HADRIAN

Comment la Gestion de l'Exposition Réduit les Risques Sur le Bord

Une solution moderne pour protéger les actifs les plus importants des organisations.

Le contour n'est plus délimité

Plus d'actifs existent sur le périmètre que jamais auparavant

Dans le monde rapide d'aujourd'hui, les entreprises sont obligées d'adopter la transformation numérique pour rester compétitives. Les avantages de la transformation numérique sont significatifs et étendus.

- **Amélioration de l'expérience client** – En exploitant des technologies telles que les applications mobiles, les réseaux sociaux et les chatbots, les entreprises peuvent créer des interactions personnalisées avec leurs clients.
- **Augmentation de l'efficacité et de la productivité** – Les outils numériques ont automatisé les processus manuels, réduisant les erreurs et améliorant la précision. Cela libère les employés pour se concentrer sur des tâches à plus forte valeur ajoutée telles que l'innovation et le développement commercial.
- **Plus grande agilité et flexibilité** – Les applications cloud à la demande ont aidé les organisations à échelonner rapidement leurs opérations à la hausse ou à la baisse. Et, les outils de travail à distance permettent aux employés de travailler plus efficacement.

En embrassant la transformation numérique, les organisations ont pu rester en avance sur la courbe, s'adapter aux conditions changeantes du marché et profiter des opportunités émergentes. Cependant, les activités de transformation numérique ont brouillé le périmètre de sécurité des organisations. Avec plus d'employés, de clients et d'applications tierces accédant à l'infrastructure d'entreprise, la gestion des risques est devenue de plus en plus difficile.

40%

des entreprises adopteront une stratégie prioritaire native du cloud en 2023 dans le but d'augmenter l'agilité et l'efficacité tout en réduisant les coûts, selon l'enquête sur l'infrastructure cloud de Forrester de 2022.

24%

de travailleurs en plus ont choisi de travailler à distance en 2022 par rapport à 2021.

87%

des cadres supérieurs, comme rapporté par Gartner en 2021, ont identifié la transformation numérique comme une priorité majeure pour leur organisation.

Les acteurs de menaces exploitent la nouvelle frontière

Les attaques ciblent de plus en plus les actifs exposés

La transformation digitale apporte également de nouveaux risques et défis, particulièrement en termes de cybersécurité. Les cybercriminels et les acteurs de menaces exploitent rapidement les vulnérabilités dans l'infrastructure digitale, résultant en des violations de données, des pertes financières et des dommages à la réputation pour les organisations.

Dans la précipitation d'adopter de nouvelles technologies et de devancer la concurrence, les considérations de sécurité sont souvent négligées. Le cloud computing, les dispositifs IoT et les applications mobiles, parmi d'autres, ont mené à une surface d'attaque élargie que les acteurs de menaces peuvent exploiter.

> “
>
> Il y a la perception que les organisations concentrent leurs efforts de sécurité autour de leurs environnements « connus » traditionnels. Cela crée une incitation pour les acteurs de menaces, car ils sont plus susceptibles de trouver un actif exposé sur internet qu'ils peuvent exploiter.
>
> **Olivier Beg - Chef du Hacking chez Hadrian**

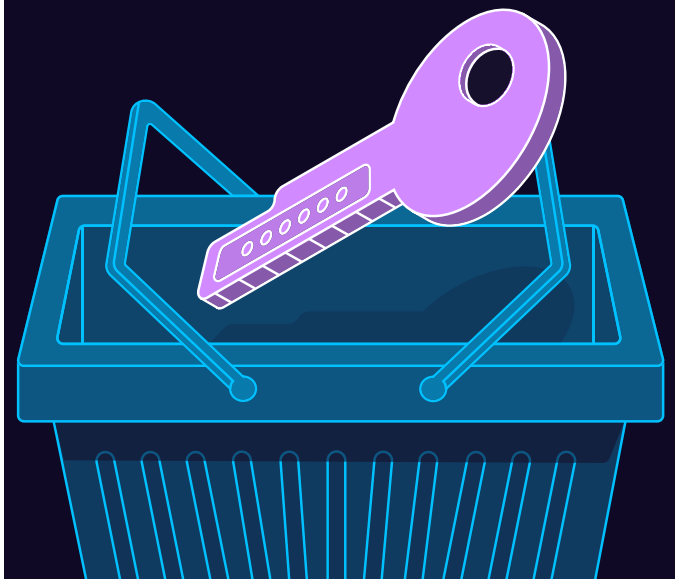
Les organisations devraient se concentrer sur les avantages de la transformation digitale et adresser les risques et les menaces qui l'accompagnent. Les acteurs de menaces exploitent ce manque de considérations de sécurité en ciblant les vulnérabilités dans les nouvelles technologies et en les exploitant pour accéder à des données sensibles.

69%

des organisations ont subi une attaque ciblant un actif externe inconnu, mal géré ou géré de manière inadéquate.

10/55

les vulnérabilités zero-day exploitées en 2022 impliquaient des dispositifs à la périphérie d'Internet.



Comment le paysage des menaces est remodelé

Les courtiers d'accès initial ont des incitations très différentes de celles des acteurs de menaces traditionnels

Les courtiers d'accès initial (IAB) font partie d'une tendance croissante à la collaboration dans le monde criminel. Historiquement, les gangs de ransomware et d'autres acteurs de menaces réalisaient tous les aspects d'une attaque eux-mêmes, de l'obtention de l'accès à un réseau au chiffrement des données et à la négociation des rançons. Cependant, cela a changé avec l'émergence des IAB. Ces attaquants se concentrent sur l'obtention de l'accès aux réseaux puis vendent cet accès à d'autres criminels.

Les IAB ont souvent des compétences limitées et ne sont pas capables de développer des malwares ou d'exécuter des programmes de ransomware sophistiqués. Ils font souvent un profit en vendant l'accès à de nombreuses organisations à d'autres cybercriminels pour l'utiliser dans des attaques.

L'arrangement est également bénéfique pour les gangs de ransomware et d'autres groupes de menaces persistantes avancées qui ont souvent été limités par le nombre de systèmes qu'ils peuvent pirater.

Au lieu de cibler des industries ou des organisations spécifiques, les attaques par les IAB sont comparativement indiscrètes. Ils utilisent souvent des vulnérabilités connues et recherchent tout actif vulnérable sur le bord d'une organisation qu'ils peuvent exploiter. À mesure que les IAB s'établissent, il est prévu que les gangs de ransomware pourront attaquer un nombre croissant d'organisations.

25,059

records CVE ont été publiés en 2022, une augmentation d'environ 25 % par rapport à 2021.

15 minutes

après une annonce de CVE, les acteurs de menaces commencent à scanner Internet, selon les recherches.

Les processus existants ne peuvent pas suivre

Les programmes traditionnels de gestion des vulnérabilités ne sont plus adaptés

Le principe de la gestion des vulnérabilités est simple : les organisations priorisent les vulnérabilités en fonction de leur gravité et du niveau de risque qu'elles représentent. Cependant, comme montré, le nombre de violations utilisant des vulnérabilités se produit encore à des taux élevés. Les programmes de gestion des vulnérabilités luttent généralement pour trois raisons :

- **Manque de visibilité** – Pour que les programmes de gestion des vulnérabilités fonctionnent, les organisations doivent connaître leur surface d'attaque. Cependant, selon Forrester, en moyenne, les organisations ont une surface d'attaque 30 % plus grande que ce qu'elles pensaient avoir.
- **Découverte inefficace** – Identifier les vulnérabilités dans la surface d'attaque présente deux défis ; le premier est d'en identifier autant que possible, car celles qui sont manquées pourraient entraîner une violation. Le second est de minimiser le nombre de faux positifs, qui ralentissent les équipes et les empêchent de remédier aux vrais risques.
- **Priorisation inexacte** – De nombreuses organisations échouent à prioriser les vulnérabilités et se concentrent plutôt sur la remédiation des vulnérabilités en fonction de leur âge ou de scores décontextualisés tels que le CVSS. Cette approche peut entraîner le fait que des risques critiques soient laissés non traités, ce qui peut conduire à des violations de sécurité.

56%

des grandes entreprises gèrent plus de 1 000 alertes de sécurité chaque jour.

66%

des équipes de sécurité disent qu'il est difficile de protéger des surfaces d'attaque complexes et en constante évolution.

68%

de toutes les cyberattaques exploitent des vulnérabilités pour lesquelles un correctif était disponible depuis plus d'un an.

Une approche moderne pour un problème moderne

Introduction à la Gestion Continue de l'Exposition aux Menaces

La Gestion Continue de l'Exposition aux Menaces (CTEM) est le suivi continu et l'identification des menaces, vulnérabilités et risques en temps réel. Elle permet aux organisations d'identifier et de répondre rapidement aux menaces, réduisant le risque d'une attaque réussie.

> D'ici 2026, les organisations qui priorisent leurs investissements de sécurité sur la base d'un programme de gestion continue de l'exposition seront trois fois moins susceptibles de subir une violation.
>
> **Gartner**

La manière dont vous réduisez les risques est unique à votre organisation, cependant le CTEM fournit l'architecture pour relever les défis auxquels vous êtes confrontés :

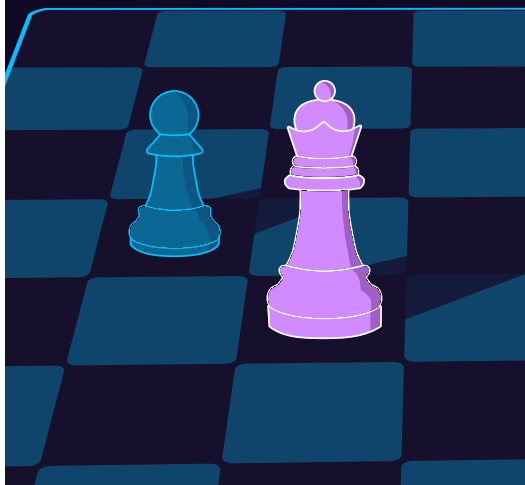
- Minimiser le nombre d'incidents de sécurité auxquels les organisations sont actuellement confrontées.
- Créer des environnements sûrs dans des contextes en constante évolution.
- Identifier les points faibles de votre posture de sécurité qu'une attaque pourrait exploiter.
- Réduire le risque créé par la technologie qui soutient les travailleurs à distance.
- Déplacer les fonctions commerciales critiques vers des services ou plateformes tiers.

87%

des cadres supérieurs priorisent la transformation digitale comme une priorité organisationnelle, selon le rapport de Gartner.

85%

des cadres supérieurs priorisent la transformation digitale comme une priorité organisationnelle, selon le rapport de Gartner.



Comprendre la Gestion de l'Exposition

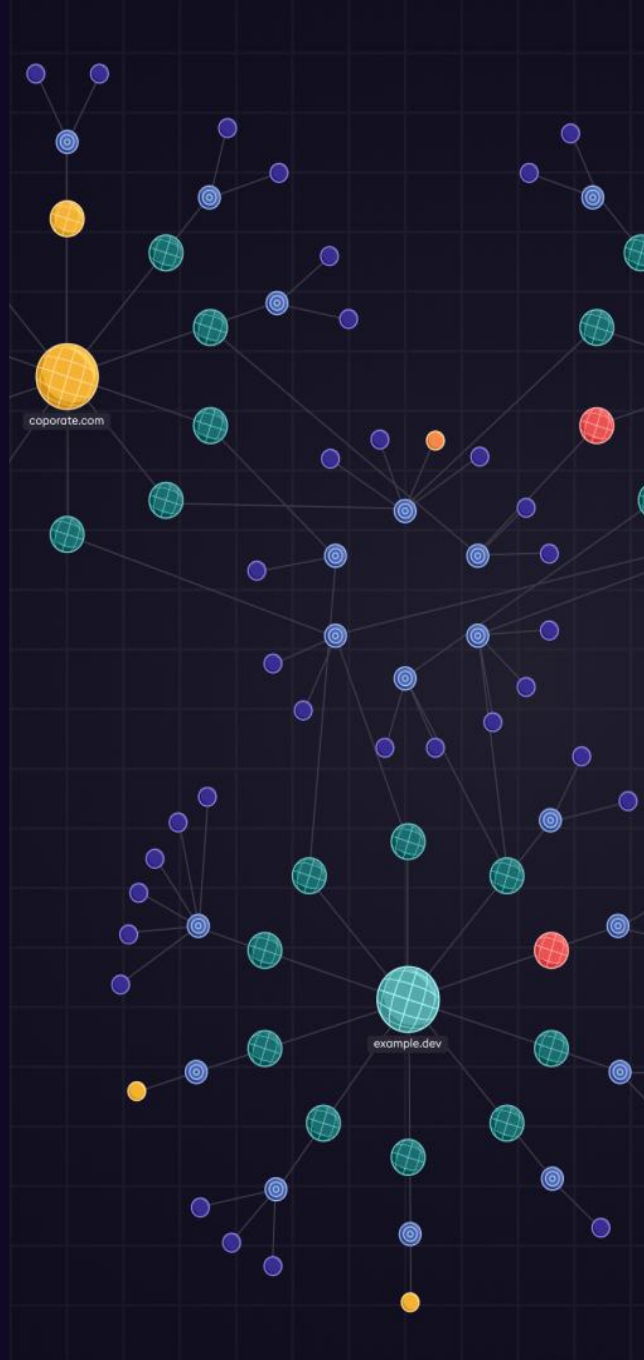
Fournir ce que la gestion des vulnérabilités ne peut pas

Les programmes de gestion de l'exposition vont au-delà de la gestion des vulnérabilités de plusieurs manières :

- **Évaluer la posture de sécurité** en incluant l'ensemble de la surface d'attaque de votre organisation, pas seulement les actifs connus et catalogués manuellement.
- **Déterminer la probabilité et l'impact de l'exploitation** basés sur l'ensemble de l'environnement de l'organisation, pas seulement en regardant le risque dans des cas isolés.
- **Recommander des activités de remédiation** pour que l'organisation plus large les mette en œuvre, pas seulement les équipes responsables de la correction des vulnérabilités.

Pour mettre en œuvre avec succès un programme de gestion de l'exposition, plusieurs capacités sont nécessaires :

- Découverte continue des actifs orientés vers l'extérieur.
- Détection autonome des risques exploitables.
- Priorisation précise des risques.
- Validation que les risques ont été résolus.



L'Orchestrateur de Hadrian

Prévenir les violations avec la gestion de l'exposition

Hadrian fournit une couverture continue du cycle de vie de la gestion de l'exposition externe, pour réduire les risques, améliorer l'efficacité et simplifier la conformité. Au cœur de notre plateforme se trouve l'Orchestrateur, qui effectue des analyses 24x7x365 comme un adversaire du monde réel en chaînant dynamiquement plus de 200 modules "hacker".

1

Actifs

L'Orchestrateur découvre des actifs inconnus en traitant 1.1Tb de données quotidiennement pour découvrir chaque actif appartenant à votre organisation. Pour éviter les surprises indésirables, l'Orchestrateur scanne en continu à la recherche de signes de nouveaux actifs et de changements.

2

Contexte

La plateforme de Hadrian contextualise vos actifs pour comprendre comment un adversaire mènerait une attaque. Hadrian identifie les informations sur le système d'exploitation, les modules, les bibliothèques, les champs de saisie, les méthodes d'authentification et bien plus encore pendant cette étape.

3

Risques

L'Orchestrateur utilise sa connaissance de votre environnement pour sonder les faiblesses, apprenant au fur et à mesure et affinant les techniques qu'il utilise. Hadrian identifie de manière fiable les risques précédemment non découverts pour votre organisation avec moins de faux positifs.

HADRIAN

Hadrian est un fournisseur leader de solutions de Gestion de la Surface d'Attaque Externe (EASM), de Test Rouge Automatisé Continu (CART) et de Gestion Continue de l'Exposition aux Menaces (CTEM). Notre plateforme catalogue les actifs connus et inconnus où qu'ils se trouvent, enquête sur les vulnérabilités en exécutant des exploits comme le ferait un acteur de menace, et priorise les risques pour une remédiation rapide basée sur votre environnement unique.

Réserver une Démo

En Savoir Plus

(1) Forrester, Infrastructure Cloud Survey (2022)
(2) Owl Labs, State of Remote Work (2022)
(3) Gartner, Speed Up Your Digital Business Transformation (2019)
(4) ESG, Security Hygiene and Posture Management (2022)
(5) Madiant, Move, Patch, Get Out the Way: 2022 Zero-Day Exploitation Continues at an Elevated Pace (2023)
(6) CVE, Metrics webage (accessed April 2023)
(7) Palo Alto, Incident Response Report (2022)
(8) Sumo Logic, State of SecOps and Automation (2020)
(9) Ponemon, The Cybersecurity Illusion: The Emperor Has No Clothes (2019)
(10) Abdalslam, Patch Management Statistics, Trends And Facts (2023)
(11) Cloud Native Computing Foundation, Cloud Native Security Microsurvey (2021)

Approuvé Par

BIOLANDES

CTC GLOBAL

beyond.

KCK

KINGSWAY CAPITAL

bank prov.

LEROY MERLIN

London Business School