elastic | Doctolib

SUCCESS STORY

Doctolib met en place un centre d'opérations de sécurité interne puissant avec Elastic Security, réduisant les faux positifs de 50 % et gérant 12 fois plus de données

Region
France

Industry
Software & Technology

Solution
Elastic Security, Elastic Observability, Kibana

Internalisation du SOC et réduction de 50 % des faux positifs, avec une réponse aux menaces plus rapide

Doctolib a internalisé son SOC avec Elastic Security, bénéficiant d'alertes avancées, réduisant les faux positifs de 50 % et améliorant considérablement les temps de réponse aux menaces.

Doctolib multiplie par 12 la rétention des données tout en réduisant les coûts de 75 %

En passant d'OpenSearch à Elastic, Doctolib a étendu la rétention de ses données d'un mois à un an, tout en gérant 12 fois plus de données et en payant quatre fois moins au total.

Réduction des temps de réponse aux incidents et des tâches répétitives des analystes

Les fonctionnalités de machine learning et d'alertes automatisées d'Elastic ont permis à Doctolib de réduire le temps moyen de détection, d'enquête et de résolution des incidents, tout en améliorant l'efficacité générale des analystes.

Elastic permet à Doctolib d'optimiser ses opérations de sécurité et de réaliser des économies sans compromettre sa scalabilité

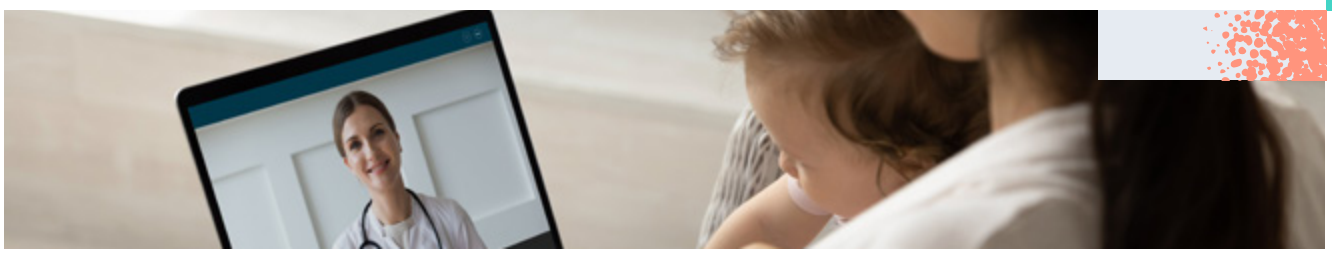
Doctolib, leader de la e-santé en Europe, met en relation plus de 90 millions de patients avec plus de 400 000 professionnels de santé en France, en Allemagne, en Italie et aux Pays-Bas. À mesure que la plateforme s'est développée, elle a dû relever des défis majeurs : sécuriser d'importantes quantités de données sensibles, se conformer à des réglementations strictes en matière de santé, et garantir une expérience optimale à des millions d'utilisateurs. De plus, leur centre des opérations de sécurité externalisé souffrait de faux positifs fréquents, de délais de réponse trop longs et de coûts élevés.

L'expansion rapide de la plateforme, notamment en période de forte pression comme lors de la pandémie de COVID-19, a mis en évidence le besoin d'une solution de sécurité plus résiliente et capable de s'adapter à une montée en charge. Doctolib devait internaliser son SOC, réduire les faux positifs et améliorer la détection et la réponse aux menaces — tout en gérant un volume de données toujours croissant.

Face à ces défis critiques, Doctolib s'est tourné vers Elastic Security. L'objectif : construire un SOC robuste, capable de répondre aux exigences d'aujourd'hui et de s'adapter à celles de demain.

> Elastic n'a pas seulement renforcé notre sécurité, il nous a donné les outils pour évoluer efficacement tout en maintenant des standards élevés.

Jordan Langue
Équipe Plateforme Sécurité, Doctolib



Cybersécurité renforcée : la création d'un SOC interne

Face à la montée des menaces et aux limites d'un SOC externalisé, Doctolib a rapidement compris qu'il fallait reprendre le contrôle de ses opérations de sécurité. « Elastic a été la clé pour internaliser notre SOC », explique Othmane El Massari, Ingénieur Sécurité des Plateformes chez Doctolib. Auparavant, Doctolib utilisait un SOC externalisé géré par OpenSearch, ce qui entraînait des problèmes comme des faux positifs fréquents et des délais de réponse plus longs.

Grâce au SIEM d'Elastic, l'entreprise a pu internaliser ces opérations, lui offrant l'autonomie nécessaire pour gérer sa sécurité avec plus de précision et de rapidité. Après avoir internalisé son SOC, Doctolib a conservé des règles d'alerte similaires mais plus pertinentes, ce qui a directement réduit les faux positifs. « En utilisant Elastic, nous avons réduit les faux positifs de 50 %, ce qui permet à notre équipe de se concentrer sur les vraies menaces », ajoute Tanguy Segarra, responsable de la Blue Team chez Doctolib.

Unification des opérations de sécurité grâce à une solution SIEM complète

Elastic Security est devenu le pilier de la stratégie de sécurité informatique de Doctolib. En centralisant le logging, la surveillance et les alertes sur plusieurs sources de données — y compris Google Drive, Jira et les applications internes — et en migrant d'OpenSearch vers Elastic, Doctolib a consolidé ses opérations de sécurité en une plateforme unifiée et cohérente. « Passer à un SOC interne avec Elastic nous a permis de prendre un contrôle sans précédent sur nos opérations de sécurité », explique Tanguy Segarra. L'intégration a été fluide et les résultats immédiats : moins de faux positifs, avec des réponses plus rapides et plus efficaces face aux menaces potentielles.

Optimisation de l'observabilité pour soutenir les équipes de développement

Au-delà de l'équipe sécurité, Elastic a également transformé le travail des développeurs de Doctolib. « Aujourd'hui, Elastic est largement utilisé par presque toutes les équipes techniques chez Doctolib », déclare Tanguy Segarra. « Les développeurs ont désormais accès aux logs des applications sur lesquelles ils travaillent, ce qui n'était pas possible avec notre solution précédente. Cette transparence a énormément facilité le travail de nombreuses équipes, notamment lors du débogage », explique-t-il. Grâce à la polyvalence d'Elastic, Doctolib peut travailler de manière plus efficace et performante à travers plusieurs départements.

Augmentation de la rétention des données tout en réduisant les coûts

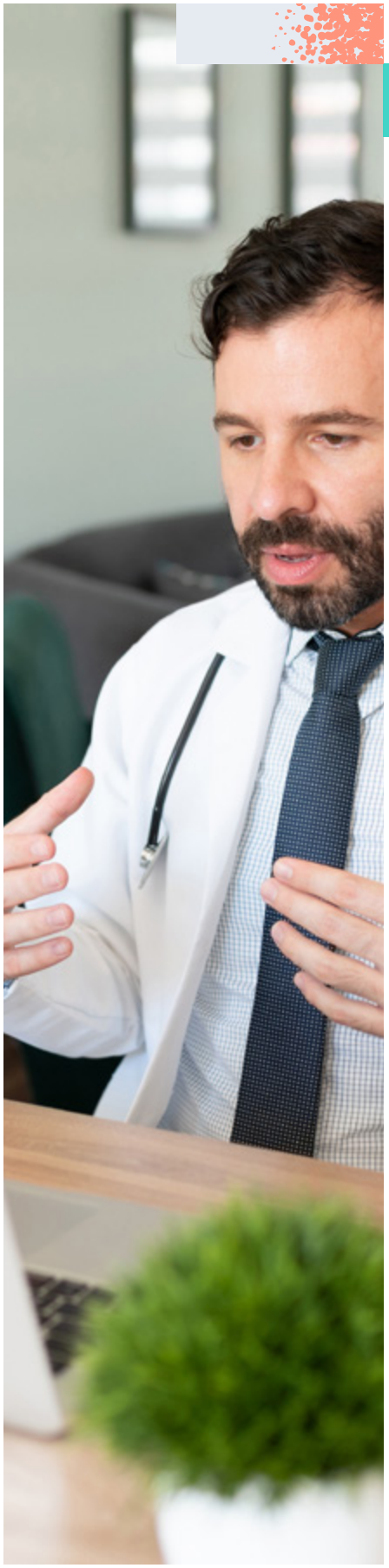
Avec la croissance de Doctolib, ses besoins en matière de rétention des données ont également augmenté. Auparavant, avec OpenSearch, Doctolib ne parvenait pas à allonger la rétention de ces données de manière rentable, ne conservant qu'un mois de logs. L'architecture évolutive d'Elastic a permis à Doctolib d'étendre cette période de rétention d'un mois à un an, tout en gérant 12 fois plus de données.

Avec 2 To de logs par jour et un besoin accru de rétention des données, Doctolib a investi dans Elastic pour faire évoluer ses opérations. Même si leurs coûts ont doublé, ils peuvent maintenant traiter 12 fois plus de données. Le coût par téraoctet a donc baissé de 83 %, ce qui rend la solution bien plus efficace et rentable que s'ils avaient utilisé OpenSearch. « Nous avons considérablement amélioré notre stratégie de rétention des données, en passant d'un mois à un an sans exploser les coûts », explique Jordan Langue.

Amélioration de la gestion des incidents et des performances des analystes

Grâce à ses fonctionnalités d'alertes automatisées et de machine learning, Elastic a amélioré la performance des analystes en sécurité de Doctolib. « Elastic a rendu nos analystes plus productifs en réduisant les tâches répétitives et les faux positifs, leur permettant ainsi de passer plus de temps à enquêter sur de véritables menaces plutôt que de les chercher », affirme Jordan Langue.

Grâce à Elastic, les alertes automatisées et la réduction de 50 % des faux positifs ont permis à l'équipe de moins se focaliser sur le temps moyen de détection (MTTD), leur donner l'opportunité de se concentrer sur les priorités : réduire le temps moyen d'enquête (MTTI) et de résolution (MTTR) des incidents de sécurité. Cette amélioration de la productivité a renforcé la posture de sécurité de Doctolib, leur permettant de gérer les menaces de manière plus proactive.



Intégration fluide et support continu d'Elastic

Le déploiement des solutions Elastic dans l'environnement cloud AWS de Doctolib s'est déroulé sans difficulté, grâce à l'équipe de support dédiée d'Elastic. De la configuration initiale à la gestion continue, l'équipe des services professionnels d'Elastic a fourni les conseils et l'expertise nécessaires pour assurer une transition en douceur depuis OpenSearch.

« L'équipe de support d'Elastic nous a aidés à voir le potentiel des solutions d'Elastic dans notre contexte », explique Othmane El Massari. « Ils ont personnalisé la solution pour qu'elle réponde à nos besoins et ont veillé à ce que la transition se passe sans accroc,» ajoute-t-il. Après cette intégration réussie, Doctolib a pu se concentrer sur l'essentiel : offrir des services de santé de haute qualité.

Capacités futures en IA pour une sécurité de pointe

Le partenariat entre Doctolib et Elastic a joué un rôle clé dans l'internalisation de son SOC. Il a permis la réduction des faux positifs de moitié, la prolongation de la rétention des données à un an, et l'amélioration de l'efficacité des analystes — tout en réduisant les coûts. Alors que Doctolib continue de se développer en tant que plateforme de santé numérique majeure en Europe, Elastic reste un allié essentiel dans son engagement pour une sécurité de haut niveau.

À l'avenir, Doctolib prévoit de renforcer l'utilisation des outils de machine learning et d'IA d'Elastic pour améliorer la détection des menaces et renforcer ses mesures de sécurité. « Le machine learning d'Elastic nous aide déjà à repérer des problèmes que nous aurions pu manquer auparavant », explique Othmane El Massari. « Nous prévoyons d'aller encore plus loin en utilisant l'IA pour identifier et stopper les menaces avant qu'elles ne deviennent des problèmes, » conclue-t-il.

> Elastic nous a donné la visibilité nécessaire pour répondre rapidement aux incidents et améliorer notre posture de sécurité, afin que nous puissions rester à la pointe de la technologie dans le secteur de la santé.

Othmane El Massari
Platform Security Engineer, Doctolib

