

SUCCESS STORY

FRANCE | TRAVEL & TRANSPORTATION | ELASTIC SECURITY

ID Logistics sécurise ses opérations mondiales et réduit ses coûts de plus de 60 % avec Elastic Security sur Elastic Cloud

Fondé en 2001, ID Logistics est un acteur mondial de la logistique, spécialisé dans la logistique contractuelle, le transport de marchandises et les solutions de gestion de la chaîne d'approvisionnement pour des entreprises majeures du retail, du luxe et de la santé. Présente dans 19 pays et doublant son chiffre d'affaires tous les cinq ans, l'entreprise a connu une croissance rapide, notamment par fusions et acquisitions, ce qui a généré un défi majeur en matière de cybersécurité : gérer un paysage IT particulièrement diversifié et hétérogène.

 © 2025 Elasticsearch B.V. All rights reserved.



Réduction de plus de 60 % des coûts de gestion des données

Grâce à la gestion du cycle de vie des données et aux fonctionnalités avancées d'Elastic, ID Logistics a considérablement réduit ses coûts liés aux logs.



Accélération de la détection des menaces, de plusieurs heures à quelques minutes

Grâce à la plateforme unifiée d'Elastic Security, qui regroupe logs, métriques et données d'observabilité, ID Logistics détecte désormais les anomalies en quelques minutes, contre plusieurs heures voire plusieurs jours auparavant.



Unification des données sécurité et IT Ops dans un environnement mondial hétérogène

ID Logistics centralise les logs de sécurité et d'infrastructure issus de 19 pays avec Elastic Security, mutualise les ressources et aligne les équipes sécurité et IT.

Pour Cécile Bardou, CISO, et Hamza Kondah, Secops lead, ce défi était double. D'une part, l'entreprise devait faire face à un environnement de menaces en constante évolution et de plus en plus sophistiqué, tout en intégrant des systèmes disparates et des niveaux de sécurité variables à chaque nouvelle acquisition. « Nous réalisons de nombreuses fusions et acquisitions, et lorsque nous rachetons une entreprise, nous héritons aussi de son passé, avec les menaces et les mauvaises pratiques associées », explique Hamza Kondah. « Il est difficile d'harmoniser rapidement toutes les entités dans un cadre de sécurité mature. »

D'autre part, la solution SIEM existante manquait de flexibilité et de maîtrise opérationnelle pour accompagner la croissance du groupe. Elle limitait la capacité d'ID Logistics à intégrer rapidement de nouvelles entités et leurs systèmes hétérogènes. L'entreprise a compris qu'elle devait dépasser le modèle SIEM traditionnel et adopter une plateforme capable de devenir un véritable hub de sécurité et de gestion des logs piloté par la donnée. Cette plateforme devait unifier la télémétrie issue d'un large éventail de pare-feux, de solutions de sécurité et de logs d'infrastructure à l'échelle mondiale, afin d'offrir à l'équipe interne la vitesse et la visibilité nécessaires pour faire évoluer le SOC (Security Operations Command) plus rapidement que le rythme des acquisitions.

> « Nous ne voulions pas seulement renforcer la sécurité, mais aussi augmenter la valeur ajoutée de nos données. Nous avions besoin d'une solution mature, dotée de capacités avancées, nous permettant de combiner données d'observabilité et données de sécurité pour éclairer nos décisions. »
>
> **Hamza Kondah**
> Secops lead, ID Logistics

 © 2025 Elasticsearch B.V. All rights reserved.

Unifier les données et la détection sur Elastic Cloud

ID Logistics a choisi Elastic car il s'agissait de l'outil le plus efficace pour faire évoluer rapidement son SOC, en standardisant les données de sécurité et d'infrastructure à l'échelle de son environnement IT mondial. En migrant vers Elastic Cloud début 2025, l'entreprise a bénéficié d'un déploiement simple et rapide.

En exécutant Elastic Security sur Elastic Cloud, ID Logistics bénéficie d'une plateforme stable et évolutive. L'auto-scaling ajuste automatiquement la capacité pour absorber les pics de données, garantissant la continuité d'activité. La sécurité au niveau de la stack assure quant à elle la protection et la mise à jour continue de l'infrastructure sous-jacente, réduisant la charge administrative.

> « Nous avons migré vers Elastic Cloud en seulement deux jours, sans interruption de service ni de détection. C'était extrêmement simple. »
>
> **Cécile Bardou**
> CISO, ID Logistics

Standardiser les données pour une détection homogène

ID Logistics attribue l'amélioration significative de ses capacités de détection à la base technique d'Elastic. Pour exploiter des données issues d'infrastructures multi-pays très diverses, l'équipe a adopté le système Elastic Common Schema, qui standardise les logs afin que les règles de sécurité fonctionnent de manière cohérente sur l'ensemble des sources de données. Cette standardisation permet de créer une règle de détection une seule fois et de l'appliquer partout, ce qui est essentiel pour détecter de manière fiable des menaces critiques comme les ransomwares ou les accès non autorisés, quel que soit l'origine des logs. Ce processus fait gagner du temps et réduit le risque de passer à côté d'une menace dans un environnement hétérogène.

ID Logistics a également simplifié la collecte des logs et renforcé l'évolutivité du système en remplaçant des architectures historiques complexes par Elastic Agent et Fleet, avec une gestion centralisée. Cette approche permet aux équipes d'exploiter des outils puissants, comme le langage de requête Elastic et OSQuery, pour mener des investigations approfondies et rapides sur l'ensemble des serveurs et systèmes d'infrastructure critiques.

Grâce au Cross-Cluster Search et au Cross-Cluster Alerting, ID Logistics a pu migrer progressivement depuis son ancien SIEM en connectant les nouveaux et anciens clusters jusqu'à la purge des archives. L'entreprise centralise désormais la gestion des données et des alertes entre ses clusters européens et américains, ce qui aligne les équipes sécurité et IT Ops autour des mêmes données et accélère la réponse aux incidents.

 © 2025 Elasticsearch B.V. All rights reserved.



« Elastic Security repose sur un moteur fiable et prend en charge des langages de requête avancés, ce qui rend ses capacités de détection très puissantes. Cela nous a permis de couvrir des cas qu'aucun autre SIEM ne pouvait traiter. »

Hamza Kondah
Secops lead, ID Logistics

Maximiser la valeur grâce au contrôle des coûts et à l'AIOps

Un bénéfice majeur de la migration a été son impact immédiat sur le FinOps. Elastic a permis à ID Logistics de maîtriser l'ensemble du cycle de vie des données, un point essentiel lorsque le volume de logs augmente en permanence. L'utilisation de fonctionnalités avancées comme LogsDB a permis de réduire significativement les coûts de stockage et de requête des logs moins fréquemment consultés.



« Elastic est l'une des seules plateformes qui permet de maîtriser le cycle de vie des données. C'est extrêmement puissant, car cela nous aide à contrôler nos coûts. »

Hamza Kondah
Secops lead, ID Logistics

Résultat : une réduction impressionnante de 65 % des coûts de gestion des logs, tout en collectant davantage de données de sécurité et d'infrastructure pour un coût équivalent à la solution précédente.

Au-delà des économies, la plateforme a considérablement accéléré les capacités de détection. ID Logistics utilise désormais Elastic Machine Learning pour la détection d'anomalies et déploie l'Elastic AI Assistant pour interroger les logs en langage naturel. Le temps de détection est passé de plusieurs heures, voire jours, à cinq minutes seulement, réduisant significativement la fenêtre d'exposition lors d'une attaque active.



« L'intégration et l'expérience utilisateur de l'AI Assistant sont exceptionnelles. C'est un outil très utile pour les analystes : il les aide à prioriser les alertes critiques, interroger les logs et identifier rapidement les données pertinentes. »

Hamza Kondah
Secops lead, ID Logistics

 © 2025 Elasticsearch B.V. All rights reserved.

Elastic a également renforcé de manière significative la posture de sécurité proactive de l'entreprise. L'équipe sécurité s'appuie sur la Threat Intelligence Platform intégrée d'Elastic, qui centralise différentes sources de renseignement et met à disposition des tableaux de bord dédiés au suivi. Elle exploite aussi les fonctionnalités de gestion des vulnérabilités, qui automatisent le suivi des mises à jour et l'analyse des vulnérabilités.

Sécuriser l'avenir de la logistique mondiale

Alors qu'ID Logistics poursuit l'intégration de ses opérations sur la plateforme Elastic, l'entreprise prévoit d'approfondir son observabilité, notamment avec l'APM pour ses applications web, et d'élargir le périmètre de détection en intégrant les logs issus de nouvelles solutions IAM et PAM.

Avec Elastic comme référentiel central de données, ID Logistics dispose désormais d'une plateforme de sécurité autonome, évolutive et optimisée en coûts, prête à accompagner son expansion mondiale.

> « Elastic est aujourd'hui au cœur de nos systèmes de détection des menaces et de supervision des performances IT. C'est devenu l'outil de référence pour la donnée à l'échelle du groupe. Utiliser Elastic est désormais un réflexe chez ID Logistics. »
>
> **Cécile Bardou**
> CISO, ID Logistics



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.