais les résultats indiquent une plus grande déconnexion au sein des grandes organisations. Une déconnexion entre les cadres dirigeants et leur capacité à vraiment comprendre les tenants et aboutissants de leur plus grand défi : la cybersécurité.

Comprendre l'impact d'une attaque sur les opérations commerciales, ses conséquences financières et la manière dont la réputation d'une organisation peut être affectée par une faille de sécurité n'est plus une option pour les décideurs. Il est inquiétant de voir les conseils d'administration des grandes organisations ne pas mesurer l'importance de la cybersécurité et de la veille sur les menaces pour leur entreprise, procédant d'une déconnexion entre les spécialistes techniques et les décideurs. Bien que le conseil d'administration n'ait pas nécessairement besoin de comprendre les subtilités complexes de la cybersécurité en tant que telle, il doit comprendre facilement l'impact que les menaces peuvent avoir sur l'entreprise

David Emm
Principal Security Researcher, Global Research and Analysis Team chez Kaspersky

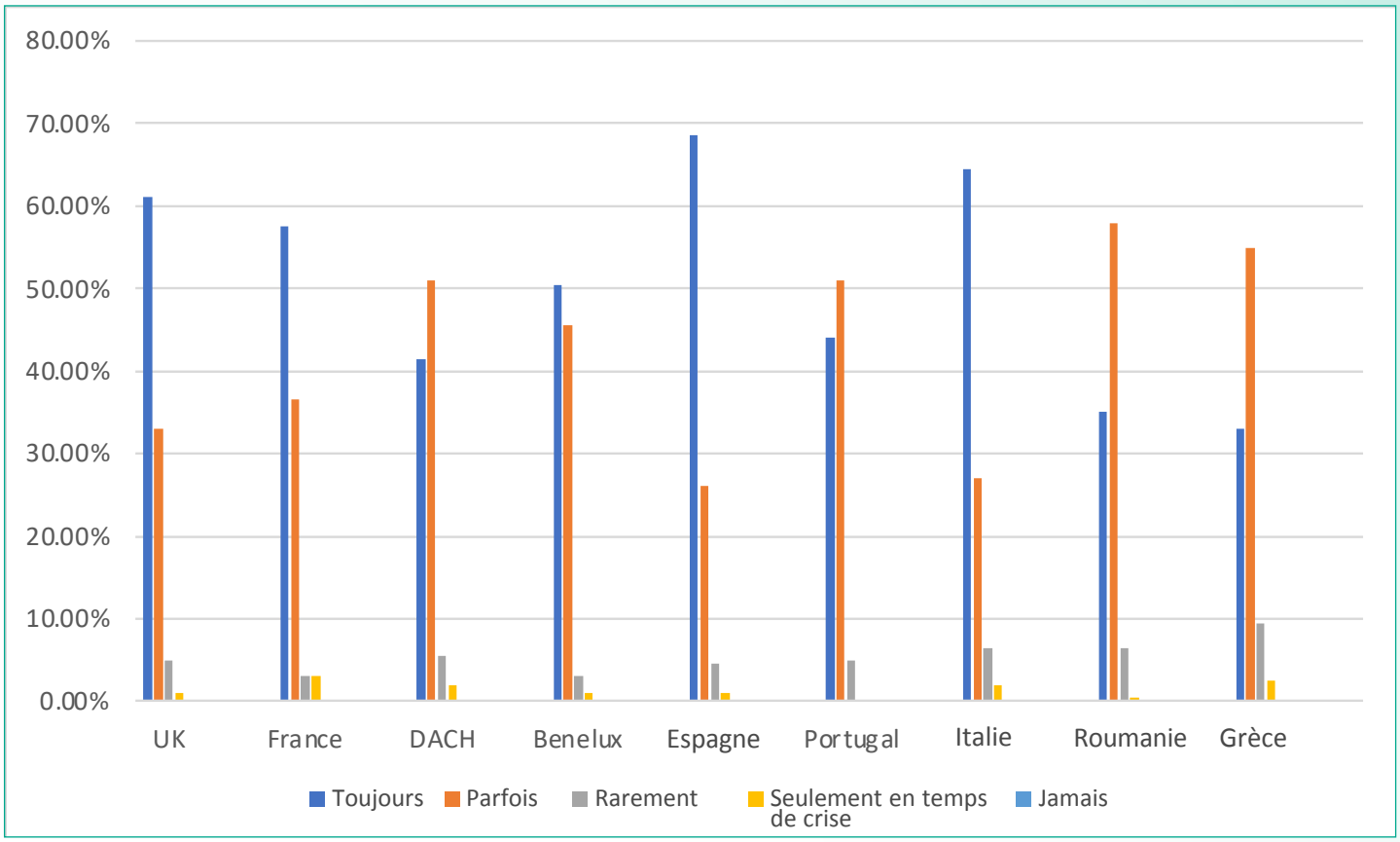

Fig. 2 La cybersécurité est-elle un sujet à l'ordre du jour des réunions de direction et des conseils d'administration ?

L’écueil principal, c’est de ne pas comprendre ce que ces termes spécifiques signifient vraiment

Bien que la cybersécurité soit une préoccupation claire pour les cadres dirigeants et leurs entreprises, près de la moitié (48 %) des spécialistes de la sécurité, de la conformité et des risques pensent que le jargon et les termes techniques spécifiques représentent le plus grand obstacle pour l’équipe de direction élargie qui doit gérer les problèmes de cybersécurité, aussi bien concernant le sens de ces termes que ce qu'ils doivent faire à leur sujet.

Cela est particulièrement visible dans la région DACH (Allemagne, Autriche, Suisse : 47%), au Portugal (47 %), en Espagne (44 %) et au Royaume-Uni (42 %) avec des cadres dirigeants spécialistes de la sécurité déclarant que le jargon est la principale barrière pour la compréhension de leur équipe de direction des menaces de cybersécurité les plus pressantes (40 % en France).

Pour preuve, **38 % de toutes les personnes interrogées ont déclaré qu'elles trouvaient les termes de base de la cybersécurité, comme “malware”, “phishing” et “ransomware” déroutants.** C’est particulièrement prégnant en France avec 46 % des cadres interrogés ayant avoué trouver ces termes confus. Les expressions un peu plus techniques utilisées, telles que “Zero Day Exploits” et “Suricata rules”, ont connu des niveaux de confusion similaires, 39 % des répondants (près de 48% des français) affirmant ne pas bien comprendre ces termes..

Parmi tous les cadres dirigeants interrogés, ce sont les Italiens qui sont le plus susceptibles de trouver les termes Malware, Phishing et Ransomware déroutants, avec exactement la moitié des répondants (50 %) avouant que ces termes n'étaient pas entièrement compris. Les personnes interrogées en France sont elles les plus à même (47 %) de trouver le terme «APT (attaque d’un Etat nation)» déroutant. Toujours en France, il apparaît que le terme le mieux compris est la notion d’«Exploit Zero Day», avec «seulement» 39% des Français le trouvant déroutant, contre plus de 44% de confusion pour tous les autres termes.

Globalement, ce sont les restrictions budgétaires (47 %) mises en place par l'entreprise et le manque de formation (43 %) au sein de l'équipe de direction qui complètent les trois principaux obstacles à l’établissement d'une bonne défense en cybersécurité. Parmi les pays interrogés, ce sont les cadres dirigeants basés au Royaume-Uni (56 %) et en France (52 %) qui ont déclaré que c'était le budget qui les contraignait le plus, alors qu'en Italie et DACH, 42% ont déclaré que l'insuffisance des formations en était la cause principale.

Pour résumer, les résultats des recherches de Kaspersky révèlent qu'il existe des barrières importantes qui empêchent les cadres dirigeants de développer une compréhension globale et une sensibilisation aux problèmes de cybersécurité les plus importants auxquels sont confrontées leurs entreprises. C'est le langage utilisé pour transmettre et arbitrer ces problèmes qui entrave actuellement la capacité d'une organisation à développer une culture des meilleures pratiques en matière de cybersécurité, à partager les connaissances et, en fin de compte, à transmettre des renseignements exploitables.

Nos données suggèrent que la cybersécurité, à des degrés variables selon l'emplacement géographique, est une industrie qui se parle à elle-même, utilisant un langage qui peut être incompréhensible pour ceux qui n'ont pas de formation spécialisée en sécurité. La prise de conscience et la compréhension peuvent suivre, mais pour que cela se produise, un pont est nécessaire pour interpréter le lexique et le verbiage utilisés sur le dark web et dans les conventions communément comprises dans les comités de direction.

Petit glossaire la Threat Intelligence

Malware/Maliciel	Terme générique désignant les programmes informatiques conçus pour être installés sur l'ordinateur d'une personne et lui infliger des dommages de diverses manières. Contraction “malicious software” (logiciel malveillant, “maliciel” dans sa version francisée). Les malwares courants incluent les virus, les vers, les chevaux de Troie, les logiciels espions, les logiciels publicitaires et les rançongiciels.
Attaques phishing	Le phishing est une méthode d'ingénierie sociale employée à la fois dans les activités cybercriminelles et les attaques APT, dans laquelle les cibles sont contactées par courrier électronique, téléphone ou SMS par une personne se faisant passer pour une institution légitime afin de compromettre un appareil et d'accéder à des données sensibles. Ces données peuvent également être utilisées à des fins d'usurpation d'identité, ou encore de fraude financière.
Attaques d’Etat-Nation(APT)	Il s'agit d'attaques très médiatisées visant des infrastructures critiques, dans le but d'affaiblir la puissance économique, militaire ou politique d'un pays donné.
Attaques ransomwares	Logiciel malveillant qui chiffre les données ou en bloque l'accès, exigeant de l'utilisateur qu'il paie pour débloquer ou déchiffrer les données. Différentes variétés de logiciels malveillants ciblent les systèmes de bureau et les appareils mobiles.
Attaques de la chaîne d’approvisionnement	Une attaque de la chaîne d'approvisionnement cible les éléments de la chaîne d'approvisionnement avant la vente à l'utilisateur final. Un exemple de ce type d'attaque consiste à modifier la mise à jour d'un produit de manière à ce qu'un logiciel malveillant soit envoyé à tous les clients de ce produit.
Exploit Zero-Day	Ce terme est utilisé pour décrire le code d'exploitation qui a été écrit pour tirer parti d'une vulnérabilité avant que le fournisseur du logiciel ne la connaisse et n'ait eu l'occasion de publier un correctif pour cette dernière. Le résultat est que les attaquants potentiels sont libres d'exploiter la vulnérabilité, à moins que des technologies proactives de prévention des exploits aient été mises en œuvre pour défendre l'ordinateur ciblé par l'attaquant.
Indicateur de Compromission (IoC)	Il s'agit d'un élément ou d'une activité qui, s'il est observé sur un réseau ou sur un appareil, indique une forte probabilité d'accès non autorisé au système. En d'autres termes, la présence d'un IoC indique que le système est compromis. De tels indicateurs sont utilisés pour détecter les activités malveillantes à leurs débuts ainsi que pour prévenir les menaces connues.
TTPs	TTPs signifie "tactiques, techniques et procédures". Il s'agit du terme utilisé par les professionnels de la cybersécurité pour décrire les comportements, les processus, les actions et les stratégies utilisés par un acteur menaçant pour élaborer des menaces et mener des cyberattaques.
Règles Mitre ATT&CK	Adversarial Tactics, Techniques & Common Knowledge (Tactiques, techniques et connaissances communes de l'adversaire) est une base de connaissances décrivant les tactiques et techniques cybercriminelles sur la base d'observations du monde réel. La MITRE Corporation a créé cette base de connaissances en 2013 et l'objectif du projet est de développer une matrice structurée des techniques cybercriminelles pour faciliter la réponse aux cyber incidents.
Règles Suricata	Les règles Suricata sont la méthode généralement utilisée pour partager et faire correspondre les renseignements sur les menaces avec le trafic réseau.
MD5	Une fonction de hachage qui convertit un ensemble de données de taille aléatoire en un hachage, une séquence pseudo-aléatoire de caractères d'une longueur prédéfinie. Le résultat est une sorte d'identifiant pour le tableau de données cryptées. MD5 est utilisé pour vérifier l'authenticité, l'intégrité et l'immuabilité de tout ensemble de caractères (par exemple, un code informatique). Si les sommes de contrôle correspondent, cela signifie que le fichier n'a pas été modifié. Certains systèmes d'exploitation utilisent MD5 pour stocker les mots de passe.
YARA	Outil principalement utilisé dans la recherche et la détection des logiciels malveillants qui fournit une approche basée sur des règles pour créer des descriptions de familles de logiciels malveillants sur la base de modèles textuels ou binaires.

Glossaire entier disponible sur : https://encyclopedia.kaspersky.com/glossary/

La communication ne devrait pas être un frein à la cybersécurité. Nos résultats soulignent l'importance de la planification stratégique, de la budgétisation et de la recherche de personnel compétent à tous les niveaux de l'entreprises, mais aussi de la transmission des incidents pertinents du bas vers le haut, de manière claire et compréhensible, sans avoir à recourir à un langage flou ou à un jargon industriel complexe. Une communication bidirectionnelle efficace est essentielle pour une activité fonctionnelle à long terme.

Christian Funk
Responsable DACH au Global Research & Analysis Team (GReAT) chez Kaspersky

	UK	France	DACH	Benelux	Espagne	Portugal	Italie	Roumanie	Grèce
Restrictions budgétaires	56.50%	52.0%	46.5%	47.0%	47.5%	42.5%	42.5%	43.5%	45.5%
Formation insuffisante	43.00%	51.5%	42.0%	40.5%	55.0%	39.5%	42.0%	42.5%	31.5%
Jargon/ termes industriels déroutants	42.00%	40.0%	46.5%	43.0%	44.0%	46.5%	41.0%	45.0%	31.5%
Manque d'outils/ de moyens	35.00%	37.5%	40.5%	49.5%	45.5%	35.0%	44.5%	37.5%	47.0%
Manque de temps	37.50%	35.5%	28.0%	41.0%	42.0%	30.0%	40.0%	35.0%	46.0%
Nous ne rencontrons pas d'obstacles	0.50%	2.5%	2.0%	0.5%	1.5%	1.0%	8.0%	0.0%	0.0%

Fig 3. Quels sont les obstacles, s'il y en a, qui empêchent votre équipe de direction d'avoir une compréhension complète et approfondie de la cybersécurité ?

Ok, mais alors c'est quoi un malware?

Tout d'abord, il est important de comprendre ce à quoi les organisations sont confrontées.

Conçu à l'origine comme un projet du ministère américain de la Défense au début des années 1990 pour développer un réseau anonyme et chiffré qui protégerait les communications sensibles des espions américains, le dark web mène désormais sa propre vie. Bien qu'il existe différentes variantes basées sur leur mise en œuvre technique et leurs "objectifs" respectifs, il peut être défini comme un réseau hautement sophistiqué et complexe de forums hors réseau, de salons de discussion, d'hébergeurs de fichiers et d'images, et de marketplaces commerciales.

Pour les personnes vivant sous des régimes oppressifs qui bloquent une grande partie de l'internet ou punissent la dissidence politique, le dark web est une bouée de sauvetage qui permet d'accéder à l'information et de se protéger des persécutions. Mais pour l'écrasante majorité du dark web qui est utilisée pour des activités néfastes, la sophistication et la complexité de ces réseaux offrent aux criminels l'environnement idéal pour prospérer, loin des regards indiscrets des autorités.

Les pages consultables sur le dark web ne disposent pas d'une indexation standard des pages web par les moteurs de recherche du web de surface, tels que Google ou autres moteurs de recherche populaire, qui ne peuvent pas découvrir ou afficher les résultats des pages. Selon le type de dark web, il peut utiliser des tunnels de trafic virtuels via une infrastructure réseau aléatoire qui rend le dark web inaccessible par les moyens traditionnels. Pour un utilisateur non averti, il s'agit d'une forteresse impénétrable.

Afin de s'informer, et de monter en compétence concernant les menaces en provenance du dark web, **notre étude révèle que près de la moitié (47%) des cadres dirigeants, et 55% des cadres dirigeants français, se fient principalement aux articles de presse, aux blogs de**

l'industrie et aux contenus de réseaux sociaux pour avoir un aperçu des sujets de cybersécurité qui peuvent être discutés lors des réunions de conseil d'administration. Cette méthode d'éducation à la cybersécurité est un bon moyen de comprendre les menaces auxquelles les entreprises sont confrontées ; cependant, elle doit faire partie d'une approche d'éducation et de sensibilisation à plusieurs niveaux.

Les informations accessibles au public fournissent un service essentiel pour se tenir au courant des derniers problèmes, mais la dépendance aux informations sur les nouvelles tendances les plus "populaires", et le fait de s'y limiter pourrait entraver la capacité des dirigeants d'entreprise à développer une compréhension holistique de la véritable nature des menaces représentant un risque pour leur entreprise, et de la manière de s'en protéger.

Seuls 40% des cadres dirigeants interrogés, et 35,5% des cadres français ont déclaré se tourner vers des fournisseurs et/ou des experts externes pour recueillir des informations sur les dernières menaces provenant du dark web, la majorité préférant donc développer leurs connaissances en utilisant les informations disponibles publiquement. Bien que plus de deux cadres dirigeants sur cinq (46 %, et 47 % en France) utilisent des sources privées de renseignements sur les menaces pour collecter des informations, et en discuter lors des réunions du conseil d'administration, 40 %, et près de la moitié des français (48,5 %) s'appuient sur des ressources internes pour déchiffrer les menaces émergentes du dark web et illustrer ensuite les résultats lors des réunions du conseil d'administration.

Parmi tous les pays étudiés, les cadres supérieurs espagnols sont les plus susceptibles d'utiliser les renseignements sur les menaces disponibles sur le dark web et d'en discuter lors des réunions du conseil d'administration (50 %), tandis qu'à l'opposé, les cadres supérieurs interrogés au Royaume-Uni sont les moins susceptibles de le faire en Europe (34 %). La France se situe entre les deux, avec 42 % des répondants ayant indiqué utiliser des sources de threat intelligence tirées du dark web.

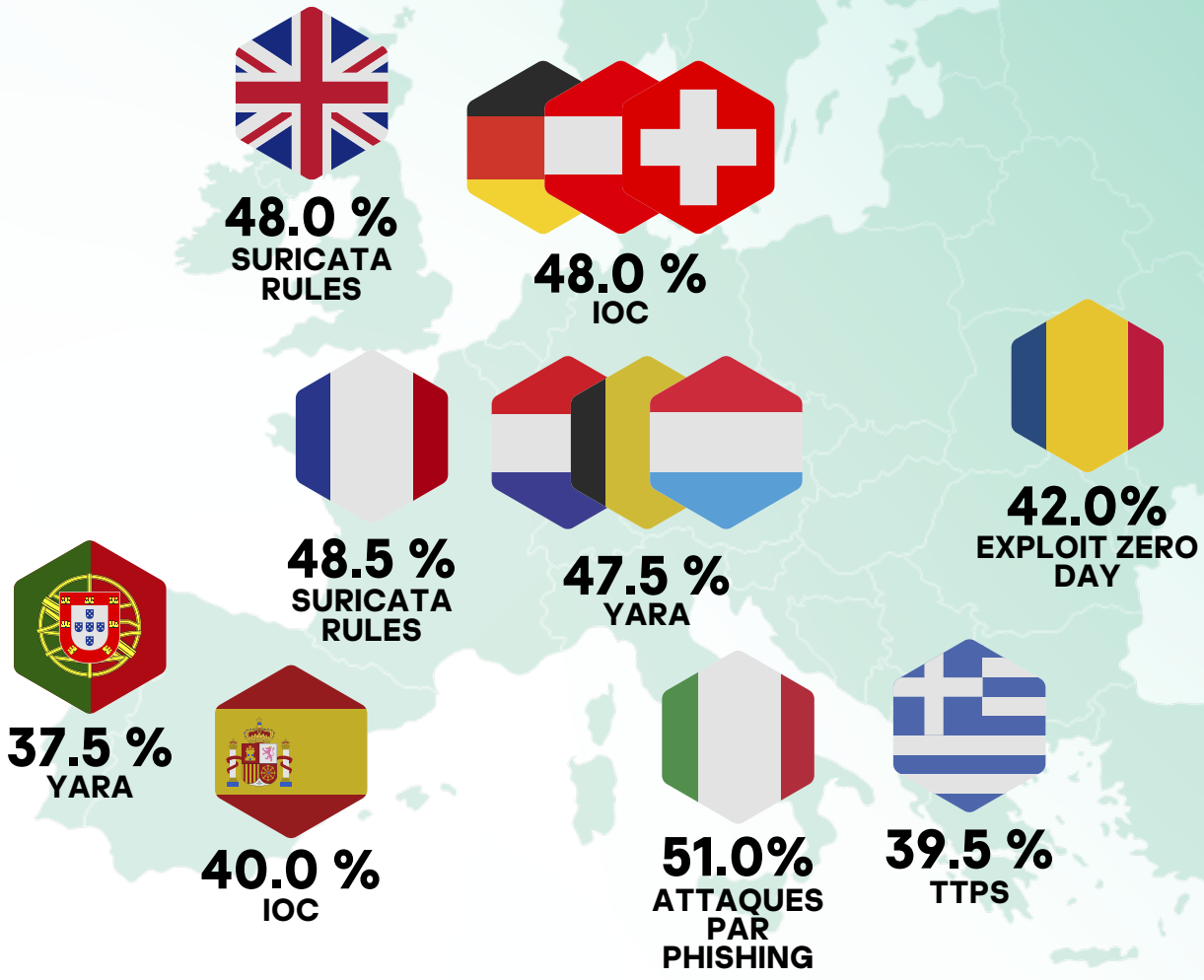

Fig 4. Pourcentage de terminologies que les cadres ont du mal à comprendre

Cybersécurité : qui allez-vous appeler ?

Les recherches dressent le portrait de cadres dirigeants qui ont besoin d'aide pour comprendre les menaces de cybersécurité auxquelles leurs entreprises sont confrontées chaque jour. Le paysage des cybermenaces est complexe et en constante évolution, fruit du travail de criminels comptant parmi les plus motivés et sophistiqués de la planète sur le plan technologique. C'est une chose d'être conscient des cybermenaces qui existent, et c'en est une autre de les comprendre.

Le langage utilisé a évolué au même rythme que les menaces. Comme nous l'avons vu au cours de ce rapport, cette la rapidité de cette évolution, dans de nombreux cas, dépasse la capacité des entreprises à suivre la cadence. La priorisation d'autres objectifs, l'évolution rapide de l'environnement économique et social ainsi que les pressions concurrentielles n'ont pas éclipsé la prise de conscience de la menace que représentent les cyberattaques, mais l'incapacité des dirigeants à comprendre leur nature et à agir en conséquence font que la cybersécurité n'est plus toujours à l'ordre du jour des réunions des conseils d'administration.

L'utilisation de ressources accessibles au public et l'augmentation du budget alloué aux formations contribuent à la sensibilisation. Toutefois, la réalité est que sans une expertise solide pour identifier, analyser et recouper les cybermenaces, les organisations ne s'arment qu'à moitié contre elles. Au cœur d'une stratégie optimale, on trouve un interprète ou un partenaire capable non seulement de parler le langage du cybercrime, mais aussi de comprendre comment la confidentialité et l'anonymat qui protègent les criminels peuvent être utilisés contre eux pour établir un rapport et extraire des renseignements essentiels.

Pour plus d'informations sur la façon dont les entreprises peuvent se protéger contre les cybermenaces, rendez-vous sur le portail Kaspersky Threat Intelligence ici.

Autres facteurs entravant la sensibilisation à la cybersécurité

- 41 % des cadres dirigeants (37% en France) estiment que le manque d'outils à leur disposition constitue un obstacle majeur à une compréhension complète et approfondie de la cybersécurité et des menaces qu'elle recèle.
- Selon les dirigeants interrogés, les responsables informatiques sont les plus susceptibles de présenter des informations sur les menaces lors des réunions de leur conseil d'administration (51 %), suivis par les RSSI (45 %), les fournisseurs externes de cybersécurité (44 %), les résumés exécutifs écrits non techniques (31 %) et enfin, les partenaires (25 %). En France, les RSSI (53.5 %) passent devant les responsables informatiques (49.5%).
- Les personnes interrogées qui utilisent et discutent des sources publiques de renseignements sur les menaces (sources ouvertes, réseaux sociaux, blogs cyber) lors des comités de direction sont plus susceptibles de dire qu'elles le font pour éviter les perturbations (56 %), plutôt que pour éviter les problèmes de coûts (53 %) ou parce que ces sources sont parmi les plus fiables (22 %).