kaspersky

Voir ce que les attaquants voient : reprenez la main sur votre empreinte numérique

Identifier, comprendre
et contrer les menaces avec
la Cyber Threat Intelligence

Dans ce guide, vous retrouverez :

Une présentation des enjeux de la Cyber Threat Intelligence et de l'empreinte numérique

Une grille de lecture pour cartographier votre empreinte numérique et vos points d'exposition

Les méthodes utilisées par les attaquants exploitant votre empreinte numérique

Un plan d'action concret pour identifier et corriger les risques liés à l'empreinte numérique

Personne n'est à l'abri d'une attaque. Comment expliquer que des entreprises bien protégées soient encore victimes de compromissions ? Tout simplement parce que les attaquants ont changé de stratégie : ils ne s'attaquent plus seulement au cœur du système d'information, mais privilégient désormais sa périphérie, ces zones exposées et souvent moins surveillées.

En effet, les entreprises laissent de nombreuses traces sur Internet, volontairement ou non. Qu'il s'agisse de leur site web, des accès SaaS, des comptes de leurs collaborateurs sur les réseaux sociaux, de leur charte graphique ou des leaks de données en vente sur le Dark Web. Tous ces éléments, soit l'ensemble des actifs, services et informations exposés, forment ce qu'on appelle l'empreinte numérique. Et tous peuvent être de potentiels vecteurs d'attaque.

Pour réduire ces risques, les équipes IT doivent mettre en place une stratégie de Cyber Threat Intelligence (CTI). La Cyber Threat Intelligence est une approche proactive de la cybersécurité, qui vise à collecter, traiter et analyser les informations sur les menaces avant qu'elles ne surviennent. Une approche qui séduit de nombreuses organisations. Selon Kaspersky, 80 % des entreprises françaises seraient prêtes à adopter de tels outils de détection.

Le but est que l'entreprise voit ce que les attaquants voient, qu'elle sache de quelles informations ils disposent. Un aspect essentiel, puisque l'organisation n'a pas forcément une pleine connaissance de l'étendue de son empreinte numérique. Le renseignement et la maîtrise de l'environnement deviennent alors la première ligne de défense.

Pour mettre en œuvre cette approche, un changement de point de vue est nécessaire. La Cyber Threat Intelligence s'est construite au départ à partir de l'intérieur du système d'information. Or, les attaquants, eux, opèrent depuis l'extérieur, faisant de l'empreinte numérique une porte d'entrée majeure.

Afin d'explorer ce sujet et de proposer des mesures activables, ce guide fera d'abord un panorama des éléments inclus dans l'empreinte numérique et des questions à se poser pour mesurer son niveau d'exposition. Puis, nous nous pencherons sur les attaques rendues possibles par l'exploitation de l'empreinte numérique. Enfin, nous verrons quelles actions mener pour contrer ces menaces grâce à la CTI.

Sommaire

01

Empreinte numérique : ce que votre entreprise expose sans le savoir

Les entreprises n'ont pas toujours une vision exhaustive de leur surface d'attaque. Certains assets sont perçus, à tort, comme anodins. D'autres sont tout simplement ignorés.

Les cibles les plus visibles

La trace numérique la plus visible d'une entreprise est bien évidemment son **site officiel**. En apparence sans risque, il révèle de nombreuses informations. Le nom de domaine mène souvent aux adresses mail des collaborateurs. Il révèle aussi les adresses IP de l'organisation avec une requête Whois. Il ne faut pas oublier non plus les éventuels sous-domaines. Par exemple, un site pour une promotion particulière ou la vitrine d'une filiale.

Les **réseaux sociaux** fourmillent aussi d'informations. Qu'il s'agisse des comptes officiels de l'entreprise ou des comptes personnels des collaborateurs. Linkedin dévoile l'organigramme plus ou moins complet de la société avec les noms et les fonctions. Sans compter que les collaborateurs dévoilent parfois des éléments sur leur localisation ou leur agenda sur leurs réseaux sociaux.

Et la base est conséquente. Selon France Num, rien qu'en France, Linkedin compte de 13,5 à 16 millions d'utilisateurs actifs par mois.

La **charte graphique** de l'entreprise, à commencer par ses logos, est une autre trace numérique très visible des entreprises. Et elle est souvent mise à disposition librement sur le site officiel.

L'**Open Data** n'est pas à négliger. Les informations du registre du commerce sont disponibles publiquement et concernent les identités des dirigeants, les comptes de l'entreprise...

Mais l'empreinte numérique est aussi faite d'assets moins visibles au premier abord mais beaucoup plus critiques.

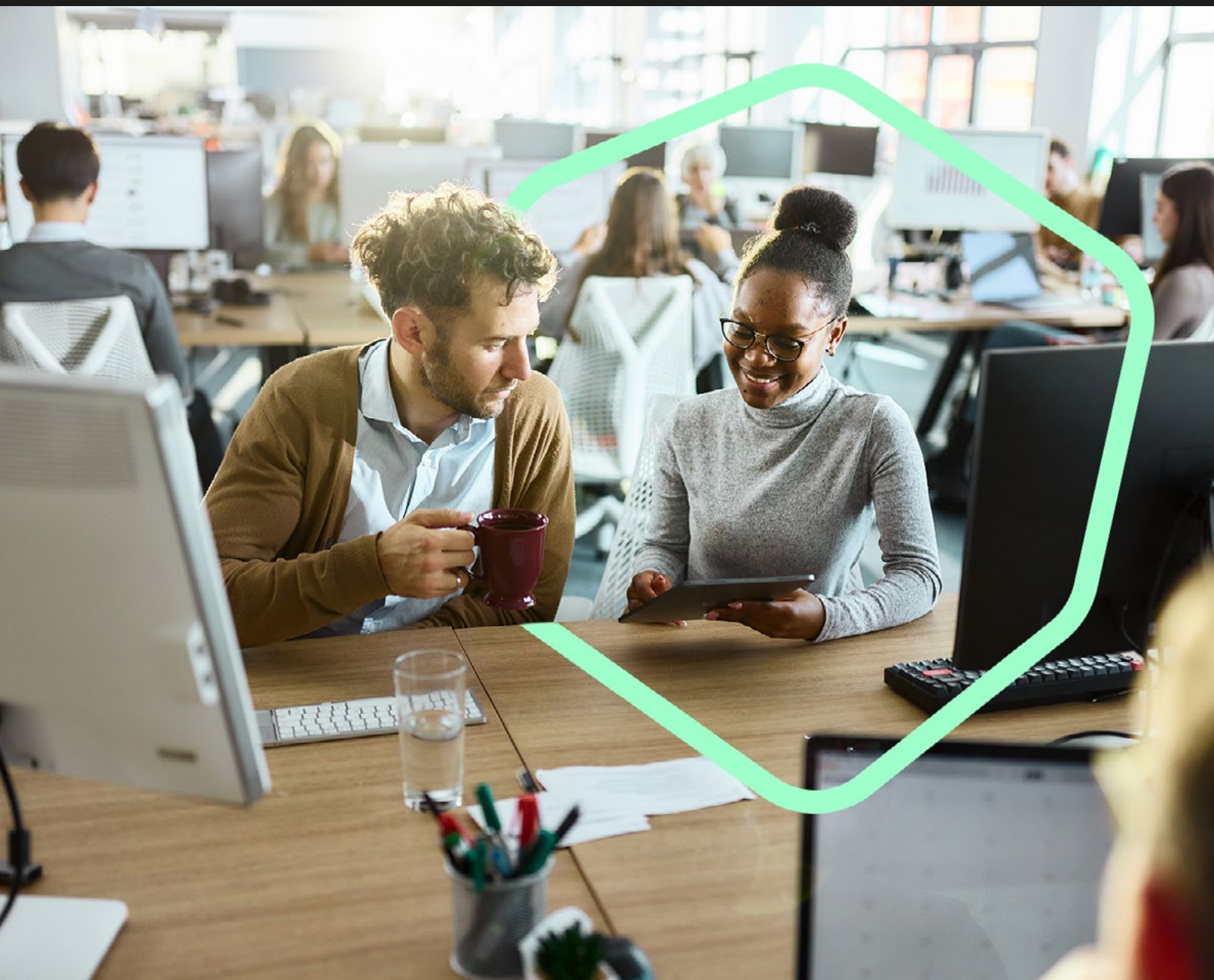
> Les entreprises n'ont pas toujours une vision exhaustive de leur surface d'attaque.

Les cibles les plus critiques

Les connexions externes au cloud ou au SaaS sont prisées des attaquants. Il arrive qu'un accès créé pour un prestataire externe, et oublié par les équipes IT, reste opérationnel. Un document peut être partagé à l'extérieur avec un simple lien sans authentification.

Ce type d'exposition est d'autant plus courant si les collaborateurs pratiquent le shadow IT (utilisation d'outils collaboratifs non approuvés par la DSI, partage de documents confidentiels…).

Tout aussi discrètes, les mentions sur des forums spécialisés dans les activités cybercriminelles ou des places de marché frauduleuses sont autant de points de départ d'une potentielle attaque. Par exemple, si des attaquants revendent des identifiants ou coordonnent une attaque DDoS.



Évaluer son degré d'exposition

Une fois ses assets identifiés, encore faut-il mesurer son niveau réel d'exposition.
Pour objectiver ce diagnostic, l'entreprise peut s'appuyer sur une grille d'analyse structurée, couvrant l'ensemble de sa surface d'attaque externe.

Zone d'exposition	**Questions à se poser**	**Niveau de visibilité**	**Niveau de criticité**	**Risque principal**
Noms de domaine	• Combien de sites Internet possède-t-elle ? (domaine principal et sous-domaines). • Le nom de domaine est-il le même pour le site corporate et les adresses mail professionnelles ? • Accède-t-on à des données sensibles (coordonnées de l'administrateur…) via une requête Whois ?	Élevé	Moyen	Phishing ciblé, reconnaissance
Identité visuelle et marque	La charte graphique et les logos sont-ils librement disponibles ?	Élevé	Moyen	Phishing, usurpation de marque
Informations sur l'entreprise	Quelles informations sont disponibles publiquement sur l'entreprise ? (dans les médias, les plateformes d'Open data : clients et partenaires, noms des dirigeants, comptes, procédures collectives…)	Élevé	Moyen	Ingénierie sociale, phishing ciblé…
Informations sur les collaborateurs	Quelles informations sont disponibles sur les collaborateurs notamment sur les réseaux sociaux ? (noms, coordonnées, fonctions, clients, localisation…)	Élevé	Moyen	Ingénierie sociale, phishing ciblé…
Accès au SaaS/cloud	• Combien de points d'entrée externes au SaaS/cloud l'entreprise a-t-elle créé ? • Sont-ils accessibles de n'importe où sans VPN ? • Le lien est-il public ou facilement découvrable (de type site.com/admin) ? • Une authentification est-elle nécessaire ? • Quelles sont les règles d'accès et les rôles définis ? • L'entreprise maîtrise-t-elle le partage de ses documents internes ou les collaborateurs détournent-ils souvent les règles ?	Moyen	Élevé	Intrusion frauduleuse, vol de données, modification d'applications…
Présence sur le Dark Web	• L'entreprise est-elle nommée sur le Dark Web ? (places de marché de revente de données, forums cybercriminels…) • Est-elle citée comme la cible de futures attaques ?	Bas	Élevé	Vol de données, attaques DDoS…

Une fois le diagnostic effectué, l'organisation sait à quels risques elle s'expose et quels leviers activer pour les contrer.

02

Comment les attaquants exploitent l'empreinte numérique

Les assets et le niveau d'exposition sont identifiés. L'étape suivante est la compréhension des méthodes employées par les attaquants pour exploiter les failles liées à l'empreinte numérique.

Usurpation de marque et ingénierie sociale : des attaques à forte crédibilité

S'il trouve les bons éléments, un attaquant a les moyens de se faire passer pour un interlocuteur crédible.

En consultant la liste des collaborateurs sur Linkedin, l'attaquant a la possibilité de contacter la bonne personne à la comptabilité et/ou de prendre l'identité d'un cadre dirigeant. Une tactique utilisable pour une arnaque au président (lorsqu'un escroc se fait passer pour un dirigeant de l'entreprise et contacte le service financier en exigeant un paiement urgent).

Autre cas : les campagnes de phishing ciblées. Par exemple, l'attaquant se fait passer pour un membre de l'équipe IT et demande la réinitialisation d'un mot de passe à un collaborateur. Selon le baromètre CESIN de 2025, le phishing représente 60 % des cyberattaques en France. Au niveau international, le Forum économique mondial estimait 42 % des organisations ont connu au moins un incident de ce genre en 2024. La mise à disposition de la charte graphique permet de produire des mails ou des documents internes en apparence authentiques.

L'attaquant peut aussi usurper l'identité d'un prestataire pour réclamer des paiements frauduleux en éditant de fausses factures avec le logo du sous-traitant concerné. L'IA générative industrialise la fabrication de tels faux documents.

Toutes ces attaques peuvent être commises sans grandes compétences techniques juste en exploitant l'empreinte numérique de l'entreprise visée. Cela montre que l'humain représente la plus grande faille en matière de cybersécurité. Une faille que les outils traditionnels ont du mal à combler. Selon Gartner, en 2026, 85 % des fuites de données auront pour origine une défaillance humaine. Ces défaillances coûtent cher, le phishing ouvrant l'accès au SaaS ou au cloud de l'entreprise.

85 %

des fuites de données auront pour origine une défaillance humaine en 2026, selon Gartner.

Accès SaaS/Cloud compromis : une porte d'entrée critique

Ce sont les attaques les plus redoutables mais qui peuvent être simples à mener pour les attaquants.

Même sans campagne de phishing et d'usurpation d'identité, un attaquant a la capacité de s'introduire frauduleusement en exploitant des traces numériques. Sur Linkedin, il est simple de connaître l'identité des collaborateurs de ladite entreprise. Si on connaît le nom de domaine de l'organisation, il est facile de connaître les adresses mail professionnelles. L'attaquant n'a plus qu'à chercher les noms des salariés dans un leak de données comprenant des mots de passe et voir si l'un d'eux utilise le même mot sur tous ses comptes.

À partir de là, l'attaquant ouvre une porte d'entrée vers des données ou documents sensibles dans un but de revente ou de rançon. Libre à lui de modifier des applications (manipulation de données financières par exemple) voire d'introduire un malware.

Il peut aussi modifier le contenu d'un site Internet ou publier des messages sur les réseaux sociaux de l'entreprise.

Une autre attaque possible est l'accès frauduleux aux boîtes mail. Selon Interpol, la compromission des adresses mail professionnelles représentait 35 % des cyberattaques enregistrées en 2024 dans 19 pays africains.

Une fois de plus, il s'agit d'attaques critiques qui peuvent être menées sans compétences avancées en codage ou cybersécurité, à cause de mauvaises pratiques numériques et d'une exposition non maîtrisée. Le problème n'est plus la technologie mais la visibilité externe. Une fois le SaaS ou le cloud compromis, le principal risque est le vol de données.

35 %

des cyberattaques enregistrées en 2024 dans 19 pays africains, provenaient, selon Interpol, de la compromission des adresses mail professionnelles.

Fuite de données : quand l'incident devient une crise

En entrant dans le SaaS/cloud de l'entreprise par leak d'identifiants ou phishing, l'attaquant prend la main sur des données sensibles. Une attaque qui peut avoir de lourdes conséquences opérationnelles et même exposer à des sanctions de la part des autorités.

Ces données peuvent être revendues sur le Dark Web à d'autres attaquants en vue de campagnes de phishing ou d'escroquerie. Les organisations gérant d'importantes bases de données nominatives sont particulièrement concernées : les administrations (France Travail, Urssaf…), les opérateurs téléphoniques… Les entreprises victimes, par une veille sur leurs mentions sur les forums cybercriminels, peuvent repérer ce type de transactions.

Autre option : l'attaquant garde les données pour lui et réclame une rançon via un ransomware. Un logiciel qui bloque les données de l'entreprise et ne les libèrera que si la victime paie une certaine somme.

Les attaquants peuvent s'appuyer sur des kits de ransomware-as-a-service sur le Dark Web pour obtenir des logiciels malveillants clés en main. Ce type d'attaque, qui ne nécessite aucune compétence en développement, a pourtant de lourds impacts opérationnels.

Les cibles et les attaques possibles étant identifiées, quel plan d'action mener pour éviter tout incident ? Pour éviter de subir un incident imprévu, adopter une posture proactive est indispensable. C'est le rôle de la Cyber Threat Intelligence.

03

4 actions prioritaires pour reprendre le contrôle grâce à la CTI

La CTI (Cyber Threat Intelligence) ne se limite pas à une simple veille, elle doit être le point de départ pour renforcer sa stratégie de cybersécurité et corriger ses vulnérabilités.

01 Collecter les renseignements sur les menaces et vulnérabilités

La première étape est la mise en place d'outils de surveillance des assets de l'empreinte numérique. Il s'agit de contrôler ce qui est en apparence incontrôlable et de protéger toute sa présence numérique volontaire ou non. L'organisation doit identifier ce qu'elle ignore elle-même, voir ce que les attaquants voient.

C'est là que la CTI prend tout son sens en tant qu'approche proactive de renseignement. La gestion des incidents a posteriori arrive trop tard, les RSSI et DSI se doivent d'agir en amont.

Il faut d'abord détecter tous les points d'entrée potentiels comme les noms de domaine, les IP ou les accès SaaS/cloud. Le portail Kaspersky Threat Intelligence, qui comprend Kaspersky Digital Footprint Intelligence, repère les ressources du réseau exposées, même inconnues, et évalue les vulnérabilités potentielles à partir des scores CVSS lorsqu'ils sont disponibles. Il ne s'agit plus de contrôler ce qu'on connaît déjà mais de reprendre la main sur des assets jusque-là invisibles.

Kaspersky Digital Footprint Intelligence surveille aussi le Dark Web (forums cybercriminels, blogs de ransomwares…) et le Web surfacique, avec certaines plateformes comme Pastebin, grâce à des techniques d'OSINT pour repérer toute mention de l'entreprise ainsi que de ses clients et partenaires. La solution repère également les menaces potentielles ou actives et les campagnes APT (Advanced Persistent Threat) ciblant l'organisation en elle-même ou son secteur.

En outre, la solution détecte les fuites de données et alerte si des informations relatives aux collaborateurs, partenaires et clients se retrouvent exposées.

L'entreprise pourra par ailleurs surveiller l'usage de sa marque et de sa charge graphique pour parer à toute utilisation de faux sites Internet ou comptes usurpateurs sur les réseaux sociaux.

02 Analyser les renseignements et prioriser les risques

Surveiller ne suffit pas, les données nécessitent d'être traitées pour être pertinentes. Avec l'aide de la solution Kaspersky CyberTrace, les équipes cyber peuvent intégrer les flux de données issus de la CTI aux contrôles de sécurité existants (comme les systèmes SIEM). Cela automatise le tri initial et identifie immédiatement les alertes qui doivent faire l'objet de plus d'investigations. Les flux de données sont exploitables au format JSON, STIX, XML et CSV.

Chaque flux d'information est enrichi avec un contexte (noms des menaces, horodatages, géolocalisation…). Ces données contextuelles permettent de mieux comprendre la situation globale, facilitant ainsi leur traitement et réduisant le temps moyen de réponse aux incidents (MTTR).

03 Intégrer la CTI dans la stratégie cyber existante

La réponse aux incidents est en effet essentielle. Les équipes IT doivent intégrer la CTI dans la stratégie globale de cybersécurité. Les données issues de la CTI sont vouées à être incluses dans les process cyber habituels pour déclencher les mesures adéquates aux vulnérabilités détectées. Si la sécurité interne est maîtrisée grâce aux technologies EDR ou XDR, l'enjeu est désormais à l'extérieur.

Les structures sont amenées à évoluer. Le SOC étend sa veille aux assets extérieurs et devient les yeux des équipes cyber sur l'empreinte numérique de l'entreprise. Il passe d'un rôle de gardien du cœur du SI à celui de vigie de tout l'environnement interne comme externe.

Un des points techniques essentiels est le complément des solutions ASM (Attack Surface Management) par des solutions EASM (External Attack Surface Management), comme celles incluses dans Kaspersky Digital Footprint Intelligence. Il s'agit d'un changement de point de vue. La cible n'est plus ce que voient les équipes IT mais ce que voient les attaquants.

Les scanners de vulnérabilité ASM sont conçus pour inspecter les actifs connus à la recherche de failles logicielles connues. Ils fonctionnent à partir d'une liste prédéfinie d'actifs et vérifient les correctifs manquants, les erreurs de configuration ou les logiciels obsolètes.

Les solutions EASM se concentrent eux sur la découverte et la surveillance de tous les actifs exposés à Internet, en particulier ceux qui peuvent être inconnus ou non gérés. Elles offrent une détection plus large des risques : services mal configurés, ports ouverts, fuites d'identifiants...

Au-delà de l'opérationnel, l'autre évolution indispensable est celle de la gouvernance. La CTI doit s'aligner avec toute la politique de cybersécurité et les objectifs business de l'entreprise : protection de la marque, lutte contre la fraude financière...

La surveillance de l'empreinte numérique dans le cadre de la CTI incite aussi à renforcer la politique IAM : redéfinition des rôles, suppression des comptes non utilisés, MFA... La CTI s'affirme donc comme stratégie globale de sécurité.

04 Corriger les risques dans la durée

Une fois la stratégie définie et les outils mis en place, les équipes IT doivent passer à l'action et corriger les vulnérabilités. En commençant par patcher toutes les applications pour éviter les connexions non autorisées.

Si un asset est compromis, il doit être isolé. Les sous-domaines devenus inutiles doivent être fermés. Les adresses IP suspectes doivent, elles, être bloquées.

Les sites malveillants usurpant la marque de l'entreprise peuvent être fermés via le service Kaspersky Takedown Service. L'entreprise soumet une URL malveillante et Kaspersky se charge de contacter les services adéquats (CERT, registars...) pour faire fermer le site.

Pour assurer un pilotage en continu, les rapports analytiques peuvent enrichir une base de données sur les attaques et être distribués aux différentes parties prenantes (DSI, DAF, direction générale...). La CTI devient alors une aide à la décision pour réduire l'incertitude.

Mais il reste encore des progrès à faire sur la diffusion du renseignement. Selon Interpol, seuls 19 % des pays africains possèdent une base nationale de données de renseignements sur les cybermenaces. L'enjeu est pourtant stratégique.

Conclusion

Les entreprises ont pris conscience de l'importance d'une bonne gestion de leur empreinte numérique et d'une politique de Cyber Threat Intelligence pour parer à toute attaque. La détection et la sécurisation des assets exposés ainsi que la mise en place d'une veille continue sur les menaces deviennent des prérequis indispensables.

Les attaques commencent avant l'incident. Pour les détecter et s'en prémunir, il faut connaître tous ses points d'entrée et leurs vulnérabilités.

Pour prendre en compte cet enjeu, la CTI a évolué et intégré pleinement la surveillance de l'empreinte numérique. Les équipes de sécurité reprennent l'initiative, en identifiant les risques inconnus et en réduisant leur exposition avant qu'un incident ne survienne. La cybersécurité n'est plus seulement défensive et se base sur les piliers du renseignement et de l'anticipation.

Une fois l'exposition maîtrisée techniquement, reste à réduire l'exposition humaine. La visibilité sur l'empreinte numérique doit s'accompagner d'une formation des collaborateurs aux risques liés à leurs usages numériques. Un chantier majeur pour les DSI.

kaspersky

www.kaspersky.fr

En savoir plus sur les solutions Kaspersky

Demander des informations complémentaires