elastic

# Comment tirer une meilleure valeur de votre solution SIEM

elastic.co/fr →

# Table des matières

# Introduction

Alors que les entreprises adoptent des initiatives de transformation numérique en vue de s'adapter aux évolutions du marché, nombre d'entre elles ont été obligées de réévaluer leur approche de la sécurité. En effet, la mise en place de nouveaux services et produits web ou d'applications mobiles, mais aussi la nécessité d'élargir le support technique pour gérer une main-d'œuvre travaillant à distance ouvrent la porte à des types inédits de cyberattaques. **Pour les contrecarrer, les équipes de sécurité doivent évoluer rapidement afin de ne pas rester à la traîne**.

Dans cette optique, un défi essentiel à relever consiste à éviter les failles susceptibles de représenter une menace pour l'entreprise, et ce malgré les efforts déployés par les équipes de sécurité. L'explosion de l'adoption des SaaS, les exigences actuelles en matière de confidentialité et les directives visant à renforcer les fonctions de sécurité complexifient encore plus les opérations.

Pour garder le contrôle tout en garantissant l'efficacité opérationnelle, il est essentiel de disposer de données au sein de votre plateforme SIEM (Security Information and Event Management). Les équipes de sécurité ont besoin de volumes exponentiels de données très variées, comme le cloud, l'Internet des objets (IoT), les sources mobiles et les données d'observabilité. Ainsi, les activités connaissent une hausse spectaculaire essentielle pour obtenir les informations exploitables nécessaires à la protection de l'entreprise.

Souvent, cette explosion de données engendre des défis opérationnels à cause des limites de la solution SIEM. **Par conséquent, il pourrait s'avérer judicieux de réviser votre approche SIEM** afin de vérifier votre capacité à relever de tels défis.

## 175 Zo

D'après les prévisions de l'IDC, d'ici 2025, le volume des données mondiales s'élèvera à 175 zettaoctets.

## 41,6 milliards

D'ici 2025, 41,6 milliards d'appareils connectés génèreront 79,4 zettaoctets de données.

## 42 milliards

Les participants à l'enquête 2020 de PwC dédiée à la fraude et à la criminalité économique dans le monde ont indiqué que les pertes liées à la fraude s'élèvent à 42 milliards de dollars.

# Évolution des exigences en matière de sécurité

Aujourd'hui, le modèle commercial des organisations étant davantage orienté vers le cloud, les équipes de sécurité se retrouvent avec plus de responsabilités pour garantir la protection des ressources les plus précieuses de leur entreprise, à savoir les utilisateurs, les applications, les points de terminaison et les données. Les tendances suivantes empêchent les équipes de sécurité d'atteindre leurs indicateurs et KPI.

## Personnel

Il est fondamental de rester au fait des nouvelles méthodes d'attaques plus sophistiquées.

- Il existe une pénurie des compétences en sécurité.
- Les équipes de sécurité surchargées s'efforcent de renforcer leur collaboration, d'accélérer leurs processus et d'optimiser leur efficacité.

## Processus

Face à l'explosion des initiatives de cloud, la pression s'accroît pour garantir l'efficacité et la vitesse des opérations.

- D'énormes quantités de données sont transférées dans le cloud.
- Davantage de solutions cloud doivent être prises en charge pour les partenaires et collaborateurs travaillant à distance.

## Technologie

La prise en charge de sources de données en grande quantité est essentielle pour garantir la visibilité des activités d'évitement et fournir les informations permettant de contextualiser une menace.

- Il est difficile de mener des analyses et des requêtes réactives sur site et dans le cloud.
- Dans de nombreux systèmes, le coût de l'accès à des sources de données en grande quantité peut s'avérer prohibitif.

Les équipes de sécurité reconnaissent la cruelle vérité : la transformation numérique élargit la surface d'attaque. Chaque nouveau service cloud ou appareil connecté peut créer un nouveau vecteur éventuel qu'un utilisateur malveillant pourrait exploiter et serait susceptible d'engendrer des menaces plus graves ou d'exposer les ressources, ce qui aggraverait les risques commerciaux. **Les exigences les plus fondamentales consistent à disposer du contexte approprié au moment opportun afin de prendre de meilleures décisions plus rapidement**.

# Redéfinition de votre stratégie de sécurité en utilisant les données comme cadre

Il est souvent difficile de garantir la visibilité d'une surface d'attaque dynamique croissante. Les architectures ou modèles de licence fondés sur le nombre d'ingestions ou d'événements qui ne respectent pas les exigences en matière d'échelle du cloud peuvent obliger les entreprises à faire des compromis. Souvent, les équipes ont besoin de temps et de ressources pour déterminer les ressources à inclure dans les opérations quotidiennes ou à exclure. Ainsi, les organisations ont une visibilité limitée de leur solution SIEM, ce qui cloisonne les données, les équipes et les processus.

Au lieu de faire des compromis et d'adopter des approches ponctuelles pour protéger des données difficiles à inclure dans votre solution SIEM (comme les informations historiques ou les sources en grande quantité), les équipes de sécurité optent de plus en plus pour une approche différente centrée sur les besoins en données. La solution SIEM moderne doit se fonder sur la capacité de gérer tous types de données, ce qui permettrait aux équipes de sécurité de les décloisonner.

**Grâce à la solution SIEM moderne, les équipes de sécurité peuvent mener des recherches rapides et précises à grande échelle** parmi une quantité astronomique de types de données (sources traditionnelles ou non ou bien en grande quantité) au sein d'un écosystème à plusieurs niveaux. Une fois cette base en place, les équipes de sécurité peuvent tirer parti d'incroyables avantages leur permettant d'**exploiter tout cas d'utilisation de sécurité à grande échelle** (monitoring et conformité, détection et prévention des menaces, identification et réponse aux incidents) tout en gérant les problèmes prioritaires, notamment ceux liés à la fraude ou à la violation de la confidentialité, susceptibles de mettre l'entreprise en péril. La solution réside dans la capacité des équipes en charge des opérations de sécurité **de recueillir des informations exploitables dans ce domaine, de les analyser, de les visualiser, puis d'agir en conséquence, le tout d'une manière unifiée**.

## Les avantages d'une approche unifiée pour votre centre opérationnel de sécurité

Une approche unifiée permet aux équipes de sécurité de bénéficier de plusieurs avantages. Un seul datastore, doté de fonctionnalités performantes de sécurité, de traitement et de visualisation des données, fournit le contexte nécessaire au sein d'environnements distribués pour obtenir de précieuses informations exploitables en matière de sécurité à partir de l'ensemble de vos données. Grâce aux analyses appropriées de la sécurité (détections optimales, tâches de Machine Learning validées et autres méthodes prêtes à l'emploi sur site et dans le cloud), les équipes dédiées peuvent améliorer leur dispositif, détecter des menaces connues et inconnues, mais aussi réagir rapidement afin d'éviter tout dégât et d'autres incidents ultérieurement. Sur le plan stratégique, **les équipes de sécurité sont capables d'évoluer rapidement au fur et à mesure des changements dynamiques**. Les spécialistes peuvent élargir le champ de leurs compétences quand :

Ils exploitent davantage le contexte afin de mieux manipuler les données et analyser les techniques.

Ils coopèrent pour étudier de nouvelles recherches ou mettre en œuvre de nouvelles détections.

Ils développent de nouvelles procédures de fonctionnement et visualisations.

Ils établissent le profil des utilisateurs malveillants et reproduisent leurs comportements.

Davantage d'équipes sont en mesure de se charger des détections. Des solides fonctionnalités d'intégration au niveau de la plateforme peuvent sous-tendre des procédures hautement efficaces capables de simplifier l'adaptation à de nouveaux types de menaces et aux dernières exigences réglementaires.

Grâce à une approche unifiée, l'équipe en charge de votre centre opérationnel de sécurité peut résoudre des problèmes complexes pour une multitude de fonctions de sécurité, notamment la détection des menaces, la gestion de l'information et des événements de sécurité (SIEM), la recherche de menaces, la conformité, l'investigation et le monitoring de la sécurité, la réponse aux incidents et l'analyse numérique, la protection des points de terminaison et la lutte contre la fraude.

### Visibilité à 360°

Recueillez des informations exploitables en matière de sécurité et intégrez toutes les sources de données requises pour obtenir des résultats pertinents pour vos activités.

### Scalabilité du cloud

Obtenez le contexte nécessaire à l'ensemble de votre organisation pour vérifier l'existence de menaces, y compris des années d'historique.

### Centre opérationnel de sécurité hautement efficace

Identifiez les problèmes hautement prioritaires, puis intégrez-les facilement et rapidement grâce à des outils et technologies accélérant les processus d'investigation et de réponse.

## Valeur pour toute l'équipe de sécurité

### Responsable et ingénieur de la sécurité

- Analyse centralisée des logs, des flux, ou encore des données contextuelles provenant de tout votre environnement, quelle que soit l'hétérogénéité de vos sources de données.
- Recherches rapides et fédérées afin d'accéder rapidement à un environnement distribué et d'y mener des recherches
- Indexation et accès facile à des sources de données en grande quantité sans générer de frais exorbitants

### Analyse de la sécurité

- Précision pour détecter plus rapidement des menaces complexes.
- Vitesse accélérant la réponse et l'efficacité.
- Détection automatisée des menaces et réduction du temps moyen de détection.

### Responsable du centre opérationnel de sécurité

- Garantie d'un haut niveau de sensibilisation au sein de l'environnement afin d'améliorer le niveau de sécurité.
- Prévention contre les récurrences des problèmes connus et identification des problèmes inconnus.
- Respect des KPI de sécurité sans générer de frais élevés.

# Votre solution SIEM est-elle un frein ?

Aujourd'hui, les données pertinentes en matière de sécurité peuvent provenir de services cloud, d'activités réseau et utilisateur, de points de terminaison, d'applications, d'appareils connectés et de nombreuses autres sources. Dans la plupart des cas, lorsque les solutions SIEM essaient d'accéder à toutes ces sources, cela engendre des déploiements au coût prohibitif ou des temps d'analyse très lents.

Certaines solutions SIEM se fondent sur des datastores distincts pour différents types d'analyses de la sécurité (un pour le Machine Learning et un pour les corrélations basées sur les événements, par exemple). Par conséquent, les équipes doivent archiver les données dans un autre datastore dédié au contexte de la détection des menaces ou aux preuves scientifiques, et ainsi de suite. Comme évoqué plus haut, ces silos peuvent engendrer des failles dans la manière dont les équipes partagent le contexte, collaborent, gèrent les cas et réagissent aux menaces.

La solution SIEM doit aider votre centre opérationnel de sécurité à évoluer plus rapidement. Toutefois, nombre de ce type de produits ne confèrent aucune scalabilité ni flexibilité aux équipes de sécurité pour leur permettre de décloisonner les données ou les tâches, ce qui restreint les workflows d'investigation. À cause des silos opérationnels engendrés, les équipes de sécurité ne peuvent pas évoluer plus rapidement, efficacement et intelligemment.

## Exemples de défis courants à relever en matière d'efficacité opérationnelle avec les solutions SIEM traditionnelles :

- Les sources de données de sécurité ne sont pas consolidées et se trouvent dans différents datastores de l'entreprise, ce qui complexifie l'obtention d'une visibilité à 360°.
- Les temps de conservation sont trop courts, ce qui oblige à faire des compromis sur les détections, le contexte d'investigation et la recherche des menaces. Lorsque les temps de détection s'allongent, il est difficile de cadrer les failles engendrées par les attaques.
- Les analystes en sécurité ne disposent pas de sources de données adéquates pour obtenir du contexte sur l'activité susceptible de ne pas indiquer de menace persistante avancée, mais constituant bien une menace réelle pour l'entreprise.
- Les équipes du centre opérationnel de sécurité ne peuvent pas exploiter d'outils de Machine Learning si elles ne comprennent dans leurs rangs aucun scientifique des données capable de développer des modèles ni spécialiste de la recherche des menaces en mesure d'interpréter le contexte.
- Les ingénieurs en sécurité doivent investir énormément dans les projets de normalisation des données ou restructurer en permanence le réseau de données sous-jacent de leur solution SIEM lorsqu'ils ont besoin d'ajouter de nouvelles sources de données contextuelles optimales (notamment celles en grande quantité). Ils doivent déjà "connaître" leurs données.
- Les équipes de recherche consacrent un temps disproportionné à développer de fragiles règles SIEM qui ne résistent pas aux techniques d'évitement. En outre, ils ne disposent pas du contexte optimal provenant des données appropriées.
- Les analystes de niveaux 1 et 2 passent trop de temps à enquêter sur des alertes pour se trouver dans une impasse ou devoir récupérer un contexte supplémentaire auprès d'autres datastores, ce qui entraîne des retards et des défaillances.
- Dans le cadre de leur rôle, les développeurs travaillent principalement à dépanner les intégrations ou à essayer de rester au fait des mises à jour des fournisseurs.

# Une solution SIEM moderne pour une meilleure protection

Une solution SIEM moderne peut accéder à toutes les données de sécurité, indépendamment de leur taille, de leur échelle ou de leur emplacement. Grâce à la visibilité de tout l'environnement, les équipes de sécurité ont accès au contexte optimal et aux historiques rétroactifs dont elles ont besoin pour mieux détecter les menaces, réagir plus rapidement et les hiérarchiser avec une plus grande précision.

**Accès à tous types de données**

**Informations exploitables historiques en temps réel**

**Rapidité maximale du centre opérationnel de sécurité**

# Efficacité opérationnelle grâce à Elastic Security en tant que votre solution SIEM

Les équipes de sécurité gèrent un volume croissant de données. Elles doivent donc être en mesure d'y mener rapidement des recherches, des analyses et des détections automatisées précises. Pour réagir aux menaces modernes, elles doivent effectuer des corrélations instantanées garantissant notamment des enquêtes, un repérage et un profilage des menaces efficaces au sein d'infrastructures cloud, de données de sécurité traditionnelles, d'applications et d'années d'historique.

Les équipes de sécurité utilisent Elastic Security pour accéder à des données consolidées, pour contextualiser les résultats par rapport aux menaces et à la situation du secteur, ainsi que pour exploiter les données historiques en vue d'identifier rapidement le meilleur plan de résolution. Elastic Security gère de nombreux cas d'utilisation, comme la SIEM, la sécurité aux points de terminaison, la recherche des menaces, le monitoring du cloud et la détection des fraudes. Ainsi, votre centre opérationnel de sécurité peut exploiter la puissance de la recherche et de la visualisation afin de protéger l'organisation à l'aide d'une approche unifiée de la détection, de la prévention et de la réponse aux menaces.

# Un travail plus intelligent avec Elastic Security

## Visibilité à 360°

Recueillez des données normalisées d'Elastic Common Schema avec Beats, et indexez toutes les données pertinentes en matière de sécurité en vue de décloisonner les informations au sein de l'organisation. Interagissez avec des tableaux de bord intuitifs prêts à l'emploi et développez des visualisations personnalisées par glisser-déposer qui répondent à vos besoins à l'aide de Kibana, Lens et Canvas.

## Informations exploitables en un tournemain

Ingérez des données à l'aide de formats de schémas de lecture et d'écriture afin d'optimiser la performance des recherches, puis d'ajouter des champs ou de les modifier en toute flexibilité. Intégrez en quelques secondes des résultats dans les tableaux de bord grâce à la vitesse légendaire de la Suite Elastic. Réduisez le nombre de fausses alertes grâce aux corrélations hiérarchisées.

## Intégration d'années de données historiques

Exploitez des snapshots interrogeables afin d'intégrer de manière rentable les quantités de données de sécurité dont vous avez besoin dans les processus de détection, de contextualisation des enquêtes, de recherche des menaces et de monitoring du cloud, entre autres. Cadrez les failles grâce à des mois, voire des années de temps de détection.

## Diminution des temps de détection.

Automatisez la détection grâce à des processus prêts à l'emploi mappés dans MITRE, qui ont été développés par l'équipe de recherche en sécurité interne d'Elastic, mais aussi à des processus personnalisés exploitant le puissant et intuitif langage de requête EQL (Event Query Language) en vue de réaliser des corrélations détectant les outils, les techniques et les procédures des menaces avancées.

## Identification des activités malveillantes anormales

Appliquez des tâches de Machine Learning non supervisées à toute source de données dotée d'un horodatage afin d'identifier les anomalies autonomes ou associées représentant une menace éventuelle. Associez les tâches de Machine Learning supervisées ou non pour identifier les méthodes utilisées, comme les algorithmes de génération de noms de domaine avec un faible nombre de faux positifs.

## Rationalisation des workflows des SecOps

Utilisez l'espace de travail interactif d'Elastic Security pour détecter les menaces, réagir en conséquence, trier les événements et recueillir des preuves selon une chronologie interactive intuitive. Exploitez la gestion intégrée des incidents et intégrez cette fonction aux workflows ainsi qu'à la solution d'orchestration et d'automatisation des processus de réponse aux incidents des principaux fournisseurs afin d'accélérer les réponses et les résolutions.

## Mise en œuvre du centre opérationnel de sécurité moderne

Elastic Security constitue la base technologique des équipes de sécurité modernes du monde entier. L'approche de la sécurité d'Elastic via une plateforme ouverte garantit une intégration, de la flexibilité et la capacité à exploiter les collaborations et les contributions de la communauté afin d'aider les équipes du centre opérationnel de sécurité à évoluer rapidement et à prendre de meilleures décisions plus rapidement.

# Conclusion

Pour protéger leurs organisations dans un paysage en croissance perpétuelle, les équipes de sécurité ne doivent pas perdre de vue la nécessité de rester efficaces sur le plan opérationnel. Lorsque vous bénéficiez de toutes les données pertinentes en matière de sécurité et de méthodes rentables pour accéder à des données historiques, vous pouvez résoudre davantage de cas d'utilisation en déployant Elastic Security comme solution SIEM et vous optimisez la valeur ajoutée globale de votre déploiement SIEM. **Les grandes équipes de sécurité optent pour Elastic Security comme solution SIEM, car elles ont besoin d'une approche unifiée de détection, de prévention et de réponse**.

Elastic vous permet d'obtenir rapidement et de manière efficace une visibilité à 360° de tout votre environnement en vue d'identifier et de résoudre les problèmes. En outre, vous bénéficiez de la scalabilité du cloud dans votre environnement hybride et votre centre opérationnel de sécurité atteint son efficacité maximale, indépendamment du degré de distribution de vos équipes ou du nombre de silos qu'elles gèrent aujourd'hui. Garantissez la protection de vos activités grâce à une nouvelle approche SIEM fondée sur Elastic Security.

# Vous souhaitez essayer Elastic Security ?

Essayez Elastic Security sur Elastic Cloud gratuitement pendant 14 jours.
(Nous ne vous demandons pas de fournir vos coordonnées bancaires.)
Vous pouvez également le déployer sur site pour en bénéficier en permanence.

**Se lancer gratuitement avec Elastic Security** ⟶

Search. Observe. Protect.



Elastic garantit des données exploitables en temps réel et à grande échelle pour les tâches de recherche d'entreprise, d'observabilité et de sécurité. Ses solutions, déployables partout, se fondent sur une seule pile technologique gratuite et ouverte. Vous bénéficiez alors instantanément de données exploitables (recherches de documents, monitoring d'infrastructure ou détection des menaces). Des milliers d'organisations ont adossé leurs systèmes stratégiques à Elastic, notamment Cisco, Goldman Sachs, Microsoft, The Mayo Clinic, la NASA, The New York Times, Wikipédia ou Verizon. Fondée en 2012, Elastic est cotée à la bourse de New York (NYSE, symbole ESTC). En savoir plus sur elastic.co/fr.

SIÈGE AMÉRICAIN
800 West El Camino Real, Suite 350, Mountain View, California 94040
Général : +1 650 458 2620 ; ventes : +1 650 458 2625

info@elastic.co