Forescout XDR

eXtended Detection and Response

FORESCOUT

Forescout XDR

eXtended Detection and Response

Des SOC 450 fois plus efficaces grâce à une meilleure détection et une réponse aux véritables menaces

Les équipes des centres opérationnels de sécurité (SOC) sont chaque jour submergées d'alertes incomplètes et imprécises, manquant d'informations contextuelles indispensables. Beaucoup d'entre elles sont des faux positifs. Résultat, les analystes passent à côté de menaces critiques ou mettent plus de temps à enquêter et à intervenir, ce qui augmente le risque d'infraction. De fait, un SOC classique reçoit environ 11 000 alertes par jour, ou 450 par heure[1] – la plupart étant peu fiables voire de fausses alertes.

Forescout® XDR permet de réduire ce chiffre à une détection concrète par heure, soit une menace probable justifiant une enquête humaine.[2]

Aperçu de la solution

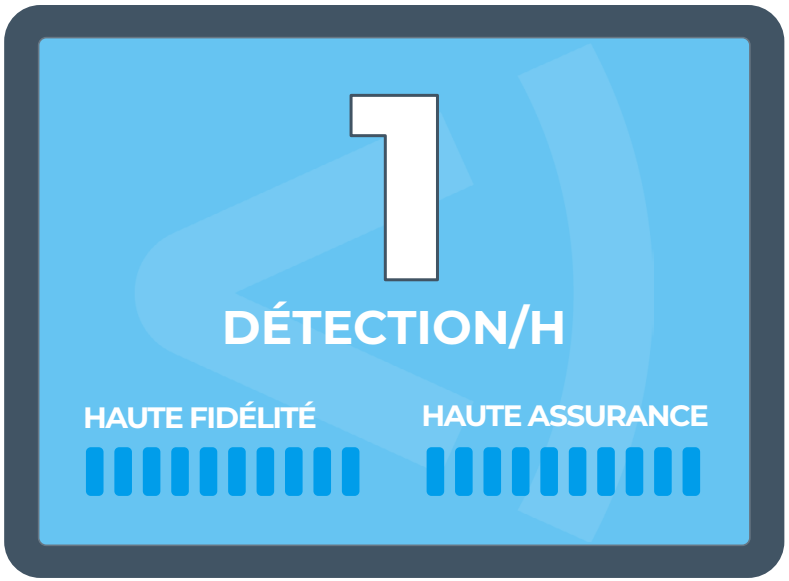
Forescout XDR permet, à partir des données télémétriques et des journaux, de générer des alertes haute fidélité de menaces probables justifiant une action du SOC.

La solution automatise la détection, l'enquête, la traque des menaces évoluées et l'intervention en conséquence sur tous les appareils connectés – IT, OT/ICS, IoT et IoMT – du campus au cloud, du centre de données à la périphérie. Forescout XDR réunit des technologies et fonctions SOC essentielles au sein d'une plateforme unifiée cloud native. Les équipes peuvent consulter les informations et intervenir immédiatement depuis une seule et même console.

Forescout XDR exploite les données de l'entreprise étendue, englobant les appareils gérés et non gérés (sans agent).

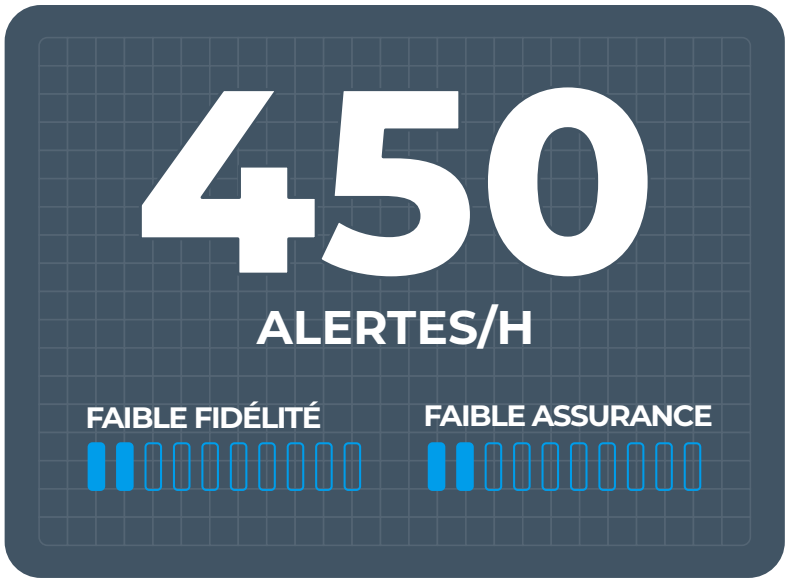
Forescout XDR est 450 fois plus efficace que les SOC classiques dans la conversion de données télémétriques et de journaux en détections directement exploitables.

Avec Forescout XDR



VS

SOC classique



*** Détection :** menace probable justifiant une action humaine de la part du SOC.

Sur la base de données agrégées en moyenne sur une année (déc. 2021-2022), parmi 30 entreprises représentatives de différentes tailles et secteurs d'activité.

11 000 alertes par jour = 450 alertes par heure.
Source : « The 2020 State of Security Operations » Forrester Consulting

Le nombre réel d'alertes reçues par un SOC dépend de divers facteurs. En font partie le nombre, le type et l'emplacement des contrôles de sécurité déployés, le réglage de ces contrôles (qui à son tour dépend de la capacité des analystes, de la tolérance aux risques et du niveau d'expertise), le nombre de collaborateurs/appareils ou encore le secteur.

Valeur pour l'entreprise

Réduction des risques pour l'activité

Forescout XDR réduit le risque et l'ampleur d'une attaque ou d'une violation de données réussie, éliminant ainsi la quasi-totalité du « bruit » généré par les alertes. Les équipes SOC peuvent détecter plus rapidement et plus précisément la plupart des menaces évoluées à l'échelle de l'entreprise, puis enquêter et intervenir en conséquence.

Forescout XDR permet ainsi d'éviter les interruptions d'activité ainsi que les coûts résultant d'une attaque ou d'une violation.

Processus de sécurité optimisés

Forescout XDR enrichit automatiquement les données clés, les normalise et met les signaux en corrélation afin de produire un petit nombre de détections haute fidélité, justifiant vraiment l'intervention des analystes. La solution simplifie et accélère les processus complexes d'enquête et de traque des menaces grâce à des informations plus complètes, plus précises et des données contextuelles, le tout depuis une console unifiée qui s'intègre aux autres solutions Forescout ainsi qu'aux SIEM, systèmes de gestion de cas et solutions d'intervention de tiers.

Forescout XDR offre une meilleure visibilité sur le cycle de vie complet des menaces via des tableaux de bord et des rapports préconfigurés et personnalisables, avec des indicateurs clés de performance (ICP) adaptés aux analystes/IR, aux ingénieurs, aux responsables SOC, aux responsables de la conformité/du risque et aux dirigeants. Les équipes SOC peuvent ainsi consacrer davantage de temps aux activités de sécurité à plus forte valeur ajoutée.

Réduction des coûts

La solution réduit les dépenses SOC liées aux éléments suivants :

- Licence et gestion de solutions SOC ponctuelles : lacs de données, analyse et orchestration de la sécurité, automatisation et intervention sur incidents (SOAR), analyse comportementale des utilisateurs et des entités (UEBA) et plateformes de renseignement sur les menaces
- Stockage de journaux
- Épuisement des analystes, turnover, recrutement et formation
- Prise en charge de nouvelles sources de données
- Création et adaptation de règles

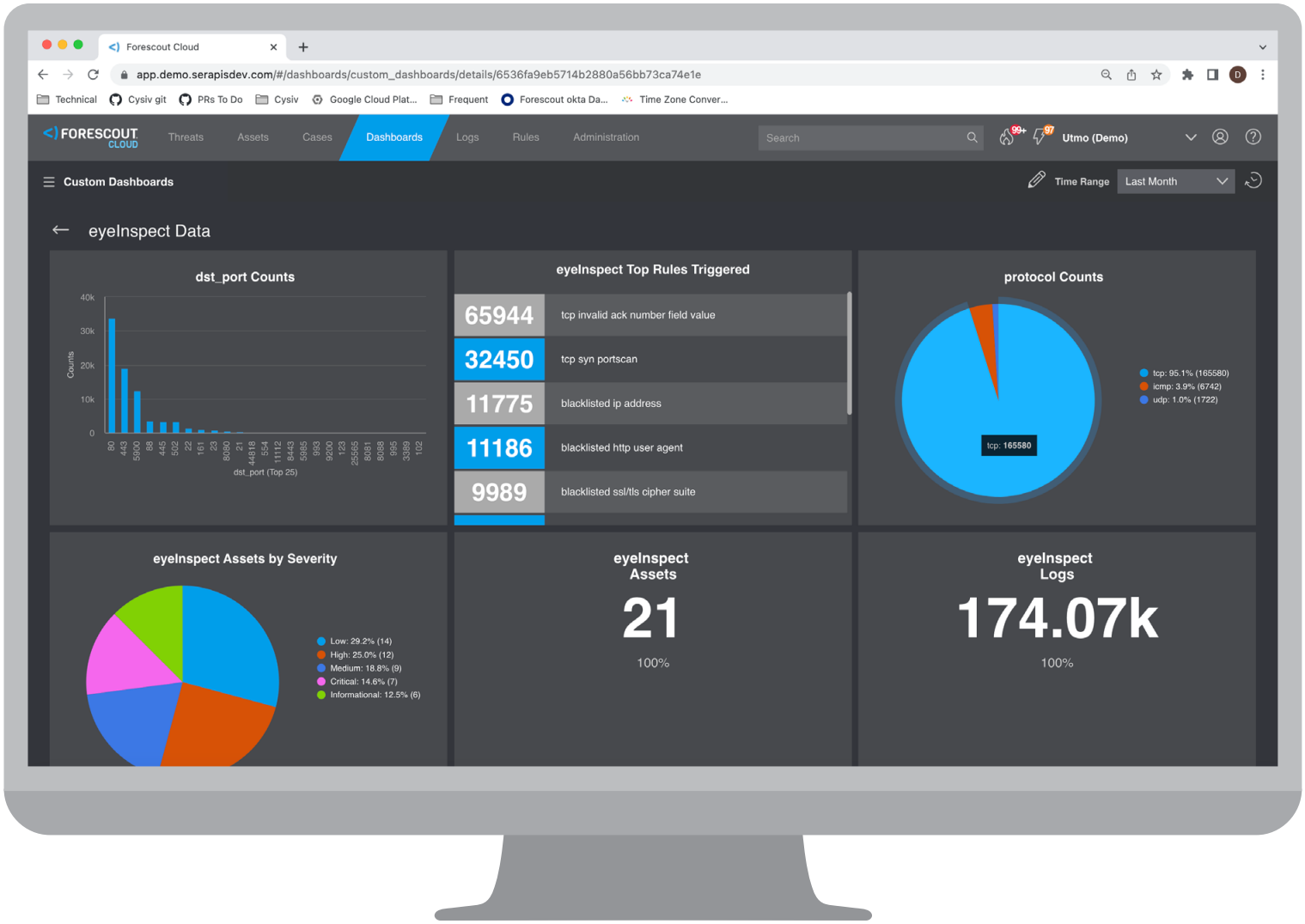
Conformité facilitée

Diverses options de stockage à chaud et à froid, la détection automatique des menaces ainsi que les renseignements sur les menaces facilitent le respect de réglementations et normes clés. Ils aident en outre à combler le laps de temps éventuel entre la constatation d'une violation ou d'une interruption et l'intervention proprement dite.

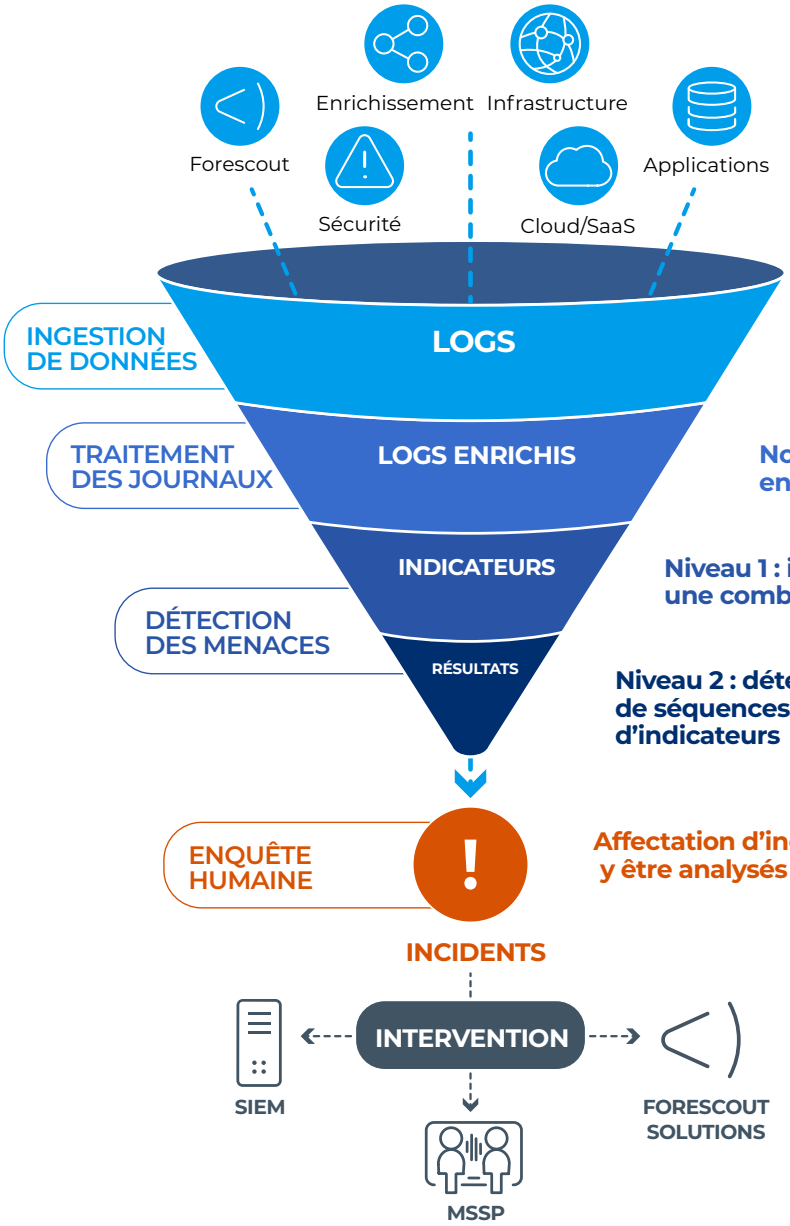
Compatibilité avec les produits de sécurité actuels

Forescout XDR accroît la valeur de vos autres solutions Forescout, mais aussi celle des capteurs de votre réseau, des terminaux et de la sécurité cloud ainsi que des points de déploiement, de quelque fournisseur qu'ils soient. Avec Forescout XDR, nul besoin d'implémenter de nouveaux logiciels ou matériels propres à un fournisseur.

Métriques et tendances clés permettant de mieux gérer les performances du SOC.



Des tableaux de bord et des rapports préconfigurés et personnalisables basés sur les personas fournissent des ICP pertinents pour différents rôles – analystes/IR, ingénieurs, responsables SOC, responsables de la conformité et des risques, dirigeants...



Prise en charge de plus de 170 sources de données de tout fournisseur et EDR

Normalisation selon un CIM et enrichissement automatique

Niveau 1 : indicateurs générés selon une combinaison de cinq techniques

Niveau 2 : détections générées à partir de séquences, schémas ou volumes d'indicateurs

Affectation d'incidents à un cas pour y être analysés plus en détail ou traités

Orchestration et intervention automatisées avec les solutions Forescout (eyeControl et eyeSight), et via les SIEM et MSSP

Pourquoi Forescout ?

Associé à d'autres solutions Forescout, Forescout XDR allie de manière unique une ingestion de données indépendante des fournisseurs et des EDR et une détection 450 fois plus efficace, avec un spectre d'intervention complet et une réduction des risques en amont, le tout à des tarifs prévisibles et abordables.

Ingestion de données indépendante des fournisseurs et EDR

- Prise en charge des produits et fournisseurs dans lesquels vous avez déjà investi
- Capacité à ingérer des données de tout appareil géré ou non géré (IT, OT/ICS, IoT, IoMT)
- Détection des menaces plus complète, plus puissante, plus flexible et plus efficace

Détection 450 fois plus efficace

- Un pipeline de données de pointe exécute un modèle de données unifié (CIM) qui normalise les données ingérées et les enrichit automatiquement d'informations sur les utilisateurs, d'attribution IP, de géolocalisation ainsi que de données vitales sur les appareils
- Un moteur de détection des menaces en deux niveaux utilise cinq techniques différentes pour réduire le bruit et accroître la fiabilité

Spectre d'intervention complet

- Puissants outils d'enquête
- Intégrations natives aux solutions de gestion de cas
- Interventions automatiques via les solutions Forescout sur tous les appareils, gérés ou non gérés

Réduction des risques en amont

- L'intégration à d'autres solutions Forescout réduit la surface d'attaque et le risque qu'un appareil compromis ou non conforme se connecte à votre réseau
- Surveillance en continu de tous les actifs connectés grâce à des politiques d'accès dynamiques

Tarifs simples, prévisibles et abordables

- Aucune pénalité pour l'envoi d'un plus grand nombre de journaux à Forescout XDR – pour une meilleure détection
- Frais de licence basés sur le nombre total de terminaux (adresse IP/MAC) de votre entreprise
- Tarifs comprenant différentes options de stockage à chaud et à froid afin de répondre à vos besoins propres

Principales fonctionnalités

Forescout XDR associe des technologies et fonctions SOC essentielles en une seule console unifiée cloud native.

Ingestion de données

Prise en charge native des données issues de Forescout eyeSight, eyeInspect et de la sécurité des appareils médicaux – et plus de 170 sources de tout fournisseur et EDR, notamment :

- **Sécurité :** pare-feux, IDS/IPS réseau, EDR, plateformes de protection des terminaux (EPP), sécurité des serveurs/charges de travail/conteneurs, sécurité des proxys Web et des messageries
- **Infrastructure :** sécurité Windows, authentification AD, IAM, DHCP, DNS, pistes d'audit cloud et métadonnées réseau
- **Enrichissement :** identité (LDAP), inventaire et classification d'actifs, gestion des configurations, résultats d'analyses de vulnérabilité et renseignements sur les menaces (indicateurs de compromission, ou IOC)
- **Applications :** bases de données, ERP, CRM et API
- **Cloud/SaaS :** AWS, Microsoft Azure, Google Cloud, Microsoft 365, Google Workspace et toute autre application SaaS

Intégration de données

Vous aide à tirer le maximum de la détection pour vos cas d'utilisation les plus importants. Les ingénieurs données de Forescout travaillent avec votre équipe pour planifier et prioriser les sources de données à intégrer, puis aident à configurer le pipeline de données et à s'assurer que vos données sont correctement analysées, nettoyées, normalisées et enrichies.

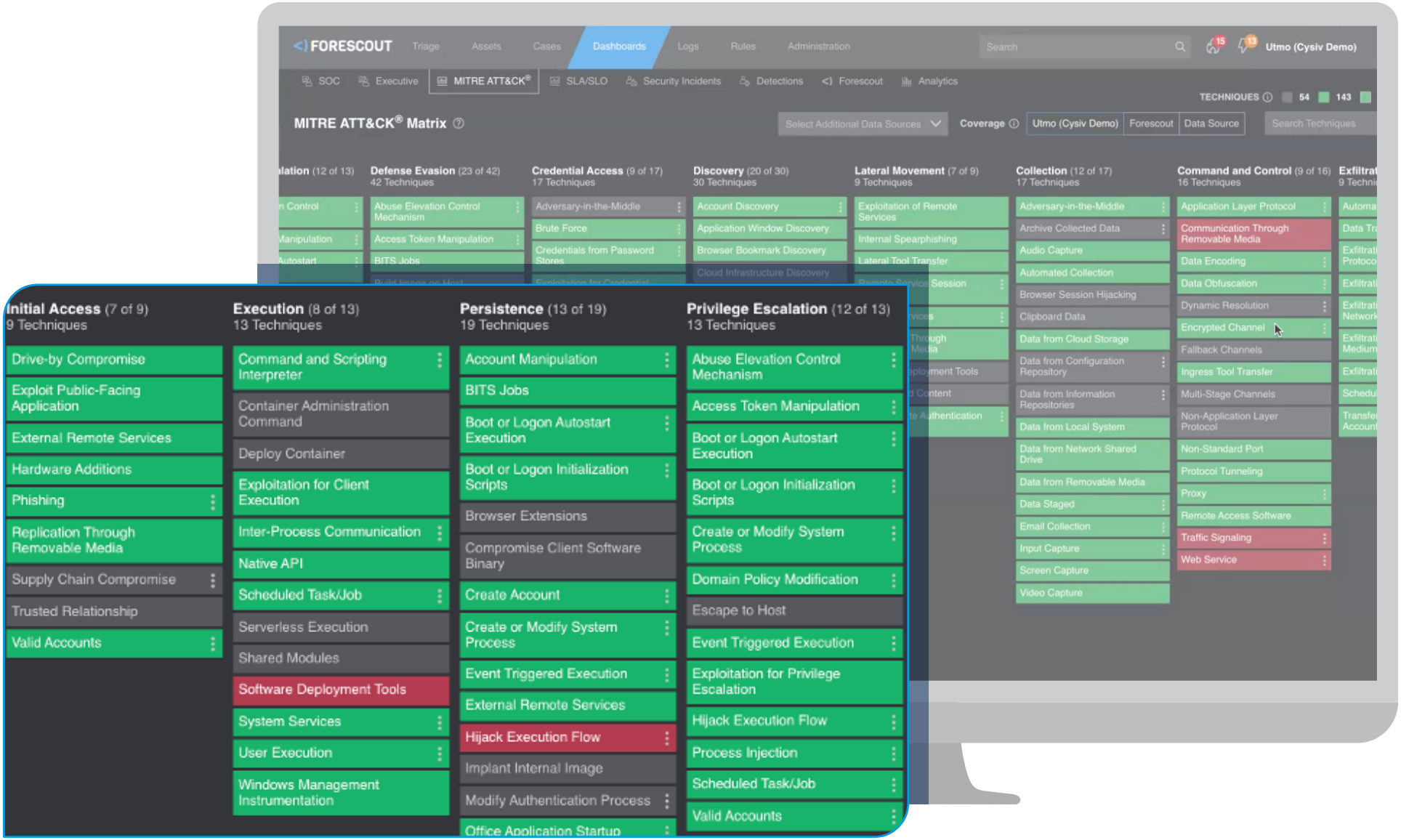
Pipeline de données de pointe

Gère les données de sources provenant de toute l'entreprise qui alimentent son moteur de détection des menaces évoluées selon une approche rigoureuse centrée sur la science des données. Dans un premier temps, Forescout XDR applique un modèle de données unifié (CIM) afin de normaliser les données ingérées. Puis il les enrichit automatiquement de divers éléments – adresse IP, géolocalisation, propriétés ADObject, données de configuration et autres données contextuelles – afin de fournir le contexte de sécurité nécessaire. Cela maximise la valeur de détection de la sécurité et accélère la mise en corrélation et la recherche de menaces à travers différentes sources de données. Enfin, un processus ETL (extract-transform-load) particulier permet une analyse des données plus rapide, plus stable et plus efficace que les processus ELT plus courants.

Intégration du cadre MITRE ATT&CK

Le cadre MITRE ATT&CK traque les tactiques et techniques des cyber-adversaires sur l'ensemble du cycle de vie des attaques. Forescout XDR s'intègre à ce cadre, ce qui vous permet de voir instantanément quelles sources de données devraient être saisies pour obtenir une couverture TTP large ou plutôt spécifique. Vous pouvez identifier les éventuels angles morts susceptibles d'être exploités et déterminer quelles sources de données supplémentaires pourraient améliorer votre couverture.

L'intégration du cadre MITRE ATT&CK permet d'identifier les angles morts potentiels et les possibilités d'améliorer la détection des menaces par l'ajout d'autres sources de données.



Détection des menaces évoluées

Exemples de menaces pouvant être détectées avec Forescout XDR

- Abus d'application
- Attaques par force brute
- Attaques par dépassement de tampon
- Analyse des ressources cloud
- Mauvaises configurations des services cloud
- Cloud : accès non autorisé
- Cloud : détection de stockage non sécurisé
- Connexion C&C
- Violations de la conformité
- Cross-site scripting
- Cryptojacking
- Exfiltration de données
- Échecs d'accès aux fichiers
- Accès illégal aux ressources
- Menaces d'initiés
- Mouvement latéral
- Logiciels malveillants/évasions
- Scan réseau
- Cassage de mots de passe
- Attaques de phishing
- Analyses de ports et de vulnérabilités
- Ransomwares
- Injection SQL
- Comportements suspects
- Accès non autorisé aux systèmes
- Modifications non autorisées des règles de pare-feu
- Redémarrages non autorisés de services
- Création non autorisée de service/processus
- Exploitation de vulnérabilités
- Mauvaise configuration d'applications Web
- Attaques d'applications Web (toutes attaques Web de couche 7)
- Infection par un virus/ver

Lac de données cloud

Lac de données indexées spécialement conçu et hautement évolutif, avec stockage hiérarchisé des données (chaudes, tièdes, froides) et recherche rapide en texte intégral. La solution assure une conservation des journaux économique à court terme et, en option, à plus long terme (de sept jours à plus d'un an) ainsi que la gestion de données télémétriques brutes ou enrichies, pour étayer les exigences en matière de sécurité et de conformité.

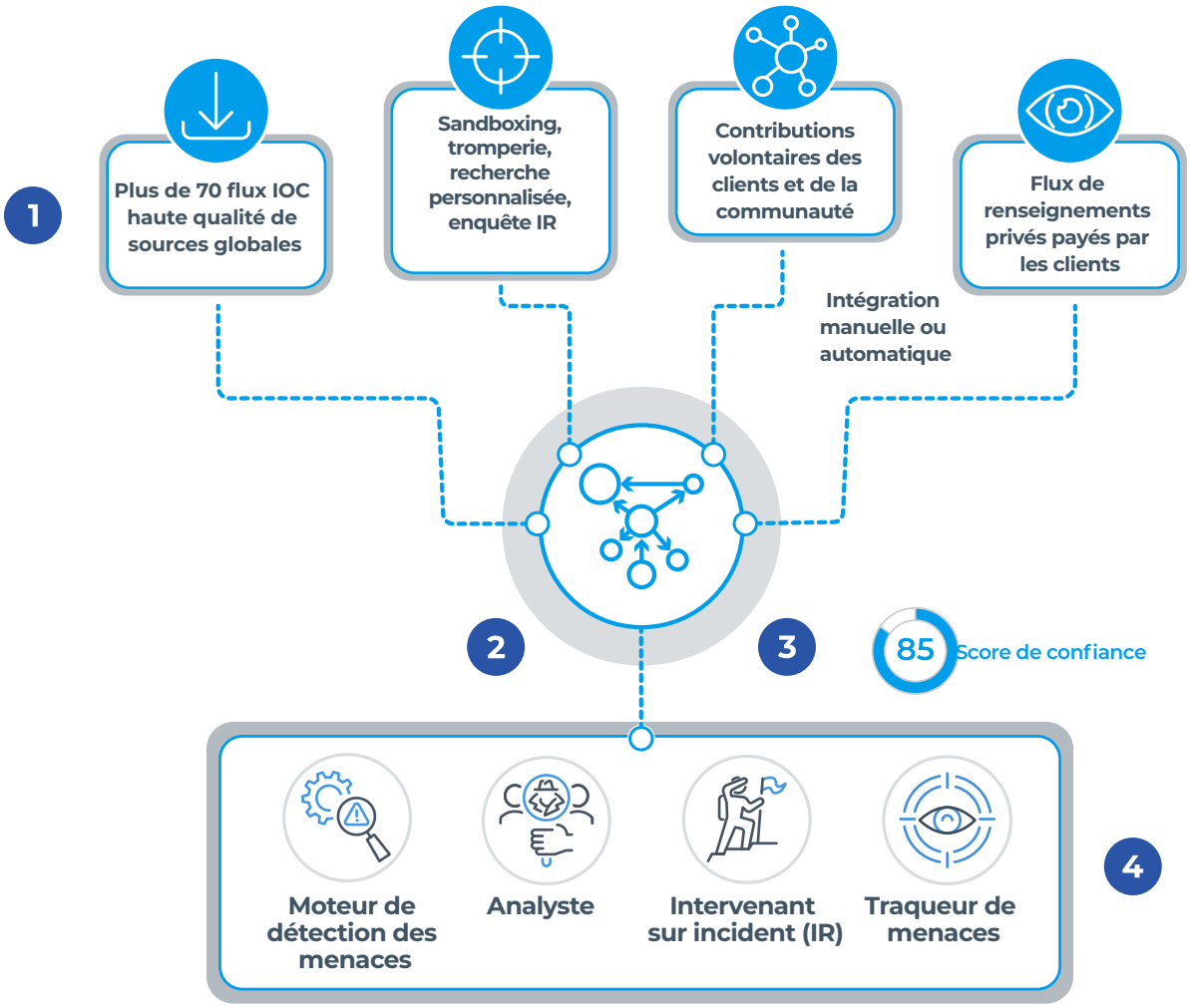
Règles de détection

La solution comprend plus de 1500 règles et modèles de détection vérifiés et prêts à l'emploi pour vos sources de données. Ces règles ont été testées sur des données de production afin de garantir qu'elles sont efficaces et créent de la valeur dès le premier jour. Des règles de détection personnalisées vous permettent en outre d'établir rapidement et de manière flexible, sur une interface utilisateur guidée, des règles d'indicateur, de détection et d'état répondant à vos exigences propres.

Moteur de détection des menaces

Un moteur de détection des menaces en deux niveaux applique cinq techniques de détection pour identifier automatiquement et avec une grande fiabilité des menaces réelles qui justifient une enquête, tout en éliminant les faux positifs (« bruit ») :

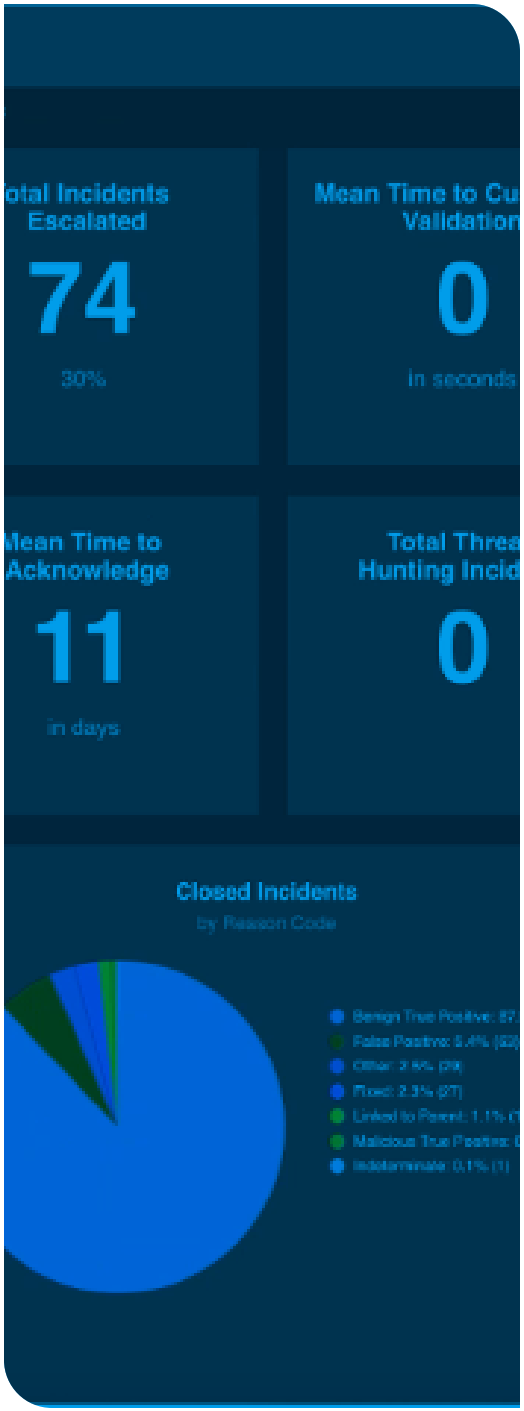
- **Signatures :** comparaison des attributs d'un objet à un objet malveillant connu afin d'identifier les menaces contenues dans la télémétrie brute, par exemple des logiciels malveillants ou des ransomwares non nettoyables.
- **UEBA :** recherche les comportements anormaux qui correspondent à un modèle numérique, à une empreinte, à une activité humaine ou à un comportement réseau connu pour être malveillant. Par exemple, un responsable commercial qui télécharge des milliers d'enregistrements de votre CRM, une activité inhabituelle en dehors des heures de bureau, du beaconing, une distance de voyage improbable.
- **Statistiques et anomalies :** identifie les activités inhabituelles à l'aide de techniques telles que le clustering, le groupage, le stacking, la détermination de références et écarts, la détection des anomalies, la régression logistique, etc. Exemples : panne de sources de journaux, attaques par déni de service.
- **Algorithmes :** utilise des techniques d'IA et de ML sensibles au contexte comme l'apprentissage supervisé/non supervisé ou l'apprentissage profond pour détecter toute activité malveillante ou anormale ou prévoir des attaques.
  Exemples : identification de voies de processus ou d'algorithmes de génération de domaine (DGA).
- **Renseignements sur les menaces :** plus de 70 sources de cyber-renseignements exploitées pour rechercher, par exemple, des portes dérobées et du trafic C&C, ou des personnes qui consultent des sites de phishing.



Renseignements sur les menaces

IOC de plus de 70 sources de haute qualité dans le monde entier, notamment de Vedere Labs, l'équipe mondiale d'experts de Forescout. Ces IOC sont classifiés, corroborés et notés afin de fournir de précieux renseignements qui sont automatiquement exploités dans le cadre du processus de détection, de traque et d'enquête sur les menaces. Vous avez accès à des rapports détaillés établis par les chercheurs de Forescout, qui dressent le profil des principaux acteurs et menaces. Anonymisées, les données IOC peuvent également être partagées entre les membres d'une communauté qui le souhaitent, notamment des ISAC spécifiques à un secteur, via un système d'échange communautaire intégré.

1. Forescout exploite les données IOC d'une vaste gamme de sources fiables.
2. Les renseignements IOC sont corrélés au sein d'une base de données graphique consultable de domaines, d'URL et d'adresses IPv4 et IPv6 « connus pour être malveillants ».
3. Chaque IOC reçoit dynamiquement une note de confiance sur la base d'une évaluation de la qualité de la source.
4. Ces informations IOC classées selon leur fiabilité sont ensuite utilisées par le moteur de détection des menaces et par les équipes SOC des clients pour accélérer et améliorer la détection des menaces et le processus d'enquête.



UEBA

Des analyses comportementales sont utilisées pour détecter les changements de comportement significatifs ou toute activité anormale d'une entité. Des profils et comportements standard sont établis pour les utilisateurs et les hôtes au fil du temps, et toute activité anormale par rapport à ces références est considérée comme suspecte.

Tableaux de bord et rapports

Des tableaux de bord préconfigurés et personnalisables basés sur les personas fournissent des ICP pertinents pour différents rôles – analystes/IR, ingénieurs, responsables SOC, responsables de la conformité et des risques, dirigeants... La diffusion et le partage proactifs de rapports et/ou de mesures permettent aux responsables de la gestion des opérations du SOC ainsi qu'aux membres de l'équipe dirigeante de disposer d'informations importantes.

SOAR

Orchestre l'ensemble du processus SOC, de la détection à l'enquête puis à l'intervention, grâce à une gestion intégrée des cas et à des notifications. Forescout XDR automatise le processus de sécurité en l'enrichissant, notamment avec la géolocalisation IP, des informations sur l'utilisateur et l'appareil, ou encore la corrélation à diverses sources de renseignement. La solution s'appuie sur Forescout eyeSight et eyeControl pour fournir des flux d'orchestration et d'intervention automatisés, capables d'atteindre chaque appareil géré ou non géré (pas d'agent possible) de l'entreprise. Et grâce à l'intégration à Palo Alto Cortex XSOAR et d'autres SOAR, vous pouvez continuer à utiliser votre solution SOAR actuelle.

Cloud natif

Rien à déployer – de nouvelles fonctionnalités, des correctifs et des règles sont mis à disposition en toute transparence, toutes les deux semaines.

Intégration SIEM

Les menaces réelles identifiées par Forescout XDR peuvent alimenter un SIEM de manière à centraliser l'orchestration et l'intervention sur incident.

Mise à jour continue du logiciel et des contenus

De nouvelles caractéristiques, fonctionnalités et correctifs, ainsi que de nouvelles règles et modèles de détection sont fournis de manière transparente à peu de semaines d'intervalle sans nécessiter d'assistance opérationnelle ni causer de perturbations.

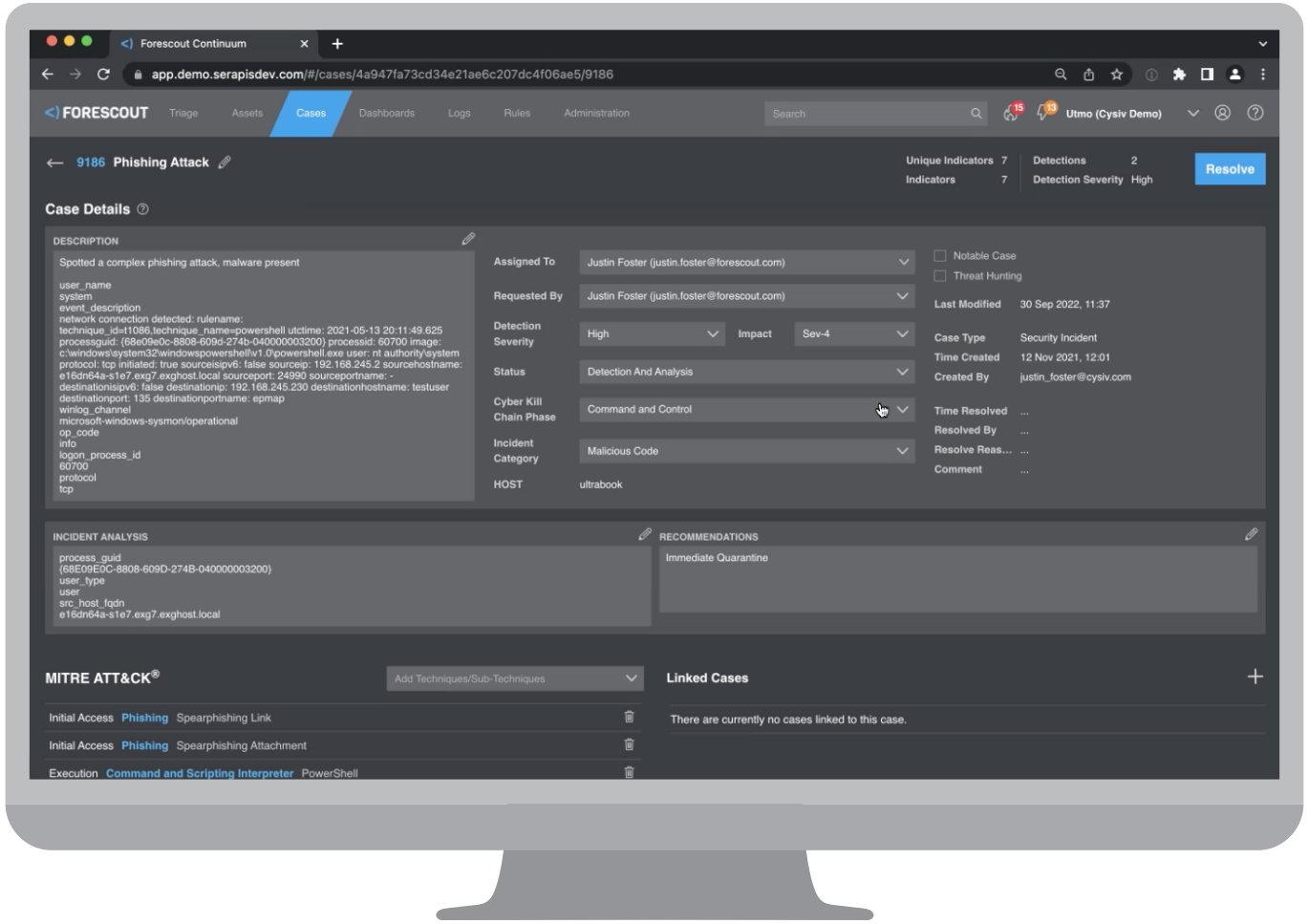
Architecture multi-locataires

Vous pouvez créer facilement des séparations logiques (ou locataires) en fonction, par exemple, du pays, de l'endroit où se situent les bureaux ou de l'unité commerciale. Vous pouvez également générer des vues agrégées et effectuer des requêtes et analyses entre plusieurs locataires et unités commerciales, jusqu'au niveau global. Cela est particulièrement avantageux pour les grandes entreprises, les multinationales, les MSSP ou encore les organisations dotées de SOC régionaux.

Architecture globale unifiée

Les exigences en matière de résidence des données et de conformité sont facilement respectées et les mesures de sécurité régionales sont prises en charge de manière économique. Vous pouvez définir où vous voulez que vos journaux soient stockés parmi 25 régions en Amérique, Europe et Asie Pacifique et, indépendamment de cela, consulter et interroger vos données à tout moment, partout dans le monde.

La gestion des cas fournit des détails exhaustifs et permet une enquête et une intervention plus rapides et plus efficaces.

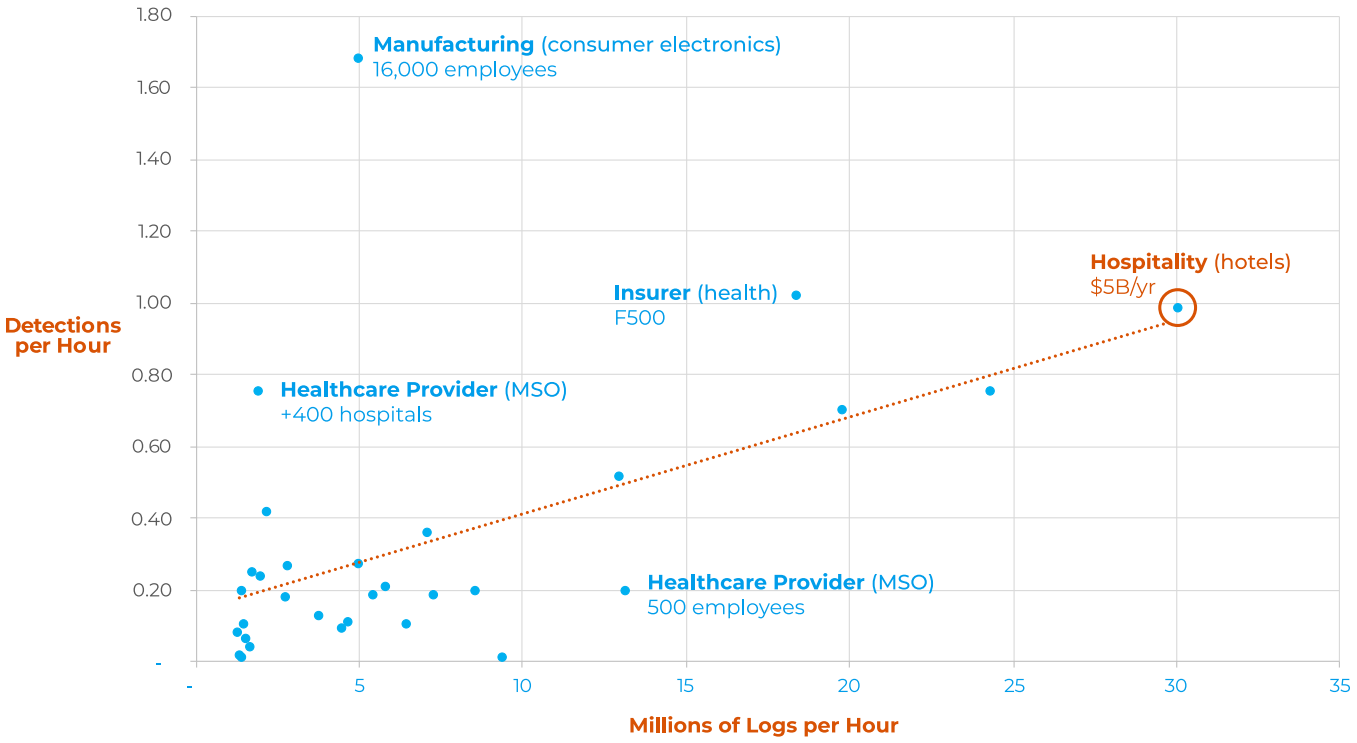


La solution assure les flux de travail, une intégration étroite, la transparence ainsi que la fluidité de la communication et de la collaboration durant le traitement des détections et la gestion des incidents. Fondé sur le cycle de vie NIST de réponse aux incidents, Forescout XDR prend en charge les intégrations avec ServiceNow, RSA Archer, Jira Software, ManageEngine ServiceDesk Plus, Palo Alto Cortex XSOAR, TheHive et ConnectWise.

Résultats

Que vous ayez des millions, des dizaines de millions ou des centaines de millions de journaux, Forescout XDR permet de couper court au déferlement de données, rapidement et automatiquement, pour ne générer qu'une très faible quantité de détections haute fidélité qui nécessiteront une intervention humaine (d'un analyste).

Le graphique ci-dessous présente les données de 31 clients pour la période d'un an commençant le 15 décembre 2021. À titre d'exemple, une entreprise hôtelière, au chiffre d'affaires de 5 milliards de dollars par an, a pu passer de quelque 30 millions de journaux par heure en moyenne à 0,98 détection nécessitant une action par heure.



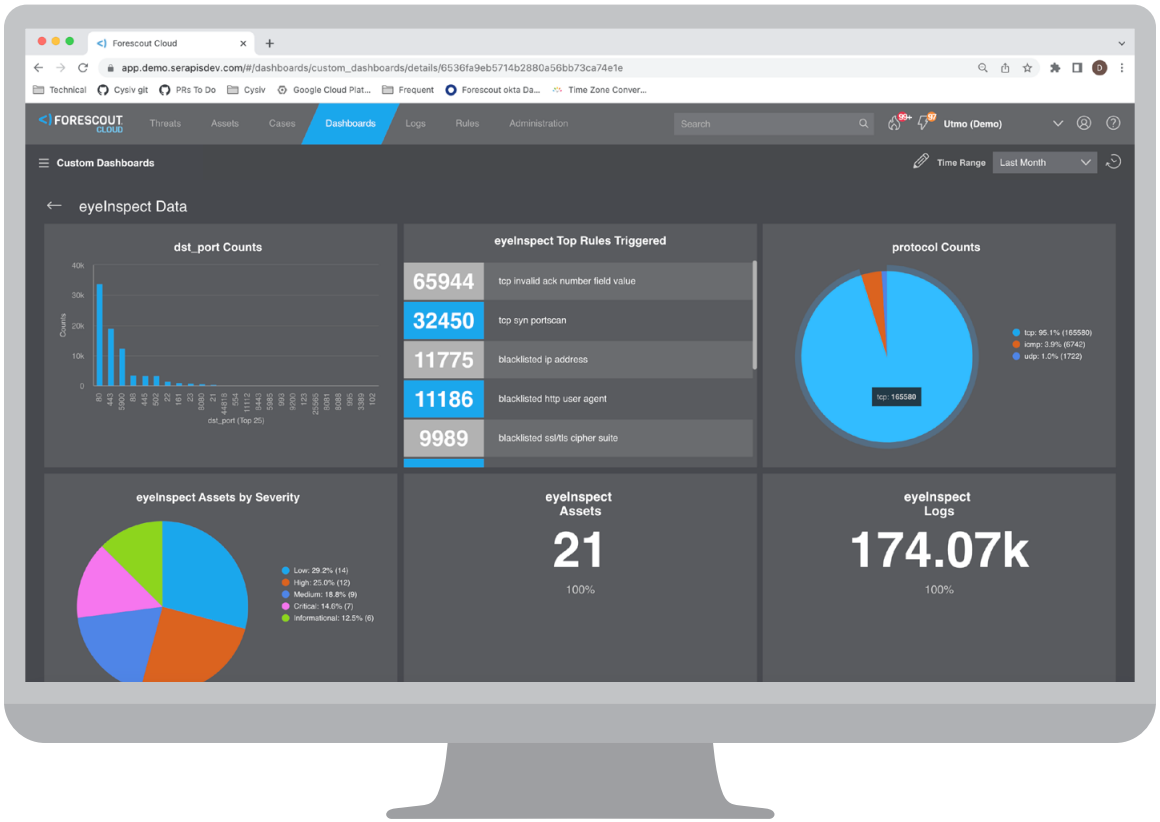
Remarques :

- Les entreprises représentées sont de différentes tailles et de différents secteurs :
  - Construction
  - Consommation
  - Énergie/services publics
  - Fintech
  - Santé
  - Assurances
  - Production
  - Industrie minière
  - Édition
  - Technologie
  - Transport/logistique
- Les résultats individuels peuvent varier et dépendent de plusieurs variables, notamment les cas d'utilisation, la sélection de journaux, le nombre total de journaux ou encore l'adaptation continue des règles.

1 The State of Security Operations, Forrester, 2020
2 Terminal se réfère à chacune des adresses MAC et IP situées sur un appareil d'utilisateur, un appareil faisant partie d'une infrastructure réseau, un appareil non attribué à un utilisateur ou sur tout composant d'une infrastructure cloud.

Forescout XDR

eXtended Detection and Response



VOYEZ FORESCOUT XDR EN ACTION

forescout.com/xdr-demo-request

FORESCOUT

Forescout Technologies, Inc.

Numéro gratuit (US)
1-866-377-8771
Tél. (intl) +1-408-213-3191
Support +1-708-237-6591

Plus d'infos sur Forescout.com

Forescout XDR

eXtended Detection and Response

FORESCOUT