

elastic | S3NS

SUCCESS STORY

FRANCE | PROFESSIONAL SERVICES | ELASTIC SECURITY

S3NS et Elastic assurent la sécurité souveraine et fiable du cloud pour la France

« Elastic Security joue un rôle essentiel pour aider S3NS à établir la confiance avec les clients, en particulier grâce à la surveillance proactive de la sécurité et à la réponse aux incidents. »

Victor Vuillard
CTO et CISO, S3NS

 © 2025 Elasticsearch B.V. All rights reserved.

Scales permet de créer une plateforme SIEM souveraine

Avec Elastic, S3NS sécurise des milliers de serveurs et de conteneurs en unifiant de grands volumes de données liées à la sécurité.

Améliore la détection des menaces

Les équipes de sécurité S3NS détectent et enquêtent sur les menaces en temps quasi réel grâce à des tableaux de bord intégrés, des requêtes programmées et des outils d'alerting.

Fournit une plateforme pour l'innovation en matière d'IA

Avec Elastic, S3NS peut réduire les faux positifs et améliorer la priorisation des alertes grâce à l'accès aux capacités de machine learning et d'IA.

Elastic Security permet à S3NS de respecter les normes de confidentialité et de security des données dans son offre souveraine de cloud

S3NS est une coentreprise entre Thales et Google Cloud, créée pour répondre à un besoin crucial de solutions cloud souveraines en Europe. Avec pour mission de fournir des infrastructures fiables aux organisations traitant des données sensibles — telles que les organismes gouvernementaux, les prestataires de santé et les opérateurs d'infrastructures critiques — S3NS combine la scalabilité et l'innovation de Google Cloud avec l'expertise en cybersécurité de classe mondiale de Thales.

Cette offre pionnière inclut une région souveraine de Google Cloud Platform exploitée indépendamment de Google. Appelée « Trusted Cloud », elle fonctionne dans trois centres de données français S3NS sur du matériel accessible, exploité et contrôlé uniquement par le personnel S3NS. Au cœur de cette solution, Elastic Security joue un rôle crucial dans la protection la plus élevée des données pour les organisations françaises.



 | © 2025 Elasticsearch B.V. All rights reserved.

elastic

Souveraineté et fonctionnalité : le meilleur des deux mondes

Les organisations françaises ont longtemps dû faire face à un compromis entre souveraineté et fonctionnalité. D'un côté, les fournisseurs cloud mondiaux proposent une efficacité des coûts, une scalabilité et des outils d'IA de pointe. De l'autre, les prestataires locaux privilégient la souveraineté, mais manquent souvent de l'ampleur, de la gamme de services et de l'efficacité économique requises par les clients ambitieux.

Avec Trusted Cloud, les organisations bénéficient du meilleur des deux mondes : l'indépendance opérationnelle et la technologie de pointe. Cela inclut une cybersécurité de pointe orchestrée par une plateforme SIEM, capable de gérer d'énormes volumes de logs et de données de télémétrie.

Il n'y avait aucune place pour le compromis en matière de sécurité. « Nous avions besoin d'un partenaire de sécurité avec une solution que nous pouvions déployer sur site pour protéger notre plateforme Kubernetes en tant que service autogérée », déclare Victor Vuillard, CTO et CISO de S3NS. « Nous avons également recherché des outils avancés pour soutenir la détection, l'enquête et la réponse aux menaces. »

Elastic Security : la colonne vertébrale d'un cloud souverain

Lorsqu'il a fallu sélectionner un partenaire, Elastic Security s'est démarqué pour de nombreuses raisons, notamment son exceptionnelle scalabilité. S3NS exécute des milliers de serveurs, hébergeant souvent des milliers de conteneurs. Le volume de données liées à la sécurité est énorme et en croissance. L'architecture d'Elastic permet à S3NS de scaler horizontalement et de manière rentable tout en assurant la maintenance des performances élevées. « D'autres plateforme SIEM ont du mal à scaler sans spécialisation des données. Il est important de noter qu'Elastic a évolué au-delà d'un lac de données. La plateforme possède désormais les capacités de traitement et d'exécution d'un SIEM, » déclare Vuillard.

La transparence était une autre fonctionnalité gagnante. S3NS utilise actuellement la version commerciale d'Elastic Security, mais la disponibilité d'une version open source a permis à Vuillard et à son équipe d'inspecter la logique de noyau et l'implémentation, s'alignant sur les exigences strictes de l'organisation en matière de code et d'examen de l'infrastructure. En fait, les API open d'Elastic et sa documentation claire ont permis un contrôle programmatique complet sur le déploiement.

Mais c'est la polyvalence d'Elastic à travers de multiples cas d'utilisation de sécurité qui a fait la différence. « Elastic excelle dans la gestion des données, » déclare Vuillard. « Nous l'utilisons pour centraliser les logs de toute notre infrastructure, y compris le calcul, le réseau et les outils de security tiers. » S3NS a également intégré des renseignements sur les menaces externes de Thales et d'autres fournisseurs avec Elastic pour identifier les indicateurs de compromission, tels que des adresses IP suspectes ou des signatures de malware.

 © 2025 Elasticsearch B.V. All rights reserved.

De plus, les équipes de security de S3NS utilisent les dashboard intégrés, les requêtes programmées et les outils d'alerting d'Elastic Security pour détecter et sonder les menaces en temps quasi réel. Ces investigations sont traçables et approfondies, grâce aux outils de chronologie d'Elastic et à ses capacités de corrélation approfondie.

Une IA avancée prête à l'emploi

En raison de son modèle d'isolement des locataires, S3NS ne peut pas accéder aux charges de travail ou aux données des clients. Cependant, il surveille les signaux d'infrastructure plus larges, comme le trafic sortant, et corrèle ces signaux au renseignement sur les menaces. Si, par exemple, l'environnement d'un locataire se connecte à un serveur de commande et de contrôle connu, Elastic signale ce comportement, permettant à S3NS d'informer le client et de soutenir son enquête.

Le déploiement d'Elastic Security positionne également S3NS pour l'innovation future. L'équipe explore les capacités de machine learning d'Elastic pour la détection des anomalies et l'IA afin d'aider à réduire les faux positifs, détecter les anomalies et prioriser les alertes. Ces outils alimentés par l'IA ne sont pas considérés comme des remplaçants de l'analyse humaine, mais comme des multiplicateurs de force, augmentant la précision et l'efficacité de la détection des menaces ainsi que la réponse nécessaire.

Vuillard souligne que la stratégie de S3NS va au-delà de la simple offre des services gérés par Google au sein de l'écosystème Google Cloud. Il prévoit également d'intégrer des technologies et services provenant de fournisseurs de logiciels indépendants. « Nous prévoyons de fournir une offre Elastic améliorée sur notre future infrastructure cloud, en s'adressant aux clients français et européens qui privilégient la souveraineté », déclare-t-il.

> « Elastic continue de soutenir les opérations cloud plus larges de S3NS au-delà de la cybersécurité. Nous apprécions particulièrement les mises à jour fréquentes qui s'alignent sur l'évolution constante du paysage de notre entreprise. »
>
> **Victor Vuillard**
> CTO et CISO,
> S3NS

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.