SentinelOne

Renforcer les opérations de sécurité à l'aide des données et de l'IA

L'intérêt d'une approche unifiée de la cybersécurité

eBook

Sommaire

L'IA générative donne vie aux données et enrichit l'expertise des professionnels de la sécurité

Si vos données de sécurité pouvaient parler, que diraient-elles ? Avec l'IA générative, il ne s'agit plus d'une question rhétorique. Si cette technologie fait des vagues dans tous les secteurs, son potentiel de transformation est particulièrement flagrant dans le domaine de la sécurité.

En matière de cybersécurité, l'IA générative ne peut pas se résumer à un chatbot. Associant les prouesses analytiques de l'IA traditionnelle à une capacité d'apprentissage et de création, **l'IA générative aide les entreprises à détecter et à résoudre les menaces plus rapidement et efficacement que jamais** en mobilisant les ressources dont elles disposent déjà. Une étude du Ponemon Institute a démontré que les modèles avancés d'IA générative sont capables d'analyser des systèmes complexes, comme des infrastructures réseau ou des applications logicielles, d'en identifier les vulnérabilités, de détecter de nouvelles menaces et de limiter les risques associés[1].

Pour ce faire, l'IA générative ne remplace pas les équipes de cybersécurité : elle en décuple les capacités. Elle transforme le fonctionnement des équipes en s'acquittant des tâches fastidieuses et en accélérant les tâches stratégiques pour que les analystes puissent se concentrer sur le travail que seuls des humains peuvent accomplir. **Les utilisateurs peuvent converser avec l'IA en langage naturel depuis une simple interface, comme s'ils avaient un analyste sécurité à leurs côtés.** Cette technologie aide tous les professionnels de la sécurité, des nouveaux arrivés aux plus chevronnés, à obtenir des renseignements cruciaux pratiquement en temps réel. Comment ? En interrogeant de vastes quantités de données, l'IA reconnaît des modèles et identifie des menaces en un temps record, tout en poursuivant son apprentissage en continu.

De fait, certaines applications parmi les plus prometteuses du moment sont axées sur l'identification et l'investigation des menaces. Par exemple, l'IA générative pourrait s'avérer un allié précieux pour contrer le phénomène de désensibilisation aux alertes. Une étude a démontré que l'IA était capable de traiter en moyenne 51 % des alertes sans supervision humaine[1]. De la même façon, alors que parcourir des données pour y repérer les signes de menaces est une tâche particulièrement chronophage pour les humains, le processus est nettement plus rapide avec l'IA générative. L'intelligence artificielle peut guider les utilisateurs lors des investigations en transformant le langage naturel en requêtes complexes, en générant des résumés automatiques sur les menaces, en suggérant des requêtes complémentaires et bien plus encore. Avec l'aide de l'IA, les équipes sont capables d'analyser un volume important de données de sécurité provenant d'environnements divers en quelques minutes plutôt qu'en quelques heures — un atout important en cybersécurité, où chaque seconde compte.

63 % des professionnels du secteur considèrent que la cybersécurité est le champ d'application le plus prometteur pour l'IA générative[2]

51 % des alertes de sécurité, en moyenne, peuvent être gérées par l'IA sans supervision humaine[1]

50 % des entreprises affirment avoir amélioré leur posture de sécurité après avoir adopté l'IA en cybersécurité[1]

69 % des entreprises environ estiment ne pas être en mesure de répondre aux cybermenaces sans l'IA[3]

[1] The State of AI in Cybersecurity Report. The Ponemon Institute and MixMode, 2024
[2] Using generative AI to strengthen cybersecurity. KPMG, 2023
[3] The Real-World Impact of AI on Cybersecurity Professionals. ISC2, 2024

L'IA générative, une arme redoutable entre les mains des cybercriminels

Les cybercriminels sont bien conscients de l'intérêt de l'IA et l'exploitent pour gagner en rapidité et efficacité.

Si la plupart des cyberattaques vous semblent familières, c'est parce que les stratégies qui fonctionnent tendent à perdurer. Mais ne vous y trompez pas : les acteurs malveillants innovent constamment et, comme beaucoup d'entre nous, **ils perçoivent le potentiel de l'IA générative pour faire évoluer leurs tactiques**. Que ce soit par la réduction de la barrière à l'entrée de la cybercriminalité ou par l'emploi des données pour identifier les vulnérabilités logicielles, l'IA générative rend les cyberattaques plus destructrices, efficaces et difficiles à détecter. D'ailleurs, le Centre national de cybersécurité britannique (NCSC) indique que tous les types d'acteurs cybercriminels, étatiques ou non, expérimentés ou amateurs, ont déjà adopté l'IA à divers degrés dans leurs attaques[1].

Prenons l'exemple du phishing. Les cyberpirates utilisent WormGPT, une version malveillante de ChatGPT d'OpenAI, pour rédiger des messages de phishing. Dépourvus des fautes de grammaire qui les trahissaient auparavant, ces e-mails frauduleux sont encore plus convaincants et efficaces pour soutirer des informations sensibles[2]. Les cybercriminels se servent également de l'IA générative pour produire du code malveillant capable d'exploiter des vulnérabilités dans les systèmes de sécurité et accéder à des données sensibles en échappant longtemps à toute détection. Malheureusement, ces cas d'utilisation ne sont que la partie émergée de l'iceberg. L'arrivée du modèle RaaS (Ransomware-as-a-Service)[3] a favorisé la création d'un marché noir où des outils sophistiqués basés sur l'IA sont vendus à grande échelle. Cette évolution a abaissé la barrière à l'entrée pour les cybercriminels et ouvert la porte à d'autres innovations, ce qui présage encore plus de dommages à l'avenir – du moins si on laisse les cybercriminels agir en toute impunité.

La meilleure des défenses : prendre les cybercriminels à leur propre jeu

La menace d'une IA exploitée à des fins illicites est une réalité, mais les tendances actuelles suggèrent que cette technologie favorise le secteur de la sécurité. Selon le Centre national de cybersécurité britannique (NCSC), le recours à l'IA dans les cybermenaces sera contrebalancé par son utilisation en cybersécurité pour renforcer la résilience, avec notamment des progrès en matière de détection des menaces et de conception des outils[1]. Ainsi, l'IA générative peut aider à prioriser les menaces en identifiant les vulnérabilités et en évaluant l'impact de potentielles menaces. Au bout du compte, les capacités mobilisées sont les mêmes que celles exploitées par les acteurs malveillants, mais mises au service du bien.

[1] The Impact of AI on Cyberthreats. National Cyber Security Centre, 2024
[2] WormGPT – The Generative AI Tool Cybercriminals Are Using to... SlashNext,com, 2023
[3] The Good, the Bad, and the Ugly in Cybersecurity, Week 15. SentinelOne, 2024

Les données, moteur des opérations de sécurité basées sur l'IA

L'adoption de l'IA en cybersécurité commence par les données

Pour combattre efficacement les menaces, les modèles d'IA générative ont besoin de données.

Sans données de qualité et en quantité suffisante, les algorithmes d'IA ne disposeront pas des informations de base nécessaires pour fournir des recommandations éclairées et des renseignements exploitables. Les résultats pourraient même être erronés ou biaisés, au détriment de l'efficacité du processus et avec des conséquences potentiellement délétères.

Intégrer l'IA dans les opérations de sécurité implique une nouvelle stratégie de données et un environnement de données unifié

Pour fournir aux modèles d'IA générative et d'IA traditionnelle les données nécessaires obtenir des résultats exacts et de bonnes performances, les entreprises doivent pouvoir exploiter des données standardisées et de qualité. Mais le parcours est parfois semé d'embûches :

- Les entreprises possèdent souvent **plusieurs Data Lakes** de conception différente, notamment en ce qui concerne les schémas, les formats et les pratiques de gouvernance des données.
- Elles stockent parfois **d'immenses volumes de données**, dont le regroupement exige un investissement considérable.
- Les **solutions et outils qu'elles utilisent ne s'intègrent pas forcément**, ce qui engendre des cloisonnements dans les données, les produits et les workflows.
- Elles ne possèdent pas toujours **la main-d'œuvre qualifiée ou le capital nécessaire** pour unifier leur environnement de données.

Les entreprises ont besoin d'une approche holistique des données et de l'IA qui couvre tous les aspects de cet environnement, depuis les sources des données et les modèles d'IA, jusqu'à la génération de renseignements à l'intention de l'équipe sécurité, tout en maîtrisant les coûts. Il est temps de décloisonner les données, les solutions et les workflows.

Les pressions réglementaires compliquent les efforts d'unification des données

De nouvelles réglementations sont adoptées chaque année en matière de sécurité et de conformité, ce qui accentue les pressions réglementaires. Rien qu'en 2023, la SEC, l'autorité des marchés financiers américaine, a pris **plus de 50 mesures liées à la cybersécurité**[1].

La gestion de ces exigences, déjà complexe par nature, devient de plus en plus coûteuse et fastidieuse à mesure que les entreprises archivent des données à des fins de conformité et créent davantage de silos. Tout cela complique encore un peu plus les efforts d'unification de l'environnement de données.

[1] Newfront Cyber Update: New Cyber Rules Coming into Force in 2024. Newfront, 2024

L'approche de plateforme unifiée est indispensable pour tirer parti des données et de l'IA – et réduire les risques

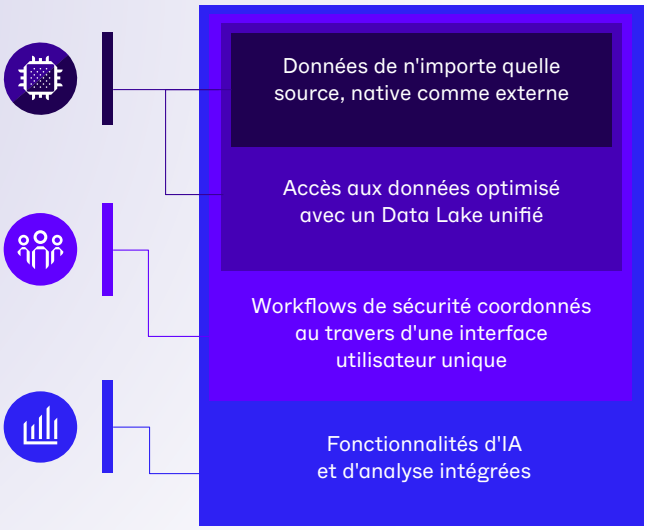
Maximiser la valeur des données pour entrer dans l'ère de l'IA

Comment exploiter les données de sécurité pour alimenter l'IA générative et améliorer les opérations de sécurité ? La réponse est simple : en adoptant une approche de la cybersécurité axée sur une plateforme unifiée. Elle pose les bases d'une infrastructure capable de gérer, d'analyser et d'exploiter efficacement les données d'une entreprise. Mais l'approche unifiée va plus loin que la simple organisation des données : elle procure une visibilité complète sur le cycle de vie de la cyberveille, de la détection à la réponse en passant par l'investigation et au-delà. La consolidation des outils et des processus que permet une plateforme unifiée facilite l'automatisation des tâches par l'IA et permet de dégager des renseignements plus pertinents à l'intention des équipes sécurité. En somme, avec moins de dépenses et d'efforts, vous améliorez votre posture de sécurité globale et vous atténuez les risques.

L'approche axée sur une plateforme unifiée : un concept qui va bien au-delà de l'interface utilisateur

Mais en quoi consiste réellement une approche axée sur une plateforme unifiée ? Fondamentalement, celle-ci repose sur une plateforme complète et totalement intégrée qui rassemble toutes les solutions de sécurité dans un **environnement de données backend et une interface utilisateur uniques**. **Elle évolue constamment** pour s'adapter aux nouvelles formes de menaces et son **caractère extensible** lui permet d'intégrer les toutes dernières approches en matière de protection. Une approche unifiée possède d'importantes qualités :

- Elle améliore l'accès à l'information, car elle permet d'obtenir des renseignements pertinents plus facilement et plus vite, grâce au **socle de données unifiées** qui comprend toutes les données d'une entreprise.
- Elle optimise l'expérience utilisateur par la **coordination des workflows de sécurité** pour toutes les fonctionnalités, ce qui étend le champ d'action des équipes sécurité et accélère leur travail.
- Elle intègre une **couche d'analyse et d'IA** qui booste les performances des équipes sécurité et favorise l'innovation.



Étudions de plus près ces caractéristiques et la manière dont elles apportent de la valeur ajoutée aux SOC, en commençant par le socle de données unifiées.

Optimiser les opérations de sécurité avec des données de qualité et faciles d'accès

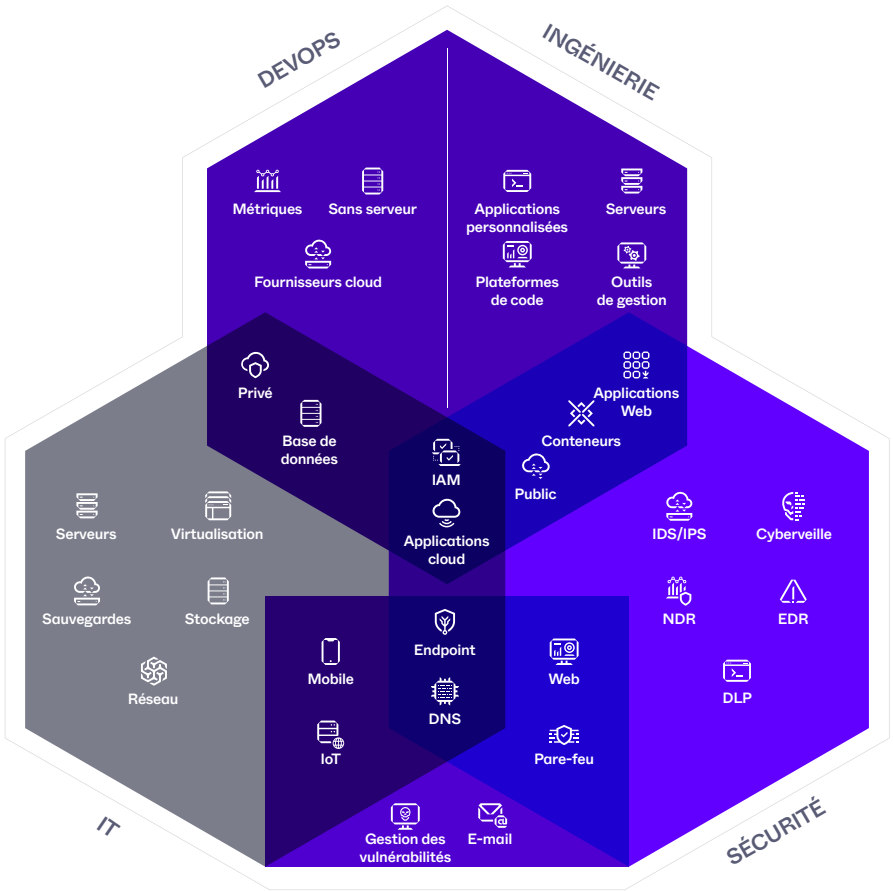
Avec un Data Lake unifié, les applications sont capables de contextualiser et de partager à la fois des données natives et externes.

Nombreux sont les fournisseurs qui prétendent proposer une « plateforme unifiée » alors que leur offre se compose en réalité de solutions disparates, simplement connectées par une interface utilisateur. D'autres proposent une suite de produits qui s'appuient sur des Data Lakes différents. Le problème de ces « plateformes » est qu'elles ne sont rien de plus qu'une interface utilisateur centralisée. **Pour être véritablement efficaces, les applications doivent aussi partager les données et le contexte au niveau du backend.** C'est pourquoi le recours au Data Lake unifié est crucial.

Un **Data Lake unifié** fournit aux différentes surfaces un référentiel unique, à partir duquel il est possible d'exploiter et de déposer des données sur l'ensemble des environnements. On reconnaît un Data Lake performant à sa capacité d'ingérer, de stocker et de gérer à la fois des **données internes et externes**, y compris l'ensemble des journaux et des investigations numériques, le tout en restant gérable et d'un bon rapport coût-efficacité.

Avec des données centralisées, les équipes peuvent effectuer des recherches sur l'ensemble des données ingérées pour produire des renseignements plus rapidement, ce qui réduit les délais moyens de détection et de réponse aux incidents. Puisqu'il n'y a plus qu'un seul Data Lake, l'approche unifiée permet également de réduire les coûts de stockage.

En ce qui concerne l'IA générative, le Data Lake unique étend la visibilité des modèles et la portée des données interrogeables. Grâce à un vivier d'informations plus riche, le processus de prise de décisions est amélioré et les réponses sont plus précises et pertinentes.



Une stratégie de données forte va au-delà de la collecte

Optimisez l'accès optimisé grâce aux normes ouvertes pour les données de cybersécurité et la portabilité des données

L'agrégation de données ne suffit pas. Un Data Lake unifié inclut des **connecteurs et des analyseurs qui normalisent et contextualisent les données** des applications selon un framework commun pour éviter les redondances et réduire les coûts de stockage. Idéalement, ce framework est élaboré selon des normes ouvertes, comme l'OCSF (Open Cybersecurity Schema Framework), afin de favoriser l'interopérabilité présente et future. Les normes ouvertes accélèrent nettement la détection, l'analyse et la réponse aux menaces, tout en réduisant la charge de travail pour les équipes cybersécurité. En effet, ces dernières peuvent se consacrer à l'optimisation proactive de la sécurité plutôt que de passer du temps à compiler et standardiser des données. Les normes ouvertes contribuent également à la **portabilité des données**. L'intégration fluide des données permet aux entreprises d'adopter des outils de sécurité en fonction de leurs besoins, tout en assurant la continuité des activités.

Simplifiez l'interrogation et la récupération des données tout en maîtrisant les coûts de stockage

Un Data Lake véritablement unifié prend en charge un **langage de requête unifié** lui aussi, pour favoriser l'interopérabilité entre les systèmes et simplifier l'accès aux données pour les utilisateurs. Avec un seul langage de requête, il n'est plus nécessaire d'apprendre à utiliser de multiples syntaxes en fonction des sources et systèmes de données, ce qui fait gagner du temps aux analystes et réduit le risque d'erreurs. Lorsque le langage de requête unifié est associé à des modèles d'IA compatibles avec des normes ouvertes comme l'OCSF, le champ des possibles s'élargit encore. L'IA améliore la vitesse et l'efficacité des opérations de sécurité en interrogeant, en exploitant et en évaluant les données natives et externes de façon normalisée.

Enfin, un Data Lake unifié accélère la réponse aux incidents et optimise les investigations en simplifiant la récupération des données, puisqu'il permet **l'intégration et la communication entre données de sources disparates** et prend en charge les **données stockées en colonne**. Avec ce type de stockage, chaque colonne de données est stockée séparément, ce qui accélère grandement la récupération et l'interrogation des données. Lorsqu'elle est **couplée à une architecture native au cloud et à une conception multitenant**, l'approche est évolutive pour s'adapter aux besoins des entreprises.

Le saviez-vous ? Les normes ouvertes prennent de l'ampleur

Les normes ouvertes, OCSF en tête, gagnent en popularité à travers le monde[1], non sans raison. Bon nombre d'entreprises adoptent davantage d'outils de sécurité pour faire face aux menaces. Dans ce contexte, les normes ouvertes sont essentielles pour que ces outils puissent communiquer entre eux et révéler leur plein potentiel.

Actuellement, les normes spécifiques aux fournisseurs créent des silos de données pour chaque application. Ce cloisonnement est doublement néfaste : les équipes sécurité perdent du temps à intégrer des outils, et les solutions de sécurité perdent en efficacité en raison de goulets d'étranglement dans l'obtention des renseignements pertinents.

La norme OCSF permet l'intégration de ces systèmes tout en préservant la confidentialité et l'intégrité. Elle aide les entreprises à s'adapter rapidement à des menaces changeantes et garantit une intégration fluide de tout futur outil, peu importe son fournisseur. Grâce à elle, les équipes sécurité n'ont plus besoin de compiler et de standardiser des données de sources différentes pour collecter des informations utiles. Enfin, l'utilisation d'une même norme ouverte favorise la collaboration à grande échelle : les développeurs peuvent s'appuyer sur le travail de leurs pairs, ce qui stimule l'innovation du secteur tout entier.

[1] The 2023 State of Open Standards. The Linux Foundation, 2023

Améliorer l'expérience des analystes avec des workflows de sécurité coordonnés et des analyses en temps réel

Les workflows dispersés représentent un risque pour la sécurité

Dans un monde idéal, les équipes sécurité consacreraient leur temps à limiter les risques et à prendre des mesures proactives contre les menaces. La réalité est tout autre, car les workflows complexes engendrent des problèmes d'efficacité. À l'heure actuelle, les workflows de cybersécurité sont souvent dispersés, car les entreprises ont adopté toute une panoplie d'outils et de processus différents pour la détection des menaces, la réponse aux incidents ou encore la gestion des vulnérabilités. Ce manque d'intégration crée des failles en matière de visibilité et de coordination. Cela se traduit au mieux par des délais de réponse plus longs et un gaspillage de ressources, et, dans le pire des cas, des compromissions aux graves répercussions.

Avec une console centralisée, plus besoin de jongler entre les outils de sécurité

L'approche de plateforme unifiée permet d'accéder à tous les outils via une interface utilisateur unique. Les équipes sécurité profitent ainsi **d'une visibilité accrue et d'une plus grande facilité d'emploi**. Elles gagnent aussi du temps, puisque le recours à une console centralisée pour la gestion et les opérations élimine la nécessité de basculer entre plusieurs outils et processus. Cette console représente le centre névralgique des équipes qui peuvent y gérer les stratégies, surveiller les événements et orchestrer les activités de réponse aux incidents. Elle les aide ainsi à mieux cerner leur environnement dans sa globalité. En prime, les analystes ont la possibilité d'adapter la console à leurs besoins et préférences grâce aux fonctionnalités de personnalisation.

Booster les fonctionnalités de base tout en préparant les opérations de sécurité à l'avenir

L'un des avantages majeurs d'une approche axée sur une plateforme unifiée est sa capacité à **booster la vitesse d'action sans compromettre l'efficacité**. Le recours à des outils tels que le XDR est plus simple et efficace à partir d'une interface utilisateur unique, puisque les équipes sécurité accèdent plus rapidement aux informations recherchées. En intégrant l'IA et l'analyse à une plateforme unifiée, les utilisateurs peuvent analyser des flux de cyberveille provenant de diverses sources et enrichir les données télémétriques de sécurité avec des informations contextuelles sur des menaces connues. L'IA applique une logique de détection et d'analyse à l'ensemble des données d'une entreprise à une vitesse inégalable pour un humain. Les équipes sécurité gagnent du temps et couvrent davantage de terrain.

Enfin, une approche unifiée crée une **base extensible pour l'avenir**. L'extensibilité facilite l'ajout de solutions internes ou externes, et ce même si elles reposent sur des systèmes hérités, pour accompagner l'évolutivité d'une entreprise et combattre des menaces changeantes. Elle permet l'adoption des dernières innovations de cybersécurité tout en maintenant l'interopérabilité et la compatibilité avec les outils et processus existants.

Limiter les risques avec une couche d'IA générative qui accélère les opérations de sécurité pour toute l'équipe

Le vocabulaire de l'IA

Intelligence artificielle (IA)
Système qui utilise une analyse et une logique avancées pour reproduire des comportements intelligents, comme la compréhension et la production d'artefacts ou de langage, et des actions d'automatisation.

Apprentissage automatique
Classe d'algorithmes dont le comportement change selon les données qui lui sont fournies.

IA générative
Sous-catégorie de modèles d'apprentissage automatique déployée à grande échelle. Elle peut apprendre d'une représentation d'artefacts et peut générer des artefacts similaires en réponse à une invite.

Grand modèle de langage (LLM)
Type de modèle d'IA générative entraîné sur d'importants volumes de textes pour comprendre les entrées de texte et générer des sorties de texte similaires à celles d'un humain.

Des renseignements en temps réel et des fonctionnalités automatisées au bout des doigts grâce à l'IA générative

L'approche conventionnelle de l'analyse de données de cybersécurité entraîne souvent des délais de traitement qui se comptent en heures, voire en jours. Autant dire son inefficacité face à la rapidité des menaces sophistiquées. En ajoutant des **solutions d'IA générative à une plateforme unifiée, les délais de traitement sont raccourcis et l'analyse des données se fait pratiquement en temps réel**. Non seulement l'apport de l'IA booste l'efficacité des activités de cybersécurité, mais il donne aussi une vue complète de la posture de sécurité d'une entreprise.

Insuffler de la vie à l'environnement de données pour en faire un collègue

Le pouvoir de l'IA générative et de l'analyse repose dans sa capacité à donner vie aux données. Avec l'IA générative, les équipes sécurité interagissent avec les données en **langage naturel**, comme si elles parlaient à un expert de leur propre équipe. Tous les professionnels du secteur en profitent, indépendamment de leur niveau d'expérience. Les analystes juniors montent en capacités, car ils peuvent interroger des données en langage naturel plutôt que de passer du temps à apprendre et affiner leurs requêtes dans un langage spécifique. Quant aux analystes seniors, ils peuvent utiliser l'IA générative pour écrire les requêtes, ce qui libère du temps pour les tâches nécessitant leurs compétences spécialisées.

L'IA générative **optimise également la détection et l'investigation** des menaces en appliquant aux données une logique de détection et d'analyse. Telle une sentinelle, elle génère pour toutes les surfaces des renseignements en temps réel susceptibles de signaler une attaque, comme un pic de l'activité du réseau. Elle **prévient aussi la désensibilisation aux alertes** en suggérant celles à prioriser, avec des recommandations guidées, et peut accélérer la résolution des alertes en déclenchant des workflows automatisés, comme des intégrations aux systèmes de gestion des tickets. L'IA est toujours vigilante et exécute des investigations autonomes en arrière-plan pour libérer les équipes des tâches de surveillance.

Enfin, c'est un puissant **outil de réponse aux incidents.** Dans un contexte d'application des stratégies, l'IA générative facilite les actions de migration en un clic et les intégrations orchestrées pour fournir des réponses personnalisées, automatisées et basées sur les playbooks. Lorsqu'une menace est résolue, l'IA génère des résumés automatiques de l'incident afin que les utilisateurs ne perdent pas de temps à documenter leurs résultats.

Une plateforme unifiée permet d'exploiter les avantages de l'IA générative et de faire monter en puissance les équipes sécurité

Une plateforme unifiée dotée de l'IA générative ne se contente pas de réduire la charge de travail en améliorant la protection : elle repousse les limites du possible en cybersécurité

Nous observons de nombreux cas d'utilisation associant une plateforme unifiée et l'IA générative et comme cette dernière va continuer de s'améliorer, il reste bien des progrès à accomplir. À l'heure actuelle, les cas d'utilisation principaux sont les suivants :

Détection des anomalies pilotée par l'IA sur les journaux de sources externes

L'IA est capable de détecter des anomalies automatiquement sur des événements provenant de sources de journaux connectées. Si une entreprise connecte des journaux de sources externes afin de les ingérer dans son Data Lake unifié, l'IA pourra identifier les menaces potentielles pour la sécurité, par exemple un compte vraisemblablement piraté à partir d'événements présentant une géolocalisation suspecte.

Tri automatisé des alertes et analyse de similitude globale

L'IA automatise le processus de tri des alertes en analysant des billions de signaux de données anonymisés à l'échelle mondiale pour identifier des alertes similaires et comprendre comment les analystes y ont répondu. Par exemple, lorsqu'un analyste vérifie une alerte, il voit que « 93 % des alertes similaires » ont été considérées comme de vrais positifs. L'IA décide donc que l'alerte est elle aussi un vrai positif. Des messages complémentaires, tels que « 32 alertes similaires sont ouvertes », aident les analystes à prendre des décisions efficaces et factuelles en réponse à l'alerte. L'IA apprend ensuite de ces réponses des analystes pour continuer à améliorer son analyse de similitude et ses calculs de probabilité.

IA et suggestions d'hyperautomatisation pour un pilotage automatique de la réponse aux incidents

L'IA suggère des actions intelligentes de limitation des risques pour réduire le délai moyen de réponse aux incidents et assurer la sécurité à grande échelle. Les analystes voient s'afficher des recommandations pour chaque alerte d'après les réponses courantes aux alertes similaires. Ils peuvent étendre l'action à toutes les alertes ouvertes similaires dans leur environnement ou créer une règle d'hyperautomatisation qui effectuera la même action pour toute nouvelle alerte similaire.

Investigations autonomes continues pour faire pencher la balance en faveur de la cybersécurité

Après avoir trié et détecté automatiquement une alerte puis déterminé de la nécessité d'investigation, l'IA va enclencher les étapes automatiques d'investigation, de vérification des journaux, de collecte des preuves et même de présentation synthétique des résultats pour les analystes. Grâce aux investigations autonomes, les équipes sécurité peuvent dire adieu aux tâches d'investigation laborieuses pour mieux se concentrer sur les résultats de celles déjà menées par l'IA.

Conserver une longueur d'avance sur les menaces présentes et futures grâce à un partenaire de confiance en cybersécurité

Tout ne se résume pas à une question de technologie

Les partenaires expérimentés jouent un rôle essentiel dans le soutien aux entreprises qui souhaitent mettre en place des stratégies de cybersécurité. Les meilleurs partenaires ont une vision claire de l'avenir de la cybersécurité et des fonctionnalités à offrir pour y parvenir. Lorsque vous cherchez un partenaire fiable pour vous soutenir dans l'implémentation d'une plateforme unifiée associée à l'IA, assurez-vous qu'ils répondent à ces critères :

- Une **vision claire de la cybersécurité** en adéquation avec les stratégies et priorités de votre entreprise
- L'expertise suffisante pour fournir des **services de détection et d'intervention gérés et de planification proactive**
- Une **gestion SaaS native au cloud** pour répondre aux exigences d'évolutivité
- Une **gestion flexible et sur site** pour répondre à vos besoins spécifiques et uniques
- Une volonté **d'aider les clients à construire les connecteurs** nécessaires pour leur adoption de la plateforme
- Un engagement à prendre en compte les **réglementations les plus récentes**, notamment sur l'IA et la confidentialité des données, pour assurer la conformité future des outils que le partenaire conçoit et maintient
- Un respect de la **confidentialité des données** ; les fournisseurs qui entraînent leurs solutions sur les données de leurs clients (informations, processus, renseignements de sécurité, etc.) sont susceptibles de ne pas respecter les normes les plus strictes en matière de confidentialité des données

Avec SentinelOne, entrez en toute confiance dans l'ère des données et de la cybersécurité basée sur l'IA

Plus de fonctionnalités. Moins de complexité. C'est possible avec SentinelOne.

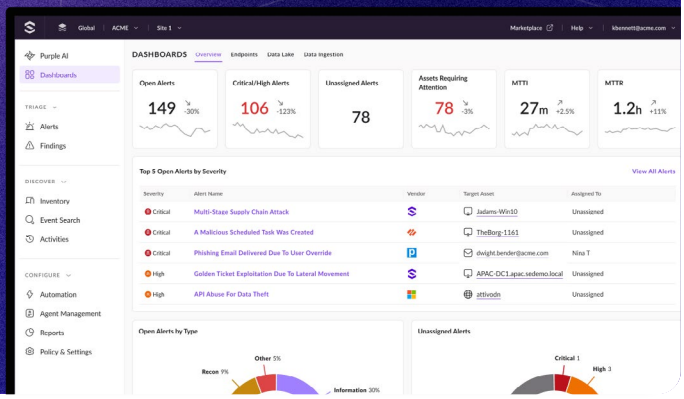
Avec sa plateforme de sécurité de pointe pilotée par l'IA, SentinelOne aide les entreprises à exploiter pleinement le potentiel des données et de l'IA pour mettre en place un dispositif de défense sans points de friction. Consultez les ressources suivantes pour en savoir plus sur notre approche unifiée.

- Rendez-vous sur SentinelOne.com pour découvrir comment nous définissons l'avenir de la cybersécurité.
- Consultez notre page Web à propos de Singularity, la plateforme de cybersécurité la plus avancée au monde.
- Découvrez comment Singularity Data Lake peut centraliser et transformer vos données en informations exploitables pratiquement en temps réel.
- Découvrez le pouvoir de Purple AI, l'analyste sécurité basé sur l'IA le plus avancé du marché.

Prêt pour une démonstration ?

Consultez le site Web SentinelOne pour plus d'informations ou appelez-nous au +1 855 868 3733

fr.sentinelone.com



Innovation. Fiabilité. Reconnaissance.

Gartner

Leader du Magic Quadrant™ 2023 consacré aux plateformes de protection des endpoints

MITRE ENGENUITY

Résultats exceptionnels à l'évaluation ATTACK

+ 100 % de protection. 100 % de détection
+ Couverture analytique exceptionnelle, 3 ans de suite
+ 100 % en temps réel, 0 retard

Gartner Peer Insights

96 % 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 · AAA · Trusted Cloud Provider CSA

Nous contacter

sales@sentinelone.com
+1-855-868-3733

fr.sentinelone.com

À propos de SentinelOne

SentinelOne (NYSE : S) propose une cybersécurité autonome de pointe, capable de prévenir, détecter et neutraliser les cyberattaques plus rapidement et plus précisément que jamais. Sa plateforme Singularity XDR protège les grandes entreprises mondiales en leur offrant visibilité en temps réel sur les surfaces d'attaque, corrélation entre plateformes et réponse aux incidents optimisée par l'intelligence artificielle. Vous disposez ainsi de plus de fonctionnalités, tout en réduisant la complexité de votre écosystème de sécurité.

Strengthening_Security_Operations_with_Data_and_AI_v2_fr_01232025