chronicle

EXCLUSIVE NETWORKS

Plateforme d'analyse de la sécurité : aperçu

Google Cloud

Les défis des analyses de sécurité

En matière de sécurité, les opérations de détection, d'enquête et de réponse font face à de nombreux défis. Ces derniers concernent à la fois les coûts (TCO), l'évolutivité, les performances, la visibilité et enfin, la productivité des analystes. Les volumes de données ont rencontré une croissance exponentielle en raison du développement des infrastructures, du nombre croissant d'applications et de la multiplication des outils de sécurité. Les coûts ne se limitent pas au stockage : ces nouveaux volumes impliquent des investissements substantiels en termes d'infrastructure, afin de pouvoir mener une analyse évolutive et performante. Sans de tels investissements, les délais d'enquête et de neutralisation des menaces finissent pas en pâtir. Par ailleurs, les modèles de tarification sont généralement fonction du volume de données ou du nombre de dispositifs surveillés, ce qui dissuade les entreprises de saisir et d'analyser toutes les informations pertinentes.

Par ailleurs, les infrastructures professionnelles évoluent. Les entreprises délaissent les infrastructures sur site au profit de plateformes IaaS/PaaS/SaaS. Ces évolutions rendent la sécurité plus complexe du point de vue de la couverture et de la visibilité. Les fournisseurs cloud comme AWS et Azure veillent principalement au monitoring de la sécurité pour leur propre pile. Cette couverture de la sécurité en silo limite la visibilité sur les cyberattaques cloud.

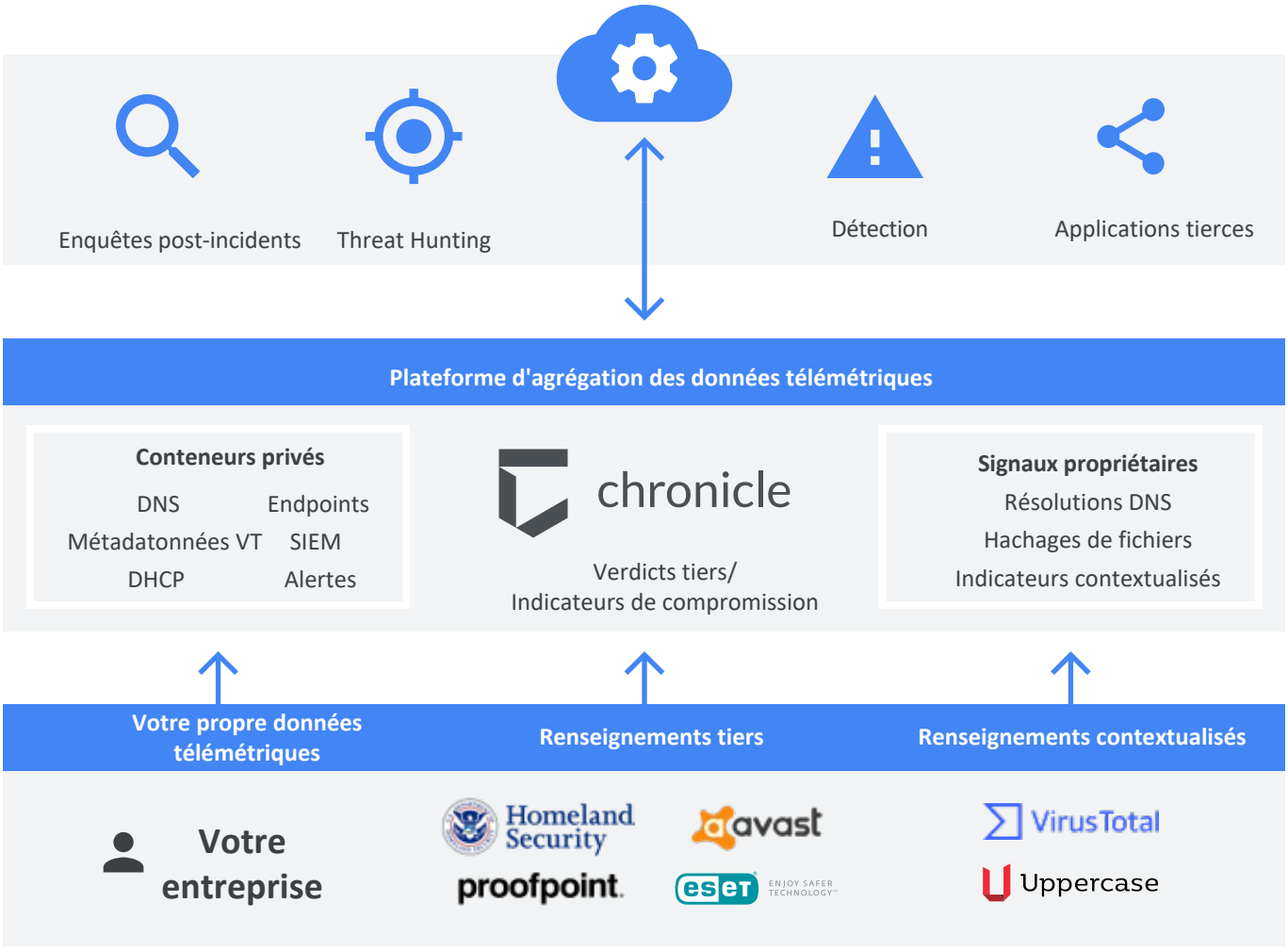
Mais le plus grand défi auquel sont confrontées les équipes de sécurité reste sans doute la pénurie de professionnels. Les modèles analytiques propriétaires et les syntaxes de recherche complexes imposées par les fournisseurs nécessitent de recourir à des analystes de niveau 2 ou 3 très expérimentés aux exigences salariales élevées, même pour le tri des attaques courantes comme le phishing. Il n'est pas surprenant que de nombreuses organisations se soient tournées vers les services de sécurité gérés pour pallier la pénurie de personnel de sécurité interne. Malheureusement, dans la plupart des cas, le problème est simplement déplacé vers une tierce partie, sans gain réel d'efficacité ou de productivité.

Nouveaux besoins en matière d'analyses de sécurité

- Coût total de possession réduit et sans surprise
- Évolutivité vers le pétaoctet
- Vitesse de recherches de niveau Google
- Visibilité cloud, on-site et hybride
- Multiplicateurs de productivité SOC

Chronicle : Aperçu

Chronicle est un service cloud, conçu comme une couche spécialisée, superposée à l'infrastructure centrale de Google, pour permettre aux entreprises de conserver, d'analyser et de mener des recherches en toute confidentialité sur les volumes considérables de données générées concernant la réseau et la sécurité. Chronicle normalise, indexe, corrèle et analyse les données pour fournir une analyse et une contextualisation instantanée des activités à risque.



Collecte de données

Chronicle prend en charge un large éventail de données de mesures de sécurité, par le biais de diverses méthodes :

Forwarder (Transmetteur)

Un composant logiciel léger, déployé sur le réseau du client. Il prend en charge syslog, la capture de paquets et les outils existants de gestion des logs / SIEM.

API d'ingestion

Des API permettant l'envoi directement de logs vers la plateforme Chronicle. Grâce à ces API, les entreprises n'ont pas besoin d'acquérir de matériel ou de logiciel supplémentaire.

Intégrations tierces

Interopérabilité avec des API cloud indépendantes pour faciliter l'ingestion des logs issus de sources comme Office 365 ou Azure AD.

Analyse de données

Les analyses Chronicle sont proposées sous la forme d'une application simple accessible via le navigateur. Des API de lecture offrent également un accès à ces fonctionnalités. L'objectif de Chronicle est le suivant : permettre aux analystes en sécurité de déterminer la nature des menaces, leur degré de sévérité ainsi que les modes de réponse adéquats.

Quelle menace ?

Voici un exemple : Si un flux de menaces vient d'informer Chronicle d'un nouveau domaine de réseau APT, Chronicle fera instantanément apparaître tous les noms d'hôtes ayant accédé à ce domaine depuis une année complète, quel que soit le volume de données. De même, Chronicle enrichit continuellement les flux d'événements entrants en corrélant les IP avec les noms d'hôtes, afin que les analystes disposent d'informations complètes, de manière instantanée, sans avoir à formuler des requêtes complexes.

Quel mode d'action ?

Les cybermenaces actuelles se situent à la croisée des chemins, quelque part entre les actifs informatiques, les utilisateurs et l'infrastructure des menaces (domaines, URL hébergés sur des adresses IP externes spécifiques et fichiers malveillants depuis ces emplacements). Chronicle fournit des aperçus élaborés pour une visibilité accrue sur les ressources, les utilisateurs et les types d'IoC. Ces aperçus sont basés sur un modèle unifié, pour permettre aux analystes d'enquêter sur les menaces rapidement et de manière intuitive.

Sécurité et conformité

Backstory repose sur une couche privée spécialisée, bâtie sur l'infrastructure centrale de Google. En tant que telle, Backstory hérite des capacités de calcul et de stockage, ainsi que de la conception sécurisée de cette infrastructure.
La conception sous-jacente à notre infrastructure de base est décrite plus en détail dans un livre blanc de Google.

Google Cloud

Quelle importance ?

Les données de mesures donnent rarement à elles seules une vision suffisamment exhaustive pour traquer, enquêter ou détecter les attaques. La contextualisation est essentielle pour donner aux analystes la possibilité de classer les menaces réelles, par ordre de priorité, tout en rejetant les faux positifs.

Comment répondre ?

Depuis quelque temps déjà, les grandes entreprises dotées de SOC bien rodés disposent de playbooks pour leurs invesigations et leurs mesures correctives. Les technologies SOAR ou d'orchestration qui automatisent ces playbooks sont maintenant de plus en plus répandues. Les API de lecture de Chronicle permettent aux entreprises (ainsi qu'aux fournisseurs de services de sécurité gérés) d'intégrer les conclusions Chronicle à leurs playbooks de sécurité, telles que les systèmes de tickets ou les outils SOC de reporting.

Résumé des fonctionnalités et avantages

Fonctionnalités	Description	Avantages
Enrichissement continu	• Corrélation automatisée entre l'IP et l'hôte • Enrichissement automatisé, continu et rétroactif des indicateurs de compromission	• Enquêtes plus rapides • Plus grande productivité des analystes
Contexte et aperçus (menaces / indicateurs de compromission, vulnérabilités, actifs informatiques, utilisateurs, fichier/ processus)	• Flux de renseignements (Proofpoint, DHS AIS, OSInt, Avast, ESET) • Renseignements sur les menaces fournis par le client • Actifs informatiques, vulnérabilités et contexte spécifique à l'utilisateur • Déduction d'informations	• Enquêtes plus rapides • Plus grande productivité des analystes
API de lecture	• Des API hautes-performances intégrant les fonctionnalités Backstory aux étapes du Playbook SOC, au MSSP et aux différents outils (tickets, orchestration, tableau de bord)	• Automatisation des playbooks du SOC • Intégration aux portails MSSP • Mesures correctives plus rapides
Ingestion des API et modèle de données unifié	• API haut-débit permettant d'envoyer des données directement au pipeline de données Backstory sans qu'il soit nécessaire de recourir à un forwarder.	• Délai de rentabilisation plus rapide • Zéro empreinte de déploiement
Analyse des logs bruts	• Accès à tous les champs non-traités • Recherche sur toutes les données de mesure brutes	• Intégration plus rapide de toutes les mesures de sécurité (télémétrie)
Sécurité / Conformité	• Respect des contrôles communs de Google Cloud • SOC 2 et SOC 3 • ISO 27001 • HIPAA BAA	• Contrôles rigoureux et documentés pour protéger vos données à tous les niveaux • Principales attestations et certifications