

Data Science et IA pour accélérer votre équipe cyber

Accélérez vos investigations et votre réponse à incidents.
Accédez à une vue unifiée de vos données de sécurité.
Donnez à votre équipe les moyens de prendre des décisions fiables.

La cybersécurité se trouve aujourd'hui dans une situation paradoxale : la croissance du volume de données de sécurité est exponentielle, tandis que les ressources humaines adéquates pour les gérer de manière efficace sont en pénurie.

Naviguer dans ce labyrinthe de données et d'outils devient un véritable défi pour les équipes de sécurité, tout en étant pourtant essentiel pour garantir une posture de sécurité optimale.

Malizen s'attaque à ce paradoxe en offrant à vos analystes une vue d'ensemble sur toutes leurs données de sécurité pour en accélérer leur exploration.



Malizen est l'interface unifiée pour l'analyse de vos données de sécurité. Elle vous permet de connecter toutes vos sources de données et de les explorer rapidement et en contexte grâce à un environnement d'investigation visuel intelligent et un assistant IA.

Bénéfices

Décidez et agissez plus vite

Obtenez rapidement les réponses dont vous avez besoin dans le cadre de vos investigations, votre threat hunting et vos réponses à incidents.

Plus loin dans vos investigations

Datamining et IA vous permettent de tirer parti du grand volume de données à votre disposition, accélérant l'identification d'un plus grand nombre d'indicateurs de compromission.

Augmentez votre potentiel humain

Seniors ou juniors, vos analystes peuvent réaliser leurs investigations à travers différents outils sans avoir à devenir experts de chaque système individuellement.

x4

Vitesse de threat hunting

+25%

Capacités opérationnelles

+100%

Indices d'attaques identifiés

Optimisation de Détection

Maximisez votre investissement SIEM. Tirez parti de tous vos efforts de threat hunting pour mettre à jour régulièrement et simplement vos règles de détection.

Threat Hunting

Le hunting visuel et interactif permet de repérer des anomalies dans vos logs et d'identifier plus rapidement les nouvelles menaces.

Réponse à Incidents

Réagissez plus vite aux incidents grâce à une normalisation assistée et une ingestion de logs optimisée qui embarque le contexte de la détection.

Qualification d'alertes

Assurez l'efficacité du triage et réduisez la fatigue d'analyse avec une contextualisation des alertes facilitée, sans devoir affronter les mêmes requêtes à répétition.



Agrégation & Corrélation

Exploitez toutes vos sources de données.

Connectez toutes vos données

Nos connecteurs vous permettent de collecter des données provenant de n'importe quelle source (SIEM, fichiers, logs, CMDB, AD, CTI, XDR..).

Investiguez en contexte

L'enrichissement des données à la volée à partir de sources contextuelles permet d'accélérer les temps d'analyse.



Investigation No-Code

Glissez. Déposez. Explorez. Comprenez.

Explorez sans requêter

Malizen remplace les lignes de commande complexes par une interface intuitive et des visualisations interactives.

Fini le dashboarding

Malizen vous évite de créer et de maintenir de nombreux tableaux de bord. Les visualisations s'adaptent automatiquement aux données que vous explorez.



Collaboration

Tirez parti de la connaissance collective.

Mobiliser toute votre équipe

Malizen permet le partage instantané des investigations entre membres de l'équipe. Il est alors possible de trouver rapidement les bons experts au bon moment.

Créez votre base de connaissance

Votre historique d'investigations est un trésor de connaissances à partager avec votre équipe et à exploiter par votre copilote.



Assistant IA

Laissez vous guider par notre intelligence embarquée.

Fini les angles morts

Notre IA vous guide tout au long de votre analyse, en vous proposant les bonnes pistes à explorer et en vous évitant de perdre du temps sur des impasses.

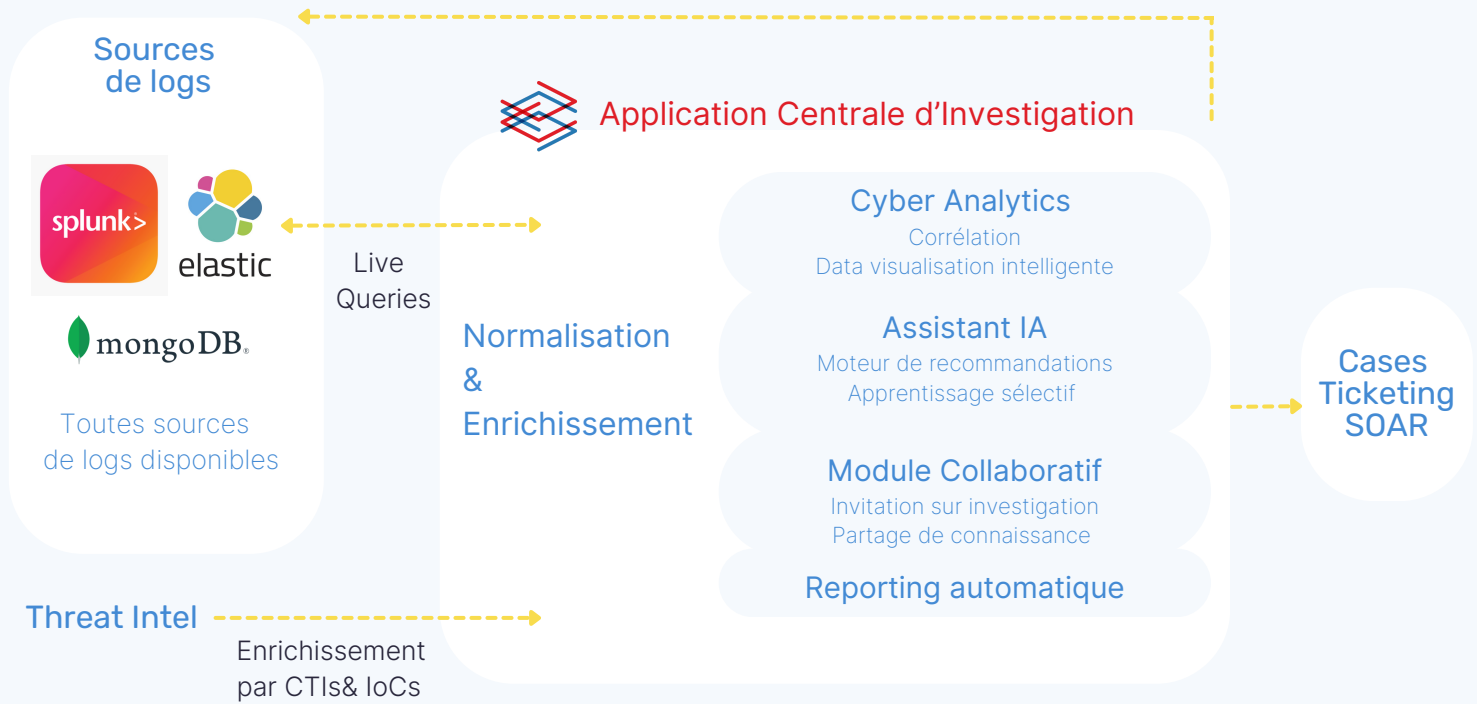
Des analystes accélérés

Votre copilote suggère des techniques et tactiques MITRE ATT&CK pertinentes pour qualifier chaque étape de l'investigation.

Reporting automatisé

Votre copilote suit chaque investigation et son contexte, ce qui lui permet de générer automatiquement des rapports complets adaptés à votre audience.

Optimisation des règles de détection



La sécurité fait partie de notre ADN.
Elle est intégrée dans tout ce que nous faisons.

Sécurité de l'application

Cycle de développement sécurisé : analyse statique systématique, gestion des vulnérabilités dans les dépendances en cycle court, tests unitaires fonctionnels, end-to-end et non-régression, fuzzing régulier ...

Sécurité des données

Chiffrement TLS des communications entre les machines des analystes et Malizen ainsi que les communications entre Malizen et sources de données. Connexion plateforme par VPN.

Sécurité physique

Confidentialité, disponibilité et intégrité de vos données. Malizen opère dans un datacenter certifié ISO 27001, ISO 50001, et TIER 3 (Institut Uptime). Notre plateforme multi-cloud permet un déploiement SecNumCloud.

Fonctionnalités produit

Gestion des politiques d'accès et de partage grâce à des options d'authentification et de connexion unique (SSO). Nous proposons des restrictions IP pour paramétrer les accès aux services Malizen.

DEPLOIEMENT SAAS

DEVELOPPÉ ET HERBERGÉ EN FRANCE

SUPPORT 8X5



Fondée en 2020 par des experts en cybersécurité issus de la R&D de la DGA et d'Inria, Malizen s'engage à transformer la manière dont les analystes opèrent au sein des SOC et des CERT.

Notre plateforme avancée intègre toutes les données de sécurité disponibles pour offrir une vue d'ensemble complète, facilitant l'investigation, la réponse et la défense contre les menaces cyber. Nous privilégions la collaboration au sein de votre équipe et offrons une assistance continue grâce à notre copilote cyber.

Nous sommes fiers de compter parmi nos clients des organisations de défense, des organismes d'importance vitale et des prestataires de services de cybersécurité.

