

Comment se préparer aux incidents de sécurité ?



Comment préparer incidents sécurité ?

se aux de

Les entreprises doivent être prêtes à agir face à des incidents de sécurité et à des attaques. Et cela passe notamment par sept points précis (par Peter Sullivan).

Un plan de préparation à la cybersécurité présente et détaille les objectifs fondamentaux que l'organisation doit atteindre pour se considérer comme prête à faire face à des incidents de sécurité informatique. La liste de contrôles qui va suivre n'est pas exhaustive, mais elle souligne des objectifs qui constituent un minimum requis pour donner un niveau raisonnable de sensibilisation à la cybersécurité et se concentrer sur la protection des actifs informationnels essentiels.

Ici, la préparation à la cybersécurité est définie comme l'état permettant de détecter et de réagir efficacement aux brèches et aux intrusions informatiques, aux attaques de logiciels malveillants, aux attaques par hameçonnage, au vol de données et aux atteintes à la propriété intellectuelle – tant à l'extérieur qu'à l'intérieur du réseau.

Un élément essentiel de cette définition est de « pouvoir détecter ». La détection est un domaine où une amélioration significative peut être atteinte en abaissant le délai de détection, couramment observé entre 9 et 18 mois. Une capacité de détection plus rapide permet de limiter les dommages causés par une intrusion et de réduire le coût de récupération de cette intrusion. Être capable de comprendre les activités régulières du réseau et de détecter ce qui diverge de la norme est un élément important de la préparation à la cybersécurité. Voici une sept objectifs que les entreprises devraient considérer.

Les objectifs à atteindre

- 1. Plan de cybersécurité**
- 2. Gestion du risque**
- 3. Gestion de l'identité**
- **Contrôle d'accès**
- **Authentification**
- **Autorisation**
- **Responsabilité**
- 4. Surveillance de réseau**
- 5. Architecture de sécurité**
- 6. Contrôle des actifs, des configurations et des changements**
- 7. Cartographie de la gestion des incidents**

...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité », « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Comment se comporte notre cerveau surchargé par le numérique



Comment se comporte notre cerveau surchargé par le numérique

Samedi 3 septembre, ARTE a diffusé un excellent reportage sur la manière dont notre cerveau se comporte face à nos vies de plus en plus hyper connectées : « HYPERCONNECTÉS : LE CERVEAU EN SURCHARGE ».

Grâce aux smartphones, ordinateurs et autres tablettes, nous sommes reliés au monde en continu. Mais ce déluge d'informations menace notre bien-être. Alliant témoignages de cadres victimes de burn out et explications de chercheurs en neurosciences, en informatique ou en sciences de l'information et de la communication, ce documentaire captivant passe en revue les dangers de cette surcharge sur le cerveau. Il explore aussi des solutions pour s'en prémunir, des méthodes de filtrage de l'information aux innovations censées adapter la technologie à nos besoins et à nos limites.

Chaque jour, cent cinquante milliards d'e-mails sont échangés dans le monde. Les SMS, les fils d'actualité et les réseaux sociaux font également partie intégrante de notre quotidien connecté, tant au bureau qu'à l'extérieur. Nous disposons ainsi de tout un attirail technologique qui permet de rester en contact avec nos amis, nos collègues, et qui sollicite sans cesse notre attention. Comment notre cerveau réagit-il face à cette avalanche permanente de données ? Existe-t-il une limite au-delà de laquelle nous ne parvenons plus à traiter les informations ? Perte de concentration, stress, épuisement mental, voire dépression... : si les outils connectés augmentent la productivité au travail, des études montrent aussi que le trop-plein numérique qui envahit nos existences tend à diminuer les capacités cognitives.

Un documentaire de Laurence Serfaty (France, 52'), diffusé sur ARTE le samedi 3 septembre à 22h20

A voir et à revoir sur Arte +7 pendant encore quelques jours !
si vous ne voyez pas la vidéo, le lien



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Hyperconnectés : le

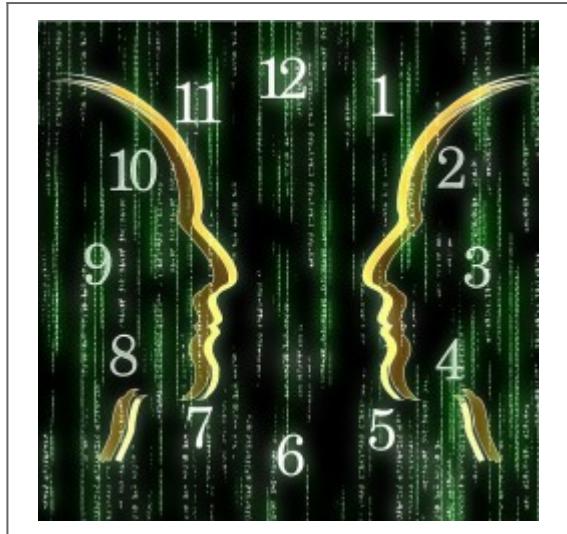
Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques

<p>Denis JACOPINI</p> 	<p>Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques</p>
--	---



Original de l'article mis en page : Conseils aux usagers | Gouvernement.fr

Les pirates informatiques recrutent des complices chez les opérateurs télécoms



Les pirates informatiques recrutent des complices chez les opérateurs de télécoms

Un rapport de Kaspersky détaille les nombreuses menaces qui ciblent les opérateurs de télécommunications, réparties en deux catégories : celles qui les ciblent directement (DDoS, campagnes APT, failles sur des équipements, ingénierie sociale...) et celles qui visent les abonnés à leurs services. Parmi les premières, le recrutement de complicités internes, sous la menace ou par appât du gain, progressent, même si elles restent l'exception.

Les opérateurs de télécommunications constituent une cible de choix pour les cyberattaques. Ils gèrent des infrastructures de réseau complexes utilisées pour les communications téléphoniques et la transmission de données et stockent de grandes quantités d'informations sensibles. Dans ce secteur, les incidents de sécurité ont augmenté de 45% en 2015 par rapport à 2014, selon PwC. Dans un rapport intitulé « Threat intelligence report for the telecommunications industry » publié cette semaine par Kaspersky, l'éditeur de logiciels de sécurité détaille les 4 principales menaces qui visent les opérateurs de télécommunications et fournisseurs d'accès Internet (FAI) : les attaques en déni de service distribué (en hausse), l'exploitation de failles dans leur réseau et les terminaux clients, la compromission d'abonnés (par ingénierie sociale, phishing ou malware) et, enfin, le recrutement de personnes capables d'aider les cyber-criminels en interne, au sein même des entreprises attaquées.

☒ Lorsque les attaques passent par des collaborateurs contactés par les cybercriminels, il est difficile d'anticiper ces risques car les motivations sont diverses : appât du gain, collaborateur mécontent, coercition ou tout simplement négligence. Certains de ces relais internes agissent de façon volontaire, d'autres y sont forcés par la menace ou le chantage. Chez les opérateurs de télécoms, on demande principalement à ces « insiders » de fournir un accès aux données, tandis que chez les fournisseurs d'accès Internet (FAI), on les utilise en appui à des attaques contre le réseau ou des actions de type man-in-the-middle (MITM). Même si le recours à des collaborateurs indélicats reste rare, cette menace progresse, selon Kaspersky, et ses conséquences peuvent être extrêmement critiques car elle peut ouvrir une voie directe vers les données ayant le plus de valeur. Le chantage est l'un des vecteurs de recrutement le plus efficace. A ce sujet, le spécialiste en technologies de sécurité remet en mémoire l'intrusion sur le site de rencontres extra-conjugales Ashley Madison, l'été dernier. Celle-ci a permis le vol de données personnelles que les attaquants ont pu confronter à d'autres informations publiquement accessibles pour déterminer où les personnes travaillaient et les compromettre.

Même des pirates inexpérimentés peuvent mener des attaques DDoS

D'une façon générale, Kaspersky répartit en deux catégories l'ensemble des menaces visant les opérateurs télécoms à tous les niveaux : d'une part, celles qui les ciblent directement (DDoS, campagnes APT, failles sur des équipements, contrôles d'accès mal configurés, recrutement de complicités internes, ingénierie sociale, accès aux données), d'autre part celles qui visent les abonnés à leurs services, c'est-à-dire les clients des opérateurs mobiles et des FAI. Les attaques en déni de service distribué ne doivent pas être sous-estimées, rappelle Kaspersky, car elles peuvent être un signe précurseur d'une deuxième attaque, plus préjudiciable. Elles peuvent aussi servir à affecter un abonné professionnel clé, ou encore à ouvrir la voie à une attaque par ransomware à grande échelle. Le 1er cas a été illustré par l'intrusion subie en 2015 par Talk Talk, l'opérateur de télécoms britannique, résultant dans le vol d'1,2 millions d'informations clients (noms, emails, dates de naissance, données financières...). L'enquête a montré que les pirates avaient dissimulé leurs activités derrière l'écran de fumée d'une attaque DDoS. L'un des éléments préoccupants de ces menaces, c'est que même des attaquants inexpérimentés peuvent les organiser de façon relativement efficace, rappelle Kaspersky.

Des équipements vulnérables et des malwares difficiles à éliminer

Les vulnérabilités existant dans les équipements réseaux, les femtocells (éléments de base des réseaux cellulaires) et les routeurs des consommateurs ou des entreprises fournissent aussi de nouveaux canaux d'attaques, de même que les logiciels exploitant des failles dans les smartphones Android. Ces intrusions mettent en œuvre des malwares difficiles à éliminer. En dépit des nombreux vols de données perpétrés au cours des 12 derniers mois, les attaques se poursuivent, exploitant souvent des failles non corrigées ou nouvellement découvertes. En 2015, par exemple, le groupe Linker Squad s'est introduit chez Orange en Espagne à travers un site web vulnérable à une injection SQL et a volé 10 millions de coordonnées sur les clients et les salariés. Par ailleurs, dans de nombreux cas, les équipements utilisés par les opérateurs présentent des interfaces de configuration auxquelles on accède librement à travers http, SSH, FTP ou telnet et si le pare-feu n'est pas configuré correctement, ils constituent une cible facile pour des accès non autorisés, explique encore Kaspersky.

En résumé, les menaces visant les opérateurs de télécommunications existent à de nombreux niveaux – matériel, logiciel, humain – et les attaques peuvent venir de différentes directions. Les opérateurs doivent donc « regarder la sécurité comme un processus englobant tout à la fois la prédition, la prévention, la détection, la réponse et l'enquête », conclut Kaspersky.

Article de Maryse Gros



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, conteneurs, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Liberté) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



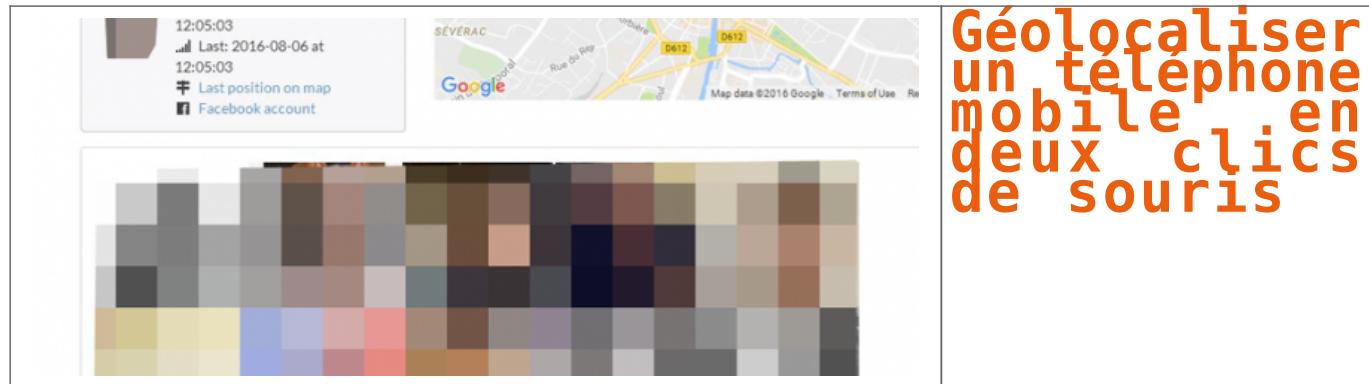
[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Les pirates recrutent des complices chez les opérateurs télécoms – Le Monde Informatique

Géolocaliser un téléphone

mobile en deux clics de souris



Géolocaliser
un téléphone
mobile en
deux clics
de souris

Cyber géolocaliser un porteur de téléphone est de plus en plus simple. Un chercheur en informatique montre à ZATAZ.COM comment créer un tracker maison devient simple comme bonjour.

Les téléphones portables, de nos jours, sont de véritables ordinateurs aux capacités de traçage, surveillance et cyber surveillance qui fait froid dans le dos. Regardez, prenons les exemples tels que Facebook et son option « amis à proximité » ou encore PokemonGo et sa capacité de géolocalisation. Du traçage au centimètre. Des technologies de « ciblage » qui deviennent simple à créer et à utiliser. Tristan, informaticien Parisien, vient de contacter ZATAZ pour présenter son cas d'étude : un outil de traçage en temps réel capable de tracer l'itinéraire de ses cibles.

Géolocaliser un téléphone : Souriez, vous êtes pistés

Depuis quelques temps Tristan s'intéresse aux applications proposées dans les mobiles, et plus précisément aux logiciels qui font transiter des informations telles que des positions de latitude et de longitude. Avec un associé, il a lancé Lynx Framework, une entité spécialisée dans la création d'outils de sécurité pour les applications web.

A parti de ses recherches, Tristan a créé un outil de « traque », de quoi géolocaliser un téléphone qui met à jour les dangers de nos mobiles et de leurs capacités à indiquer notre emplacement, mais aussi, nos itinéraires. « *En analysant les requêtes envoyées par certaines applications je me suis rendu compte qu'il serait possible de récupérer le positionnement de plusieurs personnes en même temps et de les positionner sur une carte de type google map.* » m'explique le chercheur.

A l'image des sauvegardes de Google Map que je vous indiquais en 2015, l'outil « privé » de Tristan fait pareil, mais en plus discret encore. Via un outil légal et disponible sur Internet, Burp Suite, notre chercheur a analysé les requêtes envoyées par plusieurs logiciels de rencontres disponible dans le Google Play.

Comment cela fonctionne-t-il ?

« *Le tracker prend le contrôle de plusieurs comptes d'application de rencontre et récupère la position des personnes à proximité, indique-t-il à ZATAZ.COM. Il ajoute ces informations dans sa base de données et vérifie l'existence des positions pour cette identité. Si l'application de Tristan retrouve la même personne, mais pas à la même position, il va créer un itinéraire de l'individu via son ancienne position* ». Nous voilà avec la position et le déplacement exacts d'un téléphone, et donc de son propriétaire, à une heure et date données.

Géolocaliser un téléphone : Chérie, tu faisais quoi le 21 juillet, à 12h39, à 1 cm de ta secrétaire ?

Après quelques jours de recherche, Tristan a mis en place une base de données de déplacement dans une ville. Une commune choisie au hasard. Son outil est en place, plusieurs systèmes sont lancés : Une carte avec le positionnement des personnes croisées ; une page plus explicite pour chaque personne avec la date de croisement, son âge... ; une page où notre chercheur gère ses comptes dans l'application. Bonus de son idée, un système d'itinéraire complet a été créé. Il permet de tracer un « chemin » de déplacement si la personne croisée a déjà été croisée dans le passé, dans un autre lieu. « *J'ai positionné un compte au centre de la ville, un autre à l'entrée et le suivant à la sortie, ce qui a donné en quelques heures une 50ème de données* » confie-t-il « *Il est inquiétant de voir autant de données personnelles transitées en clair via ces applications* ».

Géolocaliser un téléphone : détournement possible d'un tel « tracker » ?

Vous l'aurez compris, « tracer » son prochain est facilité par ses applications qui ne protègent pas les informations de positionnement des utilisateurs. Il devient possible d'imaginer une plateforme, en local, avec plusieurs comptes positionnés à des endroits différents dans une ville. Bilan, suivre plusieurs individus devient un jeu d'enfant. Si on ajoute à cela les applications de déplacement de type UB, qui communiquent les données de ses chauffeurs par exemple, ainsi que celles d'autres réseaux sociaux, il devient réellement inquiétant de se dire que positionner une personne et la tracer se fait en quelques secondes. Deux solutions face à ce genre de traçage : jeter votre portable ou, le mieux je pense, forcer les éditeurs d'applications à vérifier la sécurisation des données envoyées, et les chiffrer pour éviter qu'elles finissent en clair et utilisable par tout le monde.

Article original de Damien Bancal



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contenus, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Original de l'article mis en page : ZATAZ Géolocaliser un téléphone mobile en deux clics de souris – ZATAZ

L'adoption de l'analyse comportementale appelée à s'étendre



l'adoption de l'analyse comportementale appelée à s'étendre

Selon Gartner, les entreprises se tournent de plus en plus vers l'analyse comportementale pour améliorer la détection des incidents et renforcer l'efficacité de leurs SOC. De quoi pousser à une inéluctable consolidation du marché.



L'analyse comportementale – des utilisateurs comme des flux réseau ou des entités connectées à l'infrastructure – a fait une entrée remarquée sur le marché de la sécurité l'an passé. Mais selon Gartner, les solutions isolées actuellement proposées vont être rapidement appelées à s'intégrer, au point d'encourager à une consolidation des acteurs.

Dans une note d'analyse, Avivah Litan et Eric Ahm résument la situation : « les besoins des acheteurs pour détecter les brèches de tout type vont pousser à la consolidation des systèmes de détection basés sur le comportement, tels que les systèmes d'analyse du comportement des utilisateurs et des entités (UEBA), de détection et de réponse sur les points de terminaison (EDR), et d'analyse du trafic réseau (NTA) ».

Des catégories bien distinctes

Dans la première catégorie, le cabinet mentionne par exemple Securonix, LightCyber, Exabeam et Gurucul. Le premier étant notamment utilisé par HP au sein du système de gestion des informations et des événements de sécurité (SIEM) ArcSight. Pour l'EDR, il prend pour exemples Hexis et Ziften, mais pourrait également évoquer SentinelOne, notamment. En matière de NTA, le cabinet fait référence à SSS et Niara, mais il faut également compter avec Vectra Networks ou encore Darktrace, entre autres.

Mais voilà, comme le relèvent les deux analystes, les acheteurs de solutions de sécurité ne veulent pas seulement détecter les brèches, « mais aussi y répondre rapidement et efficacement ». S'il le fallait, l'édition 2016 de RSA Conference a fait la démonstration de cette tendance. Ce besoin doit conduire à une « collision du marché entre systèmes de détection basés sur le comportement et systèmes d'orchestration et de réaction ». Et cela parce que ni UEBA, ni EDR, ni NTA ne semble en mesure d'apporter, seul, une réponse complète aux besoins des entreprises.

Des capacités différentes

Ainsi, Avivah Litan et Eric Ahm soulignent que la première catégorie est efficace pour identifier des compromissions de comptes utilisateurs ou des acteurs internes malveillants, mais peut montrer ses limites dans la détection des incidents impliquant des logiciels malveillants. De son côté, « l'EDR peut être efficace pour trouver les comportements mauvais sur un hôte et identifier les objets maliciels », mais plus faible lorsqu'il s'agit de mettre le doigt sur une menace interne. Enfin, les outils de NTA « peuvent être capables de trouver les conséquences de deux types d'événements, mais n'ont pas les données relatives aux utilisateurs ou aux hôtes nécessaires pour confirmer l'incident ».

Analyse comportementale : la clé de la sécurité ?

D'autres outils peuvent venir en outre compléter l'édifice, qu'il s'agisse des SIEM ou des systèmes de gestion du renseignement sur les menaces comme ceux d'Anomali, de ThreatConnect ou encore de ThreatQuotient. Au final, pour les analystes de Gartner, le marché s'avère « bruyant, chaotique et encombré », pollué notamment par des discours marketing qui s'articulent « autour des mêmes thèmes clés tels que analytique, machine learning, automatisation, et autres termes similaires, bien que leur application de ces fonctionnalités soit largement différente en ce qui concerne ce qu'ils peuvent faire dans leurs rôles spécifiques ». Bref, la confusion règne.

Des performances à démontrer

Et cela d'autant plus que, selon Gartner, les spécialistes de l'analytique appliquée à la sécurité peinent encore à faire la démonstration de la valeur de leurs solutions. Lors d'échanges, ceux-ci cherchent surtout à se différencier en évoquant l'étendue ou le volume de leurs échantillons de données, le framework analytique utilisé ou encore la technologie analytique employée – apprentissage machine, deep learning, et intelligence artificielle sont là largement mis à contribution. Las, si le cabinet voit là des « facteurs importants et des sujets de discussions divertissants », tous « échouent à constituer un différentiateur majeur » car, pour Avivah Litan et Eric Ahm, « les éditeurs devraient d'abord se concentrer sur la manière dont le recours à l'analytique rend leur technologie meilleure en termes de résultats, de manière mesurable. Par exemple, dans quelle mesure trouver des attaques inconnues est plus efficace en pourcentage avec l'analytique que chercher à trouver un logiciel malveillant inconnu sans ».

Une inéluctable consolidation

Pour autant, les deux analystes ne contestent pas la valeur intrinsèque que l'analytique apporte à la détection de brèches. Mais ils soulignent l'importance des étapes suivant la détection. D'où la convergence anticipée entre acteurs de la détection basée sur l'analytique et de l'orchestration/réaction. Et c'est peut-être là que le SIEM est appelé à jouer une nouvelle carte, pour dépasser des limites bien connues. Dès lors, pour Gartner, les acteurs de détection devaient « soit prévoir de nouer formellement des partenariats avec des acteurs du SIEM [...] ou se préparer à reprendre des fonctions clés du SIEM ». Le cabinet s'attend donc clairement à une consolidation prochaine de systèmes de détection de menaces basés sur les comportements, mais il n'exclue pas l'émergence de solutions de type plateforme dédiées à l'investigation et à la réponse aux incidents. Des solutions sur lesquelles les composant de détection et de réponse viendreraient se greffer. Et n'est-ce pas justement ce que cherche à proposer un Phantom Cyber ?

Article de Valéry Marchive



David JACOPIN est Expert Informatique assermenté spécialisé en cybersécurité et en protection des données personnelles.
• Expertises techniques (virus, espions, pirates, fraudes, arnaques Internet...) et judiciaires (Procédures d'audit, diligences, enquêtes, mandats, contentieux, dénonciations de clientèle...);
• Expertises de systèmes de vote électronique ;
• Formations et conférences en cybersécurité ;
• Formation de C.I.L. (Correspondants Informatique et Liberté);
• Accompagnement à la mise en conformité CNIL de votre établissement.



Contacter-nous

Réagissez à cet article

Source : *L'adoption de l'analyse comportementale appelée à s'étendre*