Outpost24

Threat Compass

Élargissez votre périmètre
Gérez les risques numériques

Aujourd'hui, l'univers de la cybersécurité devient de plus en plus difficile à cerner. Les acteurs malveillants utilisent des techniques de plus en plus sophistiquées pour attaquer les organisations. Toute organisation opérant en ligne détient des données précieuses pour les cybercriminels, qu'il s'agisse d'enregistrements de transactions financières, d'informations confidentielles sur les clients, d'actifs condensés de l'entreprise ou d'éléments relatifs à la propriété intellectuelle industrielle. L'atteinte d'une de ces données peut avoir des conséquences catastrophiques pour l'entreprise, nuire à sa réputation et entraîner des sanctions pour non-conformité.

Votre entreprise est en danger. Une cyberdéfense statique ou réactive ne suffit plus. Outpost24 adopte une approche proactive de la cyberdéfense en fournissant des informations ciblées et exploitables sur les cybermenaces afin d'atténuer les risques : c'est ce que propose Threat Compass. Les renseignements ciblés sur les menaces permettent de gagner du temps et d'optimiser les ressources sécurité tout en accélérant la détection des menaces, la réponse aux incidents et les enquêtes.

Threat Compass utilise des algorithmes sophistiqués pour fournir des renseignements exploitables et automatisés sur les cybermenaces à partir de sources ouvertes, fermées et privées, notamment les réseaux de botnets malveillants. Il devient alors plus facile d'identifier et de gérer les menaces réelles qui ciblent votre organisation, pour une prise de décision plus rapide et des performances accrues. Threat Compass couvre le plus large champ de menaces sur le marché. Son architecture modulaire à la carte vous permet de ne choisir (et ne payer) que les renseignements les plus pertinents pour votre entreprise.

Chaque module de renseignement ciblé est appuyé par notre équipe interne d'analystes de premier ordre. Enrichissez et contextualisez les menaces afin de pouvoir détecter les attaques, défendre vos actifs et comprendre les plans de vos adversaires avant qu'ils ne frappent. L'architecture à la carte signifie que nos renseignements sont rationalisés, rentables et évolutifs.

L'automatisation totale du traitement des donnés nous permet de minimiser le temps et les coûts de travail de nos analystes, en révélant des informations qui apportent de la valeur à tous les niveaux : les analystes veulent savoir comment une brèche s'est produite, tandis que les dirigeants veulent savoir que cela ne se reproduira pas. Threat Compass répond à ces deux besoins.

L'intégration se fait facilement, avec une API complète et des modules flexibles, de sorte que les renseignements ciblés de Threat Compass soient immédiatement disponibles pour vos systèmes et équipes de sécurité. La facilité d'installation de la plateforme en cloud vous permet d'obtenir immédiatement puis de manière constante un état des lieux précis de la situation.

Capable de délivrer des résultats en seulement quelques minutes, Threat Compass a des coûts opérationnels extrêmement faibles et ne nécessite que très peu de personnel pour sa gestion. Mieux encore, vous n'avez pas besoin d'être un expert pour comprendre les informations fournies. Threat Compass traque les menaces en dehors de votre réseau d'entreprise, en détectant et en surveillant les activités malveillantes, les incidents et les acteurs malveillants avant qu'ils ne puissent causer des dommages au sein de votre infrastructure.

De manière automatisée, Threat Compass collecte, analyse, recoupe et fournit des données enrichies sur les menaces dans diverses catégories susceptibles d'avoir un impact sur votre entreprise. Cela recouvre l'identification des botnets et des serveurs de commande et de contrôle en passant par les variantes de logiciels malveillants ciblés ou encore le suivi des cartes de crédit volées et des informations d'identification compromises, la recherche d'applications mobiles malveillantes, d'activités hacktivistes et de campagnes d'hameçonnage ciblant votre organisation.

Vous guider au mieux à travers le paysage des menaces

- Qui cible votre organisation, et d'où ?
- Savez-vous quelle est votre présence sur le dark web ?
- Comment votre réseau d'entreprise a-t-il été compromis ?
- Qui se fait passer pour votre marque ou vos VIP ?
- Des informations sensibles ont-elles été divulguées ?
- Des informations d'identification ont-elles été compromises, sont-elles utilisées pour commettre des fraudes ?
- Savez-vous quelles sont vos obligations en matière de conformité en cas de violation ?

Une cyberdéfense complète et à la carte

Chaque module Threat Compass peut être acquis et utilisé individuellement. Il vous suffit d'acheter les modules fournissant les renseignements les plus pertinents sur les menaces qui concerne votre entreprise.

Threat Context

Threat Context fournit aux équipes de sécurité des informations intuitives et actualisées en permanence sur les hackers, les campagnes, les CIO, les logiciels malveillants, les schémas d'attaque, les outils, les signatures et les CVE. Une base de données de plus de 200 millions d'éléments offre des interrelations graphiques permettant aux analystes de recueillir rapidement des informations enrichies et contextualisées avant, pendant et après une attaque. Nous avons recueilli et mis à disposition plus de dix ans de données sur les menaces, constamment mises à jour, offrant ainsi à nos clients la plus vaste collection de menaces connues.

Dark Web

Soyez mieux informé de ce qui se passe dans le dark web, observez les activités malveillantes ciblant votre organisation et prévenez de manière proactive les futures attaques. Prenez l'avantage en gardant un œil sur le camp ennemi : soyez mieux informé sur les criminels qui ciblent votre organisation ; préparez des contre-attaques de manière proactive ; détectez les informations d'identification des utilisateurs et les actifs volés en temps réel.

Credentials

Obtenez des informations exploitables sur les fuites, les vols et les ventes d'informations d'identification de vos utilisateurs. Nous les localisons en temps réel sur les open, deep et dark web, en parallèle d'informations sur les logiciels malveillants utilisés pour voler les données. Les sinkholes, honeypots, crawlers et capteurs de Outpost24 recherchent en permanence vos informations d'identification volées dans des fuites de données, sur les forums et en temps réel dans les logiciels malveillants ciblés - ce qui permet d'éliminer les vecteurs d'attaque graves et les actions frauduleuses en quelques minutes plutôt qu'en plusieurs mois.

Data Leakage

Découvrez si les documents sensibles et le code source de votre organisation ont été divulgués sur Internet, le deep web ou les réseaux P2P – de manière intentionnelle ou non : comme par exemple à l'occasion d'un partage de documents internes via des fournisseurs de partage de fichiers mal sécurisés.

Credit Cards

En cherchant un peu, on peut trouver sur Internet toutes sortes de données relatives aux cartes de crédit. Ce module permet de réduire considérablement les dommages liés au vol et à la fraude de cartes de crédit. Nous récupérons les données de cartes de crédit volées et fournissons des informations pertinentes pour aider les organisations à limiter les dégâts.

Hacktivism

Surveillez l'hacktivisme mondial, sur les réseaux sociaux comme sur l'open et le dark web, pouvant affecter votre infrastructure. Grâce à un système avancé d'alerte précoce et à un géolocalisateur actif, le module génère des informations ciblées sur les menaces afin de se prémunir contre les vecteurs d'attaque potentiels.

Mobile Apps

Les applications malveillantes et illégales se cachent à la vue de tous sur les marketplaces non officielles, attirant vos clients et dérobant parfois leurs données. Notre module est spécialisé dans la détection des applications qui prétendent être affiliées à votre organisation ou qui utilisent les actifs de l'entreprise sans autorisation, afin de protéger votre marque et votre réputation.

Social Media

Surveillez l'empreinte numérique de votre organisation sur les réseaux sociaux et les moteurs de recherche. Repérez les sites web qui ne sont pas autorisés à utiliser vos marques ou vos logos, les actifs revendiquant un partenariat, les actifs d'affiliation et autres, afin que vous puissiez prendre des mesures proactives pour les faire fermer.

Domain Protection

Les domaines frauduleux représentent un risque pour votre organisation et vos clients finaux avec comme intention de voler des informations ou de nuire à votre marque. Combattez le phishing et le cybersquattage en détectant les attaques de manière proactive et en prenant des contre-mesures.

Demander une démo

Devenir MSSP

Threat Compass : adapté à vos besoins

Threat Compass fournit un outil de contrôle unique pour les renseignement automatisés relatifs aux menaces opérationnelles, tactiques et stratégiques.

Collection

Outpost24 automatise la collecte de données sur les menaces à partir de sources et de formats multiples.

Recoupement et enrichissement

Threat Compass offre une catégorisation puissante des informations, une validation directe du client, ainsi qu'une analyse et une notation sandbox. Nous étudions également les données collectées à partir de flux tiers afin d'identifier les acteurs et vecteurs d'attaque les plus courants.

Des informations exploitables

Les puissants outils de visualisation d'Outpost24 représentent les renseignements ciblés et exploitables sur les menaces de manière intuitive. Utilisez les informations pour créer vos propres règles YARA, obtenir un avantage tactique et développez des capacités de réponse stratégiques face aux cybermenaces.

Intégration des données sur les menaces

Des plugins sont disponibles pour les SIEM, les plateformes SOAR et les TIP les plus courants. Outpost24 prend en charge STIX/TAXII afin de faciliter le partage d'informations entre différents formats de données.

La collaboration est essentielle

Partagez les informations pertinentes au sein de vos groupes internes et avec des tiers de confiance.

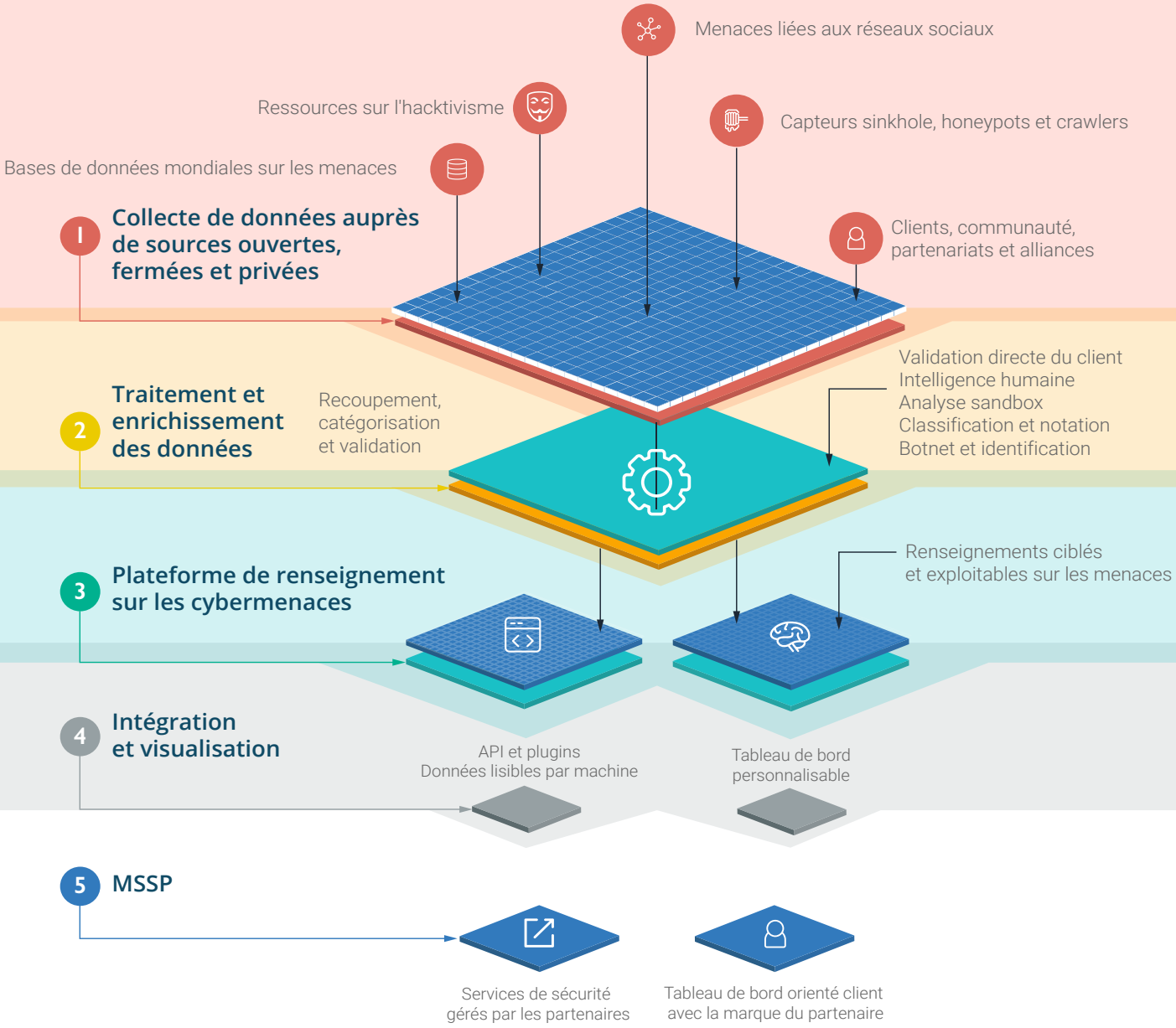
Ne permettez qu'à un seul utilisateur de collecter des données sur les menaces présentant un intérêt spécifique et de partager facilement des indicateurs de compromission pertinents, opportuns et précis sur les cyberattaques émergentes ou en cours afin d'éviter les brèches ou de minimiser les dommages causés par une attaque importante.

Une réponse accélérée et adaptative

En automatisant la collecte et la présentation de renseignements ciblés sur les menaces, vous bénéficiez d'une meilleure visibilité et réduisez les délais de réponse aux incidents. Les capacités d'analyse des big data fournissent rapidement des informations exploitables avec un minimum de faux positifs dans un tableau de bord unique - avec le contexte et les détails sous-jacents - pour une prise de décision plus rapide.

Maximiser des ressources limitées

Éliminez le tri manuel de milliers d'alertes et laissez votre équipe se concentrer sur les renseignements sur les menaces ciblées grâce à des capacités d'analyse sophistiquées.



Élaborer des réponses stratégiques

Threat Compass vous permet d'établir une liste d'adresses IP malveillantes, qui peut être ajoutée aux dispositifs de contrôle de la sécurité interne de votre périmètre. Il identifie les comptes compromis utilisés pour accéder aux ressources de l'entreprise et garantit une surveillance et un contrôle accrus des applications mobiles et des partenariats revendiqués. Grâce à Threat Compass, les utilisateurs peuvent comprendre le déroulé de la chaîne d'exécution et optimiser l'efficacité de leur sécurité interne.

Facile à déployer

L'architecture modulaire de Threat Compass est facile à déployer et permet d'obtenir immédiatement des résultats à fort impact. La solution basée sur le cloud fait disparaître le besoin d'installer du matériel ou des logiciels. Des options de licence flexibles permettent de fournir facilement une protection adaptative à l'échelle de l'entreprise pour des opérations situées n'importe où. Déployez des contrôles de conformité exactement là où vous les jugez nécessaires et obtenez des résultats en seulement quelques minutes.

A propos d'Outpost24

Le groupe Outpost24 est un pionnier de la gestion des cyber-risques avec la gestion des vulnérabilités, les tests de sécurité des applications, la Threat Intelligence et la gestion des accès - en une seule solution. Plus de 2 500 clients dans plus de 65 pays font confiance à la solution unifiée d'Outpost24 pour identifier les vulnérabilités, surveiller les menaces externes et réduire la surface d'attaque avec rapidité et confiance.

outpost24.com

info@outpost24.com

twitter.com/outpost24

linkedin.com/outpost24