elastic security labs

2024

Rapport d'Elastic sur les menaces mondiales

Tendances des menaces que les leaders des SOC doivent connaître

Conçu pour fournir des informations exploitables aux équipes de sécurité et aux directeurs de la sécurité de l'information, le Rapport 2024 d'Elastic sur les menaces mondiales présente les principales observations de plusieurs mois d'analyse sur plus d'un milliard de points de données, provenant de la télémétrie publique et de la télémétrie propre à Elastic. Ces conclusions ont été organisées en informations exploitables tirées des données et en suggestions d'actions pour votre entreprise.

Principales informations exploitables

01 Les environnements cloud sont mal configurés par les entreprises

Notre nouvelle section sur la gestion de la posture de sécurité du cloud (CSPM) a comparé les environnements aux références du Center for Internet Security (CIS) et a révélé qu'en moyenne, environ 50 % des environnements échouaient aux contrôles, quel que soit le fournisseur de services cloud (CSP).

02 L'évasion de défense reste la tactique de point de terminaison la plus fréquemment observée

L'évasion de défense représentait 38 % des comportements des points de terminaison, ce qui suggère que les utilisateurs malveillants sont à l'aise pour naviguer dans les systèmes de sécurité. Il convient de noter que ce chiffre a diminué de 6 % par rapport à l'année dernière, ce qui montre que les outils de défense fonctionnent efficacement.

03 Les alertes liées aux accès protégés par des identifiants continuent d'augmenter, en particulier dans le cloud

Dans les environnements cloud, l'accès aux identifiants représentait 23 % de l'activité. De plus, les environnements des points de terminaison ont révélé une augmentation de 3 % de ces techniques d'une année sur l'autre. Cela peut être attribué à la prévalence croissante des voleurs d'informations et des brokers d'identifiants, ainsi qu'au fait que les outils de sécurité gagnent en visibilité.

04 Les utilisateurs malveillants abusent des outils de défense pour pénétrer efficacement les systèmes

53 % des fichiers malveillants observés ont été identifiés comme des outils de sécurité offensifs, utilisés par les entreprises pour découvrir des faiblesses et exploités par des utilisateurs malveillants. Ces outils de sécurité offensifs disposent d'équipes de recherche et de développement importantes chargées de créer de nouvelles fonctionnalités, comme l'injection de processus, une forme d'évasion de défense qui a représenté 53 % des alertes Windows cette année.

05 L'IA générative n'a pas augmenté le nombre ou l'impact des attaques que nous avons observées

Les équipes de sécurité s'inquiètent de l'arrivée prochaine des attaques d'IA générative. Bien que nous ayons constaté une légère augmentation du volume des menaces, l'IA générative a largement renforcé les technologies de défense grâce à des fonctionnalités telles que la synthèse des alertes et l'automatisation des tâches.

 |

Principales suggestions

01 Auditez votre environnement régulièrement

Les utilisateurs malveillants s'appuient sur des contrôles de sécurité permissifs ou mal configurés pour s'infiltrer dans les environnements et, une fois à l'intérieur, ils se concentrent sur la falsification des capteurs et des données. L'évaluation comparative et l'évaluation des risques peuvent vous aider à déterminer si vous utilisez les bonnes pratiques et les normes du secteur pour contrôler efficacement les accès au sein de votre entreprise.

02 Préparez-vous à l'IA générative en ajustant vos contrôles de sécurité

La croissance de l'IA générative entraînera une hausse des tentatives d'ingénierie sociale. Si la formation de votre base d'utilisateurs à l'identification de ces tentatives et autres est toujours une bonne idée, les équipes de sécurité doivent également vérifier leurs contrôles et autorisations pour s'assurer qu'une tentative de phishing réussie ne causera pas de dommages à long terme.

03 Mettez en œuvre des agents de points de terminaison interactifs pour neutraliser les attaques par évasion de défense

Les attaques par évasion de défense représentent la principale tactique depuis quelques années. Bien qu'elles soient en baisse, les utilisateurs malveillants utilisent toujours ces méthodes pour s'infiltrer et naviguer dans les environnements. Les technologies de points de terminaison comme Elastic Agent offrent visibilité et fonctionnalités tout en réduisant le nombre d'outils dont vous avez besoin.

04 Créez un plan de réponse robuste pour les identifiants exposés

Nous avons observé que des techniques telles que la force brute et l'accès aux identifiants du navigateur à partir d'une mémoire suspecte étaient régulièrement utilisées. La rotation des identifiants exposés et l'organisation de workflows rapides pour répondre aux violations feront une grande différence. Les équipes de sécurité doivent imposer l'authentification multi-facteurs si ce n'est pas déjà fait.

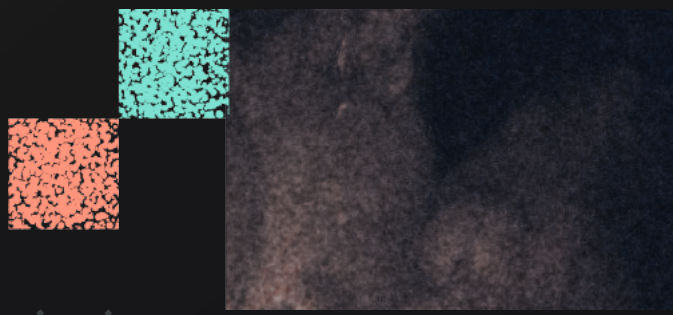
05 Comparez votre environnement cloud aux références du CIS

Les références du CIS constituent une norme du secteur et vous aideront à identifier rapidement les domaines qui nécessitent une attention particulière. Votre équipe doit élaborer un plan pour monitorer et accroître votre score, ce qui améliorera la détection des menaces et réduira les risques à long terme.

Maîtrise des menaces

Préparez-vous à l'évolution de ces menaces et d'autres encore. Consultez toutes nos suggestions et découvrez la décomposition complète des menaces d'aujourd'hui dans le Rapport 2024 d'Elastic sur les menaces mondiales. Vous pouvez également suivre nos experts @ElasticSecLabs.

Découvrez comment Elastic Security peut moderniser vos opérations de sécurité.



 |

elastic security labs