

elastic | Hermes

SUCCESS STORY

GERMANY | PROFESSIONAL SERVICES | ELASTIC SECURITY

Hermes Allemagne sécurise ses opérations logistiques critiques pour la moitié du prix de sa plateforme précédente sur site.

Hermes Allemagne, faisant partie du groupe Hermes, livre des colis et des marchandises aux domiciles et aux entreprises en Allemagne et à l'étranger. En tant que deuxième plus grande entreprise de logistique du pays, elle est officiellement répertoriée comme faisant partie de l'infrastructure critique (Kritis) de la nation.

KRITIS, abréviation de « Kritische Infrastrukturen » (Infrastructures critiques), fait référence aux services essentiels vitaux pour la sécurité publique, la sécurité et la stabilité économique. L'Office fédéral allemand de la sécurité de l'information (BSI) protège ces services contre les cybermenaces et autres risques grâce à des mesures de sécurité et à une collaboration public-privé.

 © 2025 Elasticsearch B.V. All rights reserved.



La migration vers Elastic Security dans le cloud a entraîné une réduction de 50 % des coûts

Elastic Security offre à Hermes Allemagne une plateforme de sécurité plus rapide et plus puissante à 50 % du prix de sa solution sur site précédente.



Bénéficier d'une visibilité complète sur 40 000 points de terminaison

Hermes Allemagne a facilement intégré les données provenant des scanners portatifs de ses 40 000 livreurs, améliorant ainsi la visibilité de l'ensemble de ses systèmes.



L'IA et le machine learning automatisent les workflows de sécurité

Hermes Allemagne utilise les capacités d'IA et d'apprentissage automatique d'Elastic Security pour automatiser les processus, ce qui permet à son équipe de sécurité de se concentrer sur des enquêtes plus complexes.

Comme l'explique Marco Uhl, ingénieur SIEM chez Hermes Allemagne, « Une sécurité efficace des systèmes est essentielle pour Hermes Allemagne. Ce n'est pas une question secondaire, mais cruciale pour notre entreprise et pour le pays. »

Avec la hausse des menaces de sécurité, Hermes Allemagne avait besoin d'une plateforme d'opérations de sécurité robuste et rentable pour naviguer dans le climat économique actuel. Leur ancienne plateforme tierce sur site posait des problèmes de performance et de coût, rendant difficile de stocker et de rechercher rapidement leurs vastes données de log de sécurité.

« C'était un environnement très complexe, avec des pannes fréquentes. Plus d'une fois, le cluster entier a pratiquement explosé sous nos yeux », se souvient Uhl. « C'était aussi très coûteux, avec des coûts de licence élevés, ainsi que les coûts opérationnels, tels que l'infrastructure et l'énergie, qui accompagnent son fonctionnement sur site. »

Poussée par ces contraintes, ainsi que par la stratégie d'entreprise visant à migrer toutes les infrastructures vers le cloud, Hermes Allemagne a recherché une plateforme de sécurité basée sur le cloud, évaluant un certain nombre de grands fournisseurs.

> « Nous avons choisi Elastic Security sur Google Cloud Platform, car nous préférions sa structure et son mode de traitement des données. Il est suffisamment flexible pour répondre à nos besoins et s'intègre facilement à d'autres systèmes et sources de données. »
>
> **Marco Uhl**
> Ingénieur SIEM, Hermes Germany

 © 2025 Elasticsearch B.V. All rights reserved.

Prise en charge d’une plateforme de sécurité haute performance et facile à utiliser déployée sur Google Cloud.

Hermes Allemagne a choisi Elastic plutôt que son déploiement actuel de SIEM en raison de problèmes de scalabilité avec la solution sur site et de désalignement avec la stratégie cloud-first d’Hermes. Le coût d’assurer la maintenance du SIEM existant et de la migration vers le cloud était également cinq fois plus élevé qu’avec Elastic.

Hermes Allemagne a également dû agir pour pouvoir gérer les données de 40 000 scanners de livraison portatifs, ce qui est crucial pour l’efficacité et la conformité aux normes KRITIS. Leur ancien SIEM était trop coûteux pour l’ingestion et la conservation efficaces de ces données. Elastic a proposé une solution rentable, leur permettant l’ingestion et l’analyse de données critiques sans coûts prohibitifs, garantissant la conformité réglementaire et l’excellence opérationnelle.

Hermes Allemagne s’est associée à l’équipe du support technique Elastic pour migrer vers Elastic Security. Cette collaboration a permis une installation fluide et une intégration harmonieuse des données, permettant à l’équipe de sécuirité d’Hermes Allemagne de profiter rapidement de la rapidité, de la fiabilité et des puissantes capacités de recherche de la plateforme.

> « Notre solution précédente aurait été deux fois plus chère en termes de licences uniquement. Avec Elastic Security sur Google Cloud Platform, nous avons tout-en-un : nous pouvons isoler les appareils, extraire des fichiers, interroger les processus, et nous bénéficions d’une protection des points de terminaison. C’est le package complet. »
>
> **Marco Uhl**
> Ingénieur SIEM, Hermes Germany

Les analystes de sécurité ont apprécié la simplicité d’utilisation d’Elastic Security, qui a permis d’éliminer le besoin de transfert manuel de données lors des investigations. Grâce à Elastic Common Schema, Hermes Allemagne peut désormais unifier et normaliser les données provenant de diverses sources, permettant ainsi aux analystes de visualiser et de comprendre rapidement le trafic réseau pour des investigations de sécirité efficaces.

ECS standardise la manière dont les données sont ingérées et analysées, ce qui facilite la compréhension des adresses IP de destination et du flux des connexions sur le réseau. Cette standardisation est essentielle pour une détection et une réponse précises et efficaces aux menaces, une fonctionnalité indispensable pour Hermes.

 © 2025 Elasticsearch B.V. All rights reserved.

Éliminer les angles morts grâce à une visibilité complète du système

Avec Elastic Security, Hermes Allemagne dispose d'une plateforme de sécurité complète pour une meilleure visibilité sur l'ensemble de son infrastructure. L'entreprise peut désormais ingérer et analyser des données provenant de sources auparavant négligées, telles que les scanners portatifs utilisés par son personnel de livraison, lui permettant ainsi de se protéger contre les menaces provenant de cette partie essentielle de ses opérations.

Lorsqu'Hermes Allemagne reçoit une alerte de sécurité, ses analystes exploitent la puissante fonctionnalité Elastic Timeline pour visualiser tous les événements liés de manière fluide. Grâce à un simple glisser-déposer de filtres, sans avoir à rédiger de requêtes complexes, ils peuvent enquêter rapidement sur les incidents. Ce processus intuitif leur permet de retracer le cheminement des connexions et d'identifier facilement toute activité suspecte.

Grâce à cette approche simplifiée, les analystes d'Hermes Allemagne peuvent rapidement identifier les faux positifs, filtrer les signaux parasites et reconnaître les véritables menaces de sécurité. En cas de menace réelle, ils suivent une procédure standard ou, pour les scénarios complexes, ils mobilisent une cellule de crise collaborative. Ceci garantit la sécurité de leurs systèmes et le bon fonctionnement de leurs services logistiques critiques.

Améliorer l'efficacité opérationnelle avec l'IA et le machine learning

Hermes Allemagne utilise également une gamme de capacités d'IA générative et de machine learning (ML) au sein d'Elastic Security pour rationaliser et améliorer la sécurité et renforcer ses capacités de sécurité avec le déploiement de l'Elastic AI Assistant pour tous ses analystes.

> Auparavant, le volume de données provenant de plus de 40 000 livreurs utilisant des scanners portatifs rendait leur traitement impossible. Maintenant, nous ingérons toutes ces données dans Elastic pour les analyser. Nous éliminons ainsi un point aveugle critique et nous pouvons répondre à nos exigences en tant qu'organisation Kritis.
>
> **Marco Uhl**
> Ingénieur SIEM,
> Hermes Germany



 © 2025 Elasticsearch B.V. All rights reserved.

elastic

Connecté de manière sécurisée à Google Gemini, le LLM de choix pour Hermes Allemagne, l'Elastic AI Assistant for Security leur permet de connecter en toute sécurité toutes leurs données privées avec le grand modèle de langage, permettant aux analystes de l'entreprise de résoudre les problèmes plus rapidement grâce à des interactions en langage naturel. L'Elastic AI Assistant peut aider les analystes à interpréter rapidement les messages de log et les erreurs, à optimiser le code, à rédiger des rapports et, en fin de compte, à sécuriser les systèmes de l'entreprise de manière plus efficace et efficiente.

Attack Discovery permet à Hermes Allemagne de détecter et de regrouper automatiquement les comportements suspects et les menaces potentielles en utilisant l'apprentissage automatique avancé et le renseignement sur les menaces contextuelles. Cela réduit la fatigue des alertes en triant des centaines d'alertes pour se concentrer sur celles qui sont importantes, permettant aux équipes de sécurité de se concentrer sur les menaces critiques. Le processus rationalisé accélère les temps de réponse, permettant à l'équipe de sécurité de prendre des mesures immédiates et éclairées et d'améliorer la sécurité globale.

> « Grâce à Elastic AI Assistant pour Security, nous pouvons aider à alléger la pression de nos analystes en leur permettant d'accomplir leur travail plus facilement et de consacrer leur temps à des cas plus complexes. »
>
> **Marco Uhl**
> Ingénieur SIEM, Hermes Germany

Garantir l'avenir des infrastructures critiques de Hermes Allemagne.

Alors qu'elle étend son utilisation d'Elastic Security pour protéger ses opérations, Hermes Allemagne envisage d'autres intégrations en ML et IA, tout en déployant Elastic Agent dans son infrastructure. Cela lui donnera une visibilité système plus approfondie, ainsi que des capacités d'isolement en un clic pour une réponse aux incidents. Elastic Agent et les API ouvertes de la plateforme permettront également à Hermes Allemagne d'automatiser davantage de flux de travail de sécurité et de s'intégrer de manière fluide avec d'autres systèmes, l'aidant à faire face de manière proactive aux menaces émergentes alors que l'entreprise travaille à sécuriser l'avenir de ses opérations logistiques critiques.

Commencez votre essai gratuit

Découvrez comment votre entreprise peut bénéficier d'Elastic dans le Cloud, grâce à un essai gratuit de 14 jours.

Commencer

 © 2025 Elasticsearch B.V. All rights reserved.