SentinelOne
Secure Tomorrow™

Checklist de l'architecte

Création d'une plateforme de données pour le SOC moderne

Une défense efficace contre les menaces actuelles commence par les données. Et il en faut beaucoup. Détecter, comprendre et contrer les cybercriminels sont des tâches qui exigent une parfaite connaissance de tout ce qui se passe dans votre entreprise, depuis les desktops jusqu'au cloud. La collecte, le stockage et l'utilisation de données télémétriques à grande échelle permettent aux équipes de sécurité de déployer des workflows de sécurité essentiels, dont les suivants :

Détection autonome plus sophistiquée

Grâce à l'accès en temps réel à des ensembles de données détaillés et complets, vos systèmes peuvent utiliser des algorithmes avancés et l'apprentissage automatique pour détecter de façon autonome les menaces complexes qui risqueraient sans cela de passer inaperçues. Cela permet de bloquer rapidement un plus grand nombre de menaces, parfois avant même qu'elles ne provoquent des dégâts.

Investigations plus rapides et efficaces sur les menaces

Lorsque chaque seconde compte, l'accès rapide aux Big Data permet à vos analystes de remonter rapidement la piste des cybermenaces. Comme vous pouvez identifier plus rapidement les relations et disposer d'un tableau complet de la situation, les investigations sont plus rapides et les incidents de sécurité plus vite résolus.

Chasse aux menaces

En ayant la capacité de trier un volume considérable de données, votre équipe peut détecter proactivement les premiers signes des menaces furtives qui, sans cela, risqueraient de passer entre les mailles du filet. Cette approche proactive vous permet de garder une longueur d'avance sur les cybercriminels, en identifiant et en limitant les risques avant qu'ils ne posent problème.

Premières étapes — Voici quelques questions à se poser lors du développement de votre propre plateforme de données SOC.

Disposez-vous des données dont vous avez besoin ?

La première étape de la création d'une plateforme de données de sécurité efficace est de s'assurer de disposer de toutes les données nécessaires pour détecter et comprendre les menaces, quelle que soit leur origine.

Commencez par une visibilité de référence sur les actions et comportements les plus critiques au sein de votre entreprise.

- **Endpoint**
  Première ligne de votre cyberdéfense, la capture des données des endpoints provenant de sources telles que l'EDR offre de précieuses informations sur les activités au niveau des équipements. Celles-ci sont en effet indispensables pour identifier les anomalies et les compromissions potentielles.

- **Réseau**
  Les journaux de sécurité réseau offrent une vue panoramique de l'environnement, ce qui facilite la détection de comportements inhabituels et de menaces potentielles.

- **Authentification**
  Les journaux d'authentification de l'annuaire de votre entreprise, les systèmes d'identité et les VPN offrent de précieux indices sur les personnes accédant à vos systèmes, les ressources accédées, la date et l'heure ainsi que l'emplacement. Ces informations jouent un rôle clé dans la détection des accès non autorisés et permettent de remonter la piste des activités malveillantes jusqu'à un utilisateur ou compte particulier.

- **Flux de cyberveille**
  Pour anticiper les menaces, il est impératif de connaître l'adversaire. L'intégration de flux de cyberveille permet de rester informé sur les menaces et sur les tactiques, techniques et procédures (TTP) émergentes afin de savoir quelles activités surveiller.

Allez plus loin en introduisant les données télémétriques des applications et services les plus ciblés par les cybercriminels.

Journaux des lignes de commandes
Véritable mine d'or pour les responsables des investigations numériques, ces journaux révèlent les commandes exécutées et mettent en exergue les activités de saisie clavier.

Journaux d'accès
Les journaux d'accès permettent de surveiller les activités des utilisateurs et les types d'accès dans vos systèmes.

Infrastructure cloud
Les cyberattaques dans le cloud ne cessent d'augmenter. La surveillance des environnements cloud garantit une bonne visibilité sur votre surface d'attaque étendue.

Journaux des API et des applications
Essentiels, ces journaux vous offrent de précieuses informations sur la façon dont vos applications sont utilisées et potentiellement exploitées de façon abusive.

Ajoutez un contexte avec ces sources de données à volume élevé qui capturent des informations pertinentes (qui, quoi, où).

DNS
Véritables annuaires d'Internet, les journaux DNS peuvent révéler d'importantes informations sur les sites web et les domaines avec lesquels votre réseau interagit — un vecteur courant de cybermenaces.

DHCP
Le suivi des attributions d'adresses IP via les journaux DHCP est indispensable pour retracer les attaques réseau lancées à partir des ordinateurs portables de collaborateurs. Il permet par ailleurs de détecter plus facilement les équipements non approuvés.

NetFlow
Disposer d'un suivi des multiples flux de données transitant par le réseau est essentiel pour comprendre les modèles de trafic et détecter les tentatives d'exfiltration de données.

Pouvez-vous utiliser correctement votre data lake ?

Même si vous possédez le plus gros data lake au monde, il ne vous sera d'aucune utilité si votre équipe ne peut pas accéder aux informations dont elle a besoin pour intervenir rapidement. Voici quelques questions à vous poser pour vérifier que votre plateforme de données SOC est parfaitement configurée pour vous offrir une défense optimale.

Rétention
Conservez-vous les données assez longtemps ?
Pour mener une investigation sur une menace furtive et solidement implantée ou une chasse aux menaces rétrospective, vous avez besoin, au minimum, de 6 à 12 mois de données historiques.

Coûts de stockage
Éliminez-vous des données pour faire des économies ?
Les entreprises doivent trouver le juste compromis entre rétention des données et coût. Il arrive trop souvent que des solutions de stockage onéreuses poussent les équipes de sécurité à se débarrasser des journaux à volume élevé et à faible fidélité, ce qui entrave la visibilité et peut compromettre la sécurité.

Bande passante
Limitez-vous le trafic de données en cas de problème grave ?
En cas de trafic élevé ou d'attaques DoS, certains systèmes imposent une limitation des données collectées au moment même où elles sont les plus nécessaires.

Accessibilité
Vos utilisateurs peuvent-ils accéder aux données sans formation particulière ?
Les analystes en sécurité ont rarement un doctorat en science des données. Il est important que votre équipe puisse accéder aux données et les interpréter sans devoir suivre de longues formations sur les langages de requête complexes.

Performances

Les analystes peuvent-ils extraire les données dans un délai raisonnable ?

Dans le domaine de la cyberdéfense, chaque minute compte. Une requête dont l'exécution prend plusieurs minutes (ou heures) redonne l'avantage à votre adversaire. Votre plateforme de données doit permettre d'extraire rapidement des données et des informations pertinentes en temps réel.

Contrôle d'accès

Pouvez-vous bloquer les accès non autorisés ?

Les données de sécurité peuvent inclure des informations sensibles. Avec un contrôle d'accès basé sur les rôles, les analystes voient uniquement les informations dont ils ont besoin, ce qui est capital dans le cas d'environnements multitenants.

Extensibilité

Est-il possible d'ajouter rapidement de nouvelles sources de données ?

Tenez compte du temps et des efforts nécessaires pour intégrer de nouvelles sources de données de sécurité à votre plateforme, y compris des données structurées et non structurées.

Créer ou sélectionner la plateforme de données appropriée pour votre SOC n'est pas simplement un enjeu technique, c'est aussi un impératif stratégique. Face à la complexité et à l'évolution constante du paysage des menaces, une plateforme de données complète et bien intégrée vous permet de vous concentrer sur l'essentiel : la protection de votre entreprise.

Innovation. Fiabilité. Reconnaissance.

Gartner

Un leader dans le Magic Quadrant 2023 pour les plateformes de protection des points finaux

MITRE ENGENUITY

Résultats exceptionnels à l'évaluation ATT&CK

+ 100 % de protection. 100 % de détection
+ Couverture analytique exceptionnelle, 4 ans de suite
+ 100 % en temps réel, 0 retard

Gartner Peer Insights

95 % des évaluateurs de Gartner Peer Insights™

pour les solutions EDR recommandent SentinelOne Singularity

FedRAMP · TEVORA PCI DSS Attestation HIPAA Attestation · AICPA SOC · STAR LEVEL ONE · VB100 VIRUS · SE Labs BEST Innovator WINNER 2021 · Trusted Cloud Provider CSA

À propos de SentinelOne

SentinelOne est un leader mondial dans le domaine de la sécurité optimisée par l'intelligence artificielle. La plateforme Singularity™ SentinelOne prévient, détecte et neutralise les cyberattaques en un temps record, permettant aux entreprises de protéger les endpoints, le cloud et les identités rapidement, précisément et simplement.

fr.sentinelone.com

sales@sentinelone.com
+1 855 868 3733