cybersecurity holidays notebook

elit-cyber.com

Trouver une solution cyber

Bonnes vacances !

SOMMAIRE

Juillet 2022

6 PRÉCAUTIONS DE CYBERSÉCURITÉ AVANT DE PARTIR EN VACANCES

Même durant l'été les cyber menaces ne prennent pas de vacances.

Les vacances d'été approchent à grands pas et avec elles les cyber menaces associées. Pour partir en voyage l'esprit léger et vous offrir des congés en toute sérénité, suivez nos quelques conseils. Voici les bons gestes à adopter en amont de votre départ estival :

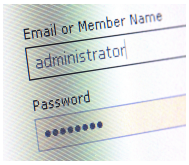
N'annoncez pas votre voyage publiquement

Il est tentant d'annoncer sa joie de partir en voyage sur les réseaux sociaux. Malheureusement, par ce biais, vous donnez alors les mêmes informations à vos amis qu'aux cyber criminels et cambrioleurs, qui peuvent donc cibler leur phishing selon votre lieu et vos dates de voyage. Faites tout autant attention à votre réponse automatique sur vos boites mails professionnelles et personnelles. Le message doit rester concis.

Faites des sauvegardes

Avant votre départ, sauvegardez toutes vos données sensibles pour les récupérer en cas de perte ou de vol de votre matériel informatique. Personne n'est à l'abri d'un malheureux accident. Une sauvegarde de vos données minimisera alors la perte. Vous pouvez multiplier cette protection en choisissant des supports physiques (clefs USB ou disques durs) et des supports virtuels via le Cloud et les Drives

Modifiez (tous) vos mots de passe



Des mots de passe forts sont la première clef d'une sécurité optimale. Alors, en amont de vos vacances, modifiez ceux des appareils et de vos applications en y intégrant majuscules, minuscules, chiffres et caractères spéciaux. Des mots de passe récents minimiseront leurs corruptions. Et évidemment, ces mots de passe doivent être différents entre les plateformes que vous utilisez. Ne faites pas l'impasse sur l'utilisation d'un gestionnaire de mots de passe.

Mettez à jour vos applications

Autre point de vigilance : les failles de sécurité. Pour les déjouer, pensez à faire une mise à jour de toutes vos applications avant de partir en vacances, que ce soient celles de votre téléphone, de votre ordinateur ou du système lui-même. Celles-ci sont régulièrement identifiées et corrigées par les développeurs et il est important de toujours avoir les dernières versions pour un minimum de risques.

Renseignez-vous

Avant chaque voyage, tâchez de connaître les principales informations sur votre lieu de villégiature pour parer aux éventuels problèmes techniques que vous pourriez être amené à rencontrer. Votre hôtel est-il équipé d'un réseau sécurisé ? Les prises de vos chargeurs correspondent-elles ? Y a-t-il des frais pour les appels vers vos proches ? Une fois ces informations acquises, prenez des mesures en conséquence : augmentation de votre forfait téléphonique, achats d'adaptateurs, installation d'application pour des appels en Wi-Fi.

Installez des outils de protection

Vous emmènerez certainement en vacances vos appareils mobiles : protégez-les. Les VPN permettront de limiter votre exposition à certaines attaques en chiffrant vos communications et en empêchant ainsi les pirates de les intercepter ou de les modifier. Si vous pensez utiliser vos appareils électroniques dans des lieux publics, posez sur l'écran un filtre de confidentialité pour qu'ils deviennent illisibles pour vos voisins. Pensez aussi à vous équiper d'un matériel vous permettant d'avoir toujours votre téléphone sur vous lorsque vous pratiquerez vos activités : une coque étanche sera notamment utile pour vous baigner avec votre smartphone, et ainsi échapper à un vol éventuel sur la plage...

Suivez ces six étapes en amont de votre départ en vacances et vous pourrez profiter de vos congés estivaux en toute sérénité !

5 conseils cybersécurité à appliquer pendant les vacances

Les vacances sont synonymes de déconnexion. Pourtant, certains d'entre nous continuent à consulter leurs informations professionnelles via leur smartphone, tablette ou ordinateur portable.
Quelques règles simples vous permettront de protéger vos données contre l'espionnage industriel ou les attaques malveillantes.

SAUVEGARDEZ VOS DONNÉES

Tout au long de l'année, il est indispensable de conserver une sauvegarde de vos données sur un support externe ou le cloud. C'est encore plus vrai lorsque vous partez en congés.

METTEZ À JOUR VOTRE MATÉRIEL

Les mises à jour proposées pour les systèmes d'exploitation IOS ou Windows sont souvent destinées à pallier des failles de sécurité. Il est donc très important de les effectuer afin de ne pas rendre votre système d'information vulnérable.

PRENEZ GARDE AUX CONNEXIONS WIFI

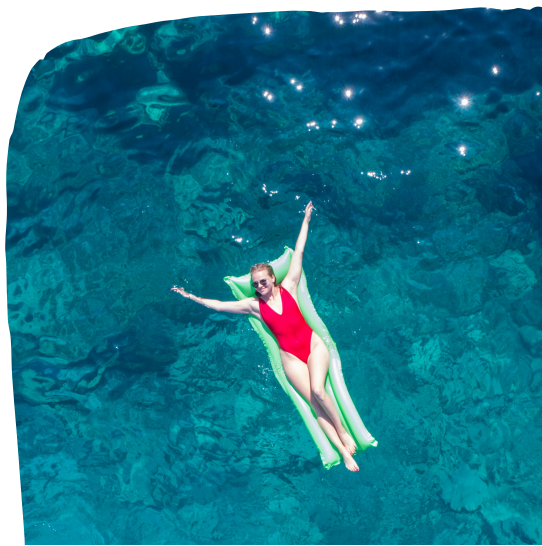
Attention aux connexions wifi sur les lieux publics. Ces réseaux ne sont pas sécurisés. Pour éviter tout risque, vérifiez bien que le site de connexion est valide avant de vous connecter.

PROTÉGEZ PAR MOT DE PASSE

C'est la première des règles à appliquer et pourtant elle n'est pas toujours respectée. Verrouillez votre ordinateur et votre smartphone par un mot de passe afin de limiter l'accès à vos données au cas où votre matériel est volé.

RESTEZ VIGILANT

Tout au long de l'année, vous êtes attentifs aux tentatives d'escroquerie par phishing et au spam. Ne relâchez pas votre attention : les cybercriminels sont actifs quelle que soit la période de l'année !



Former les utilisateurs aux bonnes pratiques : Les 10 commandements à suivre

De la TPE-PME au grand groupe, toute entreprise peut être aujourd'hui confrontée à la cybercriminalité. Développer une politique de sécurisation des systèmes d'information (SI) efficace est donc crucial. Cela commence par la formation aux « bonnes pratiques », qui sont peu coûteuses et faciles à mettre en œuvre.

1. Tout le SI, tu cartographieras
Avoir une vision globale et détaillée de son patrimoine informationnel est la première action à mener. Cela permet d'en identifier les vulnérabilités et autres surfaces d'attaque (adresses IP publiques, services cloud…) pour mieux les réduire et les protéger, et faciliter l'intervention de spécialistes en cybersécurité le cas échéant.
En pratique. Recensez tous les équipements (ordinateurs, mobiles, serveurs locaux et distants…), les logiciels utilisés, les données et les traitements de données (fichier client, informations comptables…), les accès (qui se connecte au SI et comment), et les interconnexions avec l'extérieur (points de contact entre le SI et Internet).

2. Correctement protégé, tu seras
Déployer un arsenal approprié et plus ou moins sophistiqué, en fonction de la taille et les besoins de l'organisation, permet de protéger le SI.
En pratique. Dotez vos équipements (ceux connectés en priorité) d'un antivirus professionnel, mais aussi d'outils complémentaires tels qu'un pare-feu associé à un filtrage web (proxy) ainsi qu'un réseau privé virtuel (VPN) à double authentification (idéalement). Si nécessaire, installez également diverses solutions dédiées - à la lutte contre le hameçonnage, à la sécurisation des transactions bancaires, etc.

3. Tous les accès, tu sécuriseras
Bien sécuriser les accès aux postes de travail (fixes et mobiles), au réseau interne, aux serveurs et aux sites Internet ainsi que les échanges avec d'autres organismes permet de limiter, et même d'éviter les risques d'intrusion.
En pratique. Sensibilisez les collaborateurs à l'utilisation de mots de passe robustes (difficiles à deviner ou à trouver à l'aide d'outils automatisés). Pour faciliter la gestion des noms d'utilisateur et des mots de passe, en cas de centralisation de plusieurs solutions logicielles notamment (messagerie, applications partagées, etc.), déployez un service d'authentification unifié (de type single sign-on, ou SSO). Et pour un maximum de sécurité, activez l'authentification à deux facteurs, voire multifactorielle (AMF), par jeton physique (carte à puce, token USB, etc.), par exemple.

4. Régulièrement les données, tu sauvegarderas
Effectuer des sauvegardes quotidiennes, hebdomadaires et/ou mensuelles selon le volume et la nature des données collectées permet une restauration plus rapide en cas de dysfonctionnement du SI ou d'attaque (par rançongiciel, ou ransomware, notamment).
En pratique. Identifiez les données à archiver (données sensibles, métiers, techniques…). Puis privilégiez un, voire plusieurs supports de sauvegarde (physiques et/ou dématérialisés) selon leur intégrité, leur viabilité et la pertinence du cryptage des données. Enfin, déterminez la fréquence des sauvegardes. N'oubliez pas de respecter la réglementation en vigueur relative à la protection des données dites « personnelles » (RGPD).

5. Aux mises à jour, tu procèderas
Mettre à jour les systèmes d'exploitation (Windows, macOS, Linux, Android, iOS…) et des logiciels dès la mise à disposition des correctifs de sécurité par leurs éditeurs permet d'empêcher les pirates informatiques de profiter de leurs failles pour pénétrer dans le SI.
En pratique. Activez les mises à jour automatiques, et utilisez des solutions matérielles et logicielles en usage (pas au-delà de leur cycle de vie). Exigez la même ligne de conduite des sous-traitants.

6. La messagerie, tu surveilleras
Former les utilisateurs à un usage sécurisé de la messagerie, principal vecteur d'infection des postes de travail, et mettre en place quelques outils idoines permet de préserver l'entreprise des virus et autres escroqueries répandues (hameçonnage - ou phishing, rançongiciel…).
En pratique. Sensibilisez les collaborateurs aux courriels frauduleux (par la vérification systématique de l'identité de l'expéditeur, de la cohérence du message, etc.). De plus, proscrivez l'ouverture automatique des documents téléchargés ainsi que la redirection de messages professionnels vers une messagerie personnelle. Prévenez la réception de fichiers infectés grâce à un antivirus adapté. Et chiffrez les communications (par l'application d'un protocole SSL/TLS, ou Secure Socket Layer/Transport Layer Security) entre les serveurs de messagerie et les postes de travail de sorte à garantir la confidentialité et l'intégrité des échanges.

7. Les usages informatiques, tu cloisonneras
Dissocier les usages professionnels en interne et interdire l'utilisation d'équipements professionnels dans un contexte personnel, et inversement, permet de réduire les risques d'exfiltration de données, d'intrusion, d'usurpation d'identité ou encore de détournement du SI avec une intention frauduleuse.
En pratique. Créez des comptes utilisateurs séparés et dotés de privilèges correspondant au profil métier, au niveau hiérarchique, au service, aux horaires ou encore à la nature du contrat. Interdisez les connexions directes entre les postes de travail. Et cloisonnez les activités digitales de l'entreprise à l'aide de dispositifs de filtrage physiques ou virtualisés (zone des serveurs internes, des serveurs connectés, des postes de travail, etc.). Au sein de l'organisation comme en dehors (à domicile, en mission…), exigez la séparation des usages professionnels et personnels.

8. Les utilisateurs, tu éduqueras
La cybersécurité est l'affaire de tous. Sensibiliser les utilisateurs aux bonnes pratiques permet d'en favoriser la compréhension et l'application.
En pratique. Rédigez une charte de sécurité et/ou une charte informatique annexée au règlement intérieur qui rappelle les règles de protection des données (et les sanctions encourues en cas de non-respect), les moyens d'authentification privilégiés par l'organisation, les modalités d'utilisation des outils informatiques et de communication (…). Accompagnez les collaborateurs par de la formation, des ateliers et des réunions, et responsabilisez-les (encouragez la déclaration d'incidents, notamment).

9. Les cyberattaques, tu anticiperas et déjoueras
Prévenir et savoir gérer les incidents permet de limiter les dégâts, d'intervenir rapidement et de renforcer la sécurité de l'entreprise.
En pratique. Faites de la veille, suivez l'actualité de la cybermalveillance (sur le site Cybermalveillance.gouv.fr, entre autres), et sachez quel(s) expert(s) contacter si besoin. Si possible, utilisez une solution de gestion des événements et des informations de sécurité (SIEM, ou Security Information and Event Management) pour profiter d'une visibilité totale sur l'activité du réseau et réagir aux menaces en temps réel. Prévoyez également un plan de reprise d'activité informatique (PRA), voire un plan de continuité d'activité (PCA) pour la remise en route du SI après un incident critique. Et n'oubliez pas de déposer plainte ni d'informer la Commission nationale de l'informatique et des libertés (Cnil) en cas de fuites de données personnelles.

10. Bien cyberassuré, tu seras
Être bien couvert en cas de cyberattaque permet de bénéficier d'une assistance juridique et d'être indemnisé selon les dommages et le préjudice subis (matériels, financiers, moraux…).
En pratique. Contactez votre compagnie d'assurance pour un accompagnement et une prise en charge sur mesure. Assurez-vous que les risques les plus grands pour la pérennité de l'entreprise sont couverts.

LA CYBERSÉCURITÉ : UN ENJEU COLLECTIF

Votre entreprise ne doit pas être la seule à respecter les règles essentielles à sa cybersécurité. Tous les membres de son écosystème, en particulier ceux qui gèrent et/ou ont accès à ses données, doivent les observer eux aussi. « En se protégeant - et, par capillarité, en protégeant leurs partenaires - les entreprises assurent leur pérennité et renforcent la confiance qui les lie à leurs parties prenantes. La cybersécurité représente donc un enjeu collectif majeur », affirment de conserve Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi), et Thomas Courbe, directeur de la Direction générale des entreprises (DGE) rattachée au ministère de l'Économie et des Finances, dans La cybersécurité pour les TPE/PME en 12 questions (publication de l'Anssi de février 2021).

LES PHASES D'UNE CYBERATTAQUE

Afin de protéger votre entreprise, il est important de comprendre comment les attaquants opèrent.

Découvrez ci-dessous les 4 grandes phases d'une cyberattaque :

- **Phase 1 : Identification et reconnaissance**

Les cybercriminels vont tout d'abord définir l'entreprise qu'ils souhaitent attaquer en fonction des objectifs qui se sont fixés. Leur but : élaborer une stratégie les amenant à entrer au sein de votre SI. Pour y arriver, ils collectent le maximum d'informations possibles afin de détecter une ou plusieurs failles de sécurité qu'elle soit matérielle ou humaine : ils identifient les terminaux non protégés, les serveurs vulnérables ou encore, les comportements numériques à risque de vos employés.

- **Phase 2 : Intrusion**

Une fois les informations collectées, c'est le moment pour les attaquants de s'infiltrer dans le Système d'Information de l'entreprise. L'intrusion débute à partir du moment où l'attaque devient active. Celle-ci peut prendre différentes formes, du très rependu phishing au site internet compromis, en passant par la connexion WiFi du café dans lequel vous avez l'habitude de travailler. Retenez toutefois que les effets ne sont pas forcément visibles immédiatement.

De plus, un pirate peut très bien s'introduire dans votre entreprise aujourd'hui et déclencher l'attaque plusieurs mois après.

- **Phase 3 : Capture et exploitation**

Une fois entrés dans le Système d'Information, les pirates peuvent désormais y installer des outils malveillants, se faire passer pour un utilisateur lambda et porter atteinte aux remparts de sécurité de l'entreprise. Tout cela dans un seul objectif : obtenir vos accès administrateurs. Car comprenez-le bien, ce sont bien ces accès qui sont la clé de toutes les informations confidentielles et souvent indispensables à la pérennité de votre société.

- **Phase 4 : Dissimulation**

Les pirates informatiques sont arrivés au bout de leur mission. Ils ont pris possession des données propres à votre entreprise mais aussi des informations liées à vos clients, prestataires et partenaires. Ils vont donc maintenant détruire toute trace de leur passage. Leur but : faire comme si aucune de vos données n'avaient été touchées ou compromises.

SÉCURISER LE TÉLÉTRAVAIL DANS SON ENTREPRISE

Télétravail :
5 gestes barrières pour une bonne politique cybersécuritaire

De plus en plus d'entreprises composent désormais avec le télétravail, une approche multicloud et des outils collaboratifs dispersés. Ce bouleversement du modèle traditionnel du système d'information (SI) exige des RSSI et des DSI le déploiement de solutions adaptées et performantes afin de réduire les risques en matière de cybersécurité.

1/ Cloisonnez l'accès aux ressources du SI.
Comment ? Par l'adoption d'un Principe du Moindre Privilège (PMP).
Dans le détail. Au sein de l'entreprise, les ressources utilisées par les collaborateurs diffèrent selon leur profil métier, leur niveau hiérarchique, leur département, leurs horaires ou encore la nature de leur contrat. Limiter les autorisations d'accès aux seules catégories d'informations – sensibles – indispensables à l'exercice d'une activité permet d'améliorer considérablement le niveau de sécurité de l'organisation. Dans le jargon, cette bonne pratique cybersécuritaire, qui s'accompagne de la mise en œuvre d'une politique de confidentialité en interne, s'appelle le Principe du Moindre Privilège (PMP ou PoLP, Principle of Least Privilege). Celui-ci peut s'appliquer aux personnes comme aux systèmes et services qui exigent des permissions pour effectuer une tâche. Passer par une solution de gestion et de sécurisation centralisées des identifiants à privilèges (de type IAM, Identity and Access Management) en garantit le bon fonctionnement.

2/ Activez l'authentification unique multifacteur.
Comment ? Par l'installation d'un logiciel d'authentification unique d'entreprise (eSSO, enterprise Single Sign-On).
Dans le détail. « Qu'il s'agisse des mots de passe des utilisateurs en télétravail, mais aussi de ceux en charge du support informatique, les mots de passe doivent être suffisamment longs, complexes et uniques sur chaque équipement ou service utilisé », recommande la plateforme Cybermalveillance.gouv.fr. Hélas, suivre scrupuleusement ce conseil avisé ne suffit plus aujourd'hui pour éviter les intrusions. Pour un niveau de protection élevé sans perte de confort pour l'utilisateur, mieux vaut déployer une solution d'authentification unique d'entreprise (eSSO). Celle-ci autorise la connexion à toutes les applications pour lesquelles le collaborateur a les droits, et élimine les futures demandes de mot de passe au cours de la session. Pour une sécurité renforcée, l'authentification doit être à deux facteurs (2FA), voire multifactorielle (MFA).

3/ Sécurisez les terminaux (endpoints).

Comment ? Par tous les moyens : antivirus (professionnel), pare-feu (firewall), mises à jour de sécurité, VPN (Virtual Private Network)...

Dans le détail. Ordinateurs de bureau, portables, tablettes, smartphones, serveur, imprimante... connectés au SI sont autant de terminaux, ou endpoints, qui obligent à la plus grande vigilance. Contre les attaques virales connues, et parfois le hameçonnage (phishing) et les rançongiciels (ransomware), équipez-les en solutions antivirales professionnelles (ou EPP, Endpoint Protection Platform). De même, systématisez les connexions sécurisées à l'aide d'un réseau privé virtuel (VPN) à double authentification : celui-ci crée un tunnel chiffré pour les données et préserve l'identité de l'utilisateur en masquant l'adresse IP. Procédez également, dès que possible, aux mises à jour de sécurité des appareils et logiciels afin de corriger les failles éventuelles. Enfin, hébergez les données sur un cloud. Et, pour être alerté en temps réel d'une intrusion, recourez à une solution de surveillance des sessions à distance (RDP, Remote Desktop Protocol).

4/ Tracez les accès et gérez les incidents

Comment ? Par la mise en place d'un système de journalisation (enregistrement des « fichiers journaux » ou logs).

Dans le détail. Pour détecter un accès frauduleux ou déterminer l'origine d'un incident, évaluer son étendue et y remédier, il convient d'enregistrer certaines actions réalisées sur le SI, et d'en conserver l'historique sous forme de journaux de bord appelés logs. Ces « événements pertinents » ne doivent pas se limiter aux seuls accès des utilisateurs. Pour un maximum d'efficacité, il faut, d'une part, tracer finement les accès aux ressources du SI (surveiller les flux entrants et sortants) ainsi que les échecs de connexion aux systèmes, et, d'autre part, traquer les incongruités (connexions simultanées, depuis l'étranger, à des heures inhabituelles...). Pour ce faire, il est nécessaire de déployer un système de journalisation associé, dans l'idéal, à un SIEM (Security Information Event Management), une solution capable de charger, convertir, uniformiser, corréler et interpréter les logs issus de sources hétéroclites.

5/ Sensibilisez et responsabilisez les collaborateurs

Comment ? Par le dialogue, une communication didactique et des directives claires, et l'adoption d'une charte de bonnes pratiques.

Dans le détail. Il est fondamental de « sensibiliser les utilisateurs aux risques, formaliser les responsabilités de chacun et préciser les précautions à prendre dans une charte ayant valeur contraignante », prévient la Commission nationale de l'informatique et des libertés (Cnil). Si l'entreprise doit sécuriser son SI, le collaborateur aussi doit s'impliquer. Sans surprise, le respect de bonnes pratiques de base, comme « subordonner l'utilisation des équipements personnels à une autorisation préalable de l'administrateur réseau et/ou de l'employeur » (Cnil) ou n'utiliser son matériel professionnel qu'à des fins professionnelles, limite grandement les risques. C'est d'autant plus important qu'une entreprise peut être tenue pour responsable des infractions commises pour son compte, et elle peut elle-même engager la responsabilité du salarié ou de son dirigeant.

Le must : le Zero Trust ?

Attention, « les récentes évolutions des technologies et des usages remettent en question le modèle traditionnel de défense périmétrique » des organisations, prévient l'Agence nationale de la sécurité des systèmes d'information (Anssi). Concrètement, « les pare-feux, le cloisonnement (physique ou logique) ou les VPN, rencontrent des limites ». Fort de ce constat, des entreprises se tournent vers une approche en devenir : le Zero Trust Network Access (ZTNA). « Concept d'architecture dédié au renforcement de la sécurité d'accès aux ressources et aux services », le ZTNA consiste à ne jamais faire confiance en cas de demande d'accès au SI par un utilisateur. Ainsi, quiconque souhaite se connecter doit nécessairement inspirer confiance, avec une authentification à deux facteurs, par exemple. Au gré des interactions avec le SI, le degré de confiance augmente ou, au contraire, diminue. Il permet alors, grâce aux récentes avancées de l'IA, de définir en temps réel la quantité et la qualité des accès accordés. Assurément prometteur. À ce jour, toutefois, « le recours à ces solutions est ardu, faute de maturité », poursuit l'Anssi.

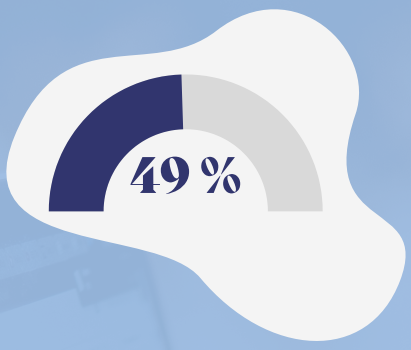
CHIFFRES CLÉS

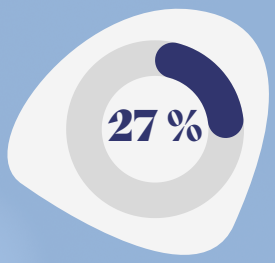
CYBER-ATTAQUES

Rapport annuel Hiscox Cyber 2021

Cible

Près d'1 entreprise française sur 2 a été visée par une cyberattaque



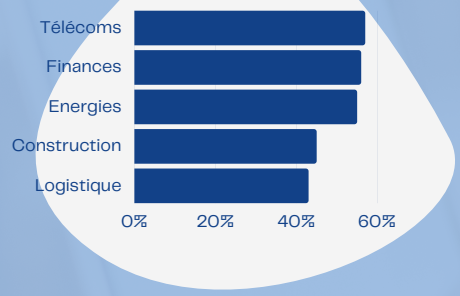


27% des entreprises ont subi au moins 10 attaques significatives

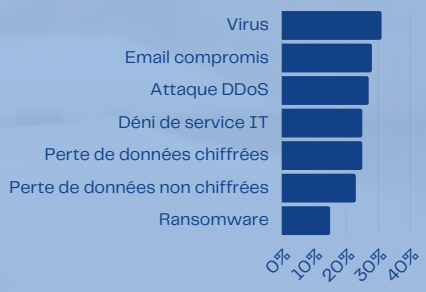
Part du budget cyber

Hausse de 63% de 2020 à 2021

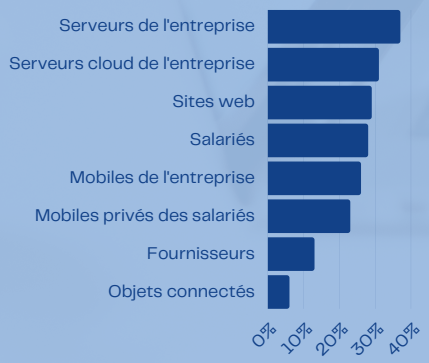
Top 5 des secteurs les plus attaqués



Différents types d'attaques



1ers points d'entrées des attaques



Coût médian par cyber-attaque dans les TPE : 6.700€

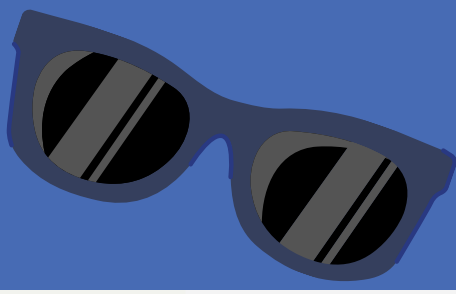
250.000€
perte moyenne subie par 5% des entreprises

9.800€
somme moyenne payée par les entreprises pour un ransomware

eLiT cyber

elit-cyber.com

8 RÈGLES POUR PROTÉGER VOS DONNÉES



JE VÉROUILLE MA SESSION

lorsque je m'absente et l'attache avec un anti-vol si possible

J'UTILISE UN MOT DE PASSE

facile à mémoriser et difficile deviner

J'utilise uniquement les

OUTILS VALIDÉS PAR LA SOCIÉTÉ

Je sauvegarde mes données

DANS LE CLOUD

DANS LES LIEUX PUBLICS JE VEILLE SUR MES ÉQUIPEMENTS

j'utilise un filtre de confidentialité et ne divulgue pas d'informations sensibles

JE NE COMMUNIQUE JAMAIS MES IDENTIFIANTS

Mots de passe, codes d'accès à des tiers par email, téléphone ou sur un site internet

JE SUIS VIGILENT AVEC MA MESSAGERIE

Je ne clique pas sur les liens ni les pièces jointes suspectes

JE SIGNALE UN INCIDENT DE SÉCURITÉ

je souhaite lever un doute, je m'interroge sur une pratique de sécurité

elit-cyber.com

eLiT cyber

Les cyber attaques

Votre entreprise représente une cible de choix pour les cyberattaquants et leurs nouveaux modes opératoires ne laissent aucune chance aux victimes non préparées.

Il existe 2 grandes familles d'attaques

Les attaques visibles

Ransomware
Attaque directe et indirecte, crise cyber pour la victime

Injection SQL
Indisponibilité de serveurs ou services

Les attaques silencieuses

Phishing / Hameçonnage non ciblé du SI

Malware Déploiement d'outils malveillants

Password cracking Cassage de mot de passe

Man in the middle Indisponibilité de serveurs ou services

DDoS Indisponibilité de serveurs ou services

Pourquoi & comment mener une analyse forensique ?

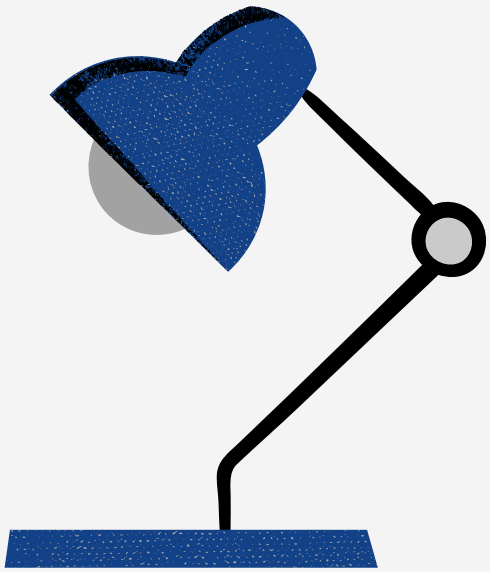
Dans quel cas mener une analyse forensique ?

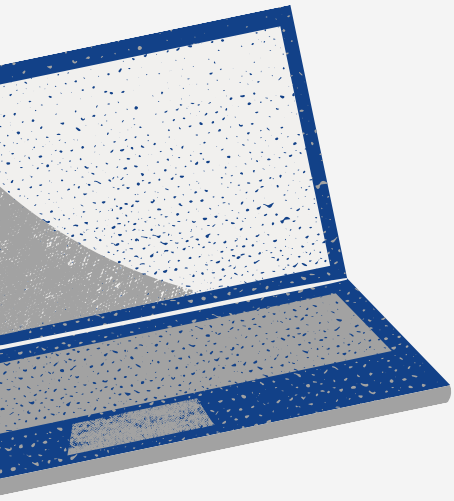
- **Fuite de données** avérée ou encore suspicion d'une fuite de données à la suite du départ litigieux d'un collaborateur
- **Activités étranges** dans les boites mail
- Quand un **malware** se réplique sur l'ensemble du SI et que l'antivirus ne peut y remédier

L'analyse forensique en informatique signifie l'analyse d'un système informatique après incident.

Méthodologie

1. **Préparation et identification :** Le but est de collecter des informations sur le déroulement de l'attaque et les preuves numériques.
2. **Analyse et corrélation des événements :** une fois les informations collectées, elles sont analysées et corrélées pour déterminer la source et la cause de l'incident.
3. **Remédiation :** Cela permet de mettre en place les mesures appropriées pour corriger tout défaut identifié et les actions pour éviter que cela se reproduise.





Comment réagir en cas de compromission ?

- **Sauvegardez** l'état des actifs compromis
- **Isoler** autant que possible l'équipement concerné du réseau et d'internet
- Faire appel à un interlocuteur spécialisé
- Effectuez les déclarations légales dans des délais imposés en cas de fuite de données personnelles ou en cas de périmètre concerné par la LPM ou le NIS

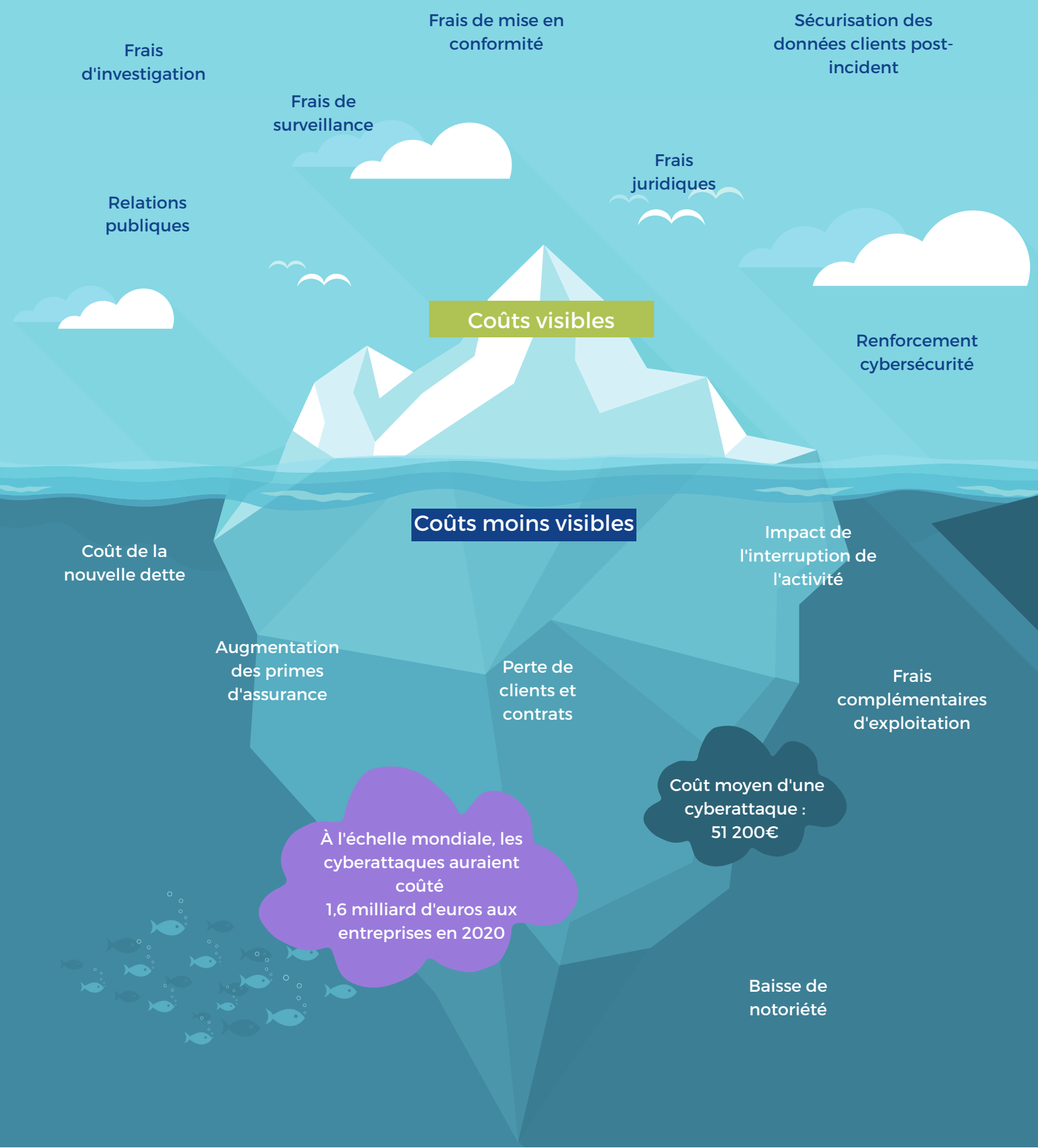
Comprendre ce qu'il s'est passé

- Qui a attaqué ?
- Quelles sont les conséquences ?
- Comment il est entré dans le SI ?
- Quels sont ses objectifs ?
- Quand l'infection a débuté ?
- Quels sont les systèmes touchés ?

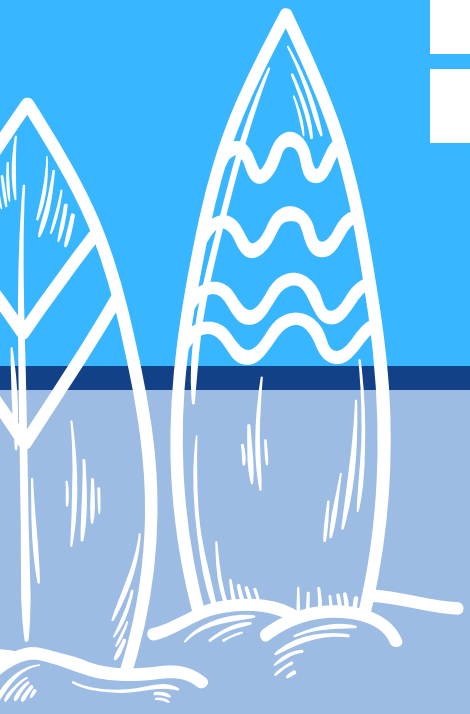
Comment s'armer en prévision d'une attaque ?

- Réalisez des **sauvegardes régulières** avec un temps de rétention suffisant.
- **Journalisez un maximum d'évènements**.
- **Externalisez le stockage des sauvegardes et des traces**.

LES COÛTS D'UNE CYBERATTAQUE



Mots croisés



1 - Logiciel indésirable conçu pour afficher des publicités intempestives sur l'écran, le plus souvent dans un navigateur web.

2 - Forme de logiciel malveillant conçu pour crypter des fichiers sur un appareil, rendant tous les fichiers et les systèmes qui en dépendent inutilisables .

3 - Logiciel utilisé par les cybercriminels pour prendre le contrôle d'un ordinateur ou d'un réseau cible.

4 - Programme informatique qui peut se copier et infecter un ordinateur sans l'autorisation ou la connaissance de l'utilisateur.

5 - Logiciel malveillant installé à l'insu de l'utilisateur final afin de voler des informations sensibles.

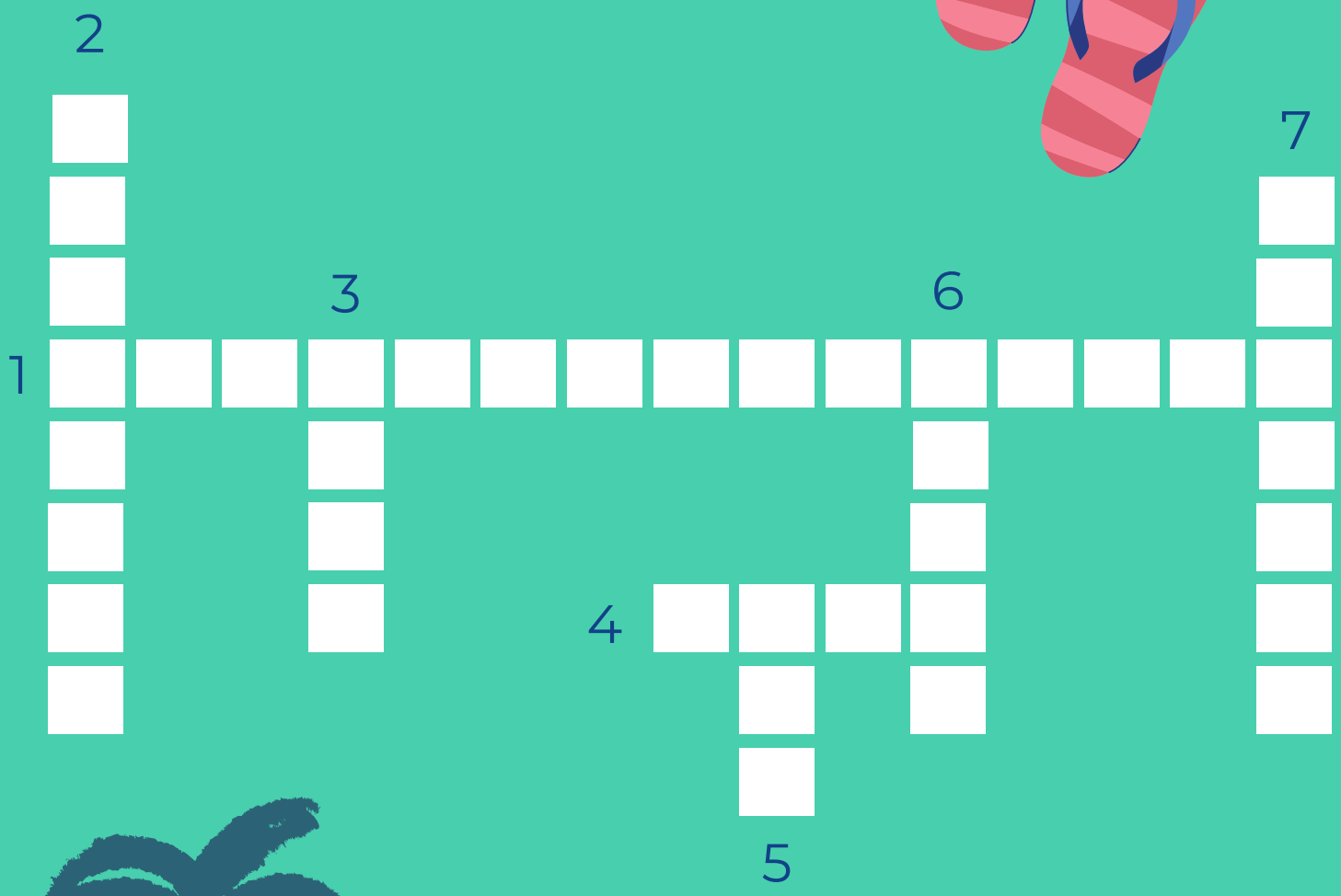
6 - Logiciel malveillant qui se télécharge sur un ordinateur déguisé en programme légitime.

7 - Type de logiciel malveillant dont la fonction principale est de s'auto-répliquer et d'infecter d'autres ordinateurs tout en restant actif sur les systèmes infectés .

8 - Protection des systèmes connectés à Internet tels que le matériel, les logiciels et les données contre les cybermenaces.

1 - ADWARE ; 2 - RANSOMWARE ; 3 - ROOTKIT ; 4 - VIRUS ; 5 - SPYWARE ; 6 - TROJAN ; 7 - WORM ; 8 - CYBERSECURITY

Mots croisés



1 - Parcours pour engager vos collaborateurs.

2 - Attaque qui tente de voler votre argent ou votre identité en vous obligeant à révéler des informations personnelles, telles que des numéros de carte de crédit, des informations bancaires ou des mots de passe, sur des sites Web prétendant être légitimes.

3 - Programme conçu pour identifier les vulnérabilités dans une application, un système d'exploitation ou un réseau.

4 -Plan d'actions défini pour maintenir un certain niveau de sécurité.

5 - Plateforme permettant la supervision et l'administration de la sécurité du système d'information au travers d'outils de collecte, de corrélation d'événements et d'intervention à distance.

6 - Analyse qui permet d'orienter la stratégie de cybersécurité en fonction des besoins de l'infrastructure existante et des cybermenaces récurrentes.

7 - Méthode qui consiste à analyser une cible en se mettant dans la peau d'un attaquant.

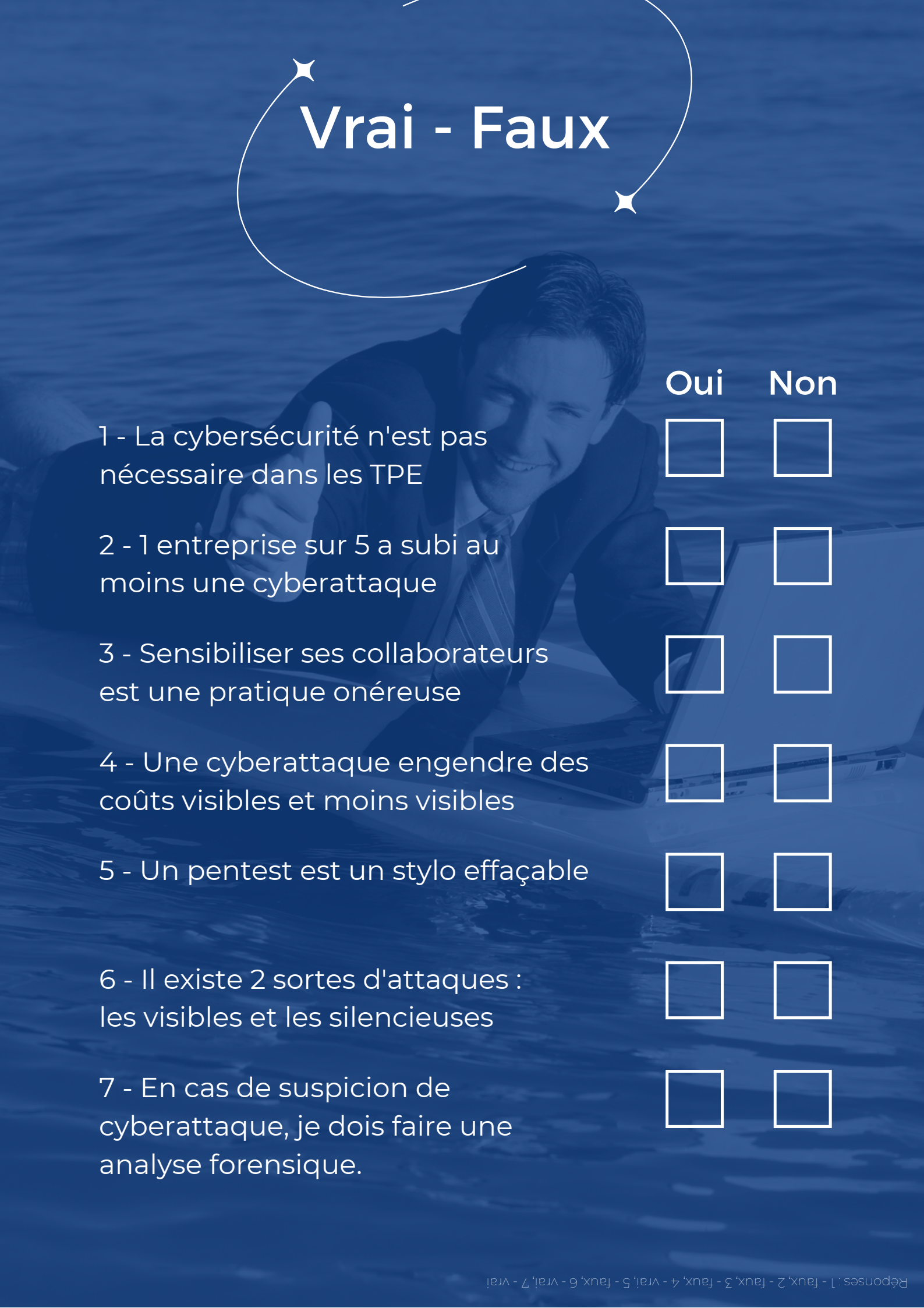
1 - SENSIBILISATION ; 2 - PHISHING ; 3 - SCAN ; 4 - PSSI ; 5 - SOC ; 6 - AUDIT ; 7 - PENTEST

CYBERSECURITÉ

5 ERREURS À NE PAS COMMETTRE

- Document confidentiel en évidence
- Post-It avec mot de passe en évidence
- Clé usb à portée de main
- Feuilles laissées dans l'imprimante
- Ecran d'ordinateur laissé ouvert

Vrai - Faux



	Oui	Non
1 - La cybersécurité n'est pas nécessaire dans les TPE	☐	☐
2 - 1 entreprise sur 5 a subi au moins une cyberattaque	☐	☐
3 - Sensibiliser ses collaborateurs est une pratique onéreuse	☐	☐
4 - Une cyberattaque engendre des coûts visibles et moins visibles	☐	☐
5 - Un pentest est un stylo effaçable	☐	☐
6 - Il existe 2 sortes d'attaques : les visibles et les silencieuses	☐	☐
7 - En cas de suspicion de cyberattaque, je dois faire une analyse forensique.	☐	☐

Réponses : 1 - faux, 2 - faux, 3 - faux, 4 - vrai, 5 - faux, 6 - vrai, 7 - vrai

Vidéos

Découvrez ce que vous procure une équipe dédiée (SOC) à la sécurité de votre SI et les conséquences possibles en cas de cyber attaque sans SOC.

Découvrez dans la vidéo ci-contre ce qu'est un test d'intrusion/pentest

Découvrez ce qu'est une analyse forensique, son déroulement, les actions à mettre en œuvre et les préconisations

eLiT cyber

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

RÉFÉRENCÉ SUR LA PLATEFORME
CYBERMALVEILLANCE.GOUV.FR
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
CYBER MALVEILLANCE GOUV.FR
Assistance et prévention en sécurité numérique

FRANCE RELANCE

elit-cyber.com

Protégez-vous avec nos prestations & solutions de cybersécurité

Partenaires

CATO NETWORKS · paloalto NETWORKS · cisco Partner · deepinstinct BEFORE YOU KNOW IT · Microsoft · Check Point SOFTWARE TECHNOLOGIES LTD. · securonix

ANALYSE DE RISQUES

Cartographiez, cotez et hiérarchisez vos risques d'entreprise sur un ou des systèmes, applications et réseaux. Priorisez les correctifs de sécurité à appliquer.

AUDIT DE SÉCURITÉ

évaluez votre niveau de conformité par rapport à votre référentiel de sécurité (PSSI, Norme ISO, etc.) sur le périmètre de votre choix (Global, Data Center, Service Achat, etc.)

ANALYSE FORENSIQUE

Collectez les preuves numériques après une attaque informatique grâce à l'analyse forensique pour identifier les vulnérabilités et portes dérobées encore présentes sur votre SI.

PENTEST

Simulez une cyberattaque contre votre entreprise afin d'évaluer les failles de sécurité de votre système d'information exploitable par un pirate informatique et des logiciels malveillants.

SOC - ÉQUIPE DE CYBERSÉCURITÉ

Surveillez et analysez en permanence l'ensemble des événements de votre SI grâce au Security Operation Center. Détectez, qualifiez et stoppez toutes les cyberattaques 24h/24 - 7j7 !

PLAN DE FORMATION

Formez vos collaborateurs en cybersécurité selon leur degrés de maturité et sensibilité au sein de votre organisation face aux différentes menaces existantes.

CAMPAGNE DE PHISHING

Évaluez le niveau de maturité en cybersécurité de vos collaborateurs par des tentatives de mails frauduleux. Analysez ensuite les résultats et adaptez votre stratégie de sensibilisation à la cybersécurité.

PSSI & PAS

- Centralisez vos mesures, processus et contrôles de cybersécurité dans la PSSI. Engagez votre direction et vos collaborateurs dans le management de la sécurité des SI.

- Réduisez votre temps de réponse aux questionnaires de conformité de vos clients et prospects grâce au PAS.

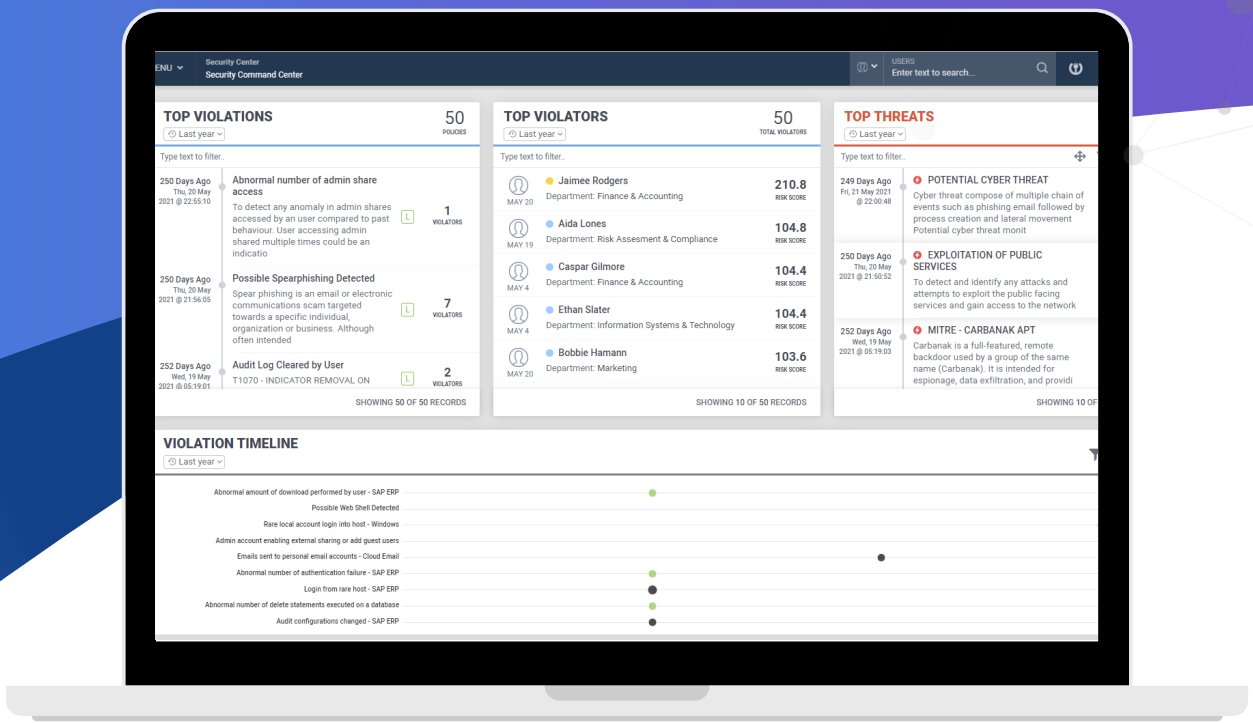
SCAN DE VULNÉRABILITÉ

Cartographiez les failles de sécurité présentes sur votre SI et rédigez une politique de Patch Management (présent dans la PSSI) pour maîtriser vos vulnérabilités.

Suivez-nous sur

01 34 48 75 30
contact@elit-technologies.fr

elit-cyber.com



SOC

Plateforme de supervision et d'administration de la sécurité du système d'information

PRÉVENTION

- Gestion des vulnérabilités
- Sensibilisation / Formation des utilisateurs
- Pentest
- Veille cybersécurité

DÉTECTION

- Qualification alertes de sécurité
- Collecte, centralisation des logs
- Détection sur seuil
- Détection comportementale

RÉACTION

- Réaction automatisée et ciblée
- Isolation & traitement
- Plan de Continuité d'Activité (PCA)
- Plan de Reprise d'Activité (PRA)

AMÉLIORATION

- Former les utilisateurs sur les bonnes pratiques
- Conseiller le client sur ses choix stratégiques et investissements
- Renforcer les règles de sécurité et de détection
- Investigation ou Forensics

elit-cyber.com

User de la ruse, c'est reconnaître des limites à sa puissance !

Suivez-nous sur

eLiT cyber

elit-cyber.com