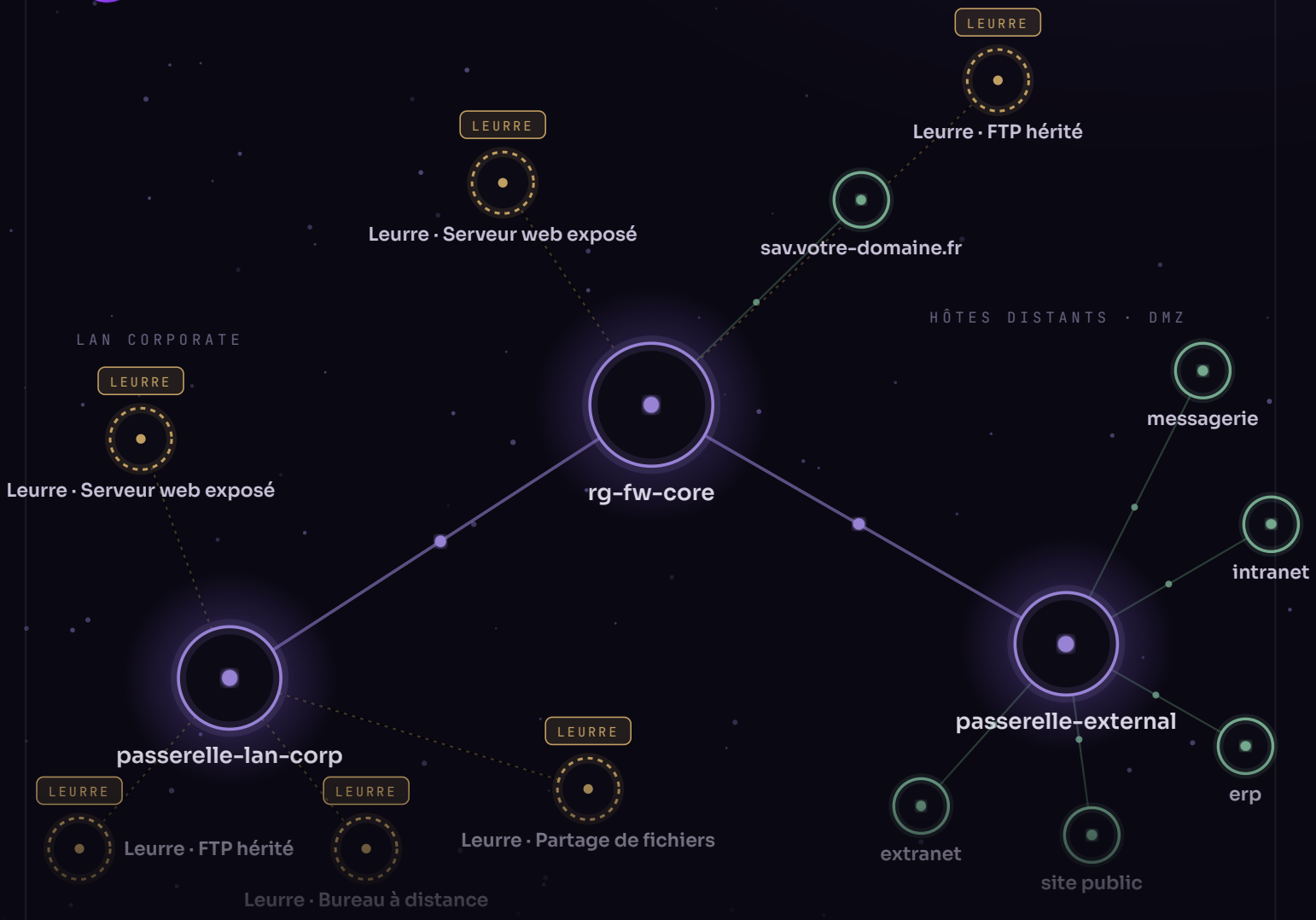
RookGuard | CYBERSÉCURITÉ SOUVERAINE



PLAQUETTE PRODUIT · SOC · SIEM · XDR SOUVERAIN

Le SOC souverain qui prouve ce qu'il promet.

Détecter, piéger, riposter, et **prouver**. Une plateforme française, hébergée en France, conçue pour les DSI et RSSI des PME, ETI et collectivités : simple devant, redoutable derrière, chaque action scellée par un horodatage tiers.

- 100 % SOUVERAIN
- HÉBERGÉ EN FRANCE
- SCELLÉ RFC 3161
- NIS2 · ISO 27001 · RGPD
- ZÉRO FAUX POSITIF PAR CONCEPTION

ROOKGUARD · 47 RUE VIVIENNE · 75002 PARIS
SIREN 105 854 715 · ROOKGUARD.FR

SEPTEMBRE 2026 · VERSION 2
REMPLACE TOUTES LES ÉDITIONS ANTÉRIEURES

Simple devant, redoutable derrière.

Un DSI n'a pas besoin d'un onzième tableau de bord. Il a besoin d'une plateforme qui **voit** son parc, **piège** l'attaquant, **riposte** sans casser la production, et lui remet une **preuve opposable** le lendemain matin.

14 000+
BOUCLIER COLLECTIF

IP HOSTILES BLOQUÉES POUR TOUT LE PARC

19 700+
VEILLE SOUVERAINE

INDICATEURS DE MENACE CONSOLIDÉS

9 400+
AU NOYAU

DÉPLOIEMENTS DE PROTECTION APPLIQUÉS

970+
CYBER TWIN

SIMULATIONS DE BRÈCHE SUR PARCS RÉELS

870+
RFC 3161

PREUVES SCELLÉES PAR UN TIERS

CHIFFRES RÉELS DE LA PLATEFORME · 7 SEPTEMBRE 2026 · AUCUNE DONNÉE SIMULÉE

Trois promesses, tenues par construction.

CERTITUDE · PREUVE · SOUVERAINETÉ

A · LA CERTITUDE

Pas la probabilité

Leurres, canaris, appâts : des surfaces et des fichiers qu'aucun usage légitime ne touche. Tout contact est une menace confirmée par nature. Zéro faux positif, par construction.

B · LA PREUVE

Pas la déclaration

Chaque blocage, isolation, décision et notification est chaînée SHA-256 et horodatée RFC 3161 par un tiers. Votre dossier NIS2 se lit sans nous croire sur parole.

C · LA SOUVERAINETÉ

Assumée

Hébergement en France, aucun CDN ni pare-feu américain devant vos données, notre propre IA souveraine. Vos journaux et vos preuves ne quittent jamais le territoire.

Dix piliers, une seule boucle.

CHAQUE PILIER A SA PAGE

01
Gardien des fichiers
stoppé au 1er fichier

02
Leurres et balise
le voleur emporte la balise

03
Cartographie
votre parc, vos pièges

04
Bouclier collectif
bloquée chez l'un, partout

05
Arthur
notre IA souveraine

06
Sentinel
voir comme l'attaquant

07
WAF souverain
4 étages, 0 dépendance

08
Opposabilité
scellé RFC 3161

09
Phishing
entraîner sans exposer

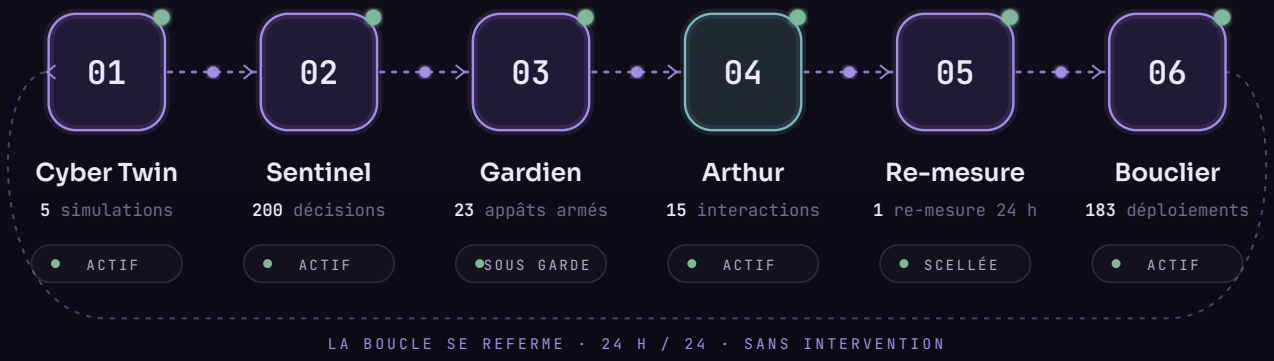
10
Mise en service
un après-midi

Six maillons. Une boucle qui tourne seule.

La plupart des outils détectent puis s'arrêtent. RookGuard **ferme la boucle** : il simule la brèche, détecte, piège, arbitre, applique, puis **re-mesure** pour vérifier que la protection a réellement fait baisser votre risque.

L'orchestration, bout en bout.

● 6 / 6 ACTIFS · TABLEAU DE BORD



LA BOUCLE SE REFERME · 24 H / 24 · SANS INTERVENTION

01 Cyber Twin simule

Monte-Carlo sur vos chemins d'attaque réels : votre probabilité de brèche, chiffrée, et ce qu'elle deviendrait après correction.

02 Sentinel détecte

Veille, IA prédictive, enrichissement, vulnérabilités réelles. Chaque fenêtre ouvre sa vue, chaque chiffre est mesuré.

03 Le Gardien certifie

Appâts et leurres : le premier geste hostile est capturé avec une certitude de 100 %.

04 Arthur arbitre

Bloque d'abord de façon conservatoire, demande ensuite. Dans son mandat il agit seul ; au doute, quarantaine réversible.

05 La re-mesure vérifie

Après chaque action, re-simulation et re-scan : la protection a-t-elle fait baisser le risque ? Le résultat est scellé.

06 Le Bouclier protège

La menace confirmée chez vous protège tous les clients, appliquée au noyau par l'agent souverain, ordres signés.

> Sur votre tableau de bord, la chaîne affiche **« 6 / 6 actifs »** avec la valeur réelle de chaque maillon. Un maillon qui ne serait pas vivant serait affiché comme tel : RookGuard ne montre jamais une tuile vide déguisée en fonctionnalité.

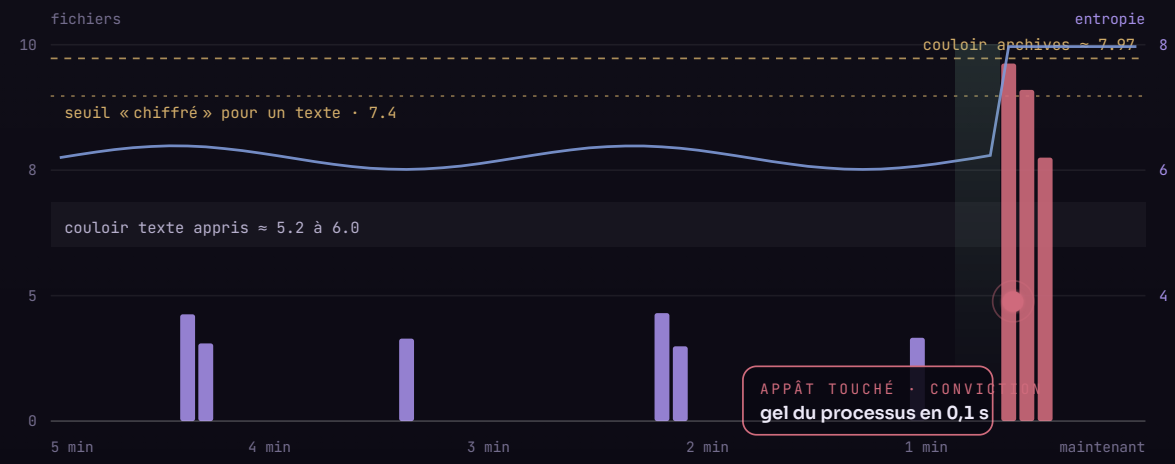
Le Gardien des fichiers. Stoppé au premier fichier.

Des **fichiers-appâts indiscernables** semés dans vos partages, un **capteur au niveau du noyau** qui mesure le comportement d'écriture, et une riposte arbitrée par Arthur, scellée et opposable. Un chiffrement malveillant touche forcément un appât : **c'est une certitude, pas une probabilité**.

703	23	13	Calme
SOUS GARDE	APPÂTS ARMÉS	ÉCRITURES · 24 H	MENACE · 24 H
FICHIERS · 23 DOSSIERS ARMÉS D'UN APPÂT	0 TOUCHÉ · 0 ALTÉRÉ	PIC PAR FENÊTRE 6 · FENÊTRES ACTIVES 9	0 CONVICTION · 0 SUSPICION

01 · L'oscillographe d'écriture

5 DERNIÈRES MINUTES · 60 FENÊTRES DE 5 S



60 FENÊTRES DE 5 S · DÉBIT D'ÉCRITURE (BARRES) · ENTROPIE MESURÉE (LIGNE)

INSTRUMENT RÉEL DE NOTRE PROPRE SOC · ÉTAT AU REPOS, PUIS UN CHIFFREMENT DE LABORATOIRE SUR UN DOSSIER TÉMOIN : CONVICTION À LA 1RE FENÊTRE, GEL EN 0,1 S

CE QUE MESURE LE CAPTEUR

Au niveau du noyau

Débit d'écritures par fenêtre de 5 s, cascade de renommages, entropie par tranches selon le type de fichier, tentatives de destruction de sauvegardes, identité du processus au moment de l'événement.

CE QUI DÉCLENCHE

La convergence, ou l'appât

Aucun signal seul ne déclenche. Débit anormal et entropie de chiffrement ensemble : suspicion. Un appât touché : conviction, immédiate, quelle que soit la vitesse du chiffreur.

CE QUI NE DÉCLENCHE JAMAIS

Votre activité normale

Une sauvegarde massive, une compression, une écriture bureautique : le débit monte, l'entropie reste dans son couloir appris, et aucun appât n'est touché. Zéro faux positif, par conception.

Deux lignes de défense. Une seule certitude.

Du contact à la preuve, en six temps.

RIPOSTE CONSERVATOIRE · JAMAIS DESTRUCTRICE

01	02	03	04	05	06
Appât	**Capteur noyau**	**Fusion**	**Gel + isolation**	**Arthur**	**Carnet scellé**
semé, jamais lu	débit · entropie · renommages	appât touché = certitude	sur l'événement, réversible	vous prévient, vous tranchez	RFC 3161 · opposable

LIGNE 1 · LES APPÂTS

Le juge de paix

Dérivés de l'identité de votre organisation, placés en tête de tri de chaque dossier surveillé, exclus de vos sauvegardes et de vos indexations : aucun processus légitime ne les touche. Une sauvegarde massive fait monter le débit, elle ne touche jamais un appât.

LIGNE 2 · LE CAPTEUR NOYAU

Le comportement, pas la signature

Débit d'écritures, cascade de renommages, entropie par tranches selon le type de fichier, destruction de sauvegardes. Aucun signal seul ne déclenche ; leur convergence, oui. Le chiffrement intermittent ne trompe pas un appât.

BASE APPRISE

Votre parc, type par type

Dès la première seconde, le capteur échantillonne vos fichiers réels : un PDF, une archive, un tableur n'ont pas la même signature d'écriture. Les outils de sauvegarde déclarés sont plafonnés. Zéro faux positif, y compris pendant vos fenêtres de sauvegarde.

RIPOSTE

Gel sur l'événement, isolation au noyau

À 300 fichiers par seconde, chaque milliseconde compte : le processus fautif est gelé à l'instant du contact, puis isolé du réseau, canal d'administration préservé. Rien n'est détruit, tout est réversible, vos sauvegardes sont intactes.

0,1 s

S

GEL DU PROCESSUS APRÈS CONTACT

300

FICHIERS / S

VITESSE D'UN CHIFFREUR MODERNE, TENUE

2

CAPTEURS

LINUX AU NOYAU · WINDOWS EN MODE UTILISATEUR

90 s

SECONDES

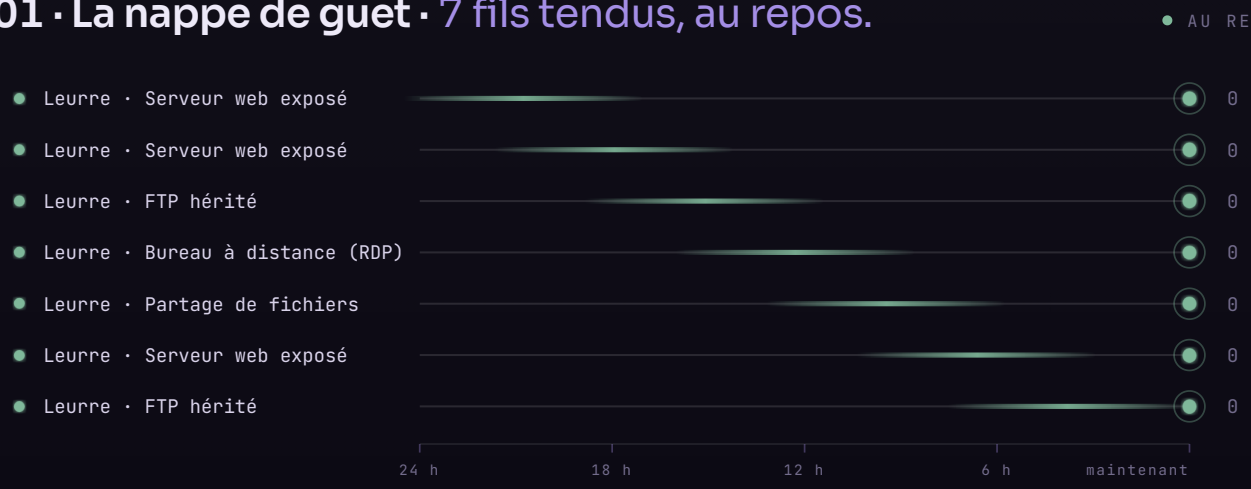
DÉMONSTRATION SUR UN PARTAGE TÉMOIN

Leurres actifs. Tout contact est une menace.

La défense par la ruse. Des surfaces d'apparence vulnérable, **isolées de votre infrastructure réelle**. Aucun usage légitime ne les touche, donc **tout contact est une menace confirmée par nature**.

7 / 7	0	0	0
TOUS ACTIFS	AU REPOS	30 J	PRÊT
LEURRES ARMÉS · À L'ÉCOUTE	CONTACTS · 24 H	CONTACTS · CUMUL TOTAL	PROPAGÉ AU BOUCLIER

01 · La nappe de guet · 7 fils tendus, au repos.



TOUTE LIGNE QUI FRÉMIT EST UN CONTACT · AU REPOS EST UNE BONNE NOUVELLE

02 · Gestion · vos surfaces.

SURFACES FACTICES, ISOLÉES DE VOTRE INFRASTRUCTURE RÉELLE

SURFACE	APPARENCE IMITÉE	SEGMENT	CONTACTS	STATUT	ACTIONS
Leurre · Serveur web exposé	serveur web · bannière nginx	serveur	0	ACTIF	PAUSE · PIÈGE · QUARANTAINE
Leurre · Serveur web exposé	serveur web · bannière Apache	serveur	0	ACTIF	PAUSE · PIÈGE · QUARANTAINE
Leurre · FTP hérité	FTP · bannière vsftpd	legacy	0	ACTIF	PAUSE · PIÈGE · QUARANTAINE
Leurre · Bureau à distance	RDP · écran de connexion	accès	0	ACTIF	PAUSE · PIÈGE · QUARANTAINE
Leurre · Partage de fichiers	SMB · partage ouvert	interne	0	ACTIF	PAUSE · PIÈGE · QUARANTAINE
Leurre · Serveur web exposé · auto	serveur web	external	0	ACTIF	PAUSE · PIÈGE · QUARANTAINE
Leurre · FTP hérité · auto	FTP hérité	external	0	ACTIF	PAUSE · PIÈGE · QUARANTAINE

Vu de l'extérieur, tout se ressemble.

Un leurre est une machine de plus dans votre parc : mêmes bannières, mêmes services, mêmes horaires. Personne chez vous n'a de raison de la toucher. Un attaquant qui explore, lui, finit toujours par le faire. **Et ce seul contact suffit.**

Votre parc, vu par l'attaquant.

PROPORTION ILLUSTRATIVE · 1 LEURRE POUR 10 ENDPOINTS

- Vos endpoints réels
- **Leurres RookGuard**, indiscernables de l'extérieur

DEUX MACHINES, UNE BANNIÈRE

A · srv-ftp-01
RÉEL · COMPTABILITÉ
220 (vsFTPd 3.0.5) · 21 · 22

B · srv-ftp-02
LEURRE · FTP HÉRITÉ
220 (vsFTPd 3.0.5) · 21 · 22

Identiques jusqu'à la bannière. La seule différence est invisible de l'extérieur : **la seconde n'a aucun usage légitime**. Qui la touche se trahit.

EXEMPLE ILLUSTRATIF · BANNIÈRES IMITÉES : NGINX, VSFTPD, RDP, SMB

Le contact, en quatre temps.

PREUVE AVANT RIPOSTE · BOUCLIER APRÈS PREUVE

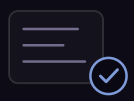
01 · IL EXPLORE

Vu de l'extérieur, soixante machines identiques. Le leurre répond comme les autres : mêmes bannières, mêmes services, mêmes horaires.

02 · IL TOUCHE

Personne chez vous n'a de raison d'ouvrir cette porte. Le premier contact n'est pas un soupçon : c'est une menace confirmée par nature.

03 · IL EST SCELLÉ



SHA-256 · RFC 3161

La capture est chaînée SHA-256, horodatée par un tiers RFC 3161, et l'adresse est bloquée au noyau. Preuve avant riposte.

04 · CONNU PARTOUT

L'adresse rejoint le Bouclier collectif : tous les parcs RookGuard sont prévenus avant même d'être visés.

PAR NATURE
Zéro faux positif
Aucun usage légitime ne touche un leurre. Chaque contact est une intention, jamais une coïncidence.

VU DE DEHORS
Indiscernable
Mêmes bannières que vos vrais serveurs : nginx, vsftpd, RDP, SMB. Rien ne le distingue de l'extérieur.

VU DE DEDANS
Isolé du réel
Une surface factice, isolée de votre infrastructure réelle : elle n'a rien à livrer, sinon l'intrus.

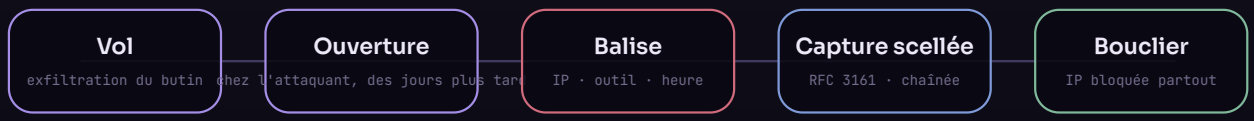
À VOTRE MAIN
Déployé seul
Vous choisissez le nombre de leurres et leur apparence depuis la console ; l'agent souverain les déploie, sans matériel.

Le voleur emporte la balise.

Un leurre qui ne contient rien n'attire personne. Le vôtre sert des faux dumps clients, de faux identifiants, de faux rapports : crédibles, cohérents, **sans une seule donnée réelle**. Parmi eux, des fichiers piégés qui **appellent à la maison** quand on les ouvre.

La balise · traçage après le vol.

EXFILTRATION · OUVERTURE · CAPTURE



BALISE PASSIVE · RIEN N'EST JAMAIS DÉPOSÉ CHEZ L'ATTAQUANT · LÉGALE ET OPPOSABLE

CE QUE VOUS VERREZ

● 91.121.50.5 EXFILTRATION

Leurre · Serveur web exposé · **butin volé ouvert** · excel · office

● SCELLÉ RFC 3161 ● PROPAGÉ AU BOUCLIER IL Y A 2 MIN

Adresse attestée par notre frontal, outil déduit, heure exacte : la capture est chaînée à la précédente, horodatée par un tiers, et l'adresse est bloquée pour tout le parc.

Des canaris propres à votre organisation

Des chemins secrets dérivés de votre identité, jamais stockés, semés là où un attaquant fouille en premier. Un chemin publié peut être grillé : RookGuard garde toujours des canaris en réserve.

Jamais une fausse capture

Le DSI qui ouvre son propre fichier piégé depuis son bureau n'est pas capturé : la liste blanche protège votre équipe. Une adresse usurpée dans un en-tête n'est jamais crue. Une balise ouverte derrière un relais inconnu est enregistrée, jamais propagée.

01 · CONTACT
Menace confirmée
aucune analyse à discuter

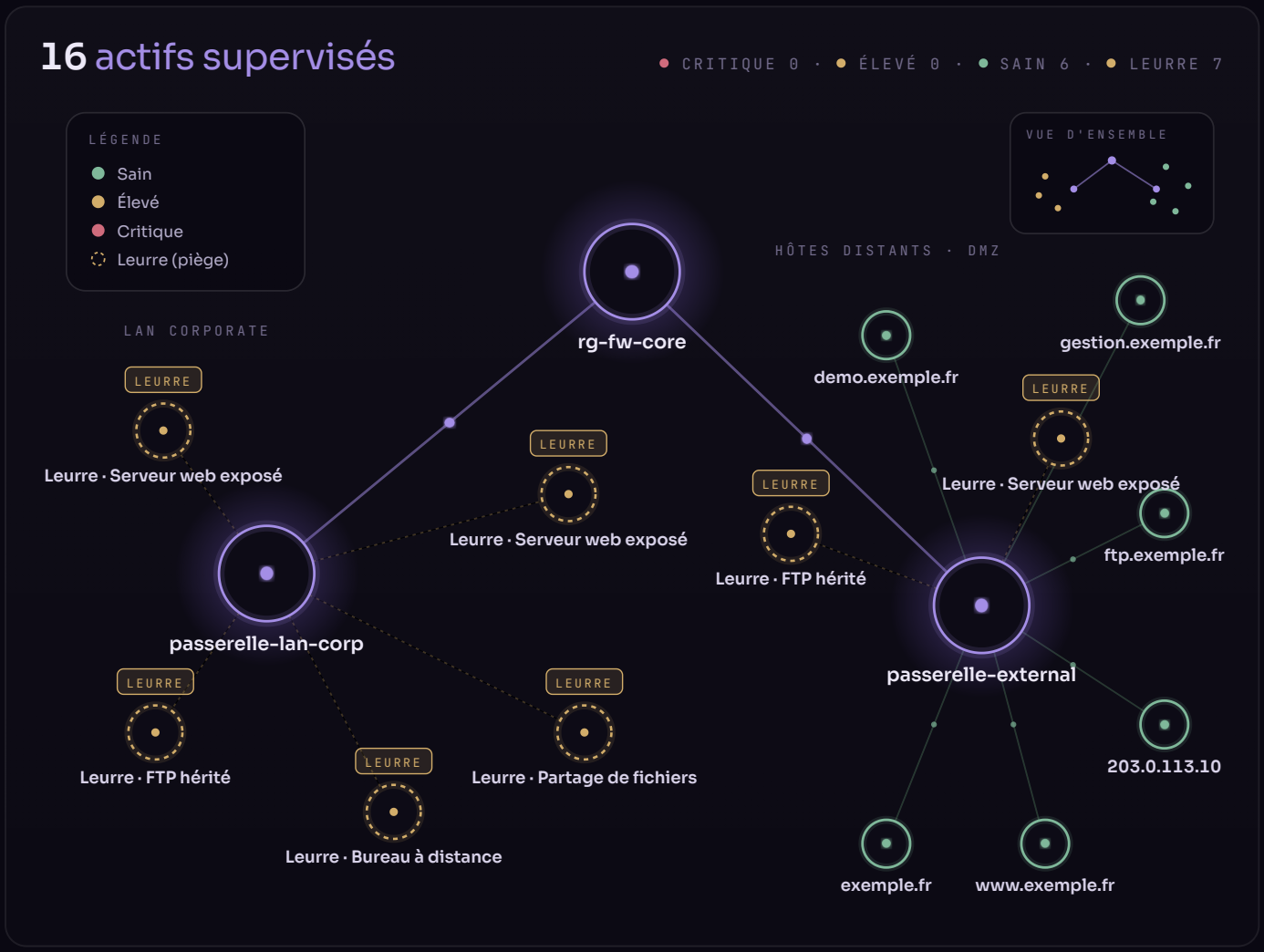
02 · SCELLÉ
Horodatage RFC 3161
journal inaltérable

03 · EMPREINTE
L'ADN de l'attaque
IP, ports, outils, techniques

04 · BOUCLIER
Bloquée partout
chez vous et chez tous les autres

Votre parc, vos pièges. Un seul plan.

Construite depuis l'inventaire réel et les leurres déployés, la cartographie montre ce qui existe, ce qui est sain, ce qui est exposé, et où les pièges attendent. Glissez, zoomez, épinglez ; simulez une intrusion ; exportez.



→ **Simuler une intrusion**
Le Cyber Twin rejoue une attaque sur ce plan et chiffre la probabilité de brèche.

→ **Leurres à leur place**
Chaque surface factice apparaît avec son badge : un attaquant, lui, ne voit pas le badge.

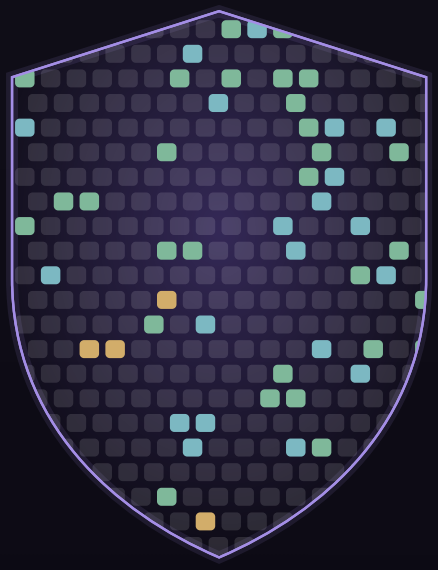
→ **Segments réels**
LAN, DMZ, hôtes distants : les segments viennent de vos actifs, pas d'un dessin.

→ **Exporter**
Le plan s'exporte pour vos audits, vos assureurs, vos comités.

Bouclier collectif. Bloquée chez l'un, bloquée partout.

L'écu

1 ÉCAILLE = 1 ORDRE



APPLIQUÉ AU NOYAU · SIGNÉ HMAC · ACQUITTÉ

14 183
IP HOSTILES

AU BOUCLIER COLLECTIF · TENANT PLATEFORME

9 438
DÉPLOIEMENTS

DE PROTECTION APPLIQUÉS AU NOYAU

19 736
INDICATEURS

DE MENACE CONSOLIDÉS, SOUVERAINS

0
JAMAIS

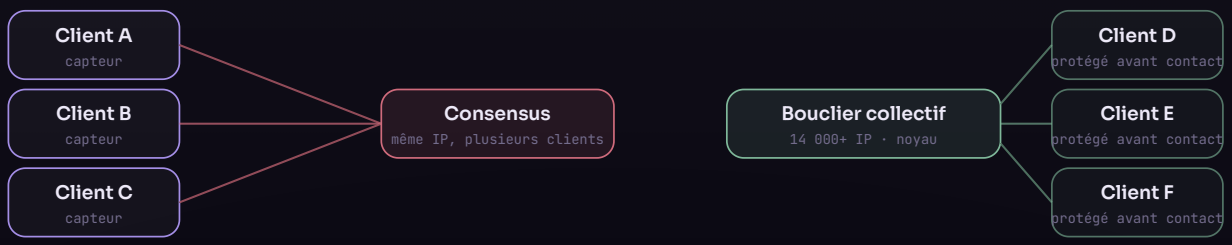
DONNÉE CLIENT PARTAGÉE

Deux plans indépendants, par conception

Visibilité : cloisonnement total entre clients, jusqu'à l'affichage. **Protection :** bouclier mutualisé. Seules les menaces confirmées par consensus se propagent : jamais une détection isolée, jamais une donnée client. Une IP hostile est une empreinte d'attaquant, pas une donnée de votre organisation.

Le consensus, souverain.

CHAQUE CLIENT EST UN CAPTEUR



01 **Ordres signés**
Chaque blocage est un ordre HMAC émis par la plateforme, récupéré par l'agent, jamais poussé par une porte ouverte.

02 **Acquittés par l'agent**
L'agent applique dans nftables puis acquitte : une écaille de l'écu n'existe que si l'ordre a réellement été posé.

03 **Réversibles au noyau**
Une levée restaure réellement l'accès sur chaque machine. Tout est daté, tout se défait, rien n'est perdu.

Trois boucliers. Quatre gardes.

BLOCAGES ACTIFS

Les vôtres

Sur votre parc, posés au noyau par l'agent souverain, réversibles en un clic, chacun avec sa raison et son sceau.

BOUCLIER COLLECTIF

Le parc

La protection mutualisée, nourrie par les leurres, les appâts, le WAF et la veille de tous. Une adresse promue protège tout le monde avant le premier contact.

BOUCLIER DIRIGEANT

Les preuves

Chaque action scellée, chaînée, horodatée par un tiers, exportable : ce que vous montrez au dirigeant, à l'assureur, à l'auditeur.

Quatre gardes anti-auto-sabotage.

AVANT TOUTE APPLICATION

GARDE 1

Jamais votre infrastructure

Un agent déployé, une adresse déclarée, le canal d'administration : refus, avec la raison écrite.

GARDE 2

Jamais une plage entière

Une IP à la fois. Un /24 est une recommandation manuelle, jamais un blocage automatique.

GARDE 3

Jamais sans certitude

Le blocage autonome est réservé aux menaces confirmées ; le reste passe par Arthur et votre décision.

GARDE 4

Jamais irréversible

Une levée restaure réellement l'accès, au noyau. Tout est tracé, tout se défait.

> Demain, le colis propagé ne sera plus seulement une adresse mais **l'ADN de l'attaque** capturé sur les leurres, éprouvé sur le jumeau numérique de chaque client avant déploiement. La fondation est en place ; cette évolution est notre feuille de route, et nous la disons comme telle.

Arthur. Il s'occupe de tout.

Une journée avec Arthur

SCÉNARIO TYPE

Arthur est notre propre IA souveraine. Il vous aide dans **toutes vos tâches** : installer un agent, lire une alerte, préparer une remédiation, produire le rapport de direction. Et pendant que vous travaillez, il **veille** : au moindre doute, la menace est mise en **quarantaine réversible** et vous décidez quand vous voulez.

02:14	Leurre touché : quarantaine conservatoire au noyau, scellée
02:15	L'adresse est propagée au Bouclier collectif
06:59	Veille du matin : ce qui attend votre décision part par e-mail
08:02	Vous ouvrez RookGuard : « Arthur attend votre réponse »
10:30	Vous enrôlez un poste : Arthur vous guide, pas à pas
14:00	Une CVE vous concerne : la remédiation est préparée
17:30	Synthèse du jour, en français, en une minute
21:00	Vous partez. Il reste.

IL VOUS AIDE

Dans toutes vos tâches

Depuis n'importe quelle vue : « installe l'agent sur ce serveur », « explique cette alerte », « prépare la remédiation », « résume la nuit ». Il guide l'enrôlement d'un poste, la mise en conformité d'une exigence, la lecture d'un incident. En français, en une minute.

IL VEILLE

Pendant que vous travaillez

Une menace évidente est bloquée dans son mandat. Un doute est contenu : quarantaine conservatoire au noyau, réversible, scellée. Rien de destructif n'est appliqué sans vous. La nuit, le matin, le week-end : la même règle.

IL VOUS PRÉVIENT

Comme vous le voulez

Dans l'application, par e-mail, SMS, Slack ou webhook. Réveillé la nuit ou retrouvé au matin : votre choix, la menace est déjà contenue. L'e-mail est actionnable : valider ou lever sans ouvrir la console.

24 / 7
VEILLE
SANS ÉQUIPE SOC DE VOTRE CÔTÉ

0
ACTION DESTRUCTRICE
HORS MANDAT, JAMAIS

100 %
RÉVERSIBLE
UNE LEVÉE RESTAURE RÉELLEMENT L'ACCÈS

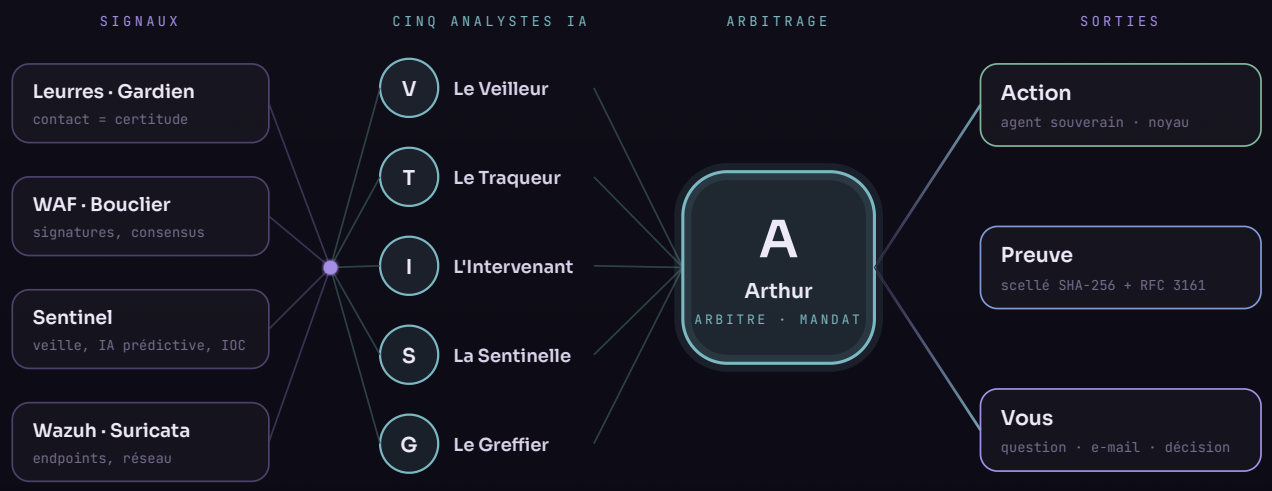
1
CLIC
POUR MAINTENIR OU LEVER, MÊME PAR E-MAIL

Il décide. avec ses Sentinelles.

Cinq analystes IA spécialisés voient, enrichissent, traquent et consignent. Arthur **arbitre** : dans son mandat il agit seul et rend compte ; au doute il contient et vous demande. Chaque décision porte ses raisons et son sceau.

La salle de décision.

SIGNAUX → ANALYSTES → ARTHUR → ACTION · PREUVE · VOUS



MENACE ÉVIDENTE : IL AGIT SEUL · DOUTE : IL CONTIENT ET VOUS DEMANDE · JAMAIS D'ACTION DESTRUCTRICE HORS MANDAT

BRANCHE 1

Menace évidente

Signature confirmée, leurre ou appât touché, consensus du parc : Arthur agit seul, dans son mandat, et rend compte avec ses raisons.

→ BLOQUÉ · SCELLÉ · PROPAGÉ

BRANCHE 2

Doute

Il bloque de façon conservatoire, ouvre sa fenêtre en direct si vous êtes connecté, et propose : maintenir ou lever.

→ QUARANTAINE RÉVERSIBLE · QUESTION

BRANCHE 3

Sensible, vous êtes absent

Quarantaine, puis e-mail actionnable. Rien de destructif tant que vous n'avez pas tranché ; la décision du matin suffit.

→ CONTENU · E-MAIL · DÉCISION

Revue et sélection des indicateurs.

LE TRAQUEUR PRÉ-MARQUE, VOUS COCHEZ

- [x] 45.148.10.188 — ABUSEIPDB · 100/100
- [x] 45.148.10.67 — THREATFOX · C2
- [x] 45.148.10.112 — ABUSEIPDB · 100/100
- [x] 45.148.10.145 — THREATFOX · CONFIANCE 100
- [ ] ~~45.148.10.208~~ — ABUSEIPDB · 98/100
- [ ] ~~45.148.10.0/24~~ — PLAGE · CONSEIL, JAMAIS AUTO

ARTHUR BLOQUE EXACTEMENT LES COCHES, SUR TOUTE LA FLOTTE, VIA LA GARDE · UNE PLAGE ENTIÈRE N'EST JAMAIS BLOQUÉE AUTOMATIQUEMENT

CONFIRMER LE BLOCAGE · 4 IP

Conçue en interne. Hébergée en France.

Arthur, ses cinq analystes, leur mandat, leurs garde-fous et leur mémoire des décisions sont **développés par RookGuard**. Aucune donnée de votre organisation ne sert à entraîner un modèle tiers. Vous confiez votre sécurité à une IA que nous maîtrisons, pas à une boîte noire.

L'anatomie, en cinq étages.

VOIR · COMPRENDRE · DÉCIDER · AGIR · PROUVER

PERCEPTION	**Voir**	capteurs au noyau, réseau, web, leurres, appâts, veille
ANALYSE	**Comprendre**	cinq analystes spécialisés : enrichir, traquer, corréler, garder, consigner
ARBITRAGE	**Décider**	Arthur : mandat en trois branches, gardes anti-auto-sabotage, mémoire des décisions
ACTION	**Agir**	ordres signés vers l'agent souverain, Bouclier collectif, quarantaine réversible
PREUVE	**Prouver**	chaque geste chaîné SHA-256 et horodaté RFC 3161 par un tiers

VOUS DÉCIDEZ · ARTHUR EXÉCUTE

CONÇU EN INTERNE

DÉVELOPPÉE EN INTERNE

Notre code, nos règles

L'arbitre, les analystes, le mandat en trois branches, les quatre gardes, les niveaux d'autonomie : tout est écrit et opéré par RookGuard. Une mise à jour de l'IA tous les trois à six mois, sans dépendre du calendrier d'un éditeur.

SOUVERAINE

Vos données restent chez vous

Hébergée en France. Vos alertes, incidents et décisions n'entraînent jamais un modèle étranger. Le cœur de raisonnement est interchangeable : la configuration décide du moteur, jamais une dépendance codée en dur.

MAÎTRISÉE

Trois niveaux d'autonomie

N0 observe et signale. N1 propose et prépare. N2 agit, dans le mandat, sous la garde anti-auto-sabotage. Chaque niveau est tracé ; chaque décision porte ses raisons, lisibles par un auditeur.

5
ANALYSTES
SPÉCIALISÉS, COORDONNÉS PAR ARTHUR

3
NIVEAUX
OBSERVER · PROPOSER · AGIR

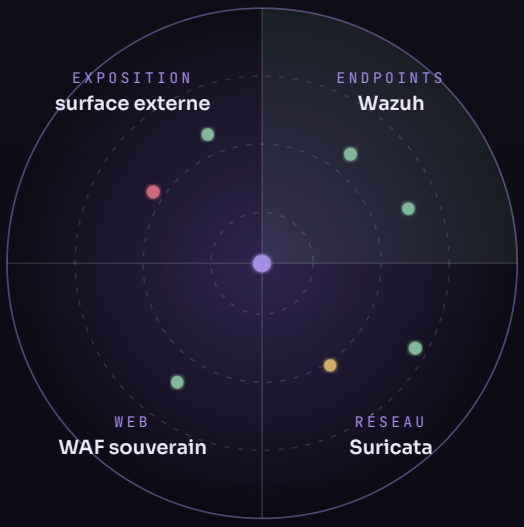
77
DÉCISIONS
NOTRE SOC · 64 DANS LE MANDAT · 13 SOUMISES

0
DONNÉE CLIENT
POUR ENTRAÎNER UN MODÈLE TIERS

Sentinel. Voir votre parc comme l'attaquant le voit.

4 plans

DE VISIBILITÉ

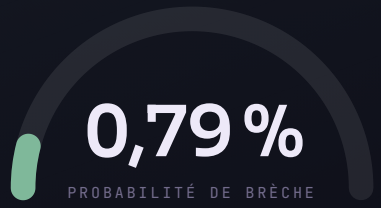


Vulnérabilités réelles, pas un mur de tickets

La veille produit plus de 2 000 CVE par an. RookGuard n'ouvre un ticket que si elle concerne votre parc : produit structuré, actif nommé, version installée comparée à la version corrigée avec l'algorithme exact de votre système.

Le noyau pas redémarré, dit comme tel

Un noyau mis à jour sur le disque mais pas redémarré est signalé « redémarrage requis », pas « vulnérable pour toujours ». Un correctif réservé au support étendu est dit tel quel. Ce qui n'est pas qualifiable est mis en file, jamais perdu, jamais inventé.



NOTRE SOC · VECTEUR : EXPLOIT HTTPS · 10 000 TIRAGES

CYBER TWIN · MAILLON 01

Votre probabilité de brèche, chiffrée

Un jumeau de votre parc réel : actifs déclarés et découverts, ports ouverts, CVE, posture NIS2 et ANSSI. Une simulation Monte-Carlo de 10 000 tirages parcourt vos chemins d'attaque et répond à la seule question qui compte : quelle est la probabilité qu'on entre, et par où ? Puis en mode « et si » : que devient-elle si vous fermez tel port, corrigez telle CVE, imposez le MFA sur tel compte ? Relancée toutes les six heures.

28 000+
CORRECTIFS

UBUNTU SUIVIS, VERSIONS EXACTES

2 000+
PRODUITS

AU CATALOGUE CVE STRUCTURÉ

0
TICKET AVEUGLE

SANS PRODUIT QUALIFIÉ : MIS EN FILE, JAMAIS PERDU

6 h
CYCLE

RE-SIMULATION AUTOMATIQUE DU JUMEAU

Les sources, consolidées chez nous.

AUCUNE DONNÉE CLIENT NE PART VERS CES SERVICES

- CISA KEV
- NVD · CPE
- EPSS
- THREATFOX
- OTX
- ABUSE.CH · FEODO
- UBUNTU OVAL · USN
- GITHUB ADVISORY
- SHODAN
- HIBP · FUITES
- INSEE SIRENE
- WAZUH
- SURICATA
- UPTIMEROBOT

Le portail. Chaque fenêtre ouvre sa vue.

Une famille de modules, chacun branché sur une donnée réelle de votre parc. Aucune tuile vide, aucun chiffre décoratif : ce qui n'est pas mesuré n'est pas affiché.

VEILLE MENACES

19 700+ indicateurs consolidés

CISA KEV, NVD, ThreatFox, OTX, abuse.ch, fuites françaises : une seule table, un score composite par indicateur.

IA PRÉDICTIVE

La prochaine technique probable

Anticipe sur votre parc, avec sa mesure de précision affichée, jamais une prédiction sans sa marge.

ENRICHISSEMENT IOC

Un verdict par indicateur

Une adresse, un domaine, une empreinte : réputation croisée, contexte, verdict, prêt pour Arthur.

CHEMINS D'ATTAQUE

Un port ouvert est une exposition

CVE ou pas. Coupure simulée en direct, neutralisation via Arthur, réactivation à la levée.

DÉCISIONS IA

La file d'Arthur

Ce qu'il a fait seul, ce qui attend votre réponse, avec les raisons et le sceau de chaque décision.

DARK WEB ET FUITES

Vos domaines, vos identifiants

Places de marché, dépôts de fuites, mentions : surveillés en continu, rattachés à vos actifs.

SIEM

La fiche d'investigation

Par actif : chronologie, alertes, décisions, corrélations. Le fil complet d'une machine, en une page.

RÈGLES ET PLAYBOOKS

32 règles Sigma · 17 playbooks

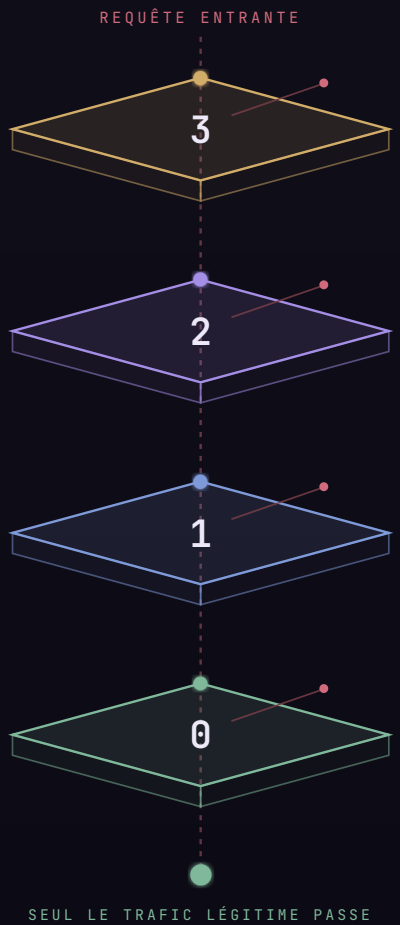
Activés par défaut à l'inscription, adaptables à votre contexte, exécutés par les analystes.

WAF souverain. Quatre étages, zéro dépendance.

Un pare-feu applicatif entièrement écrit et opéré par RookGuard : **sans Cloudflare, sans Ubika**, sans aucun service tiers devant vos données. Le noyau applique, nginx filtre, le moteur décide, les pièges certifient.

La requête traverse quatre étages.

MULTI-CLIENT PAR DOMAINE · DÉTECTION OU BLOCAGE · PARANOÏA RÉGLABLE



ÉTAGE 3 · PIÈGES SOUVERAINS

Les pièges certifient

Canaris et chemins-pièges : toute adresse qui les touche est malveillante à 100 %. Capture, blocage et propagation au premier contact.

ARRÊTE : SCANNERS, FOUILLEURS

ÉTAGE 2 · MOTEUR SOUVERAIN

Le moteur décide

Signatures maison (SQLi, XSS, traversée, RCE, scanners) et score composite par adresse : flux, comportement, consensus du parc.

ARRÊTE : INJECTIONS, RÉPUTATION HOSTILE

ÉTAGE 1 · FRONTAL NGINX

Le frontal filtre

Motifs interdits, limitation de débit, contrôle d'accès par requête. Sept surfaces RookGuard vivent déjà sous ces quatre étages.

ARRÊTE : BRUIT, RAFALES, MOTIFS INTERDITS

ÉTAGE 0 · NOYAU NFTABLES

Le noyau applique

Une adresse confirmée est bloquée dans nftables : elle n'atteint plus nginx, ni l'application, ni rien. Alimenté par le Bouclier collectif.

ARRÊTE : ADRESSES DÉJÀ CONNUES, AVANT TOUT

Réseau de défense collaboratif

Chaque client est un capteur. Une adresse qui attaque réellement plusieurs clients est promue au Bouclier de la plateforme : les autres sont protégés avant d'être visés.

Enrichissement souverain

Les adresses malveillantes des flux de menace déjà en base alimentent la liste de blocage plateforme, sans appel externe, rejouable à volonté.

Vos domaines, votre profil

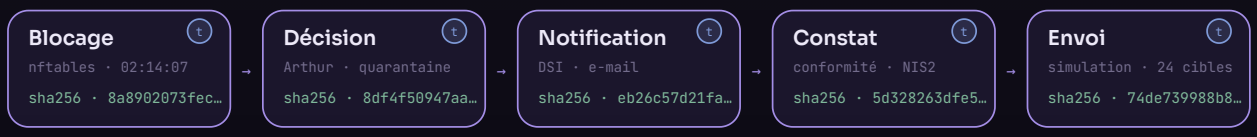
Le trafic est rattaché à chaque organisation par son domaine. Détection ou blocage, niveau de paranoïa, liste blanche de vos propres adresses : jamais un blocage de votre équipe.

Horodatage et opposabilité. Scellé à la source.

Toute action de sécurité est **chaînée SHA-256** à la précédente et **horodatée RFC 3161** par un tiers indépendant. Le journal est inaltérable par construction ; votre dossier se vérifie **sans accès à la plateforme**, et sans nous croire sur parole.

La chaîne de scellés.

870+ PREUVES À CE JOUR



CHAQUE EMPREINTE INCLUT LA PRÉCÉDENTE · JETON RFC 3161 D'UN TIERS SUR CHAQUE MAILLON

UN MAILLON MODIFIÉ ROMPT TOUTE LA CHAÎNE

LECTEUR 1

Le dirigeant

NIS2 rend la direction responsable (art. 21). Le Dossier NIS2 n'est pas une auto-déclaration : chaque exigence porte ses constats, ses preuves déposées et son sceau. Le rapport mensuel, signé Arthur, arrive au COMEX.

LECTEUR 2

L'assureur cyber

« Qu'avez-vous fait, et quand ? » Le carnet répond à la seconde près, avec un horodatage que vous n'avez pas pu produire vous-même : riposte, isolation, levée.

LECTEUR 3

L'auditeur, l'ANSSI

Export PDF vérifiable hors plateforme : empreintes recalculées, chaîne contrôlée, jetons validés. Un incident notifiable porte son compte à rebours de 72 heures et sa notification outillée.

870+
SCEAUX

PREUVES SCELLÉES PAR UN TIERS

72 h
ANSSI

COMPTE À REBOURS SUR INCIDENT NOTIFIABLE

100 %
%

DES ACTIONS DE SÉCURITÉ CHAÎNÉES

0
ACCÈS REQUIS

POUR VÉRIFIER VOTRE DOSSIER

NIS2, ISO 27001, RGPD, ANSSI. Un seul moteur.

Les exigences NIS2, les contrôles ISO 27001, les obligations RGPD et les mesures du guide d'hygiène de l'ANSSI sont suivis dans un même moteur. Les calculs automatiques alimentent le score ; les preuves manuelles se déposent et se scellent. Votre classification NIS2 est déduite de votre SIRET dès l'inscription.

NIS2 13 EXIGENCES SUIVIES

art. 21 : gestion du risque, incidents, continuité, chaîne d'approvisionnement, sensibilisation

ISO 27001 CONTRÔLES ANNEXE A

correspondance automatique avec les mesures déjà en place

RGPD REGISTRE ET PREUVES

pseudonymisation, art. 22, rapports opposables

ANSSI GUIDE D'HYGIÈNE

mesures techniques constatées par l'agent, pas déclarées

Calculé, jamais déclaré.

CE QUE L'AGENT MESURE

IDENTITÉ	CORRECTIFS	HUMAIN	CONFIGURATION	CONTINUITÉ
couverture MFA	**latence de correction**	**taux de clic phishing**	**dérive mesurée**	**fraîcheur des sauvegardes**

Ce que RookGuard ne fait jamais : une donnée simulée, une certification que nous n'avons pas obtenue, une référence client publiée. RookGuard gère la mise en conformité de **votre** organisation ; par discrétion, aucune organisation protégée n'est citée : l'alternative est le pilote de 30 jours sur votre périmètre réel.

Simulation de phishing. Entraîner, sans exposer.

01 · Le sas · quatre portes.

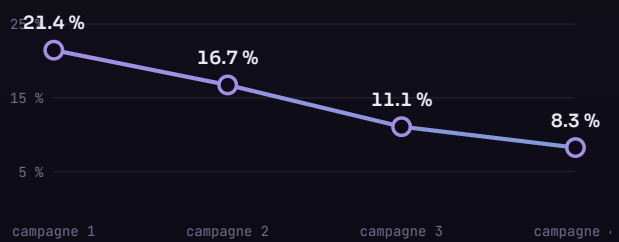
MESURÉES À CHAQUE CAMPAGNE

EXEMPLE ILLUSTRATIF · CAMPAGNE DE 89 DESTINATAIRES · VOS CHIFFRES SERONT LES VÔTRES

SCORE DE RÉSISTANCE

Lisible d'un coup d'œil

Le taux de clic de la dernière campagne donne la note, de A+ à D. La trajectoire d'une campagne à l'autre montre le progrès réel, jamais une courbe décorative.



TRAJECTOIRE ILLUSTRATIVE · CAMPAGNE APRÈS CAMPAGNE

RÉALISME

Comme les vraies

Connexion suspecte Microsoft 365, avis de livraison, message RH : des gabarits crédibles, en français, depuis notre infrastructure d'envoi souveraine.

RGPD

Formés, jamais exposés

Celui qui clique arrive sur une page de sensibilisation tracée. Profils à risque pseudonymisés (art. 22). Un mot de passe saisi n'est ni lu, ni stocké.

OPPOSABLE

Jamais confondue avec une attaque

Marqueur technique invisible pour la cible, lisible par votre SOC. Chaque envoi scellé RFC 3161 : destinataires, gabarit, horodatage.

A+	A	B+	B	C	D
MOINS DE 3 % DE CLICS	MOINS DE 6 %	MOINS DE 10 %	MOINS DE 15 %	MOINS DE 22 %	22 % ET PLUS

Protégé en un après-midi. Pas en un trimestre.

Une inscription, et la plateforme fait le travail : elle **détecte votre infrastructure**, déduit votre classification NIS2, active les règles et les playbooks. L'agent souverain s'installe en une commande, les leurres se déploient seuls. **Vous choisissez le nombre d'endpoints.**

Un après-midi, chronométré.

PARCOURS TYPE

14:00	14:10	14:30	15:00	16:00	17:00
01	02	03	04	05	06
Inscription	**Infrastructure**	**Agent**	**Leurres**	**Première simulation**	**Protégé**
…ET, domaine · NIS2 déduit	…détectée : hébergeur, DNS, …	…e commande, Linux ou Windows	…déployés à la mesure du parc	…probabilité de brèche chiffrée	…boucle tourne, Arthur …

PARCOURS TYPE · UN APRÈS-MIDI · VOUS CHOISISSEZ LE NOMBRE D'ENDPOINTS

La détection fait le travail

Dès l'inscription, RookGuard identifie votre hébergeur, votre plateforme, vos serveurs de noms et vos adresses publiques. Le diagnostic gratuit lancé avant l'inscription est rattaché à votre compte : rien à ressaisir.

Un agent souverain, une commande

Linux ou Windows, l'agent s'enrôle avec un jeton unique, remonte inventaire et télémétrie, applique les ordres signés du Bouclier. Pas de matériel, pas de VPN : vos machines parlent à app.rookguard.fr, en France.

Votre niveau, tout de suite

Sans agent, la plateforme juge sur vos actifs déclarés. Avec l'agent, précision maximale : versions installées, correctifs, redémarrages requis. L'échelle s'adapte à votre maturité sans configuration.

6
ÉTAPES
INSCRIPTION → PROTÉGÉ

1
COMMANDE
POUR ENRÔLER UN AGENT LINUX OU WINDOWS

0
MATÉRIEL
RIEN À INSTALLER, RIEN À CÂBLER, PAS DE VPN

30 j
JOURS
PILOTE SUR VOTRE PÉRIMÈTRE RÉEL

Le pilote de 30 jours, sur votre périmètre réel

Pas de démonstration sur des données de laboratoire : vous branchez un périmètre réel, la boucle tourne un mois, et vous repartez avec votre propre carnet scellé, votre probabilité de brèche mesurée et votre premier rapport de direction. Si RookGuard ne vous a rien appris sur votre parc, vous le saurez.

Souverain jusqu'au dernier octet.

Souverain n'est pas un adjectif marketing. C'est une liste de choses que nous refusons de faire : confier vos journaux à un CDN américain, placer un pare-feu étranger devant vos données, faire dépendre votre sécurité d'une IA que nous ne maîtrisons pas, partager quoi que ce soit entre clients.

FR

Hébergé en France

Plateforme, journaux, preuves et sauvegardes chez un hébergeur français, en France. DNS souverain.

0

Zéro intermédiaire

Aucun CDN, aucun WAF tiers, aucun service de réputation américain dans le chemin de vos données.

IA

Notre propre IA

Arthur et ses analystes, conçus en interne, hébergés en France. Vos alertes ne nourrissent jamais un modèle étranger.

×

Cloisonnement absolu

Chaque table, chaque requête, chaque vue scopée à votre organisation. Le Bouclier ne propage que des empreintes d'attaquants.

0
CDN
DEVANT VOS DONNÉES

0
IA ÉTRANGÈRE
DANS LE TRAITEMENT DE VOS ALERTES

0
DONNÉE CLIENT
PARTAGÉE ENTRE ORGANISATIONS

Honnête par construction. Zéro donnée simulée, zéro bouton mort, zéro promesse déguisée en fonctionnalité. Ce qui est en feuille de route est dit comme tel, dans le produit comme dans cette plaquette.

Trois approches. Une seule est née pour le terrain français.

Les références du marché sont d'excellents produits, conçus pour d'autres contraintes que les vôtres. Voici, critère par critère, ce qui change quand la plateforme est **pensée, hébergée et gouvernée en France**.

	RookGuard SOUVERAIN FRANÇAIS	CrowdStrike FALCON · ÉTATS-UNIS	ESET PROTECT · SLOVAQUIE
SOUVERAINETÉ & DROIT			
Siège & droit applicable Qui peut exiger vos données ?	France	États-Unis	Slovaquie (UE)
Hébergement exclusif en France Journaux, alertes, preuves, sauvegardes	✓	✗ cloud global, régions UE en option	~ UE, hors de France
Immunité Cloud Act & FISA 702 Lois extraterritoriales américaines	✓	✗ éditeur de droit américain	✓ éditeur de droit européen
IA développée en interne, hébergée en France Vos données n'entraînent aucun modèle tiers	✓ Arthur et ses cinq analystes	✗ Charlotte AI, cloud Falcon	~ AI Advisor, cloud de l'éditeur
Conformité NIS2 française native Référentiel ANSSI, dossier opposable	✓ Dossier NIS2 scellé	~ cadres génériques	~ cadres génériques
PLATEFORME			
SOC · SIEM · XDR · WAF · conformité unifiés Sans empilement de licences	✓ deux offres, tout inclus	~ modules facturés séparément	~ périmètre centré endpoint
Pare-feu applicatif souverain inclus Quatre étages devant vos services web	✓ nftables · nginx · moteur · pièges	✗	✗
Copilote IA en français, inclus Analyste dédié, agissant sous mandat	✓ Arthur	~ assistant IA en option	~ offre la plus haute seulement
Preuve opposable scellée Horodatage RFC 3161, chaînage SHA-256	✓	✗	✗
Simulation de phishing incluse Pseudonymisée, formation automatique	✓	✗ via partenaires	~ produit séparé
PENSÉ POUR	**PME, ETI & collectivités françaises sous NIS2**	**Grands comptes internationaux**	**Protection endpoint généraliste**

Comparaison indicative établie en septembre 2026 à partir des informations publiques des éditeurs ; les marques citées appartiennent à leurs propriétaires respectifs. ✓ inclus ~ partiel ou en option ✗ non proposé, à notre connaissance.

L'innovation souveraine, critère par critère.

Là où le marché ajoute des modules, RookGuard ferme la boucle : pièges, preuve, immunité collective et re-mesure sont inclus, et chaque action reste réversible sous votre mandat. Ce second tableau ne retient que **ce qui est documenté publiquement**.

	RookGuard SOUVERAIN FRANÇAIS	CrowdStrike FALCON · ÉTATS-UNIS	ESET PROTECT · SLOVAQUIE
INNOVATION SOUVERAINE			
Gardien des fichiers : riposte au noyau Gel arbitré en 0,1 s, quarantaine réversible	✓ gel · scellé · réversible	~ contention d'hôte, sans scellé	~ Ransomware Shield, sans scellé
Leurres actifs intégrés Machines pièges au sein de votre parc	✓ déployés par l'agent, sans matériel	~ jetons d'identité	✗
Balise dans les fichiers piégés Traçage après le vol, hors de votre réseau	✓ capture scellée, IP bloquée	✗	✗
Bouclier collectif au noyau Bloquée chez l'un, bloquée partout	✓ 14 000+ IP, ordres signés	~ renseignement mutualisé	~ réputation cloud
Cyber Twin : probabilité de brèche chiffrée 10 000 tirages sur votre parc réel	✓ re-simulée après correction	~ gestion de l'exposition	~ vulnérabilités, en option
Re-mesure après chaque action La boucle vérifie que le risque a baissé	✓ résultat scellé	✗	✗
Mandat & quarantaine réversible Rien de destructif sans votre décision	✓ 3 branches, e-mail actionnable	~ politiques de réponse	~ politiques de réponse
MODÈLE & ACCOMPAGNEMENT			
Prix public, simple, en euros Lisible avant le premier rendez-vous	✓ 15 € / 25 € par endpoint	~ en dollars, puis sur devis	✓ grilles publiques, par produit
Pilote sur votre parc réel Carnet scellé remis à la fin	✓ 30 jours	~ essai 15 jours	~ essai 30 jours
Support en France, en français Interlocuteurs directs, fuseau local	✓ équipe France	~ support international	~ via distributeurs
PENSÉ POUR	**Piéger, prouver, immuniser, re-mesurer**	**Détecter et répondre, à l'échelle mondiale**	**Protéger le poste, simplement**

Comparaison indicative établie en septembre 2026 à partir des informations publiques des éditeurs ; les marques citées appartiennent à leurs propriétaires respectifs. ✓ inclus ~ partiel ou en option ✗ non proposé, à notre connaissance.

Deux offres. Un prix par endpoint.

Vous choisissez le nombre d'endpoints à protéger : c'est votre unité de déploiement, et de facturation. Prix de référence hors taxes, par endpoint et par mois, minimum 10 endpoints. **Le tarif est dégressif selon le volume** : il se négocie lors d'un entretien téléphonique ou en visioconférence. Pilote de 30 jours sur votre périmètre réel avant tout engagement.

ESSENTIEL

15 €

HT / ENDPOINT / MOIS

LE SOC SOUVERAIN COMPLET

- ✓ Sentinel : veille, IA prédictive, enrichissement, chemins d'attaque, vulnérabilités réelles
- ✓ WAF souverain à 4 étages, Bouclier collectif, cartographie, SIEM
- ✓ Arthur en arbitrage, notifications e-mail, rapports mensuels
- ✓ Conformité multi-référentiels, Dossier NIS2, simulation de phishing
- ✓ Support 24 h / 24, 7 j / 7

SOVEREIGN · RECOMMANDÉ

25 €

HT / ENDPOINT / MOIS

TOUT ESSENTIEL, PLUS LA RUSE ET LA PREUVE

- ✓ Le Gardien des fichiers et sa riposte comportementale au noyau
- ✓ Leurres actifs, canaris, butin empoisonné et balise d'exfiltration
- ✓ Bouclier dirigeant : carnet opposable, horodatage RFC 3161 sur chaque action
- ✓ Cyber Twin, Salle de guerre, Cockpit exécutif et immunitaire
- ✓ Arthur copilote : conversation, revue des indicateurs, e-mails actionnables

24 / 7

SUPERVISION

ENGAGEMENT REPRIS AU CONTRAT

< 15 min

MIN

DÉLAI MOYEN DE RÉTABLISSEMENT

< 5 min

MIN

AUTORÉTABLISSEMENT DE LA PLATEFORME

VOLUME

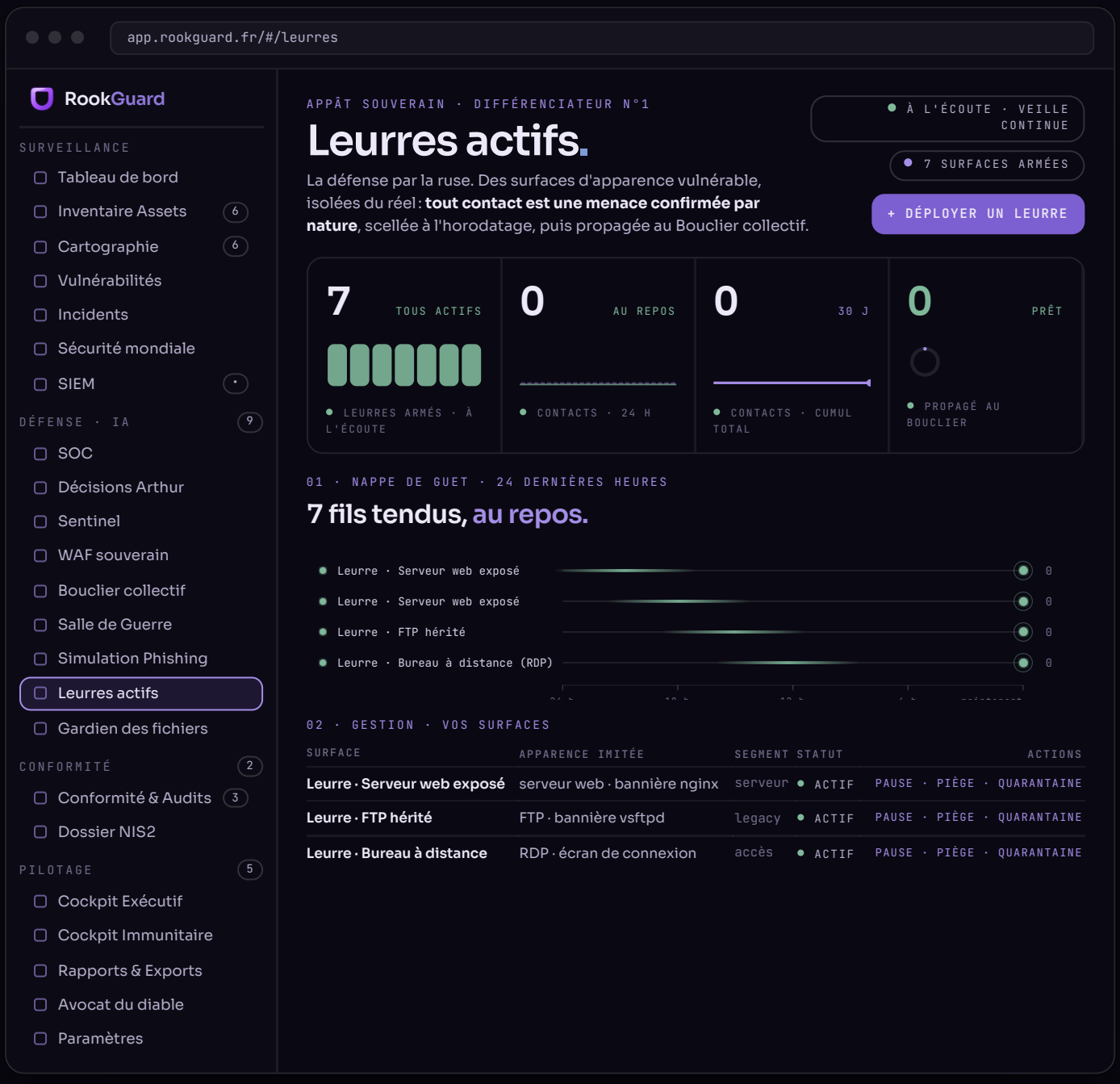
Un tarif dégressif selon votre volume, fixé avec vous.

Le prix par endpoint se négocie lors d'un entretien téléphonique ou en visioconférence, sur la base de votre parc réel. Le régime de pénalités se définit à la contractualisation.

ENTRETIEN · 30 MIN

Votre console. en un regard.

Quatre sections, vingt-trois vues, une seule grammaire : un titre, des chips d'état, un HUD de vitaux réels, un instrument signature. Ici, la vue Leurres actifs, telle qu'elle s'affiche.



SURVEILLANCE 7

Tableau de bord · Inventaire · Cartographie · Vulnérabilités · Incidents · Sécurité mondiale · SIEM

DÉFENSE · IA 9

SOC · Décisions Arthur · Sentinel · WAF souverain · Bouclier collectif · Salle de Guerre · Simulation Phishing · Leurres actifs · Gardien des fichiers

CONFORMITÉ 2

Conformité et audits · Dossier NIS2

PILOTAGE 5

Cockpit exécutif · Cockpit immunitaire · Rapports et exports · Avocat du diable · Paramètres

15 · EN UNE PAGE

Ce que vous direz à votre direction.

Douze phrases, toutes vérifiables dans le produit. Chacune correspond à une vue de votre console, avec sa donnée réelle et son sceau.

01 **Un chiffrement malveillant est stoppé au premier fichier**
gelé au niveau du noyau, la preuve horodatée par un tiers.

02 **Un attaquant qui explore touche un leurre**
et son adresse est bloquée chez nous et chez tous les clients RookGuard.

03 **Un document volé se signale quand on l'ouvre**
adresse, outil, heure, scellés.

04 **La nuit, Arthur contient la menace**
de façon réversible et nous attend le matin ; nous choisissons d'être réveillés ou non.

05 **Nous connaissons notre probabilité de brèche**
chiffrée sur notre parc réel, et ce qui la ferait baisser.

06 **Nous ne trions pas 2 000 CVE**
seules celles qui nous concernent deviennent des tickets, avec la version exacte à corriger.

07 **Notre pare-feu applicatif est à nous**
quatre étages, aucun service étranger devant nos données.

08 **Notre dossier NIS2 se vérifie sans RookGuard**
chaque preuve est chaînée et horodatée RFC 3161.

09 **Nos équipes sont entraînées au phishing**
sans être exposées : pseudonymisées, formées automatiquement.

10 **Nous avons été protégés en un après-midi**
avec un agent souverain et des leurres déployés seuls.

11 **Nos données, nos journaux et notre IA restent en France**
et rien ne circule entre clients.

12 **Nous payons par endpoint**
avec un pilote de 30 jours sur notre périmètre réel avant de nous engager.

VOIR ROOKGUARD SUR VOTRE PÉRIMÈTRE

Pilote de 30 jours, sur votre parc réel, avec votre propre carnet scellé à la fin.

Écrivez-nous : nous branchons un périmètre réel, la boucle tourne un mois, vous jugez sur pièces.

RookGuard

CONTACT@ROOKGUARD.FR
ROOKGUARD.FR · APP.ROOKGUARD.FR
47 RUE VIVIENNE · 75002 PARIS · SIREN 105 854 715