WEB SECURITY ANALYZER

NEXT-GEN CYBER-AI

LOCKHEED LLC

LOCKHEED LLC

WSA

WEB SECURITY ANALYSER

Version 1.0 | Octobre 2026

AGENDA GENERAL

Chapitre 1 . WSA : Les Principales Fonctions

Chapitre 2. L'IA Au coeur du Système

Chapitre 3. WSA face à la concurrence

Chapitre 4. Confidentiel Lockheed – Evolutions, Les Manques à combler

Chapitre 5. Distancer les offres du marché

WSA

L'intelligence cyber qui transforme la sécurité en avantage concurrentiel.



NEXT-GEN CYBER-AI

LOCKHEED

LLC

WSA transforme des signaux techniques en décisions justifiables, avec une IA gouvernée et une feuille de route précise pour automatiser la correction.



SIGNAUX TECHNIQUES
Logs, métriques, menaces, télémétries, anomalies...

DÉCISIONS JUSTIFIABLES
Contextualisées, priorisées, traçables et explicables.

IA GOUVERNÉE
Modèles transparents, contrôlés et conformes, avec garde-fous et audit.

FEUILLE DE ROUTE PRÉCISE
Plan d'automatisation, étapes, priorités, KPIs et dépendances claires.

CORRECTION AUTOMATISÉE
Remédiation orchestrée, exécutée et vérifiée en continu.

DE LA DONNÉE À L'ACTION. DE LA RÉPONSE À LA RÉSILIENCE.

NEXT-GEN CYBER-AI
LOCKHEED
LLC

POSITIONNEMENT DE WSA FACE À PALO ALTO NETWORKS

Précision opérationnelle, IA gouvernée, preuve technique.

WSA (Security Analyzer)

Analyse Web / API / IP / Hôte
Détection et analyse approfondie des surfaces d'attaque.

Preuves techniques vérifiables
Résultats concrets, traçables et reproductibles.

IA multi-LLM gouvernée
Analyse augmentée, maîtrisée et conforme.

Remédiation pilotée + re-test
Recommandations actionnables et validation des corrections.

Valeur clé : transformer des signaux techniques en décisions justifiables.

NOTRE POSITIONNEMENT

WSA ne cherche pas à reproduire un SOC universel. WSA cible l'analyse profonde, explicable et actionable.

- Plus ciblé
- Plus explicable
- Plus orienté preuve et correction

PRÉCISION & EXPLICABILITÉ

ÉCHELLE & COUVERTURE

Palo Alto Networks

Plateforme SOC / XDR à grande échelle
DéTECTION, réponse et surveillance unifiées à l'échelle.

Cloud + réseau + télémétrie massive
Visibilité étendue sur l'ensemble de l'infrastructure.

Orchestration et automatisation avancées
Playbooks, SOAR et intégrations de bout en bout.

Puissance mondiale et couverture entreprise
Présence internationale et adoption à grande échelle.

Force clé : couverture globale et opérations de sécurité à l'échelle.

MESSAGE CLÉ : WSA = une cybersécurité de précision. | Palo Alto = une cybersécurité de plateforme globale.

Positionnement stratégique visuel – synthèse marketing, non benchmark indépendant.

CHAPÍTRE 1

CHAPITRE 1 — WSA : les principales fonctions et leurs avantages



AGENDA DES FONCTIONS DE BASE

- 1.1 — Voir ce qu'un attaquant peut voir. Avant qu'il ne l'exploite.
- 1.2 — Un site web fonctionnel n'est pas nécessairement un site sécurisé.
- 1.3 — Plusieurs dizaines d'analyseurs. Une seule lecture de la sécurité.
- 1.4 — Une adresse IP n'est pas une identité. C'est un ensemble d'indices.
- 1.5 — À chaque actif, son exposition, son historique et ses risques.
- 1.6 — Une vulnérabilité isolée est un signal. Plusieurs deviennent une attaque.
- 1.7 — La criticité ne se résume pas à une note CVSS.
- 1.8 — La sécurité n'est pas une photographie. C'est une évolution permanente.
- 1.9 — Du constat technique à la décision opérationnelle.

1.1 — Voir ce qu’un attaquant peut voir. Avant qu’il ne l’emploie.

Découverte et cartographie de la surface d’attaque



1.2 — Un site web fonctionnel n'est pas nécessairement un site sécurisé.

Analyse approfondie des applications web et des API



XSS et injections SQL
(injection)



Autorisations et accès aux données
(accès)



API et JavaScript
(code/api)



Découverte de contenus web
(recherche/web)



Authentification et sessions
(clé/utilisateur)



OAuth / OpenID Connect
(protocole/identité)



TLS et en-têtes de sécurité
(certificat/en-têtes)



Technologies et composants
(stack/tech)

1.3 — Plusieurs dizaines d'analyseurs. Une seule lecture de la sécurité.

Orchestration et consolidation des résultats

DIZAINES D'ANALYSEURS

- Nmap
- Nuclei
- httpx
- testssl.sh
- Nikto
- ZAP
- Python engines



WSA

CORE ORCHESTRATEUR

COLLECTE • NORMALISE • CORRÈLE • PRIORISE

UNE SEULE VUE UNIFIÉE



- Vue consolidée et dédupliquée
- Priorisation intelligente des risques
- Contexte enrichi et corrélé
- Rapport unique de sécurité

PROFILS D'ANALYSE PRÉCONFIGURÉS

QUICK
Rapide et léger
Surface rapide

STANDARD
Équilibré et complet
Couverture standard

DEEP
Analyse approfondie
Détection exhaustive

UNE SEULE SOURCE DE VÉRITÉ. DES DÉCISIONS ÉCLAIRÉES. UNE POSTURE DE SÉCURITÉ RENFORCÉE.

WSA • ORCHESTRE. CONSOLIDE. PROTÈGE.

1.4 — Une adresse IP n'est pas une identité.
C'est un ensemble d'indices.

Intelligence IP multidimensionnelle



COMPARAISON DES SOURCES POUR DÉTECTER LES INCOHÉRENCES

SOURCES MULTIPLES
RDAP, DNS, BGP, RPKI, TLS, Réputation, Historique...

CROISEMENT & CORRÉLATION
Détection des incohérences, anomalies et signaux faibles.

VISION MULTIDIMENSIONNELLE
Au-delà de la géolocalisation ou d'un score de réputation.

UNE IP = UN POINT DE DÉPART. | PLUSIEURS DIMENSIONS = UNE COMPRÉHENSION RÉELLE.

1.5 — À chaque actif, son exposition, son historique et ses risques.

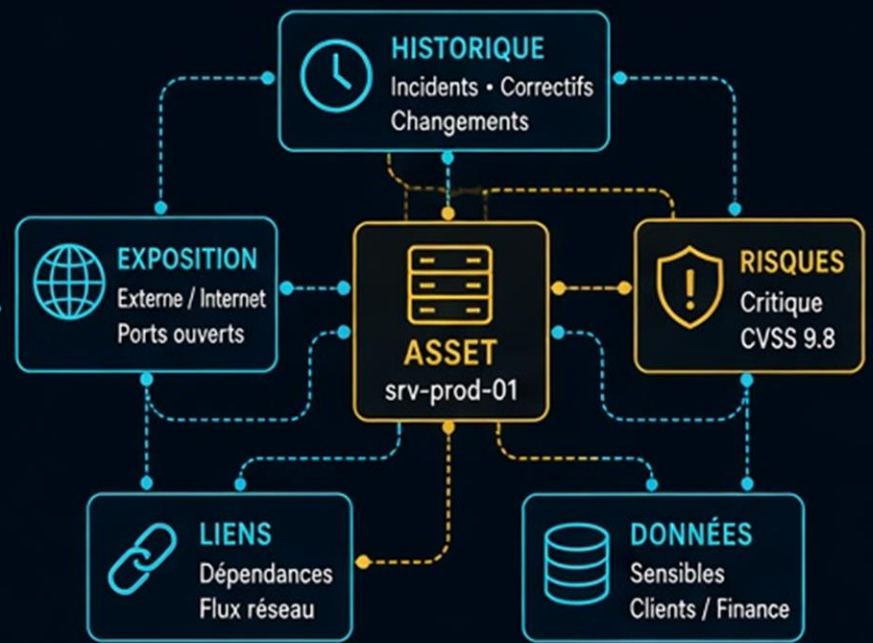
Inventaire intelligent et graphe de sécurité

INVENTAIRE INTELLIGENT

- Serveurs — srv-prod-01
- Applications — app-front
- Bases de données — db-client
- Cloud / SaaS — aws-account

Découverte continue • Classification • Contexte

GRAPHE DE SÉCURITÉ



VUE 360° & CYCLE DE VIE



RELATIONS
Dépendances et flux cartographiés

VULNÉRABILITÉS
Rattachées aux actifs et à leur contexte

AVANT : VULNÉRABILITÉS ISOLÉES

Listes fragmentées • Peu de contexte • Priorisation difficile

APRÈS : RAISONNEMENT BASÉ SUR LES ACTIFS

Contexte complet • Dépendances • Priorisation intelligente • Décisions éclairées

1.6 — Une vulnérabilité isolée est un signal.

Plusieurs vulnérabilités liées peuvent devenir un scénario d'attaque.

Corrélation des risques et analyse des chemins d'attaque

VULNÉRABILITÉS ISOLÉES
Des signaux indépendants



CVE-2024-1234
Serveur Web

CVE-2024-5678
Service Auth

CVE-2024-9012
Base de données

Signaux détectés, mais sans lien apparent.

CHEMINS D'ATTAQUE
Corrélation des vulnérabilités



Des liens techniques et contextuels font émerger des chemins.

SCÉNARIOS D'ATTAQUE
Chaînes exploitables

Accès initial (via Web Server)

Escalade de privilèges (via Auth Service)

Accès aux données sensibles (via Database)

Une séquence ordonnée = un scénario d'attaque réaliste.

GRAPHE DE CORRÉLATION
Modélisation des relations entre vulnérabilités, actifs et contextes.

CHEMINS D'ATTAQUE
Identification des chemins exploitables et de leurs prérequis.

PRIORISATION CONTEXTUELLE
Évaluation de l'impact réel et priorisation des risques critiques.

CORRÉLATION DES FAIBLESSES SUR LES ACTIFS
Regroupement des faiblesses par actif pour révéler les chaînes cachées.

Comprendre les liens. Anticiper les scénarios. Prioriser les défenses.

1.7 — La criticité ne se résume pas à une note CVSS.

Renseignement sur les vulnérabilités et contexte d'exploitation

CVE
Identifiant de vulnérabilité standardisé

EPSS
Probabilité d'exploitation dans les 30 prochains jours

CISA KEV
Catalogue des vulnérabilités exploitées connues

Renseignement sur les menaces
Exploits publics, campagnes actives, acteurs, PoC, etc.

ENRICHISSEMENT DE RENSEIGNEMENT

CONTEXTE DES ACTIFS

Actif critique
Impact métier élevé

Exposition
Internet, partenaires, etc.

Sensibilité des données
Confidentielles, réglementées

Compensations existantes
Contrôles, segmentations, etc.

TOUTES LES ALERTES DE MÊME NIVEAU NE SE VALENT PAS

NOTE CVSS SEULE
= Une vision incomplète
Ne tient pas compte de la probabilité réelle d'exploitation ni du contexte.

CONTEXTE + RENSEIGNEMENT
= Priorisation précise
Concentrez vos efforts sur les vulnérabilités qui comptent vraiment.

La criticité réelle = Sévérité × Probabilité d'exploitation × Contexte métier

Priorisez avec pertinence.
Réduisez le risque réel.

1.8 — La sécurité n'est pas une photographie. C'est une évolution permanente.

Surveillance, historique et détection des dérives

SURVEILLANCE CONTINUE DANS LE TEMPS



ANALYSES PLANIFIÉES
Régulières et automatisées

COMPARAISON DES EXÉCUTIONS
Détection des changements

ALERTES SUR NOUVEAUX SERVICES
Expositions et services inconnus

SUIVI DES RISQUES
Évolution du niveau de risque

ÉVOLUTION HISTORIQUE
Vue d'ensemble dans le temps



HISTORIQUE
Traçabilité complète des changements dans le temps.



COMPARAISON
Visualisez précisément ce qui a changé entre deux exécutions.



ALERTES
Soyez notifié des nouveaux services, ports ou comportements à risque.



NOUVELLES EXPOSITIONS
Identifiez rapidement ce qui est apparu et évaluez l'impact.



DÉTECTION DES DÉRIVES
Repérez les écarts par rapport à votre état sécurisé de référence.



SURVEILLANCE CONTINUE
Une boucle d'amélioration permanente pour une sécurité résiliente.



CE QUI A CHANGÉ
Modifications détectées

CE QUI EST APPARU
Nouveaux éléments identifiés



CE QUI A ÉTÉ CORRIGÉ
Risques traités et résolus



CE QUI EST RÉAPPARU
Éléments récurrents ou réactivés

1.9 — Du constat technique à la décision opérationnelle.

Cockpit, API, rapports et organisation des actions

UNE SEULE RÉALITÉ, PLUSIEURS VUES

COCKPIT / TABLEAU DE BORD EXÉCUTIF

Synthèse globale, KPIs, tendances, alertes prioritaires.



PRIORITÉS CTO

Vue consolidée pour arbitrer, prioriser et allouer les ressources.



PREUVES EXPERTES

Logs, endpoints, vulnérabilités, artefacts et analyses techniques.



API (PERMISSIONS LIMITÉES)

Accès contrôlé, scopes granulaires, principe du moindre privilège.

```
GET /incidents
?scope=read:alerts
```

WEBHOOKS

Notifications en temps réel pour automatiser les workflows.



RAPPORTS DÉTAILLÉS

Rapports techniques et de conformité, preuves auditables.



INVESTIGATION

Recherche, corrélation, chronologie, piste d'attaque.



DU SIGNAL À L'ACTION : ORGANISER LES DÉCISIONS QUI COMPTENT

COCKPIT / DASHBOARD

Vue globale en un coup d'œil

RAPPORTS

Preuves, audits et conformité

API

Intégration sécurisée et contrôlée

WEBHOOKS

Automatisation et réactivité

ACTIONS

Orchestration et plans d'action

DÉCISION OPÉRATIONNELLE

Décider, agir, suivre l'impact.

CHAPITRE 2

CHAPITRE 2 — L'intelligence artificielle au cœur de WSA



ANALYSE DE SÉCURITÉ

Collecte et analyse en temps réel de données massives pour détecter les menaces avancées.

COMPRÉHENSION DES RISQUES

L'IA contextualise les risques, leur impact et leur probabilité pour une visibilité claire.

DÉCISION ÉCLAIRÉE

L'IA priorise les insights et aide les équipes à prendre les bonnes décisions, vite.

ACTION INTELLIGENTE

Automatisation des actions et orchestration pour contenir, remédier et renforcer.

DÉTECTION AVANCÉE | ANALYSE PRÉDICTIVE | PRIORISATION INTELLIGENTE | RÉPONSE AUTOMATISÉE

AGENDA - L'intelligence artificielle au cœur de WSA

- 2.1 — L'IA n'invente pas les vulnérabilités. Elle interprète les preuves. »
- 2.2 — Cent alertes ne signifient pas cent problèmes indépendants. »
- 2.3 — Ne pas corriger ce qui fait du bruit. Corriger ce qui présente le vrai risque.
- 2.4 — L'IA ne propose pas seulement quoi corriger. Elle doit expliquer pourquoi et comment vérifier.
- 2.5 — Plusieurs intelligences artificielles. Aucun fournisseur imposé.
- 2.6 — Chaque affirmation importante doit pouvoir retrouver sa preuve.
- 2.7 — Un expert cyber disponible dans le cockpit, sans remplacer l'expert humain
- 2.8 — L'intelligence artificielle doit être maîtrisable techniquement et économiquement


1
2
3
Analyseurs établissent les faits
L’IA relie les informations
L’humain garde la décision

2.1 — L'IA n'invente pas les vulnérabilités. Elle interprète les preuves.



1. Moteurs déterministes WSA —

Mesures · Constats · Identifiants · Sources · Historique



2. Couche d'intelligence artificielle —

Corrélation · Explication · Causes · Risques combinés · Priorités

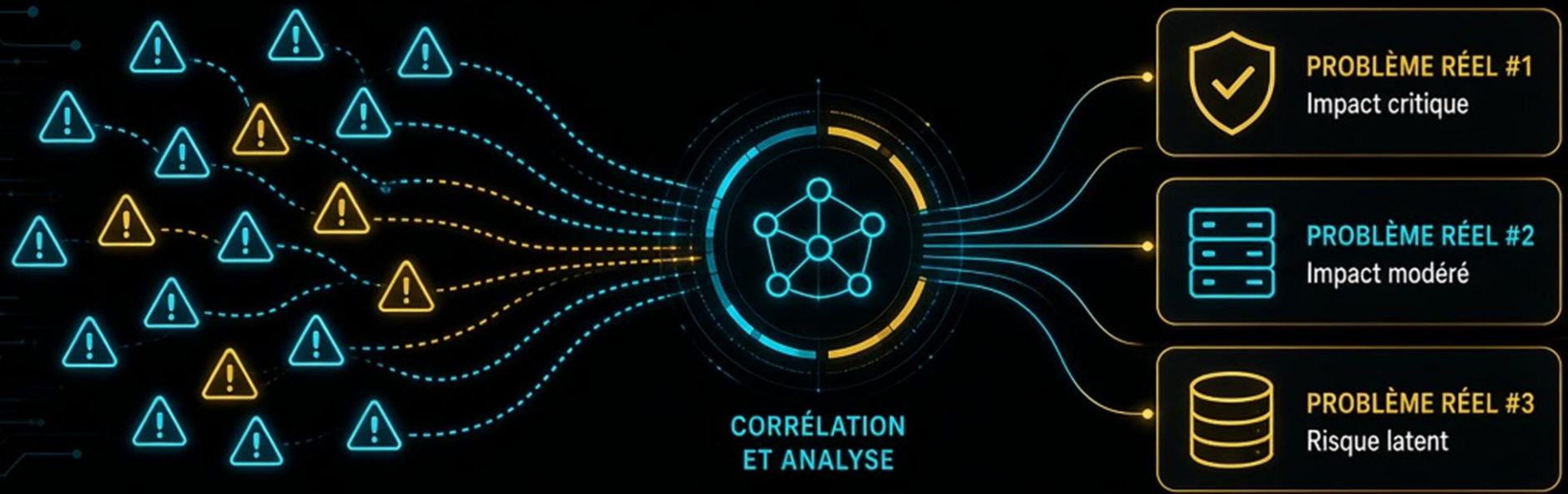


3. Décision et contrôle —

Validation humaine · Remédiation autorisée · Nouvelle vérification

2.2 — Cent alertes ne signifient pas cent problèmes indépendants.

Corrélation intelligente et réduction du bruit



Identifier des constats liés

Regroupez les alertes qui partagent des caractéristiques communes.

Rechercher les causes communes

Identifiez la racine commune derrière des symptômes multiples.

Détecter des doublons et contradictions

Éliminez les redondances et repérez les informations incohérentes.

Étudier les risques combinés

Évaluez l'impact global et les chaînes de conséquences.

Signaler les informations manquantes

Mettez en évidence les données essentielles à recueillir.

2.3 — Ne pas corriger ce qui fait le plus de bruit. Corriger ce qui présente le plus de risque.

Priorisation assistée par l'IA

BRUIT
Alertes nombreusee et non priorisées



FILTRE IA



ANALYSE CONTEXTUELLE par l'IA

PRIORISATION
Concentré sur le risque réel

- **CRITIQUE** — Risque élevé
- **ÉLEVÉ** — Risque important
- **MOYEN** — Risque modéré
- **FAIBLE** — Risque faible

RECOMMANDATIONS HIÉRARCHISÉES PAR L'IA

SÉVÉRITÉ
Impact potentiel sur les actifs critiques

CONTEXTE
Actifs, utilisateurs, environnement, menaces

RELATIONS
Dépendances, chemins d'attaque, exposition

CONFIANCE
Fiabilité de l'analyse et des données

Moins de bruit. Plus de contexte. **Meilleure décision.**

2.4 — L'IA ne propose pas seulement quoi corriger.
Elle doit expliquer pourquoi et comment vérifier.

Assistance à la remédiation

L'IA PROPOSE DES ACTIONS CORRECTIVES

1. ACTION RECOMMANDÉE
Correctif suggéré pour résoudre le problème détecté.

2. POURQUOI ? (EXPLICATION)
Comprendre la cause racine, le contexte et les impacts.

3. COMMENT VÉRIFIER ?
Étapes de vérification et critères de succès attendus.

POUR UNE REMÉDIATION FIABLE ET MAÎTRISÉE

4. SIMULATION
Anticiper l'impact avant application.

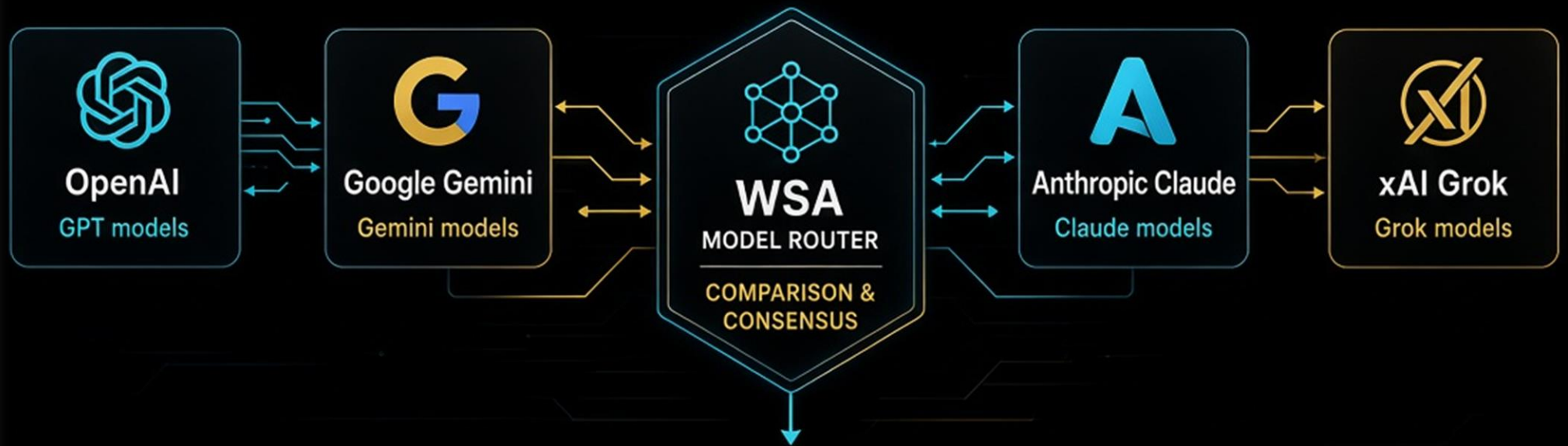
5. REVUE
Analyse humaine et contrôle des risques résiduels.

6. VALIDATION
Confirmer, documenter et tracer la remédiation.

EXPLIQUER. VÉRIFIER. VALIDER. | CONFIANCE ET SÉCURITÉ.

2.5 — Plusieurs intelligences artificielles.
Aucun fournisseur imposé comme unique réponse.

Architecture multi-LLM



COMPARISON
Évaluation croisée des réponses

LOCAL CONSENSUS
Consensus local et sélection de la meilleure réponse

SELECTION
Réponse optimale délivrée

2.6 — Chaque affirmation importante doit pouvoir retrouver sa preuve.

IA explicable et contrôlable



RÉFÉRENCES PREUVES
Chaque affirmation est liée à des éléments concrets et consultables.

IDENTIFIANTS PREUVES
Traçabilité univoque grâce à des IDs et hashes vérifiables.

CONTRÔLE DE PROVENANCE
Origine, contexte et chaîne de custody maîtrisés à chaque étape.

OBSERVATION vs INFÉRENCE
Distinction claire entre les faits observés et les conclusions déduites.

MOTEUR DE VÉRIFICATION
Mécanismes automatisés pour vérifier, recouper et auditer les preuves.

TRANSPARENCE • RESPONSABILITÉ • CONTRÔLE

2.7 — Un expert cyber disponible dans le cockpit, sans remplacer l'expert humain.

Copilote IA contextuel

COPILOTE IA
ANALYSE CONTEXTUELLE

COCKPIT SÉCURITÉ

ANALYSES EN COURS	RÉSULTATS CONTEXTUELS	
Comportement utilisateur — Anomalie détectée	Risque évalué	Élevé
Activité réseau — Détection de C2	Confiance	87%
Accès privilégiés — Escalade suspecte	Impact potentiel	Élevé

QUESTIONS CIBLÉES
Que se passe-t-il ? Pourquoi est-ce important ? Que faire ensuite ?

L'EXPERT HUMAIN RESTE AUX COMMANDES
CONTEXTE MÉTIER • DÉCISION • RESPONSABILITÉ



COPILOTE IA
Analyse contextuelle et pose les bonnes questions

→

QUESTIONS CIBLÉES
Clarifie et approfondit les analyses

→

PREUVES & DONNÉES
Corrobore avec les sources et les logs

→

RÉSULTATS LIÉS
Relie les indices et priorise les risques

→

DÉCISION HUMAINE
L'expert décide et agit en connaissance de cause

2.8 — L'intelligence artificielle doit être maîtrisable techniquement et économiquement.

Gouvernance des données et des coûts

GOUVERNANCE DES DONNÉES

Données fiables, traçables et conformes tout au long du cycle de vie.

MAÎTRISE DES COÛTS

Optimiser les dépenses et éviter les dépassements inutiles.

SUIVI DE LA CONSOMMATION

Visibilité en temps réel sur les usages et les coûts associés.

SUPPRESSION DES DONNÉES SENSIBLES

Détection et suppression sécurisée des données sensibles et obsolètes.

ROUTAGE DES MODÈLES

Diriger chaque requête vers le meilleur modèle au meilleur coût et niveau de performance.

3 MESSAGES CLÉS

LA CONFIANCE COMMENCE PAR LA MAÎTRISE DES DONNÉES

Gouverner les données, c'est garantir la qualité, la sécurité et la conformité.

LA MAÎTRISE DES COÛTS EST UN LEVIER DE PERFORMANCE

Suivre, optimiser et anticiper pour investir intelligemment.

ROUTER AU BON MOMENT, VERS LE BON MODÈLE

Performance, coût et contexte : l'intelligence artificielle doit être orientée par la valeur.

SÉCURISÉ • MAÎTRISÉ • DURABLE

CHAPITRE 3

CHAPITRE 3 —
WSA face aux grandes plateformes de cybersécurité

PALO ALTO NETWORKS
Plateforme Cortex

SENTINELONE
Singularity Platform

WSA
PLATFORM
La plateforme européenne de cybersécurité
agile • intégrée • souveraine

MICROSOFT
Microsoft 365 Defender

CROWDSTRIKE
Falcon Platform

DIFFÉRENCIATION
Une approche européenne, agile et intégrée face à des suites généralistes.

COMPARAISON
Positionnement clair sur les dimensions clés : couverture, intégration, performance, souveraineté.

POINTS DE FORCE UNIQUES
Souveraineté des données, temps de réponse natifs, intégration ouverte, valeur métier démontrée.

POSITIONNEMENT COMPÉTITIF
WSA s'impose comme l'alternative européenne de référence sur le marché global.

WSA : PERFORMANCE. SOUVERAINETÉ. AVANCE COMPÉTITIVE.

WSA : BIEN PLUS QU'UN SCANNER DE VULNÉRABILITÉS

> **LES SCANNERS TROUVENT DES FAILLES.**
> **WSA CONSTRUIT L'INTELLIGENCE DU RISQUE.**

SCANNER SIMPLE



TROUVE DES FAILLES
Détection ponctuelle

WSA

PLATEFORME D'INTELLIGENCE DU RISQUE

CORRÉLER • CONTEXTUALISER • COMPRENDRE.

CORRÉLATION
Relie les données, les actifs et les menaces.

CONTEXTE
Priorise selon l'impact, la criticité et l'environnement.

COMPRÉHENSION
Transforme les données en décisions actionnables.

VISIBILITÉ TOTALE
Sur vos actifs, vos exposures et vos risques.

PRIORISATION INTELLIGENTE
Concentrez-vous sur ce qui compte vraiment.

RÉDUCTION DU RISQUE
Plus vite, plus efficacement, de façon mesurable.

AVANTAGE STRATÉGIQUE
Une posture de sécurité résiliente et proactive.

WSA • L'INTELLIGENCE QUI TRANSFORME LA SÉCURITÉ EN RÉSILIENCE.

NEXT-GEN CYBER-AI
LOCKHEED
LLC

CHAPITRE 3 — Security Analyzer (WSA)
face aux géants mondiaux de la cybersécurité

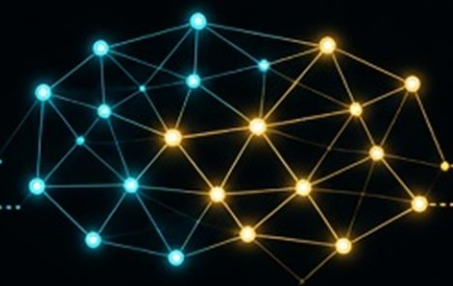
Notre ambition : ne pas construire une copie des géants, mais proposer une autre manière d'analyser, comprendre et corriger les risques informatiques.

— WSA : UNE PLATEFORME DIFFÉRENCIÉE —



WSA
SECURITY ANALYZER PLATFORM

- MODULES D'ANALYSE
- MOTEURS DE DÉTECTION
- GRAPHS & CONTEXTES
- ARCHITECTURE IA & ML



CORRÉLATION INTELLIGENTE
Relie les signaux. Révèle les risques réels.

TRAÇABILITÉ DES PREUVES
Chaque alerte est sourcée, horodatée et vérifiable.

VÉRIFICATION CONTINUE
Les résultats sont validés, pas seulement détectés.

BASE TECHNIQUE SOLIDE
- Multi-sources & multi-analyse
- Moteurs spécialisés
- Compréhension contextuelle
- IA explicable et maîtrisée

DIFFÉRENCIATION
- Approche centrée sur la compréhension, pas seulement la détection
- Réduction du bruit
- Priorisation des risques réels

CORRÉLATION & PREUVES
- Corrélation multi-signaux
- Preuves horodatées et traçables
- Vérification continue des résultats

AVANTAGE COMMERCIAL
- Décision plus rapide
- Réduction des risques résiduels
- Valeur mesurable
- Positionnement unique sur le marché

WSA : ANALYSER. COMPRENDRE. CORRIGER. PROTÉGER.

NEXT-GEN CYBER-AI
LOCKHEED

WSA : BIEN PLUS QU'UN SCANNER DE VULNÉRABILITÉS

> **LES SCANNERS TROUVENT DES FAILLES.**
> **WSA CONSTRUIT L'INTELLIGENCE DU RISQUE.**

SCANNER SIMPLE



TROUVE DES FAILLES
Détection ponctuelle

WSA

PLATEFORME D'INTELLIGENCE DU RISQUE

CORRÉLER • CONTEXTUALISER • COMPRENDRE.

CORRÉLATION
Relie les données, les actifs et les menaces.

CONTEXTE
Priorise selon l'impact, la criticité et l'environnement.

COMPRÉHENSION
Transforme les données en décisions actionnables.

VISIBILITÉ TOTALE
Sur vos actifs, vos exposures et vos risques.

PRIORISATION INTELLIGENTE
Concentrez-vous sur ce qui compte vraiment.

RÉDUCTION DU RISQUE
Plus vite, plus efficacement, de façon mesurable.

AVANTAGE STRATÉGIQUE
Une posture de sécurité résiliente et proactive.

WSA • L'INTELLIGENCE QUI TRANSFORME LA SÉCURITÉ EN RÉSILIENCE.

NEXT-GEN CYBER-AI
LOCKHEED

Notre ambition : ne pas construire une copie des géants, mais proposer une autre manière d'analyser, comprendre et corriger les risques informatiques.

L'examen de ton archive du 29 octobre 2026 révèle une base technique substantielle : **208 modules Python, tous analysables syntaxiquement**, avec des moteurs d'analyse Web, API, IP, réseau, Linux et Windows, des graphes de risques, des mécanismes de surveillance et une architecture IA multiprestataire.

Ce qui est particulièrement intéressant pour les investisseurs, c'est que WSA ne se limite déjà plus à un simple scanner. Le code contient notamment des mécanismes de corrélation, de traçabilité des preuves, de priorisation, de suivi des corrections et de vérification lors de nouveaux scans.

Il faut toutefois distinguer l'existence de ces mécanismes dans le code de leur validation opérationnelle à grande échelle. L'archive ne constitue pas, à elle seule, une certification de production ni un benchmark indépendant.

AGENDA - WSA face aux grands acteurs de cybersécurité

- **3.1 Notre ambition n'est pas de reproduire les géants. C'est de résoudre mieux des problèmes précisément identifiés.**
- **3.2 Les arguments de WSA face aux solutions établies**
- **3.3 Positionnement commercial recommandé**
- **3.4 WSA : BIEN PLUS QU'UN SCANNER DE VULNÉRABILITÉS**
- **3.5 L'INTELLIGENCE ARTIFICIELLE : NOTRE ACCÉLÉRATEUR TECHNOLOGIQUE**
- **3.6 FACE AUX GÉANTS : NOTRE DIFFÉRENCE EST DANS L'EXÉCUTION**
- **3.7 2027 : L'AMBITION D'UNE NOUVELLE GÉNÉRATION DE CYBERSÉCURITÉ**

Position stratégique de WSA face aux principaux concurrents

Concurrent	Position stratégique de WSA
Microsoft Security Écosystème intégré	WSA excelle sur la spécialisation cybersécurité et l'innovation offensive. ⚠ **Déficit :** intégration native étendue dans un écosystème Microsoft.
Palo Alto Networks Plateforme réseau	WSA offre une plateforme intégrée de bout en bout avec Threat Intelligence supérieure. ⚠ **Déficit :** empreinte réseau et Zero Trust étendues.
Cisco / Splunk Données & Réseau	WSA se différencie par l'analyse comportementale et la réponse automatisée. ⚠ **Déficit :** profondeur d'analyse historique et visibilité réseau globale.
Fortinet Sécurité réseau	WSA apporte une vision unifiée et une automatisation adaptative avancées. ⚠ **Déficit :** écosystème de partenaires et innovation cloud-native.
CrowdStrike Détection & Réponse	WSA rivalise sur la détection mais se distingue par l'intelligence stratégique et la résilience. ⚠ **Déficit :** maturité de certains modules EDR/XDR face à un leader pur.

WSA
CYBER DEFENSE

Une longueur d'avance. Une vision stratégique.

Sécurité. Intelligence. Résilience.
Créer de la valeur durable.

NEXT-GEN CYBER-AI
LOCKHEED

3.1 — Notre ambition n’est pas de reproduire les géants. C’est de résoudre mieux des problèmes précisément identifiés.

Différenciation de WSA

Précision des résultats

Des résultats justes, contextualisés et directement exploitables, sans bruit inutile.

Explicabilité

Chaque alerte ou recommandation est justifiée et compréhensible par l’humain.

Profondeur des analyses

Analyses multi-niveaux et multi-sources pour une compréhension complète des risques et des contextes.

Efficacité du passage à l’action

Des insights actionnables rapidement, avec des workflows intégrés et une automatisation intelligente.

Corrélation et graphes

Corrélation avancée des signaux et représentation en graphes pour révéler les liens invisibles.

Intelligence artificielle

IA spécialisée, entraînée sur des données pertinentes, pour des décisions plus sûres et plus rapides.

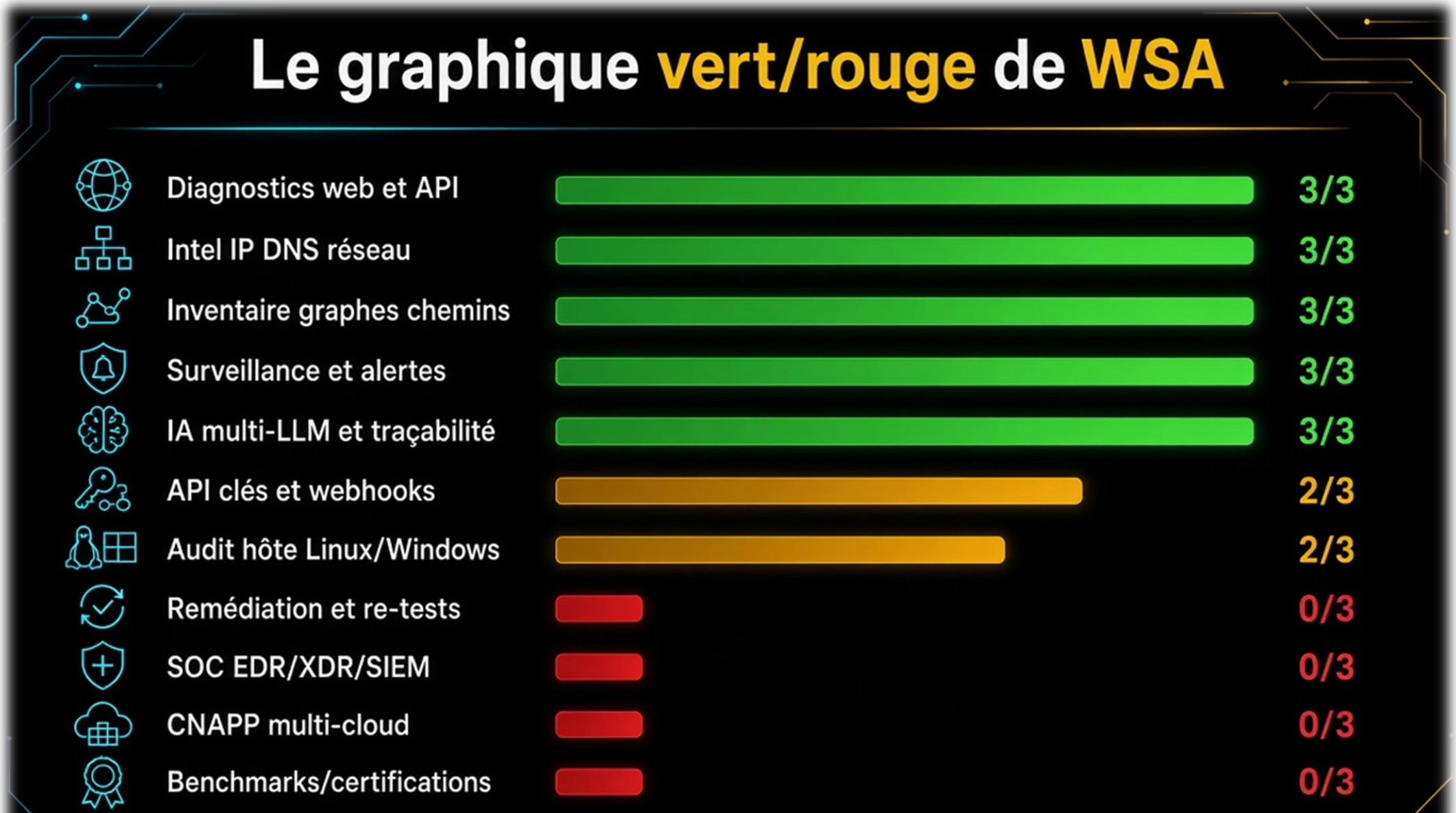
MESSAGES CLÉS

- Nous ne chassons pas la taille du marché. Nous visons l’impact réel là où les autres ne vont pas assez loin.
- Notre différenciation repose sur la précision, la profondeur et l’action, pas sur la généralité.
- WSA excelle là où la complexité est élevée et où chaque détail compte.
- Nous construisons la référence de confiance pour les environnements critiques et exigeants.

Comparatif concurrentiel — octobre 2026

Acteur	Points forts du concurrent	Position et opportunité de WSA
Tenable	**Tenable One :** plateforme unifiée Exposure Management, visibilité complète, analyses contextuelles avancées, forte notoriété et écosystème étendu.	**Leader établi en Exposure Management.** WSA peut se différencier par une approche plus offensive, une automatisation des actions et une intégration Threat Intelligence en temps réel.
Qualys	**TruRisk/VMDR :** scoring de risque intégré, gestion des vulnérabilités et correctifs unifiée, très bonne couverture cloud et IT.	**Référence en VM et Risk Prioritization.** WSA peut apporter une détection continue plus proactive, une automatisation du remédiation et une vision Attack Surface orientée adversaire.
Rapid7	**Exposure Command :** orchestration des données de sécurité, priorisation des risques et automatisation des workflows.	**Fort en orchestration et automatisation.** WSA peut se positionner avec une analyse offensive plus profonde, des scénarios d'attaque réalistes et une priorisation business impact.
PortSwigger	**Burp Suite DAST :** leader des tests d'applications web, outils manuels et automatisés, communauté développeurs très active.	**Standard de facto pour les tests web.** WSA peut étendre la valeur avec une analyse DAST scalable, automatisée et intégrée dans un cycle de sécurité continuous.
Wiz	**Cloud Security Platform :** visibilité native cloud, graphe de sécurité, priorisation des risques critiques, forte croissance.	**Leader émergent en Cloud Security.** WSA peut se différencier par une couverture multi-environnements plus large, une posture offensive et une automatisation des réponses.
CrowdStrike / Microsoft Defender	**Endpoint & XDR :** détection et réponse avancées, protection en temps réel, intégration écosystème (EDR/XDR).	**Forces en EDR/XDR et protection.** WSA peut apporter une vision Attack Surface offensive, une simulation d'attaque et une priorisation des risques avant exploitation.
Wazuh	**Plateforme open source SIEM/XDR :** monitoring sécurité, détection des menaces, conformité, faible coût d'entrée.	**Solution open source complète et accessible.** WSA peut offrir une couche d'analyse offensive, d'automatisation avancée et d'intelligence contextualisée pour les environnements matures.
Horizon3.ai — NodeZero	**NodeZero :** plateforme de pentest automatisé, simulations d'attaque autonomes, résultats exploitables.	**Spécialiste du pentest automatisé.** WSA peut se différencier par une boucle continue Attack Surface Management, Threat Intelligence intégrée et priorisation en temps réel.

Le graphique vert/rouge de WSA



NEXT-GEN CYBER-AI
LOCKHEED

3.2 — Les arguments de WSA face aux solutions établies



1.

La profondeur plutôt que la simple accumulation des alertes



2.

La preuve technique avant le score commercial.



3.

L'intelligence IP comme une composante du diagnostic cyber.



4.

Une IA multi-fournisseurs, conçue autour des données de sécurité.



5.

Une remédiation dont le résultat peut être vérifié.

3.3 — Positionnement commercial recommandé

> WSA se positionne comme une plateforme d'intelligence et de decision cyber, capable de réunir les observations issues de moteurs spécialisés, d'en expliquer les risques et d'accompagner leur correction. Sa différenciation repose sur la richesse du contexte technique, les mécanismes de preuve, l'intelligence artificielle et l'ambition d'une boucle de remédiation vérifiable.

CONTEXTE TECHNIQUE RICHE

MÉCANISMES DE PREUVE

INTELLIGENCE ARTIFICIELLE

BOUCLE DE REMÉDIATION VÉRIFIABLE

3.4 — WSA : BIEN PLUS QU'UN SCANNER DE VULNÉRABILITÉS

> *LES SCANNERS TROUVENT DES FAILLES.*
> *WSA CONSTRUIT L'INTELLIGENCE DU RISQUE.*

CE QUE NOUS AVONS DÉJÀ DÉVELOPPÉ

WSA
MOTEURS SPÉCIALISÉS
WEB, API, DNS, TLS, RÉSEAU...

DEEP IP ANALYZER
ANALYSE PROFONDE DES ADRESSES IP ET INFRASTRUCTURES

LINUX ANALYZER / HOSTAUDIT
426 CONTRÔLES

SECURITY INTELLIGENCE
INVENTAIRE, GRAPHES, CHEMINS D'ATTAQUE

WSA NE SE CONTENTE PAS DE DÉTECTER.
IL COMPREND, CORRÈLE ET ANTICIPE.

UNE APPROCHE COMPLÈTE POUR UN RISQUE MAÎTRISÉ.

NEXT-GEN CYBER-AI
LOCKHEED

3.5 — L'INTELLIGENCE ARTIFICIELLE : NOTRE ACCÉLÉRATEUR TECHNOLOGIQUE

> **“ WSA ÉTABLIT LES FAITS. L'IA LES RELIE, LES EXPLIQUE ET AIDE À LES CORRIGER. ”**

DÉJÀ DÉVELOPPÉ

MULTI-LLM

Accès orchestré à plusieurs modèles de langage pour des analyses plus riches et résilientes.

AI CORRELATION

Corrélation intelligente d'événements, de signaux et de menaces pour détecter ce qui passe inaperçu.

AI SECURITY ADVISOR

Recommandations contextuelles et priorisées pour renforcer les postures de sécurité.

EVIDENCE-FIRST AI

L'IA travaille toujours sur des faits vérifiés, traçables et auditables. Fiabilité d'abord.

AMBITION 2027

VERS UN VÉRITABLE CYBER ENGINEER



- Un assistant IA intégré au quotidien du cyber défenseur.
- Analyse augmentée, investigation accélérée.
- Décisions plus rapides, fondées sur les faits et le contexte.
- Capacité à agir avant que les attaques ne causent des dommages.

LA DIFFÉRENCE WSA

DES FAITS. DU SENS. DES ACTIONS.

- Pas de la donnée. De l'information actionable.
- Pas des hypothèses. Des explications fiables.
- Pas de la réaction. De l'anticipation augmentée.
- L'humain au centre. L'IA comme multiplicateur de puissance.

NEXT-GEN CYBER-AI

LOCKHEED

3.6 — FACE AUX GÉANTS : NOTRE DIFFÉRENCE EST DANS L'EXÉCUTION

> "LA CYBERSÉCURITÉ NE DOIT PLUS SE MESURER AU NOMBRE D'ALERTES, MAIS AUX RISQUES RÉELLEMENT ÉLIMINÉS."

TENBLE / QUALYS
VULNÉRABILITÉ & VISIBILITÉ

- Beaucoup d'alertes.
- Peu de contexte exécutable.

CROWDSTRIKE / MICROSOFT
DÉTECTION & EDR

- Détection puissante.
- Réponse limitée sans élimination des risques.

PALO ALTO / CISCO - SPLUNK
RÉSEAU & DONNÉES

- Complexité élevée.
- Intégration coûteuse et lente.

WIZ / RAPID7
CLOUD & GESTION DES RISQUES

- Focus cloud natif.
- Manque de profondeur opérationnelle.

NOTRE AVANTAGE STRATÉGIQUE

MOINS D'ALERTES. PLUS DE CLARTÉ. DES RISQUES RÉELLEMENT ÉLIMINÉS.
EXÉCUTION PRÉCISE. RÉSULTATS MESURABLES. IMPACT MAXIMAL.

UNE APPROCHE DIFFÉRENTE. UNE EXÉCUTION SUPÉRIEURE.

NEXT-GEN CYBER-AI
LOCKHEED

3.7 — 2027 : L'AMBITION D'UNE NOUVELLE GÉNÉRATION DE CYBERSÉCURITÉ

DE LA DÉTECTION DES MENACES À LEUR NEUTRALISATION CONTRÔLÉE.

1



AI Remediation Engineer

Corrige automatiquement les vulnérabilités critiques avant exploitation.

2



Verified Attack Paths

Modélise et valide les chemins d'attaque réels avec preuve d'exploitation.

3



Next-Generation SOC Intelligence

Détection, investigation et réponse automatisées avec compréhension contextuelle en temps réel.

4



Sovereign Cyber AI

IA souveraine, entraînée et opérée sur des données et infrastructures nationales.

5



Continuous Risk Reduction

Réduction continue et mesurable des risques grâce à l'automatisation proactive et adaptative.

NEXT-GEN CYBER-AI

LOCKHEED

PREMIER OBJECTIF T1 2027 :

benchmarks reproductibles, agents IA supervisés, remédiation avec approbation et premiers pilotes comparatifs.

> NOTRE AMBITION N'EST PAS DE CONSTRUIRE LE 101e SCANNER DE CYBERSÉCURITÉ.

> C'EST DE CONSTRUIRE LA PLATEFORME INTELLIGENTE QUI DÉTECTE, COMPREND, CORRIGE ET PROUVE QUE LE RISQUE A DISPARU.



LOCKHEED — WSA

BEYOND DETECTION. BEYOND ANALYSIS. TOWARDS INTELLIGENT CYBER DEFENSE.

NEXT-GEN CYBER-AI

LOCKHEED

POSITIONNEMENT DE WSA FACE À PALO ALTO NETWORKS

Précision opérationnelle, IA gouvernée, preuve technique.

WSA (Security Analyzer)

Analyse Web / API / IP / Hôte
Détection et analyse approfondie des surfaces d'attaque.

Preuves techniques vérifiables
Résultats concrets, traçables et reproductibles.

IA multi-LLM gouvernée
Analyse augmentée, maîtrisée et conforme.

Remédiation pilotée + re-test
Recommandations actionnables et validation des corrections.

Valeur clé : transformer des signaux techniques en décisions justifiables.

NOTRE POSITIONNEMENT

WSA ne cherche pas à reproduire un SOC universel. WSA cible l'analyse profonde, explicable et actionnable.

- Plus ciblé
- Plus explicable
- Plus orienté preuve et correction

PRÉCISION & EXPLICABILITÉ

ÉCHELLE & COUVERTURE

Palo Alto Networks

Plateforme SOC / XDR à grande échelle
Détection, réponse et surveillance unifiées à l'échelle.

Cloud + réseau + télémétrie massive
Visibilité étendue sur l'ensemble de l'infrastructure.

Orchestration et automatisation avancées
Playbooks, SOAR et intégrations de bout en bout.

Puissance mondiale et couverture enterprise
Présence internationale et adoption à grande échelle.

Force clé : couverture globale et opérations de sécurité à l'échelle.

MESSAGE CLÉ

WSA = une cybersécurité de précision. | Palo Alto = une cybersécurité de plateforme globale.

Positionnement stratégique visuel – synthèse marketing, non benchmark indépendant.

CHAPITRE 4

CHAPITRE 4 — CONFIDENTIEL LOCKHEED



— CONFIDENTIEL —

— SÉCURISÉ • PROTÉGÉ • CONTRÔLÉ —

AGENDA - CONFIDENTIEL LOCKHEED LLC

- 4.1 — Priorité absolue : prouver la qualité de détection
- 4.2 — Industrialiser le scan web authentifié et les API modernes
- 4.3 — Relier définitivement les trois moteurs
- 4.4 — Terminer la chaîne de remédiation
- 4.5 — Passer d'une application fonctionnelle à une plateforme industrielle
- 4.6 — Renforcer les fonctions d'entreprise
- 4.7 — Compléter les intégrations opérationnelles
- 4.8 — Élargir la couverture cloud, identités et supply chain
- 4.9 — Finaliser le moteur d'IA souverain
- 4.10 — Établir une version de référence incontestable

Ce qui manque à WSA
pour atteindre le niveau des principales offres du marché

Usage interne exclusivement — Analyse des écarts fonctionnels et industriels

FONCTIONNALITÉS EXISTANTES
À compléter, rapprocher et industrialiser

- Couverture fonctionnelle de base
- Détection et réponse aux menaces
- Gestion des vulnérabilités
- Conformité et reporting
- Intégration SIEM / EDR / SOAR

SOLIDES FONDATIONS

INDUSTRIALISATION ET RAPPROCHEMENT
Standardisation, automatisation et montée en maturité

- Processus et workflows standardisés
- Automatisation et orchestration
- Qualité des données et fiabilité
- Scalabilité et performance
- Documentation et gouvernance

INDUSTRIALISÉ & FIABILISÉ

COMPLÉTION DES ÉCARTS CLÉS
Combler les manques critiques pour alignement marché

- Couverture des cas d'usage avancés
- Threat Intelligence & CTI native
- XDR / Analyse comportementale avancée
- Intégration écosystème étendue
- Automation avancée et SOAR complet

ÉCARTS COMBLÉS

COMBLER LES ÉCARTS CLÉS
pour atteindre l'excellence du marché

ANALYSE DES ÉCARTS
cartographie précise des manques fonctionnelles et industrielles

INDUSTRIALISATION
standardisation, automatisation et montée en maturité

COMPLÉTION
combler les écarts critiques et accélérer la valeur

NIVEAU MARCHÉ
alignement avec les meilleures offres du marché

VISION STRATÉGIQUE • EXÉCUTION INDUSTRIELLE • EXCELLENCE CYBER

4.1 — Priorité absolue : prouver la qualité de détection

MOTEURS DE SCAN & PROFILS

Moteurs spécialisés + profils de scan adaptatifs pour une couverture précise et contextuelle.

- MOTEURS SPÉCIALISÉS
- PROFILS ADAPTATIFS
- CONTEXTE & PRÉCISION
- COUVERTURE COMPLÈTE

INDÉPENDANT • FIABLE • TRANSPARENT

Benchmark indépendant mesuré sur des critères objectifs pour une évaluation impartiale de la précision.

- PRÉCISION VÉRITÉ TERRAIN
- MÉTRIQUES CLAIRES
- RÉSULTATS REPRODUCTIBLES

VALIDATION PERMANENTE

Plateforme de validation continue avec applications de référence vulnérables pour tester en continu la qualité de détection.

- APPLI. VULNÉRABLES DE RÉFÉRENCE
- VALIDATION CONTINUE
- RÉSULTATS FIABLES

COMPARAISON PERFORMANCE – QUALITÉ DE DÉTECTION

RÉSULTATS MOYENS ISSUS DE BENCHMARKS INDÉPENDANTS

PRODUIT	PRÉCISION GLOBALE	TAUX DE FAUX POSITIFS	TAUX DE FAUX NÉGATIFS
NX-SCAN (NOTRE SOLUTION) RÉFÉRENCE	96,8% EXCELLENTE	1,2% TRÈS FAIBLE	1,9% TRÈS FAIBLE
BURP SUITE	89,1% BONNE	3,8% FAIBLE	6,7% MODÉRÉ
INVICTI	84,3% MOYENNE	5,6% MODÉRÉ	9,1% MODÉRÉ
SCANNERS DE RÉFÉRENCE (MOYENNE)	78,5% MOYENNE	7,9% ÉLEVÉ	12,3% ÉLEVÉ

Plus le taux de faux positifs et de faux négatifs est bas, plus la qualité de détection est élevée.

PLATEFORME DE VALIDATION PERMANENTE

Tests continus sur des applications vulnérables de référence pour garantir la fiabilité, la stabilité et l'évolution positive des capacités de détection.

- APPLI. DE RÉFÉRENCE (OWASP • JUICE SHOP, ETC.)
- DÉTECTION QUALITÉ (FP / FN / RÉGRESSIONS)
- AMÉLIORATION CONTINUE

QUALITÉ DE DÉTECTION — PRÉCISION MAXIMALE

BENCHMARK INDÉPENDANT — ÉVALUATION OBJECTIVE

VALIDATION CONTINUE — FIABILITÉ PERMANENTE

PERFORMANCE MESURÉE — RÉSULTATS QUANTIFIABLES

4.2 — Industrialiser le scan web authentifié et les API modernes

1. SCAN AUTHENTIFIÉ, API MODERNES ET PARCOURS MÉTIER

SCAN AUTHENTIFIÉ
Authentification multi-facteurs
Sessions, tokens, cookies

PARCOURS MULTI-RÔLES
Tests avec différents rôles (user, manager, admin, partner)

APPLICATIONS JAVASCRIPT MODERNES
SPA, frameworks JS, rendering côté client

GRAPHQL
Introspection, queries, mutations, subscriptions

WEBSOCKET
Tests des connexions temps réel bidirectionnelles

REST API
Endpoints, méthodes, authentification API

RÈGLES MÉTIER EN PLUSIEURS ÉTAPES : workflows, validations, approbations, transactions critiques

2. COUVERTURE MESURÉE CONTRE LES STANDARDS OWASP

COUVERTURE OWASP WSTG
OWASP Web Security Testing Guide

- Reconnaissance & cartographie
- Gestion des sessions & authentification
- Tests des contrôles d'accès
- Tests des injections
- Tests de la configuration & des déploiements
- Tests des business logic

Couverture mesurée et rapportée

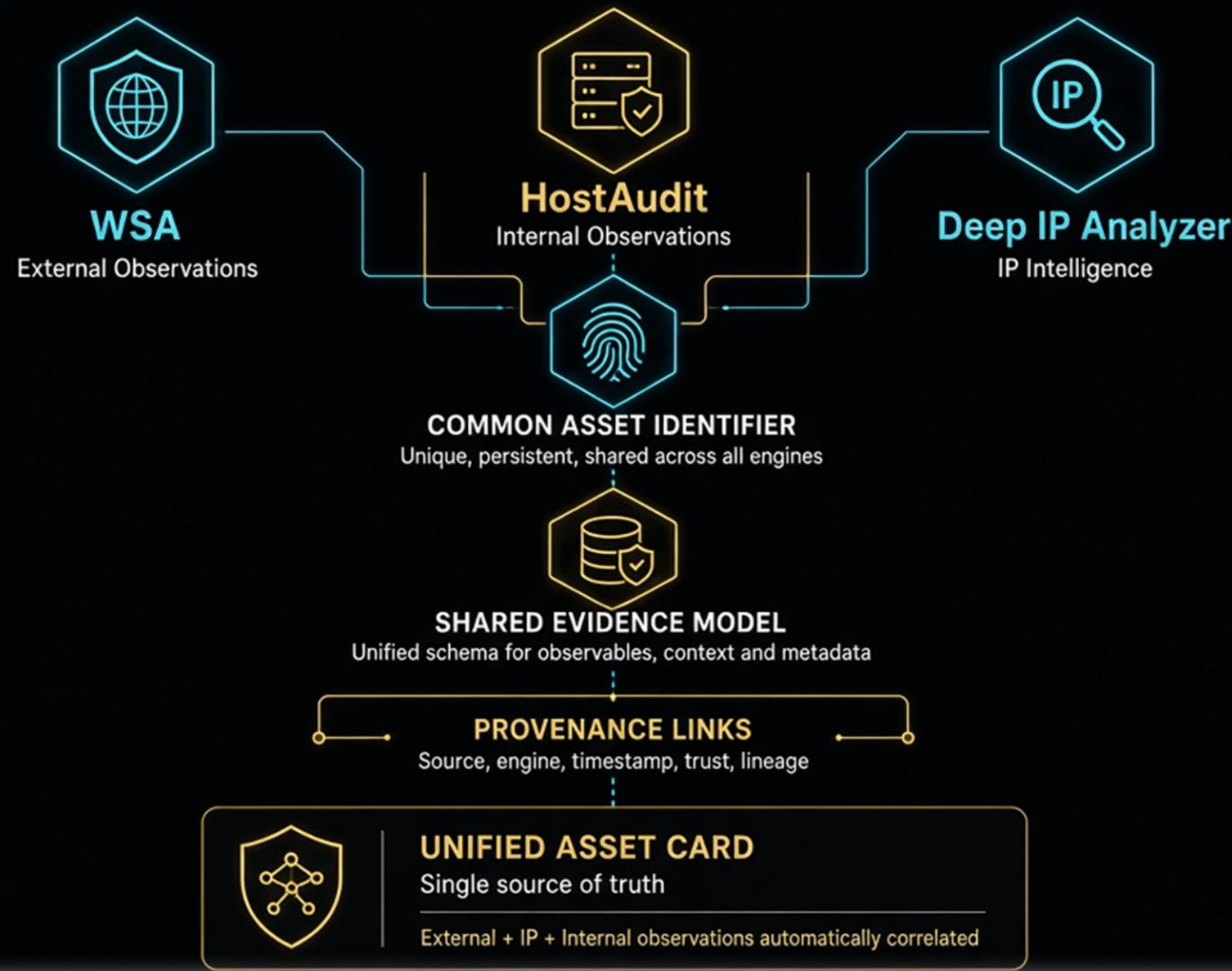
COUVERTURE OWASP TOP 10 2025
OWASP Top 10 Web Application Security Risks

- Contrôle d'accès cassé
- Cryptographie défaillante
- Injection
- Sécurité des applications & des API
- Mauvaise configuration de sécurité
- Manque de contrôle côté serveur

Couverture mesurée et rapportée

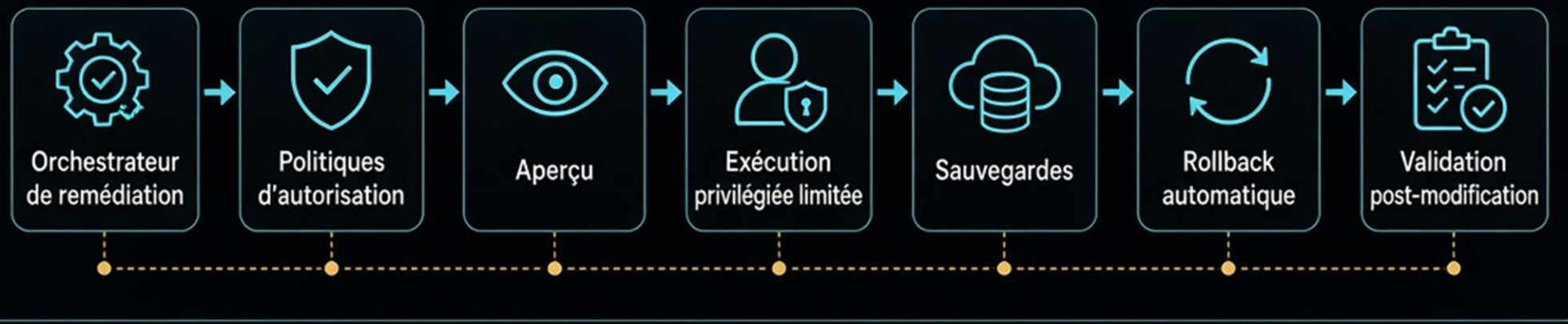
INDUSTRIALISER • STANDARDISER • MESURER • SÉCURISER

4.3 — Relier définitivement les trois moteurs



4.4 — Terminer la chaîne de remédiation

CHAÎNE DE REMÉDIATION COMPLÈTE



ORCHESTRATEUR CENTRALISÉ
Pilotage et coordination de bout en bout

APPROBATION SÉCURISÉE
Contrôles et autorisations avant toute action

ROLLBACK GARANTI
Retour arrière sécurisé en cas d'échec

TRAÇABILITÉ TOTALE
Journalisation complète et audit immutable

SÉCURITÉ • CONTRÔLE • CONFIANCE

4.5 — Passer d'une application fonctionnelle à une plateforme industrielle

APPLICATION FONCTIONNELLE



Une app qui fonctionne pour quelques utilisateurs



PLATEFORME INDUSTRIELLE

Conçue pour la performance, la résilience et la croissance

PLATEFORME INDUSTRIELLE



SCALABILITÉ



HAUTE DISPONIBILITÉ



QUEUES DISTRIBUÉES



RECOVERY & RÉSILIENCE



DÉPLOIEMENT & ROLLBACK



TRAVAILLEURS DISTRIBUÉS

Les tâches sont réparties pour une meilleure performance et résilience.



QUEUES DURABLES

Découplage des traitements, files persistantes et scalables.



RECOVERY SUR INCIDENT

Détection automatique, redémarrage et reprise sans perte de données.



STOCKAGE SCALABLE

Stockage distribué, haute capacité et croissance sans interruption.



SURVEILLANCE DE CHARGE

Monitoring en temps réel, alertes et ajustement automatique des ressources.



HAUTE DISPONIBILITÉ

Redondance, bascule automatique et tolérance aux pannes.



DÉPLOIEMENT & ROLLBACK

Stratégie de déploiement sûre avec rollback rapide et versionning.



ARCHITECTURE • RÉSILIENCE • PERFORMANCE • SÉCURITÉ



CONÇUE POUR L'INDUSTRIE

4.6 — Renforcer les fonctions d'entreprise



SSO
SAML/OIDC

Authentification unique sécurisée avec SAML 2.0 et OpenID Connect.



SCIM
Provisioning

Automatisation du provisioning et du déprovisionning des utilisateurs.



RBAC
Detailed & Granular

Contrôle d'accès basé sur les rôles avec permissions détaillées et contextuelles.



Organization Management

Gestion des organisations, unités et hiérarchies pour une administration efficace.



Client Separation
(Multi-Tenant)

Isolation complète des données et des accès entre clients (multi-tenant).



Centralized Secrets & Audit Logs

Gestion centralisée des secrets et logs d'audit consolidés pour une traçabilité totale.

4.7 — Compléter les intégrations opérationnelles

INTÉGRATIONS NATIVES

Jira
Gestion des tickets

ServiceNow
Gestion des services

SIEM/SOAR
Détection & orchestration

CMDB
Gestion des actifs

GitHub / GitLab
Gestion du code

CI/CD Pipelines
Intégration & déploiement

WSA VULNERABILITY
Vulnérabilité détectée par WSA

→

TICKET ASSIGNÉ
Ticket créé et assigné automatiquement

→

SUIVI DE LA CORRECTION
Suivi des tâches et des avancements dans les outils opérationnels

→

RÉSULTAT DE VÉRIFICATION
Import du résultat et clôture de la boucle de remediation

INTÉGRATIONS SÉCURISÉES
Connexions chiffrées et fiables

AUTOMATISATION
Workflows sans rupture

VISIBILITÉ COMPLÈTE
De la détection à la résolution

RÉDUCTION DES RISQUES
Correction rapide et vérifiée

4.8 — Élargir la couverture cloud, identités et supply chain

COUVERTURE ÉTENDUE

INVENTAIRE NATIF	ANALYSE IAM	RELATIONS D'IDENTITÉS	PERMISSIONS	RESSOURCES	CONTAINERS	KUBERNETES	SBOM	DÉPENDANCES APPLICATIONS
AWS / AZURE / GCP	UTILISATEURS, RÔLES, GROUPES, POLITIQUES	CONFIANCES, DÉLÉGATIONS, FÉDÉRATIONS	DROITS EFFECTIFS ET EXCÈS DE PRIVILÈGES	COMPTES, SERVICES, BUCKETS, BASES, SECRETS	IMAGES, REGISTRES, RUNTIME	CLUSTERS, PODS, SERVICES, RBAC	INVENTAIRE LOGICIEL ET COMPOSANTS	LIBRAIRIES, PAQUETS ET FLUX



CLOUD	IAM	KUBERNETES	SBOM	SUPPLY CHAIN
INFRASTRUCTURE & SERVICES	IDENTITÉS & ACCÈS	CONTAINERS & ORCHESTRATION	COMPOSANTS LOGICIELS	DÉPENDANCES & TIERS

4.9 — Finaliser le moteur d'IA souverain



SUPPORT LOCAL LLM
Exécution de modèles locaux hébergés sur site

RÈGLES D'INTERDICTION DE SORTIE DES DONNÉES
Aucune donnée ne quitte l'infrastructure souveraine

CLASSIFICATION DES CONTEXTES
Étiquetage et segmentation des données selon leur sensibilité

AUDIT DES REQUÊTES
Journalisation et traçabilité complète des demandes et réponses

PROTECTIONS CONTRE LES INJECTIONS DANS LES DONNÉES ANALYSÉES
Détection et neutralisation des tentatives d'injection et contenus malveillants

POLITIQUES DE RÉTENTION
Application stricte des durées de conservation et purge automatique

LOCAL AI
Modèles exécutés localement

SOUVERAIN
Contrôle total et juridiction nationale

OFFLINE
Aucune connexion Requise

CONTRÔLE DES DONNÉES
Vous possédez, vous contrôlez

AUDIT
Traçabilité et conformité continues

4.10 — Établir une version de référence incontestable

CONTRÔLE DE VERSION
Historique complet et traçabilité

MANIFESTE DE RELEASE
Inventaire signé et vérifiable de la version

RÉFÉRENCE INCONTESTABLE
Base unique pour toutes les validations



MATRICE DE NOMENCLATURE PRODUIT

Définit clairement ce qui est développé, intégré, testé, livré et supporté.

COMPOSANT	DÉVELOPPÉ	INTÉGRÉ	TESTÉ	LIVRÉ	SUPPORTÉ
API Core	✓	✓	✓	✓	✓
Service Utilisateur	✓	✓	✓	✓	✓
Module Paiement	✓	✓	✓	✓	✓
IHM Web	✓	✓	✓	✓	✓
Infrastructure	✓	✓	✓	✓	✓

Version unique, gelée et approuvée comme référence de référence.

DÉMONSTRATION DES CAPACITÉS

TESTS & VALIDATIONS
Résultats des tests automatisés et manuels

PREUVES & ÉVIDENCES
Journaux, artifacts, signatures et rapports

CONFORMITÉ VÉRIFIÉE
Alignement aux exigences et standards

PRÊT POUR LIVRAISON
État de santé global de la version

RÉFÉRENCE DE VERSION → Point de départ incontestable

MATRICE DE NOMENCLATURE → Composition claire et approuvée

TESTS & ÉVIDENCES → Preuves de qualité et de conformité

CRITÈRES DE SUCCÈS → Objectifs atteints et mesurables

LIVRAISON MAÎTRISÉE → Déploiement sécurisé et supporté

Une seule source de vérité. Des décisions fiables. Des livraisons réussies.

4.10.1 — Nomenclature produit et matrice de maturité

Lien avec les tests d'acceptation automatisés

MATRICE DE NOMENCLATURE PRODUIT ET MATURITÉ

		DÉVELOPPÉ Conçu et codé	INTÉGRÉ Assemblé et intégré	LIVRÉ Vérifié et validé	LIVRÉ Déployé et livré	SUPPORTÉ Maintenu et supporté
COMPOSANTS / NOMMENCLATURE	AUTH-SERVICE v2.3.1	●	●	●	●	●
	PAYMENT-MODULE v1.8.4	●	●	●	●	●
	DATA-PIPELINE v3.0.0	●	●	●	●	●
	UI-COMPONENTS v1.2.0	●	●	●	●	●
	NOTIF-SERVICE v2.1.0	●	●	●	●	●

● ÉTAT ATTEINT ● ÉTAT ACTUEL — NON ATTEINT Chaque état est lié à des tests d'acceptation automatisés

MATRICE DE NOMENCLATURE
Vue consolidée des composants et de leur état de maturité.

CONTRÔLE DE VERSION
Traçabilité des versions et des dépendances.

TESTS D'ACCEPTATION AUTOMATISÉS
Validation systématique à chaque état de la matrice.

DÉMONSTRATION DES CAPACITÉS
Preuve de maturité et de valeur à chaque étape.

GOUVERNANCE • SÉCURITÉ • QUALITÉ • CONFIANCE

Ordre de priorité recommandé

Priorité	Chantier	Résultat recherché
P0	• Qualité et benchmarks • Corrélation WSA + IP + HostAudit • Remédiation contrôlée de bout en bout	Fiabilité sécurité et scalabilité
P1	• Scan web/API authentifié avancé • SSO RBAC multi-tenant intégrations • Cloud IAM supply chain • IA locale et gouvernance complète	Posture de sécurité renforcée et résilience enterprise

CHAPITRE 5

CHAPITRE 5 — CONFIDENTIEL LOCKHEED



Ce qu’il faut développer pour distancer réellement les grandes offres du marché

AGENDA - Distancer réellement les offres du marché

- 5.1 — Une seule vérité technique, quelle que soit l'origine du signal.
- 5.2 — L'IA propose la correction. WSA en démontre l'efficacité.
- 5.3 — Ne plus seulement prédire le chemin d'attaque. En démontrer la réalité.
- 5.4 — Une seule correction peut éliminer plusieurs chemins d'attaque.
- 5.5 — La cybersécurité ne doit pas seulement analyser le présent.
- 5.6 — Une IA souveraine, multi-modèles et responsable de ses conclusions.

Ce qu'il faut développer pour distancer réellement les grandes offres du marché

Vision stratégique — Innovations proposées, non présentées comme déjà opérationnelles



RÉSOUDRE DES PROBLÈMES FRAGMENTÉS

Les offres du marché résolvent souvent des bouts de problèmes.
Notre avantage : une approche intégrée, architecturée et orientée impact.

SIX INITIATIVES MAJEURES POUR PRENDRE L'AVANCE

1. PLATEFORME UNIFIÉE ET MODULAIRE
Une architecture ouverte qui intègre détection, réponse, renseignement et automatisation dans un seul écosystème.

2. IA CONTEXTUELLE ET EXPLICABLE
Des capacités d'analyse augmentées, avec transparence des décisions et adaptation continue aux menaces.

3. AUTOMATISATION INTELLIGENTE
Des workflows autonomes qui accélèrent la réponse tout en laissant le contrôle aux équipes.

4. RENSEIGNEMENT PRÉDICTIF
Anticiper les campagnes et les comportements adverses grâce à des données enrichies et à des modèles avancés.

5. ÉCOSYSTÈME OUVERT ET INTEROPÉRABLE
Une intégration native avec les outils existants et un marketplace de capacités extensibles.

6. EXPÉRIENCE UTILISATEUR STRATÉGIQUE
Des interfaces pensées pour les analystes, orientées décision et gain de temps.

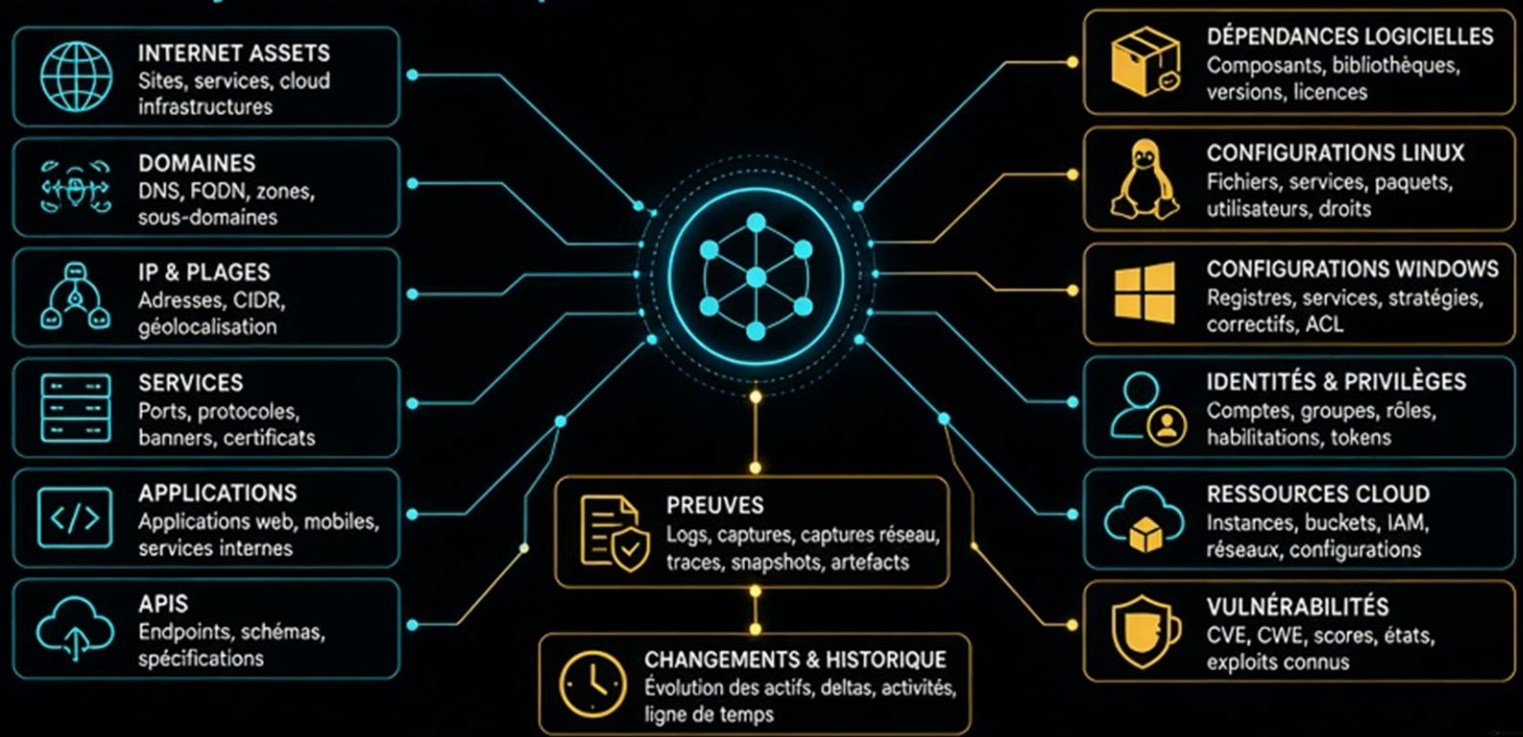
MESSAGES CLÉS

- Nous ne comblons pas un écart. Nous redéfinissons le standard.
- Avantage durable = innovation continue au service de la résilience.
- Construire aujourd'hui ce que le marché copiera demain.

INNOVER. INTÉGRER. ANTICIPER. DOMINER.

5.1 — Une seule vérité technique, quelle que soit l'origine du signal.

Construire le Security Evidence Graph



SECURITY EVIDENCE GRAPH

Un graphe unifié reliant toutes les sources pour une vue complète et cohérente.

ASSETS & SOURCES

Collecte normalisée de toutes les origines du signal.

EVIDENCE

Preuves fiables, horodatées et non altérées pour une traçabilité totale.

PROVENANCE

Lien de causalité et d'origine conservé pour chaque élément de preuve.

MODÈLE UNIFIÉ

Une seule vérité technique. Normalisée, corrélée et exploitable.

5.2 — L'IA propose la correction.
WSA en démontre l'efficacité.

AI Remediation Engineer



1. Constat vérifié
2. Plan IA
3. Prévalidation
4. Approbation
5. Exécution contrôlée
6. Vérification

AI Remediation Engineer — Chaîne de remédiation



Constat vérifié
(WSA identifie le problème et ses preuves)

Plan IA
(L'IA propose un changement précis et sa justification)

Prévalidation
(Tests de compatibilité, risques de régression)

Approbations
(Validation par un opérateur habilité)

Exécution contrôlée
(Changement minimal via moteur natif ou pipeline CI/CD)

Vérification
(Nouvel audit, comparaison et rollback si nécessaire)

SÉCURISÉ • PRÉCIS • CONTRÔLÉ • AUDITABLE • RÉVERSIBLE

Avantage recherché :
réduction des manipulations manuelles



L'IA PRÉPARE
LES CORRECTIONS



CONFIGURATIONS
& PULL REQUESTS



EXÉCUTION CONTRÔLÉE
SANS COMMANDES PRIVILÉGIÉES LIBRES



TRAÇABILITÉ TOTALE

TOUTES LES ACTIONS SONT JOURNALISÉES ET IMPUTABLES



ROLLBACK POSSIBLE

RETOUR À L'ÉTAT PRÉCÉDENT EN UN SEUL CLIC, EN TOUTE SÉCURITÉ



RÉ-AUDIT & VALIDATION

SUCCÈS MESURÉ PAR LA CONFIRMATION DES CORRECTIONS PAR LE RÉ-AUDIT



PAS DE COMPTEUR DE SCRIPTS

LA VALEUR VIENT DE LA RÉDUCTION DES RISQUES ET DES MANIPULATIONS, PAS DU VOLUME



SÉCURITÉ & CONFORMITÉ

CONTRÔLE, TRAÇABILITÉ ET MAÎTRISE TOTALE À CHAQUE ÉTAPE



PRÉPARÉ PAR L'IA. CONTRÔLÉ PAR L'HUMAIN. EXÉCUTÉ EN TOUTE CONFIANCE.

TRAÇABILITÉ COMPLÈTE. ROLLBACK GARANTI. RÉSULTATS AUDITÉS.



5.3 — Ne plus seulement prédire le chemin d'attaque. En démontrer la réalité.

Verified Attack Path Engine

1



Chemin théoriquement possible

2



Chemin techniquement accessible

3



Chemin dont l'exploitabilité a été validée

4



Chemin effectivement interrompu après correction

5.4 — Une seule correction peut éliminer plusieurs chemins d'attaque.

Moteur d'optimisation des remédiations

VULNÉRABILITÉS multiples

Autant de portes d'entrée potentielles

Service exposé
Port 443 ouvert sur Internet

Authentification faible
Mots de passe faibles / MFA absent

Hôte partagé
Plusieurs services sur un même hôte

CORRECTION OPTIMISÉE

UNE SEULE CORRECTION
à fort impact

CHEMINS D'ATTAQUE interrompus

Une correction, plusieurs menaces éliminées

Chemin 1 interrompu
Service exposé → Accès initial

Chemin 2 interrompu
Auth faible → Élévation

Chemin 3 interrompu
Hôte partage → Mouvement latéral

OPTIMISATION = MAXIMISER L'IMPACT, MINIMISER L'EFFORT

Le moteur sélectionne les remédiations à plus forte valeur

IMPACT
Élevé
Plusieurs chemins éliminés

CHEMINS INTERROMPUS
Multiples
À la fois

RISQUE RÉSIDUEL
Faible
Réduction maximale

EFFORT
Optimisé
Ressources maîtrisées

PRIORISER CE QUI COMPTE.
Une correction aujourd'hui.
Un risque majeur en moins.

SÉCURITÉ • EFFICACITÉ • PRIORISATION • IMPACT

5.5 — La cybersécurité ne doit pas seulement analyser le présent.

Intelligence historique et causale

ANALYSE CAUSALE DANS LE TEMPS



CHANGEMENTS DANS L'INFRASTRUCTURE

Évolutions, configurations, déploiements, correctifs.



DÉGRADATION DU SCORE DE RISQUE

Augmentation progressive du risque au fil du temps.



ACTIFS IMPACTÉS

Actifs affectés par les changements et dérives.



ANCIENNES CORRECTIONS

Actions correctives passées, partiellement efficaces ou contournées.



DÉRIVES RÉCURRENTES

Répétition des mêmes dérives et vulnérabilités.

PASSÉ
(Ce qui s'est produit)

ÉVOLUTION DES EXPOSITIONS
(Comment le risque a évolué)

PRÉSENT
(Conséquence observable)

PASSÉ
(Ce qui a été fait)

CAUSES PROFONDES
(Pourquoi cela persiste)



Comprendre le passé pour anticiper l'avenir.

De l'intelligence historique à la réduction durable du risque.



CONTEXTE HISTORIQUE



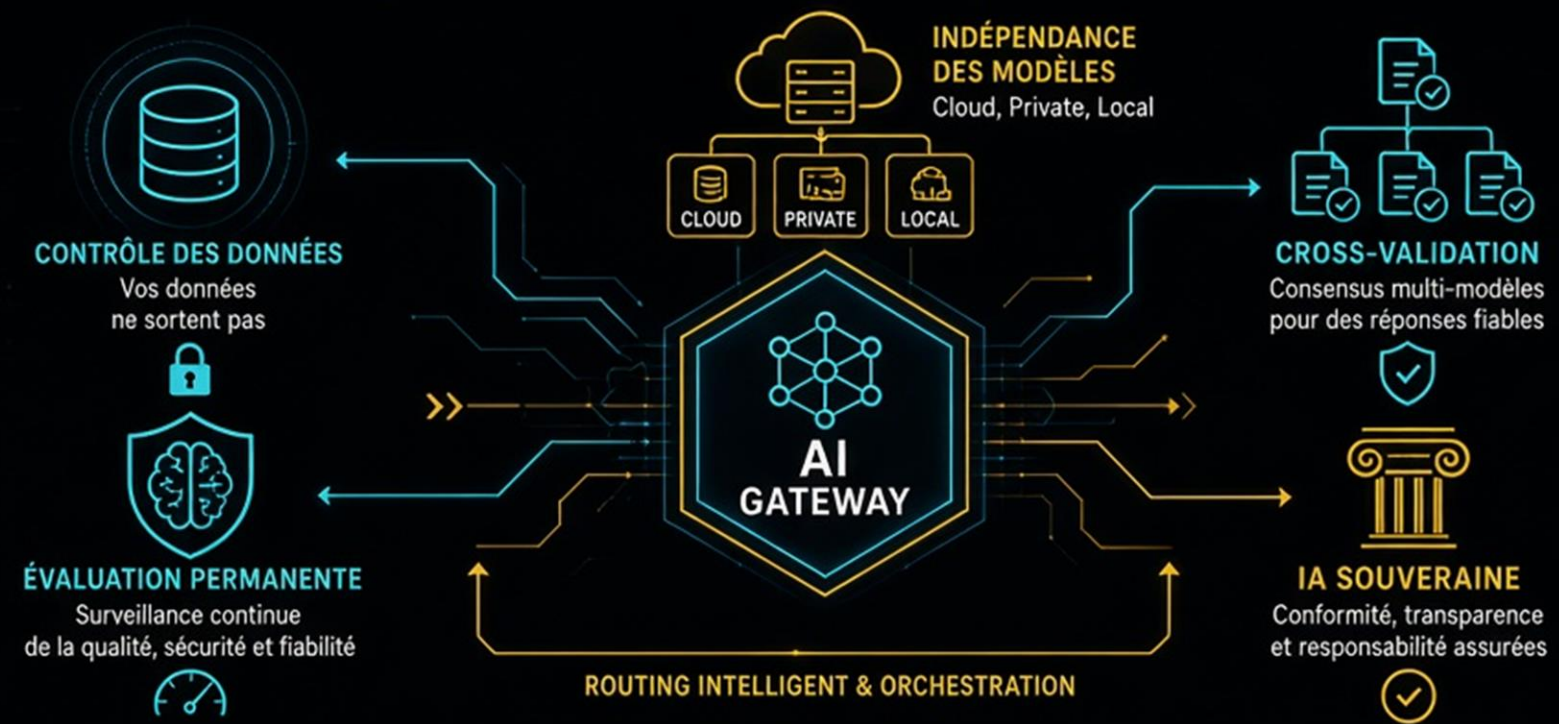
LIENS CAUSAUX



RÉSILIENCE DURABLE

5.6 — Une IA souveraine, multi-modèles et responsable de ses conclusions.

Nouvelle génération d'AI Gateway



MULTI-MODÈLES
Choix et flexibilité sans dépendance

CONTRÔLE DES DONNÉES
Souveraineté et confidentialité totales

VALIDATION CROISÉE
Fiabilité renforcée par consensus

ÉVALUATION CONTINUE
Amélioration et vigilance permanentes

IA SOUVERAINE
Confiance, conformité et responsabilité

ARCHITECTURE DE CONFIANCE • CONÇUE POUR L'EXIGENCE. CONÇUE POUR L'AVENIR

CHAPITRE 5 — CONFIDENTIEL LOCKHEED



FORECAST POUR Q1/2027

AGENDA – FORECAST Q1/2027

- 6.1 : Chapitre 1 - WSA SOC/XDR Intelligence
- 6.2 : Chapitre 2 - WSA Autonomous Remediation
- 6.3 : Chapitre 3 - WSA Enterprise Validation

SOC / EDR / XDR / SIEM temps réel — Planned Q1 2027

WSA comme plateforme centralisée d'opérations de sécurité et de corrélation IA



NATIVE SOC

AU CŒUR DE WSA

Plateforme centralisée d'opérations de sécurité avec corrélation IA et visibilité temps réel

- **HOSTAUDIT** — TELEMETRY LINUX ENDPOINT
- **WINDOWS SECURITY** — COLLECTOR
- **NETWORK SECURITY** — COLLECTOR

ARCHITECTURE MODULAIRE ÉVOLUTIVE

SOC
Supervision continue des menaces et des incidents 24/7

EDR
Détection et réponse sur les endpoints (HostAudit Linux)

XDR
Corrélation étendue à travers les endpoints, réseau, cloud et données

SIEM
Collecte, normalisation et analyse des logs à grande échelle

CORRÉLATION IA
Détection intelligente, réduction du bruit et priorisation des alertes

PLATEFORME MODULAIRE
Architecture ouverte, intégration native et évolutive

VERS UNE PLATEFORME CYBER INTÉGRÉE UNIFIÉE • MODULAIRE • ÉVOLUTIVE • CENTRÉE IA

LOCKHEED — WSA

Trois grands programmes de développement pour atteindre le niveau des leaders mondiaux de la cybersécurité

Security Analyzer (WSA) — Analyse fonctionnelle et technique · Roadmap fin 2026 / 2027

Les trois points rouges identifiés sont importants. Ils ne concernent pas uniquement des fonctionnalités manquantes : ils représentent les **trois étapes qui séparent une plateforme de cybersécurité prometteuse d'une solution industrielle capable de rivaliser avec les grands acteurs du marché.**

Je propose de les traiter comme trois programmes de développement indépendants, mais complémentaires.

Programme	Lacune principale	Objectif
01 — WSA SOC/XDR Intelligence	Pas d'équivalence démontrée en surveillance temps réel et détection des menaces	Détecter, corréler et investiguer les événements de sécurité
02 — WSA Autonomous Remediation	Remédiation de bout en bout non démontrée	Corriger sous contrôle, vérifier, revenir en arrière si nécessaire
03 — WSA Enterprise Validation	Absence de benchmarks indépendants et de validation industrielle	Démontrer les performances, la sécurité et la fiabilité du produit

Trois grands programmes de développement pour atteindre le niveau des leaders mondiaux de la cybersécurité

Security Analyzer (WSA) — Analyse fonctionnelle et technique · Roadmap fin 2026 / 2027

01 WSA SOC/XDR Intelligence



PRINCIPAL GAP

Manque de visibilité en temps réel et d'intelligence contextuelle avancée sur les menaces.

OBJECTIVE

Fournir une détection avancée, une priorisation contextuelle et une intelligence des menaces en temps réel pour un SOC/XDR étendu.

02 WSA Autonomous Remediation



PRINCIPAL GAP

Temps de réponse trop long entre la détection et la neutralisation des incidents.

OBJECTIVE

Automatiser la détection, la décision et la remédiation des menaces pour contenir et neutraliser les incidents en quelques secondes.

03 WSA Enterprise Validation



PRINCIPAL GAP

Manque de validation à grande échelle, de conformité et d'intégration native dans les environnements enterprise critiques.

OBJECTIVE

Valider la performance, la scalabilité, la conformité et l'intégration WSA dans les environnements enterprise les plus exigeants.

Chapitre 1. WSA SOC/XDR Intelligence

WSA dispose déjà de fondations importantes :

- Scans de sécurité web, réseau, services et API.
- Inventaire d'actifs, historique et analyse des changements.
- Intelligence IP, réputation et renseignements sur les vulnérabilités.
- Corrélation de risques, graphes et interprétation par l'IA.
- HostAudit Linux, capable d'examiner des configurations système, journaux et indices d'intrusion.

En revanche, ces capacités ne constituent pas encore, à elles seules, une plateforme EDR/XDR et SOC temps réel équivalente aux solutions de CrowdStrike, Microsoft ou SentinelOne.

Le manque essentiel : passer de mesures effectuées pendant un scan à la collecte, la corrélation et l'investigation continues d'événements de sécurité.

1.1 — Situation actuelle

FONDATIONS EXISTANTES

ANALYSES DE SÉCURITÉ

Web, réseau, services, API.

INVENTAIRE DES ACTIFS

et analyse des changements.

INTELLIGENCE IP

Renseignement sur les menaces et les infrastructures.

GRAPHS DE CORRÉLATION DE RISQUES

et interprétation par l'IA.

HOSTAUDIT LINUX

Audit et durcissement des systèmes Linux.

MANQUE ACTUEL :

PAS ENCORE ÉQUIVALENT À L'EDR/XDR

ni aux plateformes SOC temps réel.

EDR

XDR

SOC TEMPS RÉEL

MANQUE ESSENTIEL :

Passer des mesures à temps d'analyse (scan-time) à la **COLLECTE CONTINUE, CORRÉLATION ET INVESTIGATION** des événements de sécurité.

COLLECTE CONTINUE → CORRÉLATION → INVESTIGATION

1.2 — Première évolution : construire le SOC central de WSA



1.3 — Fonctions majeures à développer



1. REAL-TIME EVENT COLLECTOR

Collecte et normalisation des événements en temps réel depuis l'ensemble des sources.



2. THREAT CORRELATION ENGINE

Corrèle les événements et détecte les comportements suspects et les chaînes d'attaque avancées.



3. THREAT INTELLIGENCE HUB

Agrège, enrichit et partage le renseignement sur les menaces et les indicateurs de compromission.



4. SOC INVESTIGATION CENTER

Centralise les investigations, la visualisation et le triage des incidents par les analystes SOC.



5. AI THREAT ANALYST

Analyse comportementale avancée et détection des menaces par l'intelligence artificielle et le Machine Learning.



6. RESPONSE ORCHESTRATOR

Automatise et orchestre les actions de réponse, containment et remediation sur l'ensemble des actifs.



BASÉ SUR LE CADRE MITRE ATT&CK®

Couverture des tactics, techniques et procédures pour une détection, investigation et réponse alignées sur les attaques réelles.



RECONNAISSANCE



INITIAL ACCESS



ESCALATION



LATERAL MOVEMENT



EXFILTRATION

• DÉTECTION • CORRÉLATION • INTELLIGENCE • INVESTIGATION • RÉPONSE •

« UN ANALYSTE IA QUI NE VOIT PAS SEULEMENT DES ÉVÉNEMENTS, MAIS LEURS RELATIONS. »

Exemple de scénario :

Une application exposée présente une faiblesse connue. HostAudit relève ensuite une séquence inhabituelle d'authentifications. IP Analyzer apporte un contexte défavorable sur certaines adresses sources.

Un moteur traditionnel pourrait produire plusieurs alertes indépendantes.

Le futur WSA SOC devra pouvoir les réunir en un incident contextualisé :

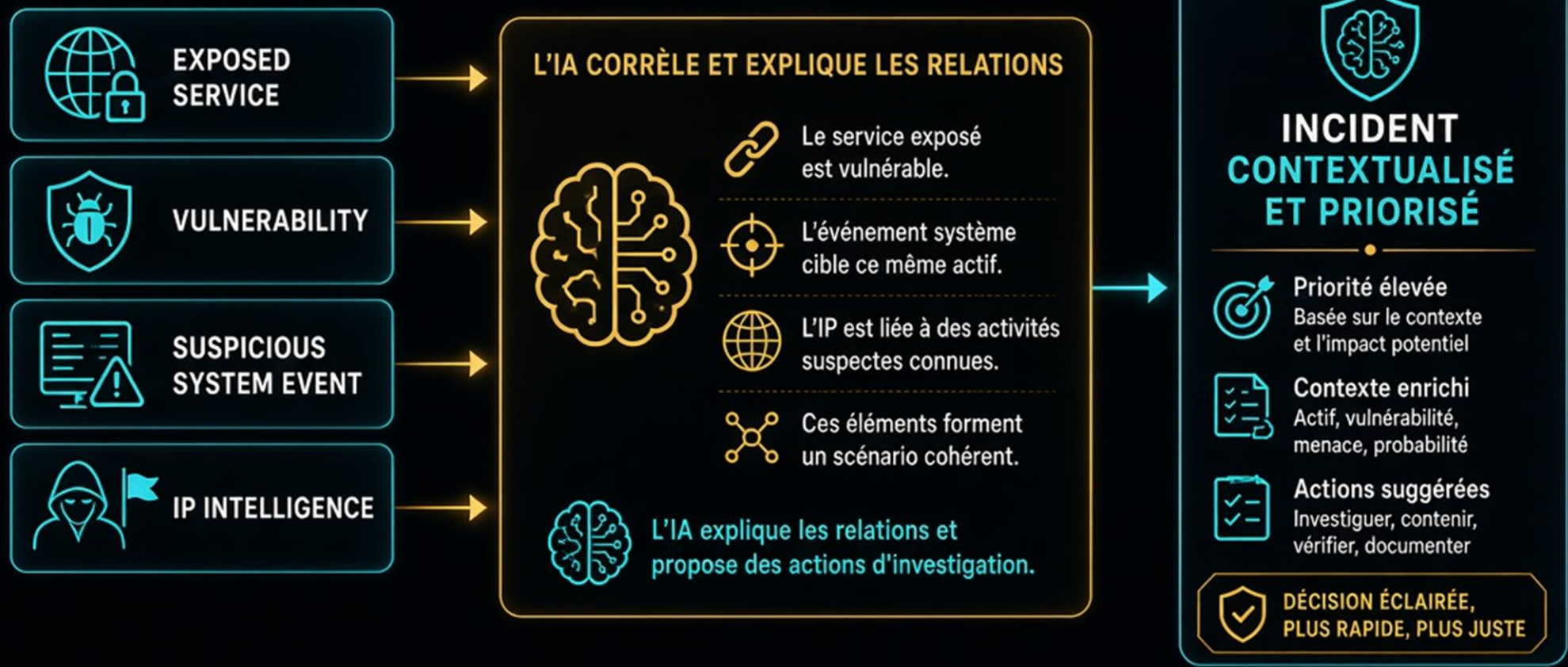
Service exposé + vulnérabilité + événement système suspect + intelligence IP = scénario justifiant une investigation prioritaire.

L'IA devra expliquer les relations, indiquer ce qui est confirmé et proposer les actions d'investigation appropriées.

Attention : une corrélation ne prouve pas, à elle seule, une compromission. Le système devra préserver cette distinction.

1.4 — La valeur de l'IA dans le futur SOC

> “ UN ANALYSTE IA QUI NE VOIT PAS SEULEMENT DES ÉVÉNEMENTS, MAIS LEURS RELATIONS. ”



DE LA DONNÉE À LA DÉCISION. DE L'ALERTE À L'INTELLIGENCE.

Définir le format commun des événements, mettre en place une ingestion fiable depuis HostAudit et construire le premier tableau de bord des incidents WSA.

Premier semestre 2027 — SOC opérationnel

Introduire les règles de corrélation, les enrichissements de threat intelligence, les investigations assistées par IA, les alertes et les premières intégrations EDR/SIEM.

Second semestre 2027 — Montée en maturité XDR

Développer les scénarios multi-sources, les réponses orchestrées, les mesures de couverture et les essais opérationnels sur des infrastructures clientes.

Pour considérer ce point comme maîtrisé, il faudra démontrer :

- Une collecte continue et fiable, y compris en cas de perte temporaire de connexion.
- Des alertes horodatées et reliées aux événements sources.
- Un taux de faux positifs et une latence de détection mesurés.
- Des investigations reproductibles et des actions correctement autorisées.
- Une couverture de détection évaluée sur un ensemble documenté de scénarios d'attaque.

Le référentiel de réponse aux incidents NIST SP 800-61 révision 3 ↗ constitue une base pertinente pour organiser ces processus. CSRC

Décision d'architecture : WSA doit devenir le centre SOC et de corrélation. HostAudit alimente ce centre depuis les serveurs. Il est plus réaliste d'intégrer d'abord les EDR reconnus que de développer immédiatement un antivirus et un EDR complets.

1.5 — Livrables attendus et validation

Fin 2026 — Socle initial

- Fondations EDR/XDR et gestion des actifs critique déployées
- Détection de base activée avec règles prioritaires
- Reporting et KPIs initiaux définis

Premier semestre 2027 — SOC opérationnel

- SOC 24/7 avec processus de triage et d'escalade formalisés
- Playbooks de réponse à incident testés et mesurés
- Tableaux de bord de sécurité en live et partagés

Second semestre 2027 — Montée en maturité XDR

- XDR étendu à l'ensemble des sources critiques (réseau, cloud, identité, email...)
- Automatisation avancée et orchestration des réponses
- Maturité proactive : threat hunting, détection adaptative et réduction des risques

CRITÈRES POUR CONSIDÉRER LE POINT MAÎTRISÉ

Couverture et qualité
Les livrables sont complets, testés et documentés

Performance mesurable
KPIs atteints et stabilité opérationnelle démontrée

Processus industrialisés
Playbooks, runbooks et workflows adoptés par les équipes

Valeur business prouvée
Réduction des risques et du MTTR validée par les métiers

Sécurité • Maîtrise • Confiance

Chapitre 2. WSA Autonomous Remediation

2.1 — Situation actuelle

ÉLÉMENTS DE REMÉDIATION EXISTANTS DANS HOSTAUDIT LINUX 0.50.0

57 FONCTIONS DE CORRECTION NATIVES

94 IDENTIFIANTS DE CONTRÔLE ASSOCIÉS

MÉCANISMES INTÉGRÉS

SIMULATION
Évaluation sans application

SAUVEGARDE
Points de restauration automatisés

VALIDATION
Vérification post-correction

ROLLBACK
Retour arrière sécurisé

MANQUE ESSENTIEL

Aucune démonstration complète d'orchestration distante fiable :

- Depuis WSA avec autorisations limitées
- Avec contrôle d'efficacité automatique
- À travers plusieurs serveurs

SÉCURITÉ • CONTRÔLE • CONFIANCE

2.2 — Développer le WSA Remediation Orchestrator



1. Détection
2. Analyse IA
3. Plan de correction
4. Validation
5. Exécution
6. Contrôle
7. Rapport

2.3 — Les six fonctions essentielles à construire



AI Remediation Planner

Analyse les risques, planifie et priorise les remédiations de manière intelligente.



Remediation Policy Engine

Définit, applique et gouverne les règles et politiques de remédiation de façon centralisée.



Secure Execution Agent

Exécute les actions de remédiation dans un environnement isolé, avec des privilèges minimaux et un contrôle strict.



Backup & Rollback Manager

Assure la sauvegarde des états critiques et permet un rollback fiable et rapide en cas d'échec.



Post-Remediation Validator

Vérifie l'efficacité des remédiations, la stabilité du système et la conformité aux objectifs de sécurité.



Remediation Audit Trail

Enregistre toutes les actions, décisions et résultats pour assurer la traçabilité, la conformité et l'amélioration continue.



RÈGLE IMPÉRATIVE : L'IA ne doit jamais avoir d'accès général au shell root du serveur.



2.4 — Définir trois niveaux d’automatisation



ASSISTED

Modifications sensibles, validation humaine

Contrôle humain



SUPERVISED

Corrections éprouvées, approbation explicite

Approbation requise



POLICY-AUTOMATED

Actions limitées préautorisées, exécution automatique conditionnelle

Exécution conditionnelle



Note : toutes les corrections n’ont pas le même niveau de risque.

2.5 — Exemple concret d'une correction WSA



CAS D'USAGE : En-tête HTTP manquant sur Nginx

OBJECTIF : Corriger, valider et sécuriser sans interruption

RÉSULTAT : Sécurité renforcée, continuité assurée

• DÉTECTION • ANALYSE • CORRECTION • VÉRIFICATION • MAÎTRISE •

2.6 — Objectifs de développement 2026–2027

Fin 2026

formaliser modèle
et intégrer premiers correctifs

Premier semestre 2027

chaîne de remédiation
supervisée

Second semestre 2027

élargir catalogue et
automatisation par politiques

CRITÈRES POUR CONSIDÉRER LE POINT RÉGLÉ

- Modèle formalisé et première vague de correctifs intégrés (Fin 2026)
- Chaîne de remédiation supervisée avec visibilité et traçabilité complète (S1 2027)
- Catalogue élargi et automatisation par politiques appliquées (S2 2027)
- Disparition des risques vérifiée et documentée sur les périmètres traités

RÉSULTAT VISÉ

WSA NE SE CONTENTE PLUS DE RECOMMANDER. IL CONTRIBUE À RÉDUIRE LES RISQUES ET EN VÉRIFIE LA DISPARITION.

- Chaque action possède une autorisation explicite ou une politique préalablement approuvée.
- Toute exécution est traçable et associée à un constat d'origine.
- Les corrections éligibles disposent de tests automatiques avant et après exécution.
- Les procédures de restauration sont testées, sans prétendre que tous les changements sont réversibles.
- Les taux de réussite, d'échec, de restauration et de régression sont mesurés.
- Les corrections IA ne peuvent contourner ni les permissions ni les contrôles techniques.

Fin 2026 : formaliser le modèle de plan de correction, les niveaux de risque et les autorisations, puis intégrer les premiers correctifs HostAudit à un orchestrateur central.

Premier semestre 2027 : construire et tester la chaîne de remédiation supervisée avec simulation, approbation, exécution limitée, vérification et restauration.

Second semestre 2027 : élargir le catalogue d'actions fiables, gérer plusieurs serveurs et introduire l'automatisation par politiques pour les corrections admissibles.

Chapitre 3 . WSA Enterprise Validation

WSA Enterprise Validation :

démontrer les performances, la sécurité et la fiabilité industrielle

> **UNE TECHNOLOGIE PROMETTEUSE NE SUFFIT PAS.**
> **IL FAUT DES RÉSULTATS REPRODUCTIBLES,**
> **MESURABLES ET INDÉPENDAMMENT VÉRIFIÉS.**

VALIDATION INDÉPENDANTE

Tests réalisés par des tiers neutres selon des protocoles rigoureux.

BENCHMARKS & PERFORMANCES

Mesures comparatives sur des scénarios réels de charge, latence, throughput et résilience.

RÉSULTATS MESURABLES

KPI quantifiables, données consolidées et tableaux de bord transparents.

FIABILITÉ INDUSTRIELLE

Conçue pour les environnements critiques : haute disponibilité, redondance et continuité assurée.

CRÉDIBILITÉ & CONFIANCE

Validation reconnue pour les exigences des grandes entreprises, banques et institutions régulées.

RÉSULTATS QUI CRÉENT LA CONFIANCE

GRANDS COMPTES | BANQUES | CTOs & DÉCIDEURS | EXIGENCES RÉGLEMENTAIRES

PREUVE PAR LES TESTS.
CONFIANCE PAR LES RÉSULTATS.

PERFORMANCE. SÉCURITÉ. FIABILITÉ. PREUVÉ. VÉRIFIÉ. INDUSTRIEL.

3.1 — Situation actuelle



208
PYTHON MODULES

Substantial technical base
but static review does not demonstrate

real detection rate, false positives/negatives, high-load performance,

portal security, reliability on large fleets, or independent certification.

ESSENTIAL GAP

Transform coded functions into technical proofs of efficacy and robustness.

- REAL DETECTION RATE
- FALSE POSITIVES / NEGATIVES
- HIGH-LOAD PERFORMANCE
- PORTAL SECURITY
- RELIABILITY ON LARGE FLEETS
- INDEPENDENT CERTIFICATION

3.2 — Créer le WSA Security Benchmark Laboratory

PERMANENT QUALIFICATION LABORATORY



SECURE BY DESIGN
TESTED BY STANDARD
TRUSTED BY ENTERPRISE

CONTINUOUS TESTING
MEASURABLE RESULTS
DEFENSIBLE OUTCOMES

DETECTION ACCURACY
Evaluate threat detection coverage and precision

AI ANALYSIS QUALITY
Assess contextual understanding, false positive reduction, and risk prioritization

REMEDIATION RELIABILITY
Validate fix effectiveness, workflow accuracy, and regression prevention

ENTERPRISE PERFORMANCE
Measure scalability, load handling, and production readiness

OWASP WSTG
Web Security Testing Guide

ASVS 5.0
Application Security Verification Standard

MITRE ATT&CK
Adversarial Tactics, Techniques & Common Knowledge

3.3 — Mesurer réellement WSA face à la concurrence

CAMPAGNES DE BENCHMARK COMPARATIF

Sous conditions comparables pour une évaluation juste et reproductible

Conditions identiques
Même périmètre, même environnement

Campagnes régulières
Mesures répétées dans le temps

Comparaison en aveugle
Élimine les biais et assure l'objectivité

Jeux de données représentatifs
Cas réels d'entreprise

TABLEAU DE BORD DE PERFORMANCE COMPARATIVE

Vulnérabilités réellement détectées	Faux positifs	Temps médian d'analyse	Temps P95 d'analyse	Coût par actif analysé	Corrections vérifiées
À mesurer	À mesurer	À mesurer	À mesurer	À mesurer	À mesurer
Comparer et mesurer	Comparer et mesurer	Comparer et mesurer	Comparer et mesurer	Comparer et mesurer	Comparer et mesurer

L'AVANTAGE CONCURRENTIEL LE PLUS PUISSANT

se mesure par une supériorité réelle sur un cas d'usage concret.

Pas seulement des promesses. Des résultats mesurés. Des impacts prouvés.

MESURER. COMPARER. PROUVER. GAGNER.

3.4 — Qualification de la montée en charge

1



Petit parc
(10-50 actifs)

Charge simulée
Faible à modérée

Objectif
Valider la montée en charge sur un périmètre réduit

2



Parc intermédiaire
(100-500 actifs)

Charge simulée
Modérée à élevée

Objectif
Vérifier la stabilité et les performances sous charge représentative

3



Grand parc
(1 000-5 000 actifs)

Charge simulée
Élevée à intensive

Objectif
Qualifier les limites, la résilience et la scalabilité de la solution

4



SOC à événements continus

Charge simulée
Continue et variable (pics inclus)

Objectif
Valider la capacité du SOC à absorber et traiter un flux continu d'événements sans perte ni latence critique

QUALIFIER AUJOURD'HUI. RÉSISTER DEMAIN.

PERFORMANCE • RÉSILIENCE • MAÎTRISE

3.5 — Audit de sécurité indépendant de WSA

AUDIT DE SÉCURITÉ INDÉPENDANT

- AUTHENTIFICATION
- MFA (MULTI-FACTEUR)
- ISOLATION DES CLIENTS
- SÉCURITÉ DES APIS
- STOCKAGE DES SECRETS
- FONCTIONS PRIVILÉGIÉES
- RISQUES SSRF
- ACCÈS IA SÉCURISÉ

INDUSTRIALISER LA SÉCURITÉ DE LA CHAÎNE D'APPROVISIONNEMENT

- TESTS DE SÉCURITÉ AUTOMATISÉS
- SBOM (SOFTWARE BILL OF MATERIALS)
- GESTION DES LICENCES
- SIGNATURES DES VERSIONS
- TRAÇABILITÉ ET CORRECTIFS

OBJECTIF : Une solution qui audite les autres doit présenter des preuves solides de sa propre sécurité.

3.6 — Certifications et attestations : choisir les bonnes

ISO/IEC 27001

NATURE

Système de management de la sécurité de l'information (SMSI). Certification de l'organisation.

INTÉRÊT POUR LOCKHEED

Démontre une approche structurée et continue de la sécurité à l'échelle de l'entreprise.

SOC 2

NATURE

Rapport d'audit sur les contrôles organisationnels relatifs à la sécurité, disponibilité, intégrité, confidentialité et vie privée.

INTÉRÊT POUR LOCKHEED

Atteste de la mise en œuvre effective de contrôles de confiance, particulièrement pertinent pour les services cloud et le traitement de données.

COMMON CRITERIA ISO 15408

NATURE

Certification de la sécurité d'un produit ou système selon des niveaux d'assurance (EAL). Évaluation rigoureuse par une tierce partie.

INTÉRÊT POUR LOCKHEED

Prouve que le produit respecte des critères de sécurité internationalement reconnus, basé sur une évaluation indépendante.

AUDIT ET PENTEST INDÉPENDANTS

NATURE

Audits indépendants et tests d'intrusion réalisés par des experts tiers. Résultats spécifiques au produit ou à l'architecture.

INTÉRÊT POUR LOCKHEED

Valide la sécurité réelle dans un contexte opérationnel. Identifie les vulnérabilités avant qu'elles ne soient exploitées.

Il n'existe pas de certification universelle unique.

Chaque référentiel répond à des objectifs et à une portée spécifiques.

1ER MILESTONE POUR WSA

Audit produit indépendant avec benchmarks reproductibles.

MESURER. VALIDER. S'AMÉLIORER.

Certifications et attestations

RÉFÉRENCE	NATURE	INTÉRÊT POUR LOCKHEED
ISO/IEC 27001	Certification ISO 27001 pour le Système de Management de la Sécurité de l'Information	Démontre un cadre robuste de gestion des risques et une protection continue des informations.
SOC 2	Rapport SOC 2 Type II attestant les contrôles de sécurité, disponibilité et confidentialité	Confirme l'efficacité opérationnelle des contrôles et la confiance dans les services fournis.
Common Criteria / ISO 15408	Certification Common Criteria (ISO 15408) pour les produits et solutions évalués	Atteste l'évaluation indépendante de la sécurité des produits selon des standards internationaux.
Audit et pentest indépendants	Audits et tests d'intrusion réalisés par des tiers indépendants et qualifiés.	Valide en continu la résilience des systèmes et renforce la confiance dans nos pratiques.

3.7 — Calendrier de validation

Fin 2026 —
construire le référentiel qualité

Premier semestre 2027 —
démontrer

Second semestre 2027 —
industrialiser et faire valider

CRITÈRES DE SORTIE DU POINT ROUGE

- Référentiel qualité construit et approuvé
- Tests et démonstrations concluants
- Processus industrialisés et documentés
- Validation indépendante obtenue

SORTIE DU POINT ROUGE

Lorsque tous les critères ci-dessus sont remplis.

RÉSULTAT RECHERCHÉ

NE PLUS DEMANDER AU MARCHÉ DE CROIRE EN WSA. LUI DONNER LES MOYENS D'EN VÉRIFIER LES PERFORMANCES.

CONFIANCE N'EST PAS DÉCLARÉE, ELLE EST PROUVÉE.

Synthèse — Les trois transformations majeures de WSA

Aujourd'hui

SOC / CORRÉLATION
Détection et corrélation des alertes de sécurité sur les actifs et identités.

REMEDIATION
Processus de réponse majoritairement manuels et fragmentés.

BENCHMARKS / VALIDATION
Mesures et reporting limités, avec peu de comparatifs et de preuves d'efficacité.

Transformation à développer

SOC / CORRÉLATION
Renforcer la corrélation contextuelle et l'enrichissement IA pour une détection plus précise et priorisée.

REMEDIATION ORCHESTRÉE
Industrialiser les playbooks, automatiser les actions et orchestrer la réponse bout en bout.

BENCHMARKS / VALIDATION
Mettre en place des référentiels, scores et benchmarks pour piloter l'amélioration continue.

Ambition 2027

SOC / CORRÉLATION
Plateforme de détection augmentée par l'IA, corrélant en temps réel menaces, vulnérabilités et comportements.

REMEDIATION ORCHESTRÉE
Remediation autonome et adaptative, orchestrée par WSA avec supervision humaine et boucle d'apprentissage.

BENCHMARKS / VALIDATION
Leader en benchmarks sectoriels et preuves quantifiables de réduction du risque et de maturité sécurité.

> *WSA ne se contente pas de détecter les risques. Il aide à les comprendre, à les corriger et à prouver que les corrections ont fonctionné.*

EN CONCLUSION

DEMAIN, LE LEADER DE LA CYBERSÉCURITÉ NE SERA PLUS CELUI QUI DÉTECTE LE PLUS DE FAILLES, MAIS CELUI QUI PROUVE QU'IL A ÉLIMINÉ LE PLUS DE RISQUES.

AVEC WSA ET L'INTELLIGENCE ARTIFICIELLE,
C'EST CETTE RÉVOLUTION QUE NOUS AMBITIONNONS DE CONSTRUIRE.



LOCKHEED — WSA

Beyond Detection. Towards Intelligent Cyber Defense.