# GATEWATCHER
# NDR PLATFORM

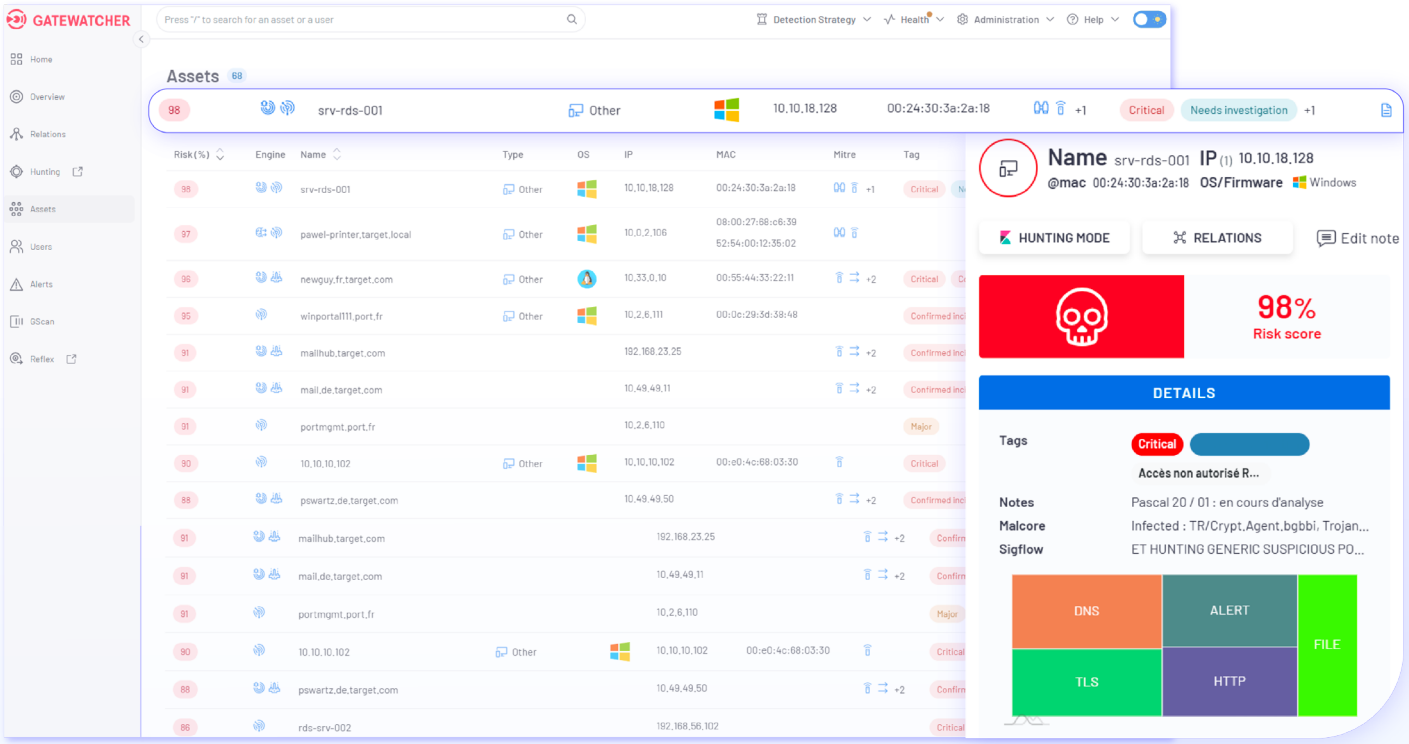
# *Network never lies*

## Fondez vos décisions sur *des données réseau irréfutables_*

**Une capture exhaustive pour des décisions précises**
Renforcez la décision grâce à une analyse transversale et une visibilité réseau approfondie incluant les comportements des infrastructures IT, OT et Cloud avec une surveillance des usages matériels, utilisateurs et applicatifs.

**Un verdict IA étayé pour réduire l'incertitude**
Combinez des preuves irréfutables issues d'une inspection réseau approfondie. Elles alimentent une analyse contextuelle IA orchestrée et exhaustive, sans laisser aucun angle mort aux acteurs malveillants.

**Une confiance opérationnelle qui sécurise votre continuité d'activité**
La corrélation autonome et transverse de multiples signaux issus des données réseau confirme rapidement toute attaque. Elle déclenche une réponse adaptée, sans dépendre d'analyses manuelles longues et complexes.




## Des données de qualité pour *des décisions exécutable_*

> ***Télémétrie haute fidélité pour des décisions précises***
Constituez automatiquement un inventaire complet des actifs réseau (IP, MAC, hostname, OS) et des flux utilisateurs, afin de relier chaque alerte à l'actif et à l'utilisateur impactés, base indispensable d'une décision centrée sur les assets.

> ***Extraction de contenu pour des preuves plus solides***
Reconstituez des fichiers en transit (HTTP, SMTP, SMB, FTP,...) qui sont analysés en temps réel par une combinaison de moteur de détection. Ils fournissent ainsi l'intégralité des preuves et garanties essentielles pour un scoring et verdict décisionel étayé.

> ***Contexte enrichi, même si le trafic est chiffré***
Collectez des données détaillées (horodatage, source/destination, protocole, contexte applicatif, empreintes, SNI, JA3...), pour corréler et analyser efficacement même lorsque le contenu n'est pas accessible.

> ***Visibilité complete dès le déploiement***
Bénéficiez d'une large couverture réseau pour que le SOC obtienne rapidement une visibilité complète et prenne des décisions dès le premier jour, à partir de signaux fiables et haute fidélité.

# *From noise to action*


## Le pouvoir de décider à travers tous *vos signaux de sécurité_*

### Propulser un contexte riche

- **Des signaux multi-sources unifiés**
  Décloisonnez l'ensemble de vos solutions de défense (NDR, SIEM, EDR, Cloud and identity security providers...) afin d'obtenir à tout instant des décisions adaptées à votre contexte opérationnel à tout instant
- **Des décisions automatiques**
  Bénéficiez d'une analyse orchestrée, fondée sur une contextualisation transversale tant technique que métier
- **Une résilience renforcée**
  Neutralisez chaque menaces avec certitude par des actions issues de preuves concrètes et auditables

### Décider en toute confiance

- **Des actions adaptées et précises**
  Transformez une analyse multi-sources en plan d'action immédiatement exécutable
- **Un pilotage sous contrôle humain**
  Gardez une maitrise totale sur tout le processus de neutralisation d'une menace, tout en ayant la capacité de l'automatiser à 100%
- **Un contrat de confiance cyber**
  Collectez l'ensemble des anomalies et preuves de compromission pour une amélioration continue de votre cyber résilience

## *Des bénéfices immédiats*

95% De réduction du bruit d'alerte + 10x Triage accéléré + 60% Réduction des coûts = Réduire Ambiguïté & fatigue du SOC + Temps moyen de décision (*MTTD*) < 5 min

- > *Agregation des alertes, réduction du bruit*
  Transformez les flots d'alertes en un ensemble priorisé et exploitable de décisions actionnables, et ainsi focaliser l'investigation du SOC sur l'essentiel.
- > *Décision centrée sur les assets*
  Traitez en priorité les assets les plus à risque afin que les équipes concentrent leurs efforts là où l'impact potentiel serait le plus élevé.
- > *Enrichissement et contextualisation automatisés*
  Agrégez le renseignement sur les menaces ainsi que le contexte technique et métier pour des prises de décision plus précises.
- > *Décision assistée par l'IA*
  Appuyez vos décisions sur un verdict clair assorti d'un niveau de confiance et de recommandations concrètes sur les prochaines actions de remédiation.
- > *Triage et réponse accélérés*
  Standardisez les workflows d'investigation et réduisez le temps de confinement (MTTR) grâce à des décisions fiables et cohérentes.
- > *Gouvernance et reporting prêts à l'emploi*
  Disposez d'une chaine de raisonnement explicable et d'un reporting multi-formats pour un pilotage du risque auditable.

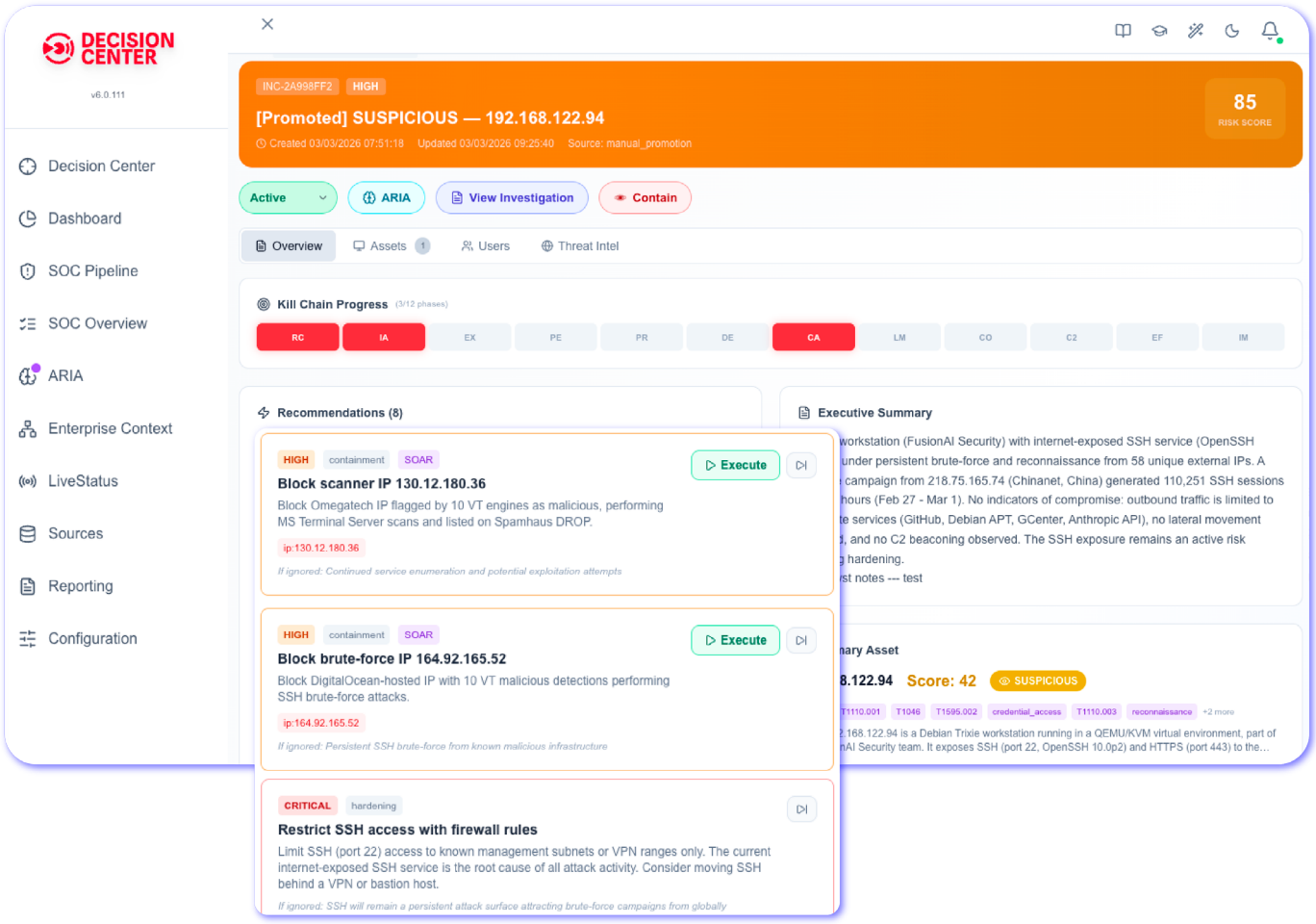
# Ahead of threats

## Transformez des détections *en décisions_*

**Une réduction du bruit pour plus d'actions**
Convertissez une surcharge d'alertes en une liste d'actifs à risque priorisés afin de produire des décisions immédiatement exécutables, en automatisant la qualification et le triage.

**Des détections multiples pour un verdict IA unique.**
Regroupez automatiquement par actifs l'intégralité des détections pour produire un verdict IA unique, des priorités claires et un plan d'action complet.

**Des décisions étayées, pas juste des alertes supplémentaires**
Détectez l'intrusion dès les premiers signaux faibles, puis laissez l'IA collecter automatiquement les preuves et prioriser pour une réaction SOC plus rapide et une charge réduite.




## Quand la détection est précise *les décisions deviennent simples_*

> ***Détection combinée pour une couverture complète de la kill chain***
Combinez des moteurs complémentaires (signature, comportemental, inspection de contenu et de code, renseignement de menace) pour répondre de bout en bout aux dernières techniques d'attaques.

> ***Alertes riches en preuves, pas de simples signaux techniques***
Fournissez des artefacts et du contexte enrichis afin que l'investigation démarre avec des preuves, plutôt qu'avec des suppositions.

> ***Réglage fin des capacités de détection pour un minimum de faux positifs***
Ajustez finement les paramètres de détection (seuils, fréquences, contexte) pour les aligner sur les environnements réels et réduire de façon déterminante les faux positifs.

> ***Intégration fluide à votre écosystème pour une efficacité totale***
Pilotez la réponse via des playbooks automatisés et des actions de remédiation, pour transformer la détection en résultats cohérents, traçables et auditables en renfort de vos solutions de défenses existantes.

# DES DÉCISIONS RAPIDES ET SANS COMPROMIS

## *Pourquoi trier du bruit quand vous pourriez piloter des décisions ?_*

Decision Center transforme des signaux **fragmentés en un framework décisionnel** : des verdicts structurées, **traçables, auditables et directement actionnables.**

En corrélant des alertes multi-sources centrées **Asset** (contexte + historique + renseignement de menace), il élimine le bruit à grande échelle et délivre des **analyses cohérentes et explicables** pour que vos équipes agissent avec confiance au lieu de débattre d'hypothèses.

Decision Center exécute en continu une chaîne
**COLLECTER → DÉDUPLIQUER → ENRICHIR → ANALYSER → CONCLURE** pour convertir un très grand volume de télémétrie en une file priorisée d'assets à risque, et non une liste infinie d'alertes.
Résultat : **faux positifs supprimés, triage en quelques secondes,** et **confinement accéléré** via des parcours de réponse intégrés.

## *Combien de temps passez-vous à reconstituer le contexte complet avant de débuter votre investigation et de pouvoir décider ? _*

Les solutions de sécurité génèrent des volumes massifs de signaux réseau, identité, cloud et menaces. Pris isolément, ils créent du bruit et obligent chaque organisation à reconstruire unitairement et manuellement le contexte. **Decision Center transforme cette surcharge en résultats réellement actionnables** en unifiant, dédupliquant et corrélant des signaux multi-sources dans un flux de décision unique, centré sur l'asset. Cela vous permet ainsi d'agir sur ce qui compte, pas sur ce qui semble faussement le plus critique.

**La singularité du Decision Center** tient en sa capacité à qualifier le risque en temps réel. **Il intègre en continu le contexte métier de nos clients :** criticité de l'asset, son usage en environnement de production vs. non-production, son exposition corrélée avec les renseignements de menaces et de réelles preuves comportementales. Le résultat : le verdict est structuré puis étayé par l'intégralité, avec un niveau de confiance et des recommandations et d'actions claires, intégrant l'impact réel pour l'activité.

Et tout cela reste sous votre contrôle. **Decision Center peut recommander, orchestrer et accélérer la réponse,** mais l'exécution demeure gouvernée par le SOC, avec de points de validation, une supervision par les analystes et la traçabilité complète des décisions. Vous gagnez en vitesse et en cohérence, en délivrant des actions de sécurité explicables, auditables et défendables mais en conservant le contrôle.

## *Et si la décision la plus rapide était aussi la meilleure ?_*

Au lieu d'obliger les analystes à échanger du temps contre de la confiance, **Decision Center corrèle et contextualise les signaux dans un espace de décision unique**, applique une qualification du risque tenant compte du contexte métier, et délivre des décisions cohérentes et explicables. Résultat : **un confinement plus rapide en cas de compromission,** moins d'erreurs, et des décisions que vous pouvez assumer.

Agir trop vite, c'est risquer la perturbation. Enquêter trop longtemps, c'est augmenter l'exposition. **Decision Center supprime ce dilemme** en transformant des signaux fragmentés entre réseau, identité, cloud et exposition en décisions structurées s'appuyant sur **des preuves et un scoring de confiance lié au contexte métier.** Vous savez quoi faire et conservez le contrôle.

**Découvrez nos cas d'usage**

gatewatcher.com

# Cybersecurity for business *serenity_*

*Explorez nos solutions...*


contact@gatewatcher.com

+33 (0)1 44 51 03 93

Campus Cyber • Puteaux, France

GATEWATCHER

GATEWATCHER Official

@GATEW4TCHER