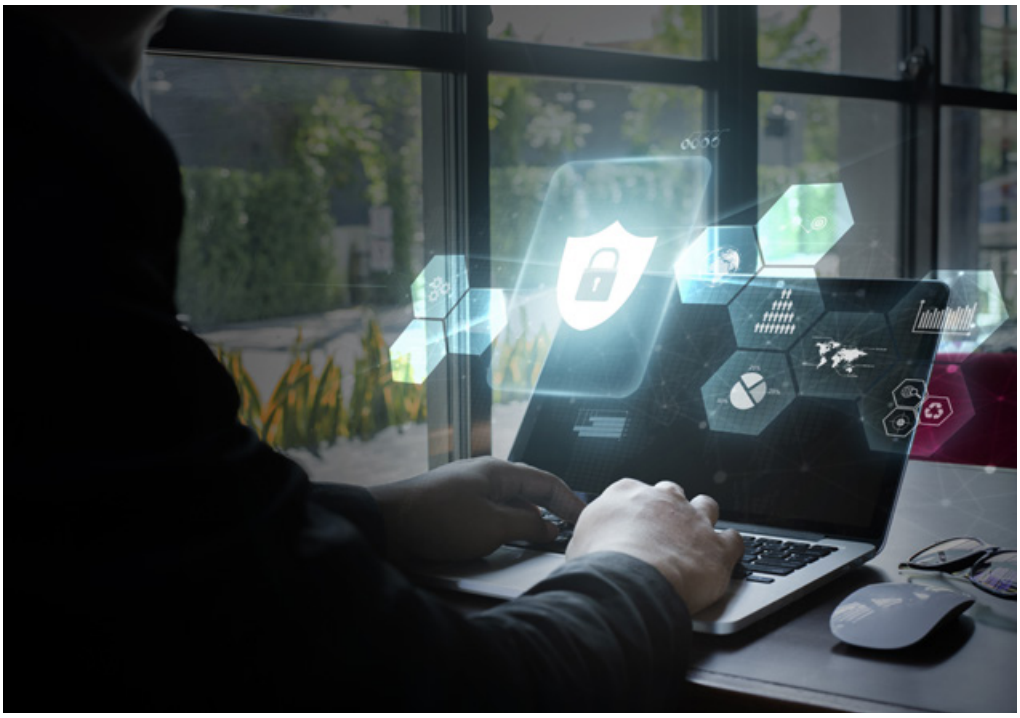
LA CYBERSÉCURITÉ
DE NOUVEAUX DÉFIS



Dans un contexte de digitalisation croissante, de recours massif aux services et travail à distance, le nombre de cyberattaques explose. Il a été multiplié par 4 en France rien qu'en 2020. Face aux menaces croissantes qui pèsent sur les données et ressources informatiques de l'entreprise et à des hackers qui se « professionnalisent », une stratégie de cybersécurité s'impose comme une priorité.

+255 %, c'est le taux d'augmentation, sur la seule année 2020, du nombre d'attaques informatiques répertoriées en France, selon l'Agence nationale de sécurité des systèmes d'information (ANSSI). La plateforme Cybermalveillance.gouv.fr confirmait cette augmentation de la menace cyber dans son rapport d'activités : celle-ci disait avoir enregistré une hausse de fréquentation de +155 % cette même année par des victimes venues y chercher de l'assistance, dont 10 000 entreprises.

Les attaques aux rançongiciels (ou ransomware) constituent aujourd'hui la plus grande menace : elles sont passées en 2020 à 192 contre 54 en 2019, soit une multiplication par 4, avec une demande de rançon de 130 000 euros en moyenne selon l'ANSSI, et représentaient 17 % de demandes d'assistance sur Cybermalveillance.gouv.fr contre 8 % l'année précédente. Suivent ensuite principalement :

- les attaques par déni de service distribué, c'est-à-dire par saturation d'une cible pour tenter de surcharger les serveurs et empêcher que les requêtes légitimes soient traitées ;
- l'hameçonnage ou phishing, qui consiste à envoyer un message en apparence authentique de manière à tromper la vigilance du destinataire, qui a connu une accélération sans précédent ;
- les piratages informatiques ;
- les piratages de comptes.

« Les rançongiciels ont connu une intensification sans précédent en 2020, avec des conséquences souvent désastreuses »
Cybermalveillance.gouv.fr

Un coût financier et réputationnel

« Intensification sans précédent en 2020 », avec « des conséquences souvent désastreuses », c'est le constat que fait le site Cybermalveillance.gouv.fr concernant ces attaques, notamment les rançongiciels. Le désastre ? Leur coût. Exorbitant. La rançon moyenne par incident a en effet augmenté de façon spectaculaire ; elle dépasse les 10 millions de dollars et dans 30 % des incidents, elle est supérieure à 30 millions de dollars, selon le rapport annuel Barracuda Networks qui se penche sur les attaques par ransomware qui se sont produites entre août 2020 et juillet 2021, et le coût de la cybercriminalité à l'économie mondiale a été évalué à 1 000 milliards de dollars par an par McAfee et le groupe américain de réflexion Center for Strategic and International Studies (CSIS) dans dans leur rapport 2020 ! ➤

Photos : ©ADOBESTOCK

FORTINET

La plateforme de cybersécurité intégrée et automatisée

Face à l'empilement des technologies de protection, Fortinet a conçu la Fortinet Security Fabric, une approche plateforme dans laquelle s'intègrent toutes les solutions de cybersécurité. Le point avec Christophe Auberger, responsable cybersécurité évangéliste.

Qu'est-ce qui vous démarque sur le marché de la cybersécurité ?

Christophe Auberger : Aujourd'hui, il n'existe pas de technologie « magique » qui peut protéger de toutes les menaces à la fois. On assiste à un empilement des technologies : en moyenne, les entreprises ont 12 solutions de sécurité et les gens passent plus de temps à faire marcher les produits entre eux qu'à résoudre les problèmes ! Nous avons donc conçu la Security Fabric, une plateforme dans laquelle on va plugger ces solutions : elle peut intégrer la quasi-totalité des solutions du marché - nous avons plus de 500 partenaires - et pas seulement celles de Fortinet, et apporter de l'automatisation. Nous sommes parmi les seuls éditeurs à avoir cette démarche « plateforme » et à proposer ainsi une sécurité large, totalement intégrée, automatisée et haute performance sur l'ensemble de l'infrastructure IT.

L'offre de Fortinet est plus large…

C. A. : Nous sommes partis du Firewall et avons enrichi, au fur et à mesure des innovations et de la transformation numérique des entreprises, nos fonctionnalités et solutions. Pour la sécurité du réseau, nos solutions traitent de manière automatique les droits des utilisateurs où qu'ils se trouvent, donnée importante alors qu'a explosé le télétravail. Parce que les données transitent désormais partout, nous avons fait aussi évoluer le SD-WAN qui gère les connectivités de manière « intelligente » : la solution choisit en temps réel le meilleur lien parmi les options de connectivité et le sécurise. En téléphonie IP par exemple, elle est capable d'opter pour le lien qui a la latence minimum pour assurer une meilleure qualité de communication. Face aux difficultés que peuvent avoir des entreprises à recruter pour assurer leur cybersécurité, nous proposons aussi des solutions pour les SOC. Nous avons également une offre de sécurité dynamique du Cloud, intégrée et automatisée. Les entreprises sont aujourd'hui massivement sur du multi-cloud : ce système permet de sécuriser n'importe quelle application sur n'importe quel Cloud. Nous avons également une offre complète qui assure un accès en toute confiance au réseau de l'entreprise, le Zero Trust Network Access. Les entreprises ont besoin de plus de solutions pour définir les zones de confiance dans leur système d'information alors que les utilisateurs peuvent être sur site ou à l'extérieur et que beaucoup d'objets se connectent au réseau. Il s'agit ainsi de ne jamais faire confiance par défaut et vérifier que ce sont bien les personnes et les équipements autorisés qui se connectent et accèdent aux ressources, y compris sur le Cloud. Enfin, nous proposons un système d'analyse des données pour détecter les comportements à risques, auquel nous ajoutons de l'IA ce qui n'existe pas dans toutes les solutions : les analystes croulent sous les informations alors que 80 % des événements détectés ne sont pas des attaques ; l'IA permet d'identifier ces « faux positifs » et de ne soumettre que 20 % des événements.


Christophe Auberger, responsable cybersécurité évangéliste

Qui utilise vos solutions ?

C. A. : Tout type de structures, PME, ETI, grands comptes… Nous bénéficions de nombreuses reconnaissances, dont le classement, en 2021 pour la 12e fois, dans le Magic Quadrant de Gartner pour les pare-feux d'entreprise, et 7 certifications d'ICSA Labs sur nos solutions.

En quoi consiste votre fonction d'« évangéliste » ?

C. A. : Nous faisons beaucoup de sensibilisation, auprès des entreprises pour identifier leurs problématiques, leurs besoins et voir ce que l'on pourrait leur proposer, mais aussi auprès des écoles d'enseignement supérieur, pour former sur la technologie et inciter les étudiants à entamer une carrière dans le secteur, car celui-ci est confronté à des difficultés de recrutement d'experts en cybersécurité.

FORTINET®

fortinet.com/fr

« Le volume des cyberattaques a augmenté de 238 % à l'échelle mondiale pendant la pandémie »

Rapport HP Wolf Security Blurred Lines & Blindspots – mai 2021

Si l'on déduit de ce coût les dépenses de cybersécurité, les pertes financières engendrées par les cyberattaques (rançons et fortes baisses de la productivité des entreprises face à l'indisponibilité des services informatiques engendrées par ces attaques) sont estimées à pas moins de 945 milliards de dollars !

Et évidemment, être victime d'espionnage, de détournement ou de destruction d'informations à valeur commerciale ou de données personnelles, peut avoir aussi des conséquences désastreuses pour la réputation de l'entreprise.

Tous concernés

Et, triste classement, en 2020, la France était 8e dans le top 10 mondial des crimes commis en ligne, selon le rapport annuel du FBI publié en mars 2021. En tête des cibles privilégiées des hackers, apparaissaient les États-Unis, avec également des pays comme le Canada et le Mexique, et, côté européen, le Royaume-Uni, la Grèce et l'Allemagne.

Tout le monde peut être compromis. Différents rapports observent néanmoins que les attaques par ransomware ciblent fortement les collectivités territoriales, les services de santé et l'éducation, et les entreprises, celles des secteurs du voyage, des services financiers, ou encore celles liées aux infrastructures critiques. En France les exemples ne manquent pas.

Hôpitaux, collectivités, entreprises : des cibles de « choix »

En 2020, les hôpitaux ont fait l'objet de 27 cyberattaques majeures, des rançongiciels. Elles ont visé des centres hospitaliers de Marmande, Albertville, Dax, Villefranche-sur-Saône ou encore Rouen. Depuis 2021, il y en a une par semaine.

D'autres structures publiques constituent des cibles de choix. Des pirates ont, par exemple, profité des failles de sécurité pour rendre indisponibles les listes d'émargement des métropoles d'Aix Marseille ou Charleville-Mézières juste avant les élections municipales. Le 21 mai 2021, les réseaux de la Métropole et de la ville de Grenoble étaient touchés par une cyberattaque de type déni de service distribué. À l'occasion du retour de l'enseignement à distance en avril 2021, la plateforme du CNED « Ma classe à la maison » subissait plusieurs cyberattaques mettant enseignants et élèves face à des pages qui ne fonctionnaient pas.

Les entreprises ne sont pas en reste non plus. Le 24 janvier 2019, l'entreprise Altran voyait une partie de ses activités européennes interrompue à cause d'une attaque rançongiciel. En novembre dernier, une cyberattaque a entraîné le blocage provisoire des paiements par cartes bancaires dans les terminaux des boutiques du groupe New-Orch-Orchestra, tandis que des milliers de données de clients étaient piratées. Le groupe courtier en assurance Adelaïde subissait le même mois une cyberattaque qui paralysait totalement ses services. ➤

GLOSSAIRE

- **OIV :** Opérateur d'importance vitale
- **OSE :** Opérateur de services essentiels
- **MSP :** Managed Service Provider, fournisseur de services informatiques
- **RSSI :** Responsable de la sécurité des systèmes d'information
- **SI :** Système d'information
- **SSII :** Société de service et d'ingénierie informatique
- **SIEM :** Security Information and Event Management
- **SOC :** Security Operations Center
- **VPN :** Virtual Private Network ou réseau privé virtuel

SANS INSTITUTE

Une référence mondiale dans la formation en cybersécurité

Le SANS Institute a pour mission de doter les professionnels de la cybersécurité des compétences pratiques et des connaissances dont ils ont besoin.

Dans un monde où n'importe quel réseau informatique peut faire l'objet de cyber attaques, les entreprises ont relevé le défi : la cybersécurité est devenue un enjeu essentiel pour n'importe quelle société. Les professionnels de la cybersécurité ont toujours besoin de se former, de réactualiser leurs méthodes, de faire face à de nouveaux défis... C'est à leurs besoins que le SANS Institute répond.

Fondé en 1989, et présent en France depuis 2017, le SANS Institute (SysAdmin Audit Network Security Insitute) est un organisme de formation et de recherche ayant pour but de fournir les compétences et le savoir nécessaire à la protection des réseaux et données afin de lutter contre les attaques et permettant ainsi aux professionnels de la cybersécurité de réduire les risques. Des programmes de formation dispensés par des praticiens mondialement connus et reconnus de la cybersécurité ont ainsi été suivis par plus de 200 000 personnes dans plus de 40 pays.

Plus de 80 formations alliant en moyenne 50 % de théorie et 50 % de pratique sont proposées couvrant ainsi diverses problématiques du champ de la cybersécurité tels que le Cloud Security, le Penetration Testing ou encore l'Industrial Control System, et abordant aussi bien les fondamentaux que des sujets spécialisés tels que l'Advanced Exploit Development.

Le SANS Institute est en permanente mutation comme le sont les cyberattaques. La cybersécurité est toujours en renouvellement et de nouveaux défis tels que les ransomwares font constamment leur apparition, ce qui nécessite de rechercher sans cesse de nouvelles méthodes pour conter les nouvelles attaques et, comme le souligne Axelle Saim, directrice France-Luxembourg, « il faut se mettre à jour en permanence » et « avoir une longueur d'avance sur les attaquants ».

Axelle SAIM, SANS EMEA, Directrice France & Luxembourg

Les professionnels de la cyberscurité ont toujours besoin de se former, de réactualiser leurs méthodes, de faire face à de nouveaux défis... C'est à leurs besoins que le SANS Institute répond.

SANS SECURITY AWARENESS

Le SANS Security Awareness (SSA), un programme dédié aux comportements des utilisateurs face aux problèmes de sécurité.
Le SANS Security Awareness, lancé en 2011, est un programme de sensibilisation à la cybersécurité pour les utilisateurs aussi bien que les professionnels qui a très vite rencontré un vif succès dans le monde entier. Développé par des figures renommées de la SSI, ce programme se veut modulable et adaptable aux besoins des différentes entreprises et publics visés. Meagan Tudge, responsable SSA EMEA, le résume ainsi à travers deux objectifs clés : « s'assurer que les entreprises ont toutes les cartes en main pour déployer de nouveaux programmes et pouvoir en suivre le succès » et « revitaliser les programmes existants qui ont échoué par manque d'engagement des utilisateurs ou par manque de mesure d'efficacité ».

Meagan Tudge, SANS Security Awareness, Manager EMPAC

SANS aide également ses clients à construire un programme en partant de zéro, en se focalisant sur les objectifs à atteindre en termes de prise de conscience ou de conformité.

L'enjeu est de responsabiliser et d'éduquer les personnes face aux cybermenaces en leur permettant d'acquérir les bonnes pratiques en matière de cybersécurité. Il s'agit à la fois de donner une prise de conscience des risques et de se détacher d'une certaine « paranoïa » que l'on peut observer notamment en milieu professionnel. Axelle Saim relève qu'on peut observer une différence entre les comportements selon qu'on se situe dans un contexte personnel ou professionnel. Ainsi, de très grandes craintes peuvent survenir au bureau lors de la moindre ouverture de pièce jointe alors que dans la vie privée il y a un certain détachement par rapport aux cyber risques. Le programme SANS Security Awareness offre la possibilité de changer les comportements de l'utilisateur final aussi bien au sein de l'entreprise, et en fonction de son rôle, que dans sa vie personnelle.

SANS | GIAC CERTIFICATIONS

Contact France :
asaim@sans.org
Tél. +33 (0)7 67 82 75 52
www.sans.org

Renforcer la sécurité dans le cadre du télétravail

Ces chiffres donnent le tournis. Pourtant les cyberattaques et leurs répercussions sont connues depuis plus d'une décennie, même si la pandémie de Covid-19 leur a donné un coup d'accélérateur, notamment via le déploiement du télétravail.

Les lacunes dans les défenses des systèmes informatiques ont bien été identifiées par l'ANSSI qui souligne dans son rapport que « le manque de sensibilisation aux risques cyber, l'absence de maîtrise des systèmes d'information, le non-respect des mesures d'hygiène informatique, la pénurie d'experts en cybersécurité et, dans une certaine mesure, l'augmentation de la surface d'attaque du fait de la généralisation du télétravail, sont autant de faiblesses exploitées par les cybercriminels ».

La moindre porte dérobée est utilisée pour rentrer dans les SI et le travail à domicile en a ouvert une béante, notamment avec le déploiement de solutions qui facilitent la collaboration à distance et la migration massive vers le Cloud pour donner aux collaborateurs accès aux applications métiers, ressources, informations de l'entreprise.

En mai 2021, l'étude HP Wolf Security « Blurred Lines & Blindspots » révélait une augmentation des cyber-risques provoquée par l'adoption du télétravail. Pourquoi ? Parce que 70 % des employés de bureau interrogés admettaient utiliser leurs appareils professionnels pour des tâches personnelles, 69 % utiliser des terminaux personnels pour des activités professionnelles et 30 % avoir laissé une autre personne utiliser leur équipement professionnel ! L'augmentation des cyberattaques se chiffrerait d'ailleurs, selon l'étude, à plus de 238 % à l'échelle mondiale pendant la pandémie.

Sécuriser les terminaux, mais aussi les accès au SI de l'entreprise, y compris sur les Clouds où ils se sont étendus largement, sont donc des priorités.

1 MILLIARD, 1 AGENCE DE SÉCURITÉ ET 1 UNITÉ SPÉCIALE POUR LA CYBERDÉFENSE

> L'ANSSI (Agence nationale de la sécurité des systèmes d'information) est l'autorité nationale qui apporte son expertise et son assistance technique aux administrations et aux entreprises : elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques ; elle promeut la culture de la cyber sécurité ; elle contribue au développement de la recherche en matière de cyber sécurité ; en cas d'attaque, le Centre opérationnel de la sécurité des systèmes d'information (COSSI) assure la défense des services de l'État et des opérateurs privés les plus sensibles.

> Un milliard d'euros a été investi par la France pour renforcer le secteur de la cyberdéfense, en plus des moyens alloués à l'ANSSI.

> Une unité spéciale de gendarmerie, le ComCyberGend, dotée de 7 000 cyber enquêteurs (et 10 000 prévus d'ici fin 2022) a été créée en 2021.

Faire face à la prolifération des objets connectés

Les portes dérobées, ce sont aussi les partenaires de l'entreprise. Les pirates privilégient les supply chain attacks, attaques qui ciblent la chaîne logistique, donc les fournisseurs d'une entreprise afin d'aller chercher « par rebond » les données de celle-ci.

Enfin, autre facteur de risque, les objets connectés, car tout appareil qui a un IP offre une porte d'entrée pour une attaque, et l'augmentation des interconnections et de la mobilité des données.

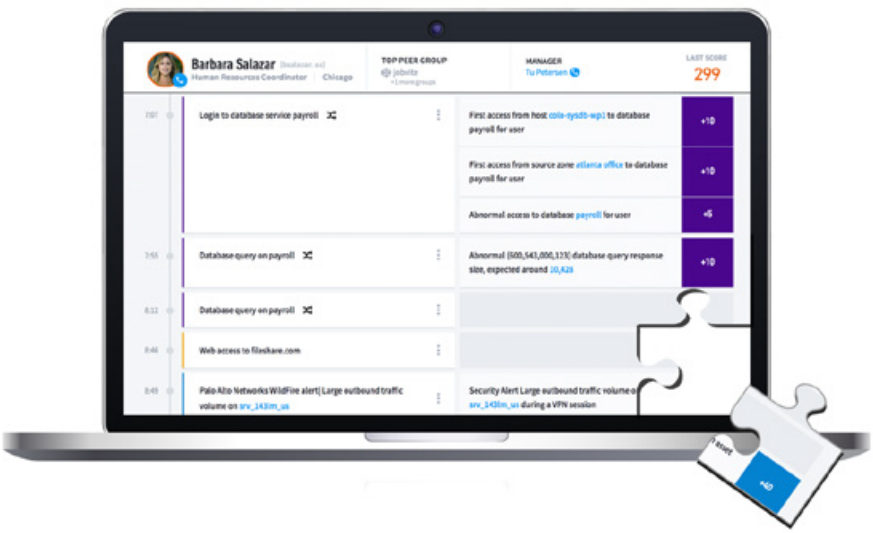
➤

EXABEAM

Une logique de combat face aux cyberattaques

Exabeam, éditeur de logiciel de SIEM (Security Information and Event Management) et d'XDR (Extended Detection and Response), définit de manière pragmatique des méthodes pour contrer les cyberattaques.

Exabeam, société basée à Foster City, dans la Silicon Valley et implantée dans divers pays américains et européens dont la France, ainsi qu'au Japon et en Australie, fournit des solutions de détection et de réponse aux cyberattaques. Le principal enjeu est de prévenir et empêcher les attaques, ce qui n'est jamais garanti, et d'offrir une détection efficace et une reponse rapide afin que « l'ennemi » soit délogé le plus rapidement possible. Les solutions proposées par Exabeam sont fournies dans le Cloud en mode « Software as a Service », et c'est là l'une de ses principales forces car, ainsi, comme le souligne Gorka Sadowski, Chief Strategy Officer d'Exabeam, les clients bénéficient d'une facilité de déploiement, de maintenance et d'utilisation quotidienne afin de faciliter l'adoption de ces solutions. Exabeam a toujours investit dans l'innovation, véritable maitre-mot dans le domaine de la cybersécurité : outre l'invention de techniques tels que l'User and Entity Behaviour Analytics (UEBA), technique d'intelligence artificielle et de machine learning permettant de découvrir les problèmes cyber dans une montagne de données, les équipes de R&D travaillent en permanence pour définir les menaces qui sont en constante évolution. Tout cela implique une mise à jour des moteurs, mais également du contenu. C'est pourquoi Gorka Sadowski insiste particulièrement sur l'importance de l'accompagnement des clients par Exabeam. Un point ayant particulièrement retenu l'attention des équipes de R&D d'Exabeam est le problème des ransomwares, phénomène en prolifération durant l'année 2021 et dont l'importance est amenée à croître au cours des prochaines années. Une des dernières grandes réussites d'Exabeam en la matière est d'avoir effectué l'automatisation de l'investigation des attaques ransomware : les techniques d'intelligence artificielle permettent d'identifier la nature de l'attaque, les systèmes attaqués, etc. XDR Alliance, la nécessité d'une union face à l'ennemi Exabeam eut un rôle décisif dans la création d'Extended Detection Response Alliance (XDR Alliance), alliance entre les principaux fournisseurs de technologies de cybersécurité. Il s'agit d'un travail collectif fournissant une couverture globale contre les menaces qui pèsent sur les organisations aujourd'hui. Ce programme est né d'une prise de conscience que face à la prolifération des ransomwares attaquant les hôpitaux, les écoles et autres organisations, il est contreproductif que les professionnels de la cybersécurité travaillent chacun de leur côté. Une union des solutions permet une collaboration pragmatique pour le bénéfice des clients. En effet, Gorka Sadowski déplore que trop souvent les alliances entre professionnels de la cybersécurité reposent sur des alliances marketing ou sur des démarches trop académiques et trop théoriques alors que le véritable enjeu est de « gagner la guerre contre l'ennemi ! ».



À PROPOS D'EXABEAM :

Exabeam est un leader mondial de la cybersécurité qui réinvente l'analyse et l'automatisation pour simplifier la détection, l'investigation et la réponse aux menaces de sécurité critiques qui sont difficiles à identifier. La plate-forme d'Exabeam tire parti du Machine Learning et de l'automatisation et permet d'aider les équipes de sécurité à mieux détecter les menaces, les utilisateurs compromis et malveillants tout en minimisant les faux positifs. Pour plus d'informations, visitez www.exabeam.com.

exabeam

info@exabeam.com
www.exabeam.com

Une stratégie sur le long terme

La cybersécurité est donc l'un des défis les plus importants auxquels sont confrontées les entreprises modernes, d'autant que les attaques deviennent de plus en plus complexes.
Comment la mettre en place ? Ni solution unique, ni solution miracle, mais pour se protéger, il faut avoir une approche proactive et établir et coordonner des dispositions sur plusieurs fronts, dispositions qui doivent être d'ordre techniques, juridiques et humaines. Cette stratégie visera d'abord à identifier les points faibles de l'organisation, puis à installer outils et process pour pouvoir prévenir et détecter des attaques en temps réel, pouvoir y répondre et récupérer suite à celle-ci. Et cette stratégie doit être inscrite sur le long terme, avec des processus vérifiés et mis à jour régulièrement.

Prévenir et détecter

Il est bien sûr crucial d'être équipé de solutions de sécurité techniques pour protéger les réseaux et les systèmes sur site, les systèmes et applications dans le Cloud et tous les points d'extrémité, appareils, Internet des objets (IdO), routeurs et tout autre point d'entrée aux réseaux et systèmes (avec des pare-feux de nouvelle génération, des solutions antivirus, de gestion des identités et des accès, de gestion des administrateurs, de gestion des mots de passe, de filtrage des URL et des messageries, des systèmes d'analyse, de détection et de remédiation, des assistants d'optimisation de système...). ➤

RECONNAÎTRE LA QUALITÉ

Des labels, reconnaissances, certifications permettent d'attester les niveaux d'efficacité, de robustesse et de confiance de solutions, la qualité d'un service ou de process... :

- Les certifications de l'ANSSI : Certification critères communs (CC) qui atteste qu'un produit est conforme à sa cible de sécurité et Certification de sécurité de premier niveau (CSPN), aussi appelée « Visa de sécurité », qui permet d'identifier les solutions les plus fiables à l'issue d'une évaluation réalisée par des laboratoires agréés ;
- Le label ExpertCyber, attribué par Cybermalveillance.gouv.fr, qui identifie les sociétés qui peuvent intervenir en cas d'actes malveillants ;
- Les notes de laboratoires indépendants tels qu'AV-Comparatives, ICSA Labs ou encore IDC MarketScape ;
- Les rapports d'analystes, comme ceux de Gartner, de Forrester et de Radicati.

CEFCYS

Femmes et Cybersécurité : enjeu sociétal majeur ?

À n'en pas douter au regard de la pénurie d'experts et de l'explosion des menaces. Le rôle des femmes est des plus stratégiques pour Nacira Salvan, responsable de la Sécurité et des Systèmes d'Information au ministère de l'Intérieur et fondatrice du Cercle des Femmes de la Cybersécurité (Cefcys). Explications.

Nacira Salvan, Présidente fondatrice du CEFCYS

Avec une cyber attaque toutes les 14 secondes, la cyber menace ne connaît pas la crise ?

Nacira Salvan : Effectivement, mais la cyber protection, elle, connaît une pénurie préjudiciable de main-d'œuvre ; il n'y a pas moins de 3,5 millions d'emplois à pourvoir dans le monde ! Elle est en état d'urgence absolue face à l'explosion et la professionnalisation des cybers attaques.

Les femmes seraient-elles l'avenir de la cyber sécurité ?

N. S. : Parfaitement. Face au déficit d'experts, elles représentent un vivier important de talents qui permettrait de répondre à l'urgence. Aujourd'hui, la cybersécurité a besoin des hommes ET des femmes. L'augmentation de la proportion des femmes est désormais un enjeu sociétal et économique.

Alors, comment expliquez-vous qu'elles ne soient que 10,6 % en France* ?

N. S. : Plusieurs raisons y concourent : Leur faible représentativité dans les domaines de la techno, des sciences, de l'ingénierie ; le manque de connaissance et de sensibilisation aux métiers de la filière ; des offres d'emploi trop genrées ; des clichés stéréotypés (filière purement technique, métier d'hommes...), sans oublier aussi l'acceptabilité d'une femme dans une équipe d'hommes... Autant de facteurs qui altèrent leur perception de ces métiers, mais aussi leur capacité à les embrasser. Pour aboutir au syndrome de l'imposteur, qui annihile toute initiative. Et pourtant, elles y ont toute leur place. Croyez-moi.

Les lauréates 2021 de l'European cyber women day, le trophée qui célèbre des femmes aux parcours et aux réalisations remarquables à travers toute l'Europe.

Vous créez le Cefcys en 2016. Pour changer la donne ?

N. S. : Tout à fait. Changer la donne en matière de comportement, de pratiques, faire reconnaître ce savoir-faire féminin, offrir une réelle visibilité à la filière et à ses opportunités. Et montrer sans démontrer que les femmes peuvent être des acteurs clés. Et depuis, nous sommes plus de 300 adhérents/sympathisants en France et en Europe à innerver ce changement.

Quelles sont les ambitions du Cefcys ?

N. S. : Valoriser et professionnaliser les compétences des femmes ; organiser et/ou participer à des évènements ; déployer des actions auprès des plus jeunes à l'usage sécurisé du numérique et sensibiliser l'éco système à l'importance de la parité homme/femme. Notre futur label Cefcys viendra, à terme, labéliser les entreprises qui œuvrent dans ce sens.

Master classes, formation, recrutement... vous apportez un accompagnement complet !

N. S. : Nous sommes partenaire des femmes de A à Z. Cela passe par des sessions de sensibilisation et des masters classes qui leur dévoilent les métiers de la cybersécurité. Nous les conseillons dans le choix d'une formation, et restons à leurs côtés dans leur recherche d'emploi via des salons et des job dating que nous co organisons avec avec Cyberjobs. Et continuons à les accompagner durant leur prise de fonction.

Quel est l'objectif de vos programmes de mentoring personnalisé ?

N. S. : De transmettre et d'accompagner de jeunes étudiantes, des femmes en reconversion comme des femmes en poste. Il leur permet de donner un nouvel éclairage à leur orientation professionnelle, définir leurs objectifs de carrière, planifier la bonne stratégie, éviter les écueils... Dans ce prolongement, nous avons aussi mis en place du mentorat groupé notamment pour l'IAE Gustave Eiffel.

Je ne porte pas de sweat à capuche, pourtant je travaille dans la cybersécurité

Attiré par les métiers de la Cyber ? Alors, procurez-vous ce guide2 qui recense les métiers, formations et opportunités et met en lumière 23 témoignages de CyberWomen. Éditions E-theque.

À quand votre propre centre de formation en cyber sécurité ?

N. S. : Certainement l'année prochaine puisqu'en 2022, nous rejoignons le Campus Cyber, l'endroit idéal pour former directement les femmes et les accompagner vers la spécialisation dans ces métiers.

**Enquête Anssi 2021*

nsalvan@cefcys.com
www.cefcys.fr

Le rapport HP montre d'ailleurs qu'en 2020 les terminaux connectés à Internet ont subi 1,5 attaque par minute et met en évidence l'importance d'une solide sécurité des terminaux, tout autant que la sécurité du réseau pour protéger contre les intrusions.

Parmi les grandes avancées technologiques dans le domaine de la prévention, figurent les solutions de type SIEM. S'appuyant sur des algorithmes robustes, voire de l'IA, elles permettent de surveiller, détecter et alerter sur des événements ou incidents de sécurité, de fournir une visibilité totale sur l'activité du réseau, et de réagir aux menaces en temps réel. À ces technologies s'ajoutent aussi des SOC (Security Operations Center), centres de commande avec des

professionnels de la cybersécurité chargés, en s'appuyant sur ces technologies, de surveiller, d'analyser et de protéger contre les cyberattaques, que certains éditeurs ou fournisseurs vont proposer aux entreprises en services managés externalisés. Ces SOC externalisés peuvent constituer aujourd'hui une réponse pertinente pour des entreprises, notamment TPE, PME et ETI (entreprises de taille intermédiaire) exposées à des problématiques de moyens et de recrutement.

Protéger les données stockées et en transit

Les technologies évoluent aussi pour le stockage et le partage des données. Des éditeurs se spécialisent sur la protection des connexions et communications, en développant des VPN d'entreprises par exemple. D'autres proposent des solutions plus sécurisées pour l'envoi de fichiers sensibles, pour pallier les manques de traçabilité et de sécurité de la messagerie traditionnelle ou des espaces de stockage partagés. Il s'agit ainsi, comme le souligne Guillaume Loth Demay, qui a développé la solution MFT online, de « pouvoir paramétrer les autorisations d'envoi en fonction d'adresses email, de types de documents, de niveau d'habilitation, d'une classification donnée à un document, etc., pouvoir prédéfinir la durée de vie d'un document celui-ci étant ainsi effacé de la plateforme d'une façon définitive à une date donnée ». ➤

ARCSERVE

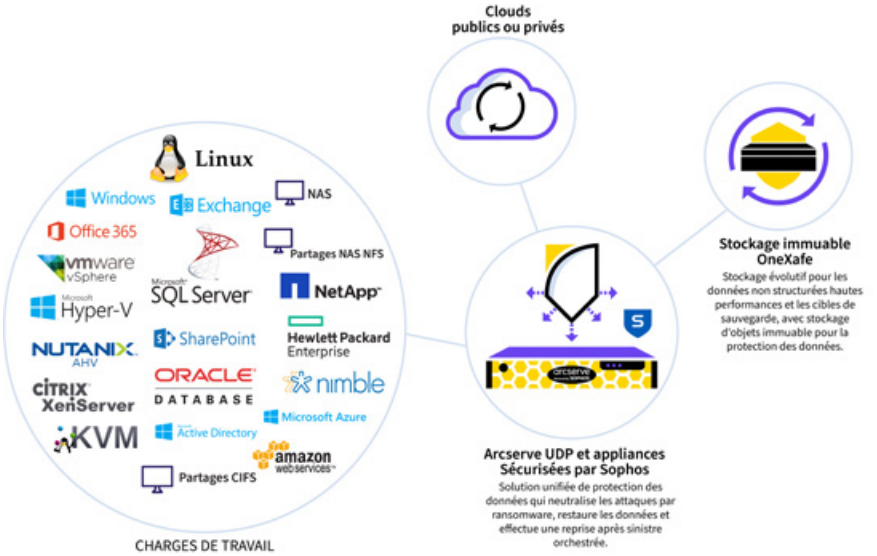
Votre première et dernière ligne de défense pour la protection des données

Parce que le risque zéro n'existe pas, minimiser l'impact d'une attaque fait aussi partie d'une politique de cybersécurité. En proposant une offre large de sauvegarde et de restauration des données, et de stockage immuable, Arcserve se positionne comme un acteur majeur sur ce marché. Explications de Florian Malecki, Vice Président, International Product Marketing.

Florian Malecki, Vice Président, International Product Marketing.

Pourquoi se positionner sur ce créneau de la sauvegarde, restauration et stockage des données ?

Florian Malecki : Les entreprises pensent prévention et omettent bien souvent la partie sauvegarde et restauration des données de leur politique de cybersécurité. C'est une erreur. Notamment à cause des ransomware qui se sont encore davantage multipliés durant la pandémie. N'importe qui peut être compromis et il y aura toujours des failles logicielles ou humaines, d'où l'objectif de minimiser l'impact de l'attaque. Assurer la restauration orchestrée des données, avec stockage immuable, constitue l'un des 3 piliers essentiels d'une stratégie de cybersécurité avec les produits de prévention (pare-feux de nouvelle génération, gestion des identités et des accès, gestion des administrateurs, filtrage des URL et des messageries) et la partie formation et information.



Que propose Arcserve ?

F. M. : Arcserve propose une suite de solutions afin de garantir la résilience des données. Les clients peuvent utiliser soit toutes les briques, soit certaines d'entre elles : une offre de sauvegarde et restauration logicielle (y compris sur bandes magnétiques) et appliance, backup de Microsoft 365 et Google Workspace, Disaster Recovery as a Service, ainsi qu'une offre de stockage immuable. Le stockage immuable est important car on va pouvoir restaurer 100 % des données, même lors d'une attaque de type ransomware.

Qu'est-ce qui fait la force d'Arcserve sur le marché de la cybersécurité ?

F. M. : Qu'on le veuille ou non, la sauvegarde et la restauration des données constituent la dernière ligne de défense de l'entreprise. Notre valeur ajoutée ? Arcserve a une énorme expérience en la matière, depuis 1983, et peut protéger les environnements virtuels, physiques et SaaS. Arcserve inclut également une offre cybersécurité dans ses produits, comme une fonctionnalité à part entière : nous pouvons en effet nous suppléer aux solutions existantes la technologie Sophos, leader mondial dans la sécurité informatique, qui permet de bloquer une attaque si celle-ci passe au travers des mailles du filet. Quasiment aucun de nos concurrents ne propose de fonctionnalité de cybersécurité « embarquée » ! Quant à notre offre de stockage immuable, elle constitue un vrai différenciateur aussi. Si la prévention échoue, si l'attaque n'est pas bloquée, les données sont de toute façon protégées sur notre baie de stockage. Et autre spécificité, nous mettons à disposition nos propres data centers, dans lesquels nos clients et partenaires peuvent exporter leurs données de backup et remonter virtuellement des serveurs en cas de pannes d'équipements. Ce qui permet d'assurer la continuité d'activité de l'entreprise.

À qui s'adressent ces offres ?

F. M. : À toutes les entreprises, de la PME aux grands comptes en passant par les ETI, ainsi que les MSP qui offrent des services hébergés. Nous ne vendons pas en direct mais via des distributeurs, SSII ou MSP qui offrent des services hébergés. Nous comptons 19 000 intégrateurs partenaires dans le monde et 235 000 clients, dans 150 pays. En France, on peut citer notamment le SDIS 62, Aramys, Dorégrill ou encore Figeac Aéro.

De quelles reconnaissances bénéficiez-vous ?

F. M. : Grâce à la fusion avec StorageCraft, Arcserve s'est hissée dans le top 5 mondial des fournisseurs de solutions de protection et de gestion des données. Et elle a été nommée Challenger dans le dernier classement Magic Quadrant de Gartner 2021 « Enterprise Backup & Recovery Software Solutions » pour ses solutions de sauvegarde et reprise pour l'entreprise.

arcserve®

www.arcserve.com/fr/

Anticiper la reprise après un sinistre, mais aussi la continuité des opérations en cas de système paralysé ponctuellement, est aussi primordial. Il s'agira donc d'assurer la résilience des données via des solutions de sauvegarde en software ou hardware, dans et hors site.

Une nécessaire mise en conformité avec les réglementations

Le succès d'une politique de sécurité passe aussi, comme le soulignait à l'occasion de la sortie du rapport HP, Ian Pratt, Global Head of Security pour la division Systèmes Personnels chez HP, par sa nécessaire intégration « autant que possible dans les schémas et les flux de travail existants, avec une technologie discrète, sécurisée par conception et intuitive pour l'utilisateur ». Les éditeurs ont bien compris qu'il fallait tendre de plus en plus vers des solutions simples d'utilisation et intuitives, comme le souligne Arnaud Dufournet, Chief Marketing Officer de la société TheGreenBow, qui édite des solutions VPN d'entreprise : « Si votre VPN n'est pas activé et pas utilisé, ça ne sert à rien, vous n'avez pas de protection. L'objectif est donc de le rendre totalement transparent pour les utilisateurs : qu'il n'y ait rien à faire et qu'il s'active automatiquement ».

Les entreprises et organisations ne peuvent pas faire l'impasse sur la mise en conformité avec les réglementations :
• le RGPD (Règlement général sur la protection des données) qui encadre le traitement des données personnelles sur le territoire de l'Union européenne ; ➤

Communiqué

CAEIRUS

L'expertise et le conseil au service des PME, TPE et ETI

Ce cabinet d'expertise en cybersécurité propose des solutions adaptées aux TPE, PME et ETI qui ne disposent pas de la culture et des compétences en cybersécurité. Le point avec son directeur général, Grégory Commin.

Quelles prestations propose Caeirus ?

Grégory Commin : De l'expertise, des audits sécurité et tests d'intrusion, et de la cybersurveillance. Nous faisons du pré-diagnostic pour évaluer le niveau de maturité de l'entreprise en cybersécurité et ce dont elle a besoin. Et nous la conseillons et l'accompagnons dans la mise en place de solutions.

À qui sont destinées ces offres ?

G. C. : L'idée est de proposer à des TPE, PME et ETI, qui n'ont pas forcément les connaissances en interne et la culture de la cybersécurité, des solutions adaptées à leurs structures sans chercher à leur vendre un « package » complet. Elles choisissent les options et le coût de l'accompagnement se fait en fonction de celles-ci. Et nous les conseillons en tenant compte de leurs contraintes et enjeux. Par exemple, pour pallier le coût considérable d'un SOC, nous pouvons les orienter sur notre solution Cloud, plus flexible en termes de ressources et de fonctionnalités. Notre valeur ajoutée ? Notre expertise et la transparence des coûts, grâce à des offres sur-mesure, et le travail en proximité avec le client. Nous sommes d'ailleurs implantés aux Antilles-Guyane pour pallier l'absence d'expertise sur ces territoires.

Grégory Commin, directeur général de Caeirus

Vous faites aussi de la formation et de la sensibilisation…

G. C. : L'autre demande forte porte sur la formation. Avec un centre certifié Qualiopi, nous proposons des modules de formation certifiante et de sensibilisation. Ces derniers fonctionnent sur des mises en situation, sur des thématiques choisies par l'entreprise : phishing, connexion à un accès Wifi ouvert… Objectif, piéger les collaborateurs pour une prise de conscience sur ce qu'est le risque, comment est menée une attaque et comment s'en prémunir. Outre de très bons retours sur nos prestations, nous avons obtenu le label ExpertCyber, en plus d'être référencés par la plateforme cybermalveillance.gouv.

caeirus

caeirus.com

ESET

Cybersécurité, alliance technologique et humaine indispensable

Premier éditeur européen de solutions de sécurité, ESET propose à la fois des logiciels autonomes qui éradiquent les fi chiers malveillants, mais aussi des solutions associées à des services pour détecter les comportements malveillants. Le point avec Benoît Grünemwald, expert cybersécurité ESET France & Afrique Francophone.

Benoît Grünemwald, expert cybersécurité ESET France

Pouvez-vous nous présenter ESET ?

Benoît Grunemwald : Nous avons 13 laboratoires R&D, 2 000 collaborateurs dans le monde et une présence dans plus de 200 pays. Cela représente 110 millions de clients, mais aussi 1 milliard d'internautes qui utilisent Chrome et Play Store que nous protégeons en partenariat avec Google. Dans un monde où les menaces et les cyber-attaquants évoluent très vite, protéger un aussi grand nombre d'utilisateurs permet d'avoir une vue mondiale sur les attaques et de faire évoluer très rapidement les solutions. Nous recevons à peu près 500 000 nouvelles menaces chaque jour et ce volume est traité par des humains et l'intelligence artificielle.

Pourquoi la protection du particulier et de l'entreprise sont-elles toutes les deux à prendre en compte ?

B. G. : Notre société subit une transformation numérique qui a été accélérée par le télétravail. L'utilisateur utilise de plus en plus ces technologies pour accéder à des ressources de son entreprise qui, alors, s'ouvrent à l'extérieur. Or, l'utilisateur est plus vulnérable parce que son réseau n'est pas maîtrisé comme il peut l'être par la DSI de l'entreprise. Du coup, il est important que le travailleur considère comme primordial, sur son réseau du domicile, de protéger ses données et celles de l'entreprise. Notre protection de Microsoft 365 est d'ailleurs l'une des solutions plébiscitées pour le télétravail, car elle réunit aussi des outils collaboratifs. Parce qu'il y a toujours une longueur d'avance entre l'attaquant et le défenseur, nous avons aussi créé une sandbox hébergée dans le Cloud, technologie qui consiste à exécuter des logiciels dans un environnement protégé afin de les analyser en toute sécurité. Cette offre intéresse les sociétés qui souhaitent améliorer leur cyber protection sans pour autant engager de ressources humaines supplémentaires. Le client n'a rien d'autre à faire qu'activer la licence. À côté de ces produits 100 % autonomes destinés à éradiquer des fichiers malveillants, nous proposons des solutions associées à un service, des ingénieurs sécurité, qui travaillent à détecter des comportements anormaux, sachant que les techniques, tactiques et procédures mises en œuvre par les cybercriminels deviennent de plus en plus complexes. Une offre plutôt destinée aux PME, ETI et grandes entreprises qui hébergent des données sensibles comme les secrets industriels et les données personnelles qui peuvent tomber sous le coup de réglementations, comme celle du RGPD.

ESET fait aussi de la sensibilisation, pourquoi ?

B. G. : La meilleure des technologies ne suffit pas pour se protéger, il faut aussi un comportement adéquat. À des campagnes de sensibilisation menées avec cybermalveillance.gouv.fr et l'association e-enfance, s'ajoute la production de contenus, sur le site dédié WeLiveSecurity et sur le blog SaferKidsOnline pour la protection des plus jeunes.

Qui fait confiance à ESET ?

B. G. : Nous comptons notamment la Gendarmerie nationale, cybermalveillance.gouv.fr, Canon et Toshiba. Nous avons obtenu de nombreuses distinctions, comme le prix « Outstanding Product Award » (produit remarquable) d'AV-Comparatives et la plus haute distinction dans les tests de SE Labs sur la protection des terminaux d'entreprise.

Quels sont vos projets ?

B. G. : Protéger avec davantage d'automatismes et d'accompagnement. Nos laboratoires analysent les comportements malveillants pour intégrer davantage d'automatismes dans les solutions grâce à l'IA. Une partie est aussi dédiée à l'analyse des groupes APT et des campagnes de cyberespionnage. Nous lançons aussi le projet ESET Campus, à Bratislava en Slovaquie, où se rencontreront chercheurs, étudiants et start-up. Il a vocation à devenir un centre majeur de recherche et d'innovation en sécurité.

Le projet d'ESET campus à Bratislava, où a été fondé le groupe

clientsfinaux@eset-nod32.fr
eset.com

• la Loi de programmation militaire (LPM) de 2013 qui a imposé aux opérateurs d'importance vitale (OIV) la sécurisation de leurs systèmes d'information critiques ;
• la transposition dans le droit français de la directive européenne NIS (Network and Information System Security) qui a élargi ces contraintes aux opérateurs de services essentiels (OSE).

Éduquer, former

Enfin, et on aurait pu commencer par ce « pilier » tellement il est fondamental pour réussir sa stratégie cybersécurité, il faut éduquer et former. Car si les personnes qui composent l'écosystème de votre entreprise n'implémentent pas les processus et technologies requis, ne les utilisent pas, ne les connaissent pas, vous n'obtiendrez pas les résultats souhaités. Plus que les former aux bonnes pratiques, il faut les sensibiliser aux enjeux pour créer une culture de sécurité plus collaborative. Culture toujours absente au regard d'un autre rapport de HP Wolf Security de 2021, Rebellions & Rejections, qui souligne de fortes résistances et rejets face aux mesures de sécurité. Notamment pour les contrôles imposés à la maison ou parce que les règles sont jugées contraignantes ou comme une perte de temps (par 48 % des employés et jusqu'à 64 % chez les 18-24 ans). Résultat, près d'un tiers déclaraient ne pas hésiter à les contourner et, face à ça, 91 % des équipes informatiques reconnaissaient avoir compromis la sécurité au profit de la continuité des activités ! ➤

ISSA FRANCE SECURITY TUESDAY

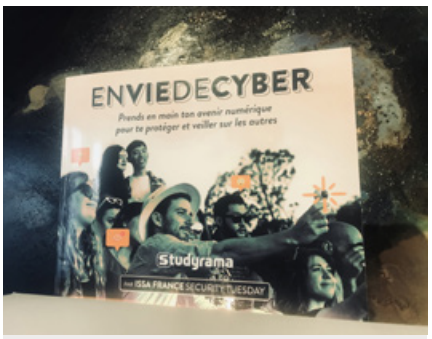
Comprendre son public pour produire le bon message

Avec son dernier ouvrage, Envie de cyber, qui s'adresse aux 15-30 ans, l'association ISSA France Security Tuesday poursuit son objectif de sensibilisation du grand public à la cybersécurité, et touche « juste » en adoptant les codes et le langage de son public.

« Tout le monde peut vivre une mésaventure numérique. » Hadi El Khoury, le cofondateur d'ISSA France aime souligner que c'est ce constat qui motive chacun des projets que mène l'association en direction du grand public. Celle-ci, créée en 2010 par des acteurs du domaine de la cybersécurité, avait pourtant commencé par des échanges entre « sachants », sous forme d'afterworks, avant de s'ouvrir dès 2013 au grand public, en réalisant un premier clip de sensibilisation.
Aujourd'hui, après avoir également édité et traduit en 7 langues le cahier de vacances des 7-11 ans Les As du web, l'association publie Envie de cyber.

Décloisonnement et pédagogie

Sur plus de 120 pages, se côtoient notamment culture cyber (Deep/Dark Web, histoires de hack gangs, géographie du monde numérique…), état des lieux des risques (chantage à la webcam et sextorsion, piratage de compte, hameçonnage, test pour calculer son IMC, son Indice de Masse Cyber…) et informations pratiques (s'informer, se protéger, se former…). Avec une sélection de six portraits de jeunes qui parlent de leur relation très particulière au numérique.



On peut commander Envie de cyber sur la boutique en ligne de Studyrama.

L'ouvrage sera en librairies et en ligne sur les autres plateformes de vente dès le 12 janvier 2022.

Hadi El Khoury et Diane Rambaldini, les cofondateurs de l'association ISSA France Security Tuesday

« Nous avons été les premiers à avoir décloisonné et à avoir fait de la pédagogie », poursuit le cofondateur. « Sur chaque projet, nos comités réunissent experts et pédagogues. Surtout, nous interrogeons la cible, son monde, ses codes, son langage pour produire un message lisible et compréhensible. Sans cela, toute sensibilisation est vouée à l'échec ! »

Hygiène numérique, vocations, innovation respectueuse

Cette mission d'éducation prend aussi la forme d'ateliers, notamment à l'école. L'association œuvre pour la voir intégrée « au cœur des programmes scolaires dès le CM1, pour dépasser le seul sujet du cyberharcèlement », explique la présidente cofondatrice, Diane Rambaldini. « Il s'agit d'inculquer des notions d'hygiène numérique, de susciter des vocations et d'éveiller aussi les jeunes porteurs de projets à une innovation plus responsable plus protectrice, un des grands messages d'Envie de Cyber ».
Car, pas question non plus, soulignent les auteurs de l'ouvrage, d'aborder le sujet de façon isolée et « uniquement sous un angle technique ou technologique ».

« La problématique du civisme sur Internet, par exemple, innerve celle du civisme en général, de la même façon que le Revenge Porn, pratique illégale qui consiste à divulguer sans le consentement de la personne reconnaissable du contenu sexuellement explicite, a de fortes résonances avec la problématique générale des relations homme-femme. Se protéger en ligne, veiller sur les autres, adopter les valeurs de la République - aussi en ligne - devraient être dans l'idéal abordés à l'école dans le 'Parcours citoyen' destiné à faire des enfants des citoyens responsables et libres ».
L'ensemble de ces objectifs dirigent tous les projets montés en crowdfunding par l'association, pour lesquels fondations, entreprises, mécènes… sont évidemment attendus, à l'instar de ces grandes organisations qui ont déjà répondu présentes sur de précédents projets, comme la SNCF, La Poste et Aéroports de Paris.

ISSA
Information Systems Security Association
FRANCE
Security Tuesday

securitytuesday.com

Former à l'hygiène numérique mais aussi pour susciter des vocations

Au-delà du rôle d'information que jouent des acteurs publics, comme Cybermalveillance.gouv.fr, l'ANSSI et le Haut fonctionnaire de défense et de sécurité du ministère de l'Économie et des finances, de plus en plus d'acteurs du marché tentent d'apporter des réponses dans ce domaine. Souvent sous la forme de formations « à la carte », et certaines en situation pour mieux faire appréhender la réalité d'une attaque (comment le piratage se fait-il, comment s'en prémunir).

Les fondateurs de l'association ISSA France Security Tuesday, Diane Rambaldini et Hadi El Khoury, voient de leur côté dans la sensibilisation un intérêt « non seulement pour inculquer des réflexes d'hygiène numérique, mais aussi pour susciter des vocations et inciter les jeunes générations à innover au service d'une société plus responsable et durable ».

Enfin, la sensibilisation est indispensable pour pallier aux problèmes de recrutement d'experts cybersécurité. C'est le fer de lance de l'association CEFSYS (Cercle des Femmes dans la Cybersécurité) qui souhaite, elle, encourager plus de femmes à s'engager dans la filière alors que celles-ci, d'après les études de l'ANSSI, ne représentent que 10,6 % des emplois en France et moins de 20 % dans le monde d'après ISC2. « Allez-y, osez, engagez-vous ! », invite Nacira Salvan, la présidente fondatrice. « Il ne faut pas avoir peur de la technique, d'autant que ça n'est pas que du technique. Et ce sont des métiers passionnants, dynamiques, où les femmes ont toute leur place ! » ●

CYBERINI

Se former dans la peau d'un hacker

Apprendre l'attaque pour mieux se défendre et sur un mode très flexible qui permet d'avancer à son rythme : c'est l'approche doublement originale que propose Michel Kartner, fondateur de l'organisme de formation Cyberini, pour s'initier à la cybersécurité.

Michel Kartner, fondateur de Cyberini

Pourquoi Cyberini ?

Michel Kartner : Lorsque j'étais en Master en réseaux informatiques, j'ai été frappé par la pauvreté des cours en cybersécurité. Il est dommageable que des personnes amenées à construire des systèmes d'information n'aient pas de bases alors que l'on fait face tous les jours à des problèmes de cybersécurité. Et même si on ne travaille pas dans le domaine, on est aussi potentiellement la cible de cyberattaques. Après avoir créé un blog au travers duquel je livre un « code de la route numérique » avec des bonnes pratiques, j'ai créé Cyberini. Il fallait aller plus loin parce que les pirates informatiques se servent aussi de ces bonnes pratiques pour nous tromper.

Qu'est-ce qui fait la spécificité de vos contenus de formation ?

M. K. : On dit que « la meilleure défense, c'est l'attaque », j'ai choisi cette approche pour mes cours de Hacking Ethique, se mettre dans la peau de hackers pour comprendre leurs logiciels, leurs méthodes, alors qu'il n'existe pas beaucoup de formations orientées tests d'intrusion. Autres atouts, mon centre de formation est 100 % spécialisé en cybersécurité et chacun apprend à distance et à son rythme, les cours étant accessibles 24/7. La formation donne une large place à la pratique (QCM, exercices, challenges et pratique par machines virtuelles qui seront hébergées prochainement dans le Cloud) et, c'est une exclusivité, à la fin les apprenants continuent à avoir accès aux supports et à du contenu additionnel.

En quoi cette offre répond-elle à un besoin ?

M. K. : On assiste à une demande croissante des entreprises alors que se multiplient les rançongiciels, ainsi que des étudiants et des personnes en reconversion. Cyberini est certifié Qualiopi et une formation ouvre le droit de passage d'une certification professionnelle reconnue. Les retours sont très positifs. Plus de 40 000 étudiants ont déjà suivi ces cours.

Cyberini

support@cyberini.com
cyberini.com

Communiqué

PARK ADAMS

La gouvernance au cœur de votre stratégie cybersécurité

Face à la professionnalisation des hackers et à la fragilisation des entreprises confrontées à une digitalisation croissante, une complexification des technologies et au télétravail, la société de conseil Park Adams place la gouvernance au cœur de la stratégie de cybersécurité.

« Face aux menaces, les technologies ne peuvent plus être l'unique réponse de défense. La cybercriminalité trouve ses leviers dans l'exploitation du facteur humain et des failles de gouvernance. Il faut donc placer le collaborateur et l'organisation au cœur de la stratégie cyber ». Ce positionnement, résumé par Yannick Mériguet, l'un des deux fondateurs, est à l'origine de l'offre articulée autour de trois axes : rendre plus compétents tous les collaborateurs, travailler sur une gouvernance renforcée pour augmenter la résilience de l'entreprise et accompagner les stratégies de développement « pour sécuriser la croissance ».

Yannick Mériguet et Arnaud Waechter, les fondateurs de Park Adams

Accompagner sur le long terme

La société propose une offre de formation innovante, via une plateforme qui soumet évaluations et analyses régulières. L'idée ? « Éduquer sur le long terme, en mesurant les performances, en s'adaptant à la culture de l'entreprise et en intégrant les nouvelles menaces pour que la sensibilisation soit un succès », explique Arnaud Waechter, cofondateur.

Quantifier financièrement les risques, et non plus les qualifier, est au cœur du deuxième service. « En les modélisant financièrement avec le framework FAIR™, on rend ainsi compréhensible la priorisation des investissements à mettre en place », observe Yannick Mériguet. Cette modélisation constituera un « outil clé » au service du RSSI, pour communiquer avec le comité de direction et l'aider dans ses choix technologiques. Enfin, parce que les cybercriminels ont compris que les transformations des entreprises sont au cœur de leurs stratégies de croissance, Park Adams les accompagne à intégrer des projections de risques cyber dans leurs plans opérationnels et ainsi « permet aux RSSI de protéger la création de valeur de leur organisation dans le long terme ».

Park Adams
Consulting for Security Leaders

Tél. +33 (0)7 56 80 33 11
office@park-adams.io
park-adams.io

THEGREENBOW

Le haut niveau de protection des connexions

Protéger les communications et les données échangées est un enjeu majeur pour toutes les entreprises. Ce à quoi répond TheGreenBow avec des solutions de VPN d'entreprise disposant de visas de sécurité de l'ANSSI. Le point avec Arnaud Dufournet, Chief Marketing Officer.

À quels défis majeurs sont confrontées les entreprises ?

Arnaud Dufournet : Le poids des réglementations (RGPD, LPM et directive NIS), la prolifération des objets connectés et le télétravail. Une récente enquête HP Wolf Security est très révélatrice à ce sujet. Elle montre que 91 % des équipes de sécurité font face à un dilemme et admettent compromettre la sécurité de leur entreprise pour assurer la continuité des activités depuis la pandémie.

Quelles réponses leur apporte TheGreenBow ?

A. D. : D'abord un haut niveau de sécurité. Nos VPN d'entreprise vérifient qu'un terminal est autorisé à entrer dans le réseau et chiffrent les données grâce à des algorithmes extrêmement robustes assurant ainsi la confidentialité. Ils garantissent aussi leur intégrité, donc leur transmission sans perte ou altération. Contrairement aux services VPN destinés aux particuliers, ils répondent à des exigences de sécurité très élevées ; raison pour laquelle TheGreenBow a été le 1er fournisseur européen de VPN à obtenir en 2013 un visa sécurité de l'ANSSI. Enfin, nous garantissons la facilité de déploiement et d'intégration, grâce à notre interopérabilité avec les principales solutions du marché et avec tout système d'exploitation, et la simplicité d'utilisation.

Qui vous fait confiance ?

A. D. : Des grands comptes, notamment des OIV : ministère de l'Intérieur, Dassault Aviation, La Poste, des collectivités et des organismes publics comme Le Mans Métropole ou l'INSEP... Plus de 2 millions de licences sont activées dans plus de 70 pays. Depuis 2020, nous proposons une offre très attractive pour le secteur public, le VPN français, avec un prix de licence à moins d'1 euro par mois.

Arnaud Dufournet, Chief Marketing Officer chez TheGreenBow

THEGREENBOW

thegreenbow.com | levpnfrancais.fr

Communiqué

FLK TECH

Hardware, filaire et biométrique pour une très haute protection des données

L'originalité des solutions développées par FLK ? Garantir un haut niveau de sécurité à vos données via l'association d'une application avec système d'authentification renforcé et d'un appareil filaire qui chiffre les données. Explications du fondateur, Flaubert Le Khem.

Comment est née la société FLK Tech ?

Flaubert Le Khem : Nous utilisons des objets connectés, téléphones, montres, etc., dont on ne connaît pas les failles. Or, il y en a sur tous les moyens de communication sans fil. Mon expertise et mes compétences acquises en cybersécurité, que je partage à travers des vidéos sur YouTube, LinkedIn et Facebook, m'ont incité à développer une technologie qui offre un haut niveau de protection aux données.

Flaubert Le Khem, fondateur de FLK Tech

Comment fonctionne cette technologie ?

F. L. K. : Beaucoup d'éditeurs font des solutions centrées sur la protection des données. Notre différence ? Nos solutions s'appuient sur trois piliers : les applications web, les applications mobiles et un appareil biométrique qui sert principalement au chiffrement de données. Cet ensemble permet d'offrir une sécurité numérique renforcée : le matériel hardware est le plus difficile à attaquer – il faut avoir l'objet – et il est filaire pour accroître encore la sécurité ; l'application associée, à installer sur le poste sur lequel vous connectez cet appareil, permet le transfert des données chiffrées et de contrôler l'accès à ces données grâce à plusieurs systèmes d'authentification dont la reconnaissance d'empreintes. Nous proposons 2 versions DDevice, dont l'une sans lecture d'empreintes afin de réduire le coût, et 3 packs ACM (Access control management) qui embarquent cette technologie, « Family », « Professionnal » et « Corporate », qui se différencient principalement par le nombre de licences activables.

Comment acquérir vos solutions ?

F. L. K. : Les entreprises peuvent s'adresser à nous pour demander des démonstrations – et nous nous déplaçons pour ce faire – et pré-commander ces solutions.

Be your own security

support@flaubertlekhem.com
https://flaubertlekhem.com

Communiqué

SOPHOS

Les entreprises doivent faire face aux menaces actuelles, tout en préparant l'avenir

Si les analystes du secteur se tournent déjà vers le futur en matière de cybersécurité, la réalité au sein des entreprises est bien différente. Ces dernières doivent s'efforcer de faire avant tout face aux menaces ransomware qui les visent aujourd'hui quelles que soient leur taille et la nature de leurs activités.

Pour Kevin Isaac, SVP EMEA Sales, Sophos : « En France, comme partout ailleurs, tandis que les équipes de sécurité doivent constamment se battre et affronter les problèmes actuels, comme les ransomwares ; elles doivent également préparer l'avenir. Il est donc essentiel d'identifier un fournisseur capable de conjuguer ses deux activités et c'est précisément ce que nous proposons chez Sophos ».

Conçues pour répondre aux besoins des entreprises de toutes tailles, les technologies de Sophos sont intégrées dans une plateforme unique permettant à ses clients de gérer et de réduire les risques en toute simplicité. Au cours des 10 dernières années, Sophos a opéré sa transition dans le cloud, et offre ainsi à ses clients la possibilité de bénéficier de solutions dites « de nouvelle génération » pour encore plus d'agilité et de réactivité face aux menaces.

Kevin Isaac, SVP EMEA Sales, Sophos

Aujourd'hui, l'entreprise se concentre sur ses services de réponses aux incidents pour donner à ses clients la capacité de réduire les risques de manières proactive. Selon Kevin Isaac « En France et en Europe, nous observons, de manière générale, que les entreprises s'orientent actuellement vers l'intégration de produits et services qui gèrent les menaces avec encore plus de proactivité. »

Chez Sophos, cette proactivité se traduit par le recours à l'IA pour automatiser les processus et faire évoluer les services en conséquence. Cette tendance devrait se poursuivre dans les années à venir selon Kevin Isaac, notamment avec l'utilisation du Machine Learning pour analyser une attaque et y répondre ; ajouter à cela une plus grande intégration du SASE et du Zero Trust aux architectures de sécurité des entreprises. Ces améliorations devraient également permettre aux entreprises de combler le déficit actuel de compétences en cybersécurité, qui peut avoir un impact sur les moyens de défense contre les attaques.

ITRUST

Leader européen de l'IA appliquée à la cybersécurité

Précurseur dans l'utilisation de l'IA appliquée à la cybersécurité, ITrust continue d'innover en adaptant aussi ses produits et services à des besoins et métiers spécifiques. Le point avec son fondateur, Jean-Nicolas Piotrowski.

Jean-Nicolas Piotrowski, fondateur, de ITrust

Que propose ITrust ?

Jean-Nicolas Piotrowski : Créée en 2007 autour du service en sécurité informatique (audits intrusifs, audits de code, analyse forensique, formations, mise en place de politiques sécurité…), ITrust a progressivement déployé son activité sur l'édition de logiciels. Nos trois produits de protection permettent de résoudre les problématiques auxquelles les entreprises sont confrontées en matière de cybersécurité : la prévention, la détection et la remédiation.

« 100 % de protection depuis 4 ans chez tous nos clients. »

Comment ITrust s'est-elle adaptée aux nouveaux besoins des entreprises en matière de sécurité ?

J.-N. P. : La pandémie a donné un coup d'accélération au télétravail et au Cloud, ce qui a induit deux demandes majeures pour lesquelles nous étions déjà prêts, intervenir sur des attaques en cours et assurer la supervision de leur sécurité aux entreprises qui le demandent, au sein de notre SOC hébergé dans le Cloud. Nous avons aussi commencé à faire évoluer nos solutions afin de répondre aux problématiques liées au nomadisme et à l'ouverture des systèmes informatiques sur l'extérieur. Car le télétravail a induit une mauvaise hygiène de travail : les collaborateurs ont eu tendance à se connecter n'importe où et ont exposé leurs entreprises à des risques plus importants. Nous avons eu beaucoup d'attaques liées à ça.

Qu'est-ce qui fait la force d'ITrust ?

J.-N. P. : Le fait d'avoir intégré l'IA dès le départ dans les algorithmes grâce à des partenariats avec des laboratoires tels que le LAAS (Laboratoire d'analyse et d'architecture des systèmes), l'IRIT (Institut de recherche en informatique de Toulouse), le LIPN (Laboratoire d'informatique de Paris Nord) ou l'IRT SystemX. Aujourd'hui, ITrust est le leader en Europe pour l'IA appliquée à la cybersécurité. L'IA nous permet d'optimiser les temps de détection et la priorisation des alertes. Grâce à l'IA nous avons déjoué 120 attaques sur les 12 derniers mois et nous obtenons 100 % de protection depuis 4 ans chez tous nos clients. Aujourd'hui, nous faisons davantage de la R&D appliquée, avec des clients, pour adapter les produits à des besoins ou métiers spécifiques. C'est la cybersécurité de demain. Nous avons travaillé par exemple avec la SNCF sur le développement d'algorithmes qui savent analyser le comportement du train, celui du conducteur, etc., et détecter des anomalies. L'un des atouts d'ITrust est aussi de proposer la vente comme un abonnement à la demande et à l'utilisation. Si de grosses structures préfèrent installer nos solutions SOC en interne, une PME ou ETI pourra préférer notre SOC Cloud, qui permet de diminuer les coûts en ressources humaines et dispense de toute installation. C'est vraiment de la sécurité à la demande. Nous développons aussi un modèle de SOC mutualisé pour des ensembles de collectivités et hôpitaux afin de proposer des services à des coûts très bas.

Qui s'adresse à ITrust ?

J.-N. P. : ITrust compte plus de 350 clients dans le monde, dont une centaine en SOC. Nous comptons des grands groupes ou organismes comme Agrica, Burger King, Cegos et Thales Aliena Space, des ministères (la Défense, l'Agriculture et la Justice), des hôpitaux, des collectivités, des ESN, des entreprises high-tech, des hébergeurs, et majoritairement des entreprises du mid market. Nous nous déployons en Europe, en Afrique du Nord et au Canada, y compris grâce à nos partenaires stratégiques qui proposent leurs services de cybersécurité (MSSP/MDR) à leurs clients en s'appuyant sur nos produits et nos process.

De quelles reconnaissances bénéficie ITrust ?

J.-N. P. : ITrust est labellisée France Cyber par l'ANSSI, la CNIL mais aussi, et c'est le seul centre de supervision en cybersécurité à l'être, par les armées françaises. C'est aussi la seule société française cyber à avoir été citée dans le rapport Villani sur l'IA, qui a donné lieu à la création du Hub France IA dans lequel nous copilotons le Groupe cybersécurité. Parmi nos trophées, compte celui de la cybersécurité 2019.

ITrust
IT Security Services

itrust.fr

EBRC

Résilience d'entreprise « Mode d'Emploi »

Plus aucune entreprise n'échappe aux ransomwares, malwares et autres attaques lancées par les cybercriminels. Pour EBRC, elles doivent aussi mieux anticiper, en analysant l'ensemble des risques auxquels elles sont exposées, pour mieux réagir et ainsi garantir la continuité de leurs activités.

EBRC est née en 2000, au Luxembourg, des besoins exprimés par les entreprises et le régulateur du secteur de la finance afin de sécuriser et garantir leurs activités dans un contexte de digitalisation accrue de l'économie. « Pour commencer nous avons construit des datacenters de haute qualité. certifiés Tier 4. Cela nous permet d'assurer à nos clients 100 % de disponibilité, en d'autres termes, zéro seconde d'indisponibilité depuis 20 ans, une performance ! explique Jean-François Hugon, Head of Marketing EBRC. « Puis nous avons développé une gamme complète de services Trusted Services Europe. EBRC opère son propre cloud souverain européen EBRC-Trusted Cloud Europe. Par ailleurs, EBRC a rejoint l'initiative GAIA-X en tant que « Day-One Member » et a lancé une initiative GAIA-X dans le secteur du spatial avec trois autres partenaires. L'entreprise est présente dans toutes les grandes villes de France via sa filiale DIGORA.

Certifiée ISO 27001 (sécurité de l'information) et ISO 22301 (Continuité des affaires), EBRC connaît un développement rapide de son activité conseil dans des secteurs ultra-sensibles.

« À nos yeux, les entreprises font face à deux enjeux principaux. Elles doivent d'abord s'assurer d'une bonne compréhension de leurs besoins métiers en termes de sécurité et de continuité, et d'une cartographie claire de leurs activités. L'objectif est de garantir la capacité de leur infrastructure informatique (interne, externe ou externalisée), et de celle de leurs partenaires et fournisseurs, à supporter ces besoins en cas d'incident opérationnel ou d'attaque. Il s'agit d'anticiper les moyens nécessaires pour assurer la continuité de l'activité. Et le deuxième enjeu est d'évaluer le plus justement les risques IT auquel elles sont exposées », détaille Philippe Dann, directeur de l'activité Consulting chez EBRC.

La cybersécurité ne suffit plus...

EBRC a fait de la cyber-résilience une stratégie centrale pour approcher ses clients. Une approche visant non seulement à mettre les outils en place pour se défendre face aux attaques, mais incluant aussi une organisation à même de réagir vite et de maintenir ses activités, même dans le cas où l'incident se produirait.

« La résilience, une valeur pour l'entreprise, une garantie pour les actionnaires. »

Certifiée ISO 27001 et ISO 22301, la société peut faire bénéficier ses clients de retours d'expérience via des évaluations de maturité et a conçu une auto-évaluation disponible gratuitement en ligne. « Cette première étape permet de dresser un état des lieux pour les accompagner dans des programmes d'amélioration de leur sécurité ou de continuité d'activité, poursuit Philippe Dann. Nous intervenons donc comme consultants conseil. Nous avons aussi développé une application unique – Le Cyber Resilience Portal – qui permet justement de lier les besoins métiers en termes de continuité et de sécurité avec la capacité informatique à supporter ces besoins. » EBRC a noué, au sein d'Hexatrust, un partenariat avec la société française Egerie, dont la solution logicielle de pilotage des risques et de la conformité permet de réaliser des évaluations très fines et de manière efficiente.

« Cette approche préventive permet à chaque entreprise de définir les réponses adaptées à son activité de façon spécifique et optimisée. Mieux préparées elles sont mieux armées pour faire face aux menaces et préserver leurs activités, une garantie importante pour les actionnaires. » estime Jean-François Hugon. Et Philippe Dann de conclure : « le terme cyber-résilience prend tout son sens dans une organisation puisqu'une organisation n'est pas une accumulation d'activités mais plutôt un ensemble d'activités qui ont des interdépendances internes et externes qu'il convient d'avoir à l'esprit quand on veut bien se protéger ».

ebrc
TRUSTED DATACENTRE, CLOUD & MANAGED SERVICES

www.ebrc.com/fr

BITDEFENDER

Des technologies de pointe et un SOC managé de haut niveau

En 20 ans, l'éditeur Bitdefender a su à la fois développer des technologies de pointe en cybersécurité mais aussi une expertise de très haut niveau qu'elle propose via un service de SOC managé. Explications de Laurent Tombois, Country Manager France et pays francophones.

Que propose Bitdefender ?

Laurent Tombois : Bitdefender propose un ensemble de solutions adaptées à tout type d'entreprises, de la TPE aux grands comptes en passant par les ETI : pour la sécurisation des endpoints, du cloud, des réseaux, des emails... Elle ne vend pas seulement ses propres solutions, mais se positionne aussi sur un modèle OEM en mettant à disposition d'autres éditeurs - plus de 150 aujourd'hui - ses technologies de pointe. Nos offres vont de la solution de prévention et détection de menaces à une solution EDR de détection, investigation et remédiation déclinée en service managé. Ce SOC d'experts est capable en temps réel d'assister les entreprises 24/7 en analysant les alertes et en y remédiant.

Qu'est-ce qui fait la force de Bitdefender ?

L. T. : Nous nous avons une expérience de 20 ans dans ce domaine, sommes présents dans 170 pays, soit via nos filiales, soit via nos country partners, et employons 1 600 collaborateurs, dont la moitié sont sur la R&D. En multipliant nos « capteurs » dans le monde, en collectant plus de datas, nous développons encore davantage nos capacités à détecter et analyser les menaces, et à concevoir des technologies de plus en plus évoluées alors que les cyberattaques sont de plus en plus complexes. Être un éditeur européen a aussi du poids, notamment au regard des problématiques de stockage de données pour lesquelles les réglementations divergent. Notre SOC répond aussi très clairement à une attente, alors que durant la pandémie nous avons assisté à une augmentation importante d'attaques. Si de grandes entreprises ont déjà investi sur des SOC managés, les entreprises de plus petites tailles n'ont en revanche pas toutes les moyens de gérer un SOC internalisé, auquel il faut pouvoir dédier a minima 5 personnes. Les solutions EDR font de la remontée d'informations mais il faut pouvoir les traiter !

Laurent Tombois, Country Manager France et pays francophones chez Bitdefender

« Sur des attaques critiques, notre SOC répond en moins de 30 minutes ! »

Quels sont tous les atouts de ce SOC ?

L. T. : Notre service managé a reçu une certification de très haut niveau, SOC2 Type 2, preuve de son engagement en faveur de la préservation des données, et les entreprises ont la garantie que les données françaises restent en Europe. Le SOC s'appuie aussi sur des équipes qui ont une forte expertise à travers des attaques qu'elles ont vécues - certains ont travaillé pour des entités gouvernementales comme la NSA, la Navy ou l'US Air Force -. Très peu d'éditeurs proposent ce service à ce niveau de qualité. Sur des attaques critiques, notre SOC répond en moins de 30 minutes ! Et, autre différenciateur, nous dédions une personne à notre client qui fait le lien avec les équipes SOC, connaît les infrastructures et les habitudes de son entreprise, les mesures de remédiation définies en amont. Au contraire, au sein de micro-SOC, plus répandus chez d'autres éditeurs, les services sont mutualisés entre plusieurs clients.

Qui utilise vos solutions ?

L. T. : Aujourd'hui, nous nous déployons fortement, entre autres dans les secteurs de la santé et du public, et de plus en plus de nos clients migrent vers notre offre de SOC. Nous connaissons une croissance de +30 % et affichons de fortes ambitions. Nous lançons d'ailleurs notre solution XDR, extension de l'EDR qui va pouvoir collecter des données à l'échelle de l'infrastructure. Cette solution sera aussi couverte par le SOC managé dès 2022.

Avez-vous d'autres reconnaissances que celle obtenue pour le SOC ?

L. T. : Fin 2020, nous avons obtenu d'AV Comparatives un score parfait (15/15) contre les menaces persistantes avancées. En plus de notre certification SOC2 Type 2, nous avons notamment obtenu l'ISO 27001 et l'ISO 9001, et nous sommes récompensés régulièrement par des cabinets tels que Forrester et Radicati. Récemment, nous l'avons aussi été par Gartner pour notre offre de SOC managé.

Bitdefender®

BUILT FOR RESILIENCE

bitdefender.fr

Relevez le Défi
de la Cyber-Résilience

Depuis 20 ans, EBRC gère et protège vos informations sensibles et vous accompagne pour relever le défi de la Cyber-Résilience, **en toute sérénité**.

▸ **Testez la maturité de votre organisation.**

Découvrez notre offre **Trusted Services Europe**

Advisory | Managed Services | Cloud | Security | Resilience | Data Centre

ebrc

TRUSTED DATACENTRE, CLOUD & MANAGED SERVICES

www.ebrc.com