
LOCKHEED
LLC
WEB SECURITY
ANALYZER
LOCKHEED LLC
NEXT-GEN
CYBER-AI
LOCKHEED LLC
W
WSA
WEB SECURITY
ANALYZER
https://www.lockheed-llc.com
Live Demo
contact@lockheed-llc.com
Get in Touch

WSA (Security Analyzer)

High-Level Operating Model

From attack surface visibility to AI-assisted remediation

1 Inputs & Targets

- Websites & Web Apps
- Domains & DNS
- Public IPs & Exposure
- Linux Servers (optional agent)

2 Data Collection

External Scanning

- Transport Security
- URL / Redirect Analysis
- Reputation Checks
- Multi-target Scans

Internal Linux Analysis

- OS & Services
- Network & Ports
- Nginx / Configuration Review
- Keys, Permissions & Hardening

3 WSA Core Intelligence

- Normalization & Evidence Storage
- Correlation Engine
- Risk Scoring & Prioritization
- AI Investigation & Decision Support

Combines technical evidence, context, and explainable analysis.

4 Analyst & Management Cockpit

- Executive Dashboard
- Decision Wheel
- Micro-Timeline
- Investigation Workspace

5 Outputs & Business Value

- Prioritized Findings
- Actionable Remediation
- Alerts & Visibility
- Reports / Export Center
- History & Trends

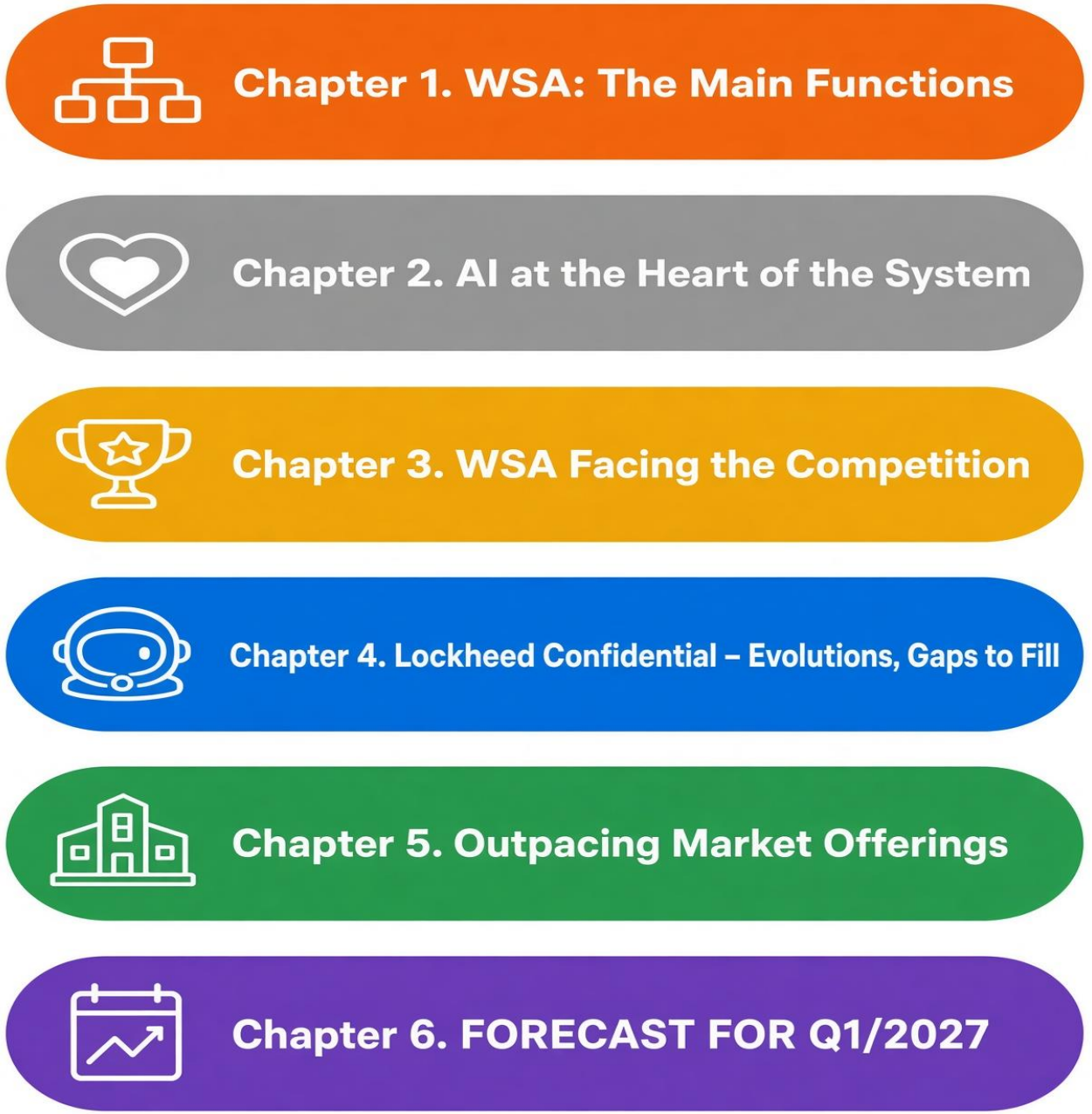
Investor Value

- Faster detection
- Clearer prioritization
- Reduced analyst workload
- Continuous security improvement

Validate fixes → Re-scan → Measure progress

WSA unifies external attack surface analysis, optional internal Linux auditing, and AI-assisted investigation in a single platform.

GENERAL AGENDA



NEXT-GEN CYBER-AI
LOCKHEED
LLC

WSA

The cyber intelligence that transforms security into a competitive advantage.



NEXT-GEN CYBER-AI

LOCKHEED

LLC

WSA transforms technical signals into justifiable decisions, with governed AI and a precise roadmap to automate correction.



TECHNICAL SIGNALS
Logs, metrics, threats, telemetries, anomalies...

JUSTIFIABLE DECISIONS
Contextualized, prioritized, traceable and explainable.

GOVERNED AI
Transparent, controlled and compliant models, with safeguards and audit.

PRECISE ROADMAP
Automation plan, steps, priorities, KPIs and clear dependencies.

AUTOMATED CORRECTION
Orchestrated, executed and continuously verified remediation.

FROM DATA TO ACTION. FROM RESPONSE TO RESILIENCE.

POSITIONING OF WSA VS PALO ALTO NETWORKS

Operational precision, governed AI, technical proof.

WSA (Security Analyzer)

Web / API / IP / Host Analysis
In-depth detection and analysis of attack surfaces.

Verifiable technical evidence
Concrete, traceable and reproducible results.

Governed multi-LLM AI
Augmented, controlled and compliant analysis.

Guided remediation + re-test
Actionable recommendations and validation of corrections.

Key value: transforming technical signals into justifiable decisions.

OUR POSITIONING

WSA does not seek to replicate a universal SOC.
WSA targets deep, explainable and actionable analysis.

- More targeted
- More explainable
- More focused on evidence and correction

PRECISION & EXPLAINABILITY

SCALE & COVERAGE

Palo Alto Networks

Large-scale SOC / XDR platform
Unified detection, response and monitoring at scale.

Cloud + network + massive telemetry
Extended visibility across the entire infrastructure.

Advanced orchestration and automation
Playbooks, SOAR and end-to-end integrations.

Global power and enterprise coverage
International presence and large-scale adoption.

Key strength: global coverage and security operations at scale.

KEY MESSAGE: WSA = precision cybersecurity. | Palo Alto = global platform cybersecurity.

Visual strategic positioning – marketing synthesis, not an independent benchmark.

CHAPTER 1

CHAPITRE 1 — WSA : the main functions and their advantages



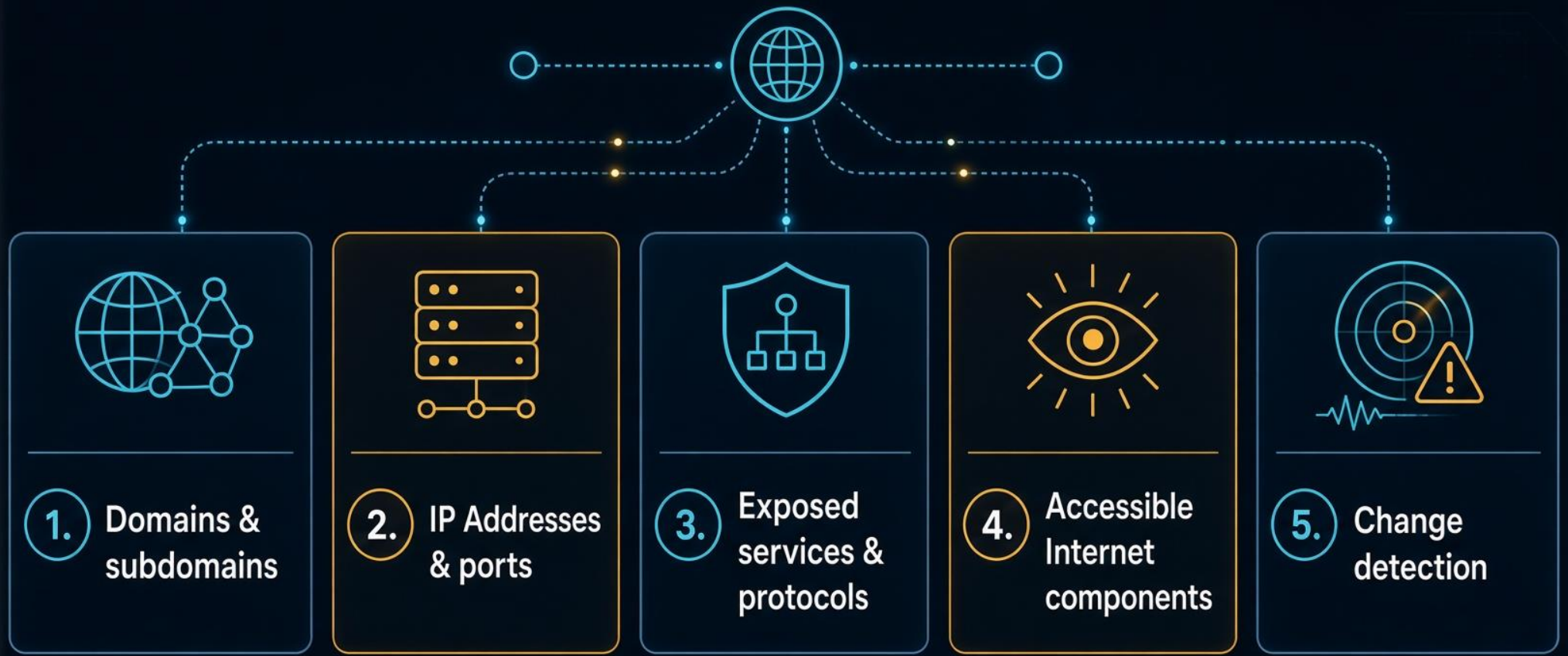
BASIC FUNCTIONS AGENDA



- 1.1 — See what an attacker can see. Before they exploit it.
- 1.2 — A functional website is not necessarily a secure website.
- 1.3 — Several dozen analyzers. One single reading of security.
- 1.4 — An IP address is not an identity. It is a set of clues.
- 1.5 — For each asset, its exposure, its history and its risks.
- 1.6 — An isolated vulnerability is a signal. Several become an attack.
- 1.7 — Criticality is not limited to a CVSS score.
- 1.8 — Security is not a photograph. It is a permanent evolution.
- 1.9 — From technical observation to operational decision.

1.1 — See what an attacker can see. Before they use it.

Discovery and mapping of the attack surface



1.2 — A functional website is not necessarily a secure website.

In-depth analysis of web applications and APIs



XSS and SQL injections
(injection)



Authorizations and data access
(access)



API and JavaScript
(code api)



Web content discovery
(search/web)



Authentication and sessions
(key/user)



OAuth / OpenID Connect
(protocol/identity)



TLS and security headers
(certificate/headers)



Technologies and components
(stack/tech)

1.3 — Several dozen analyzers. One single reading of security.

Orchestration and consolidation of results



A SINGLE SOURCE OF TRUTH. INFORMED DECISIONS. A STRENGTHENED SECURITY POSTURE.

WSA • ORCHESTRATES. CONSOLIDATES. PROTECTS.

1.4 — An IP address is not an identity. It is a set of clues.

Multidimensional IP intelligence



SOURCE COMPARISON TO DETECT INCONSISTENCIES

MULTIPLE SOURCES
RDAP, DNS, GBP, RPKI, TLS, Reputation, History...

CROSS-CHECKING & CORRELATION
Detection of inconsistencies, anomalies and weak signals.

MULTIDIMENSIONAL VISION
Beyond geolocation or a reputation score.

UNE IP = A STARTING POINT. | MULTIPLE DIMENSIONS = REAL UNDERSTANDING.

1.5 — For each asset, its exposure, its history and its risks.

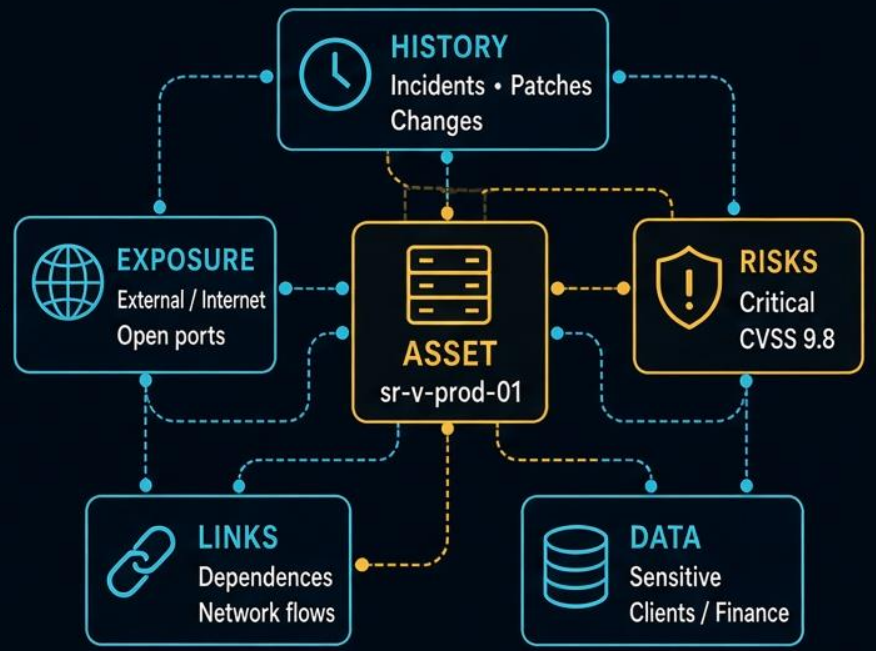
Intelligent inventory and security graph

INTELLIGENT INVENTORY

- Servers — sr-v-prod-01
- Applications — app-front
- Databases — db-client
- Cloud / SaaS — aws-account

Continuous discovery • Classification • Context

SECURITY GRAPH



● Context & exposure ● Risk & history

360° VIEW & LIFECYCLE



RELATIONSHIPS
Dependences and mapped flows

VULNERABILITIES
Linked to assets and their context

BEFORE: ISOLATED VULNERABILITIES

Fragmented lists • Little context • Difficult prioritization

AFTER: ASSET-BASED REASONING

Complete context • Dependences • Intelligent prioritization • Informed decisions

1.6 — An isolated vulnerability is a signal.

Several linked vulnerabilities can become an attack scenario.

Risk correlation and attack path analysis

ISOLATED VULNERABILITIES
Independent signals



CVE-2024-1234
Web Server

CVE-2024-5678
Auth Service

CVE-2024-9012
Database

Signals detected, but without apparent link.

ATTACK PATHS
Vulnerability correlation



Technical and contextual links make paths emerge.

ATTACK SCENARIOS
Exploitable chains



Initial access
(via Web Server)

Privilege escalation
(via Auth Service)

Access to sensitive data
(via Database)

An ordered sequence =
a realistic attack scenario.

CORRELATION GRAPH
Modeling of relationships between vulnerabilities, assets and contexts.

ATTACK PATHS
Identification of exploitable paths and their prerequisites.

CONTEXTUAL PRIORITIZATION
Assessment of real impact and prioritization of critical risks.

CORRELATION OF WEAKNESSES ON ASSETS
Grouping of weaknesses by asset to reveal hidden chains.

Understand the links. Anticipate the scenarios. Prioritize the defenses.

1.7 — Criticality is not limited to a CVSS score.

Vulnerability intelligence and exploitation context

CVE
Standardized vulnerability identifier

EPSS
Exploitation probability in the next 30 days

CISA KEV
Known Exploited Vulnerabilities catalog

Threat intelligence
Public exploits, active campaigns, actors, PoC, etc.

INTELLIGENCE ENRICHMENT

ASSET CONTEXT

- **Critical asset** — High business impact
- **Exposure** — Internet, partners, etc.
- **Data sensitivity** — Confidential, regulated
- **Existing compensations** — Controls, segmentations, etc.

NOT ALL ALERTS OF THE SAME LEVEL ARE EQUAL

CVSS SCORE ALONE
= An incomplete view
Does not take into account the real probability of exploitation or the context.

CONTEXT + INTELLIGENCE
= Precise prioritization
Focus your efforts on the vulnerabilities that really matter.

Real criticality = Severity × Exploitation probability × Business context

Prioritize with relevance.
Reduce real risk.

1.8 — Security is not a photograph. It is a permanent evolution.

Monitoring, history and drift detection

CONTINUOUS MONITORING OVER TIME



SCHEDULED ANALYSES
Regular and automated

COMPARISON OF EXECUTIONS
Detection of changes

ALERTS ON NEW SERVICES
Unknown exposures and services

RISK MONITORING
Evolution of the risk level

HISTORICAL EVOLUTION
Overview over time



HISTORY
Complete traceability of changes over time.

COMPARISON
Precisely visualize what has changed between two executions.

ALERTS
Be notified of new services, ports or risky behaviors.

NEW EXPOSURES
Quickly identify what has appeared and assess the impact.

DRIFT DETECTION
Spot deviations from your reference secure state.

CONTINUOUS MONITORING
A permanent improvement loop for resilient security.



WHAT HAS CHANGED
Detected modifications

WHAT HAS APPEARED
New elements identified

WHAT HAS BEEN CORRECTED
Treated and resolved risks

WHAT HAS REAPPEARED
Recurring or reactivated elements

1.9 — From technical observation to operational decision.

Cockpit, API, reports and organization of actions

ONE SINGLE REALITY, SEVERAL VIEWS

COCKPIT / EXECUTIVE DASHBOARD
Global synthesis, KPIs, trends, priority alerts.



CTO PRIORITIES
Consolidated view to arbitrate, prioritize and allocate resources.



EXPERT EVIDENCE
Logs, endpoints, vulnerabilities, artifacts and technical analyses.



API (LIMITED PERMISSIONS)
Controlled access, granular scopes, principle of least privilege.

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

WEBHOOKS
Real-time notifications to automate workflows.



DETAILED REPORTS
Technical and compliance reports, auditable evidence.



INVESTIGATION
Search, correlation, timeline, attack trail.



FROM SIGNAL TO ACTION: ORGANIZE THE DECISIONS THAT MATTER

COCKPIT / DASHBOARD
Global view at a glance

REPORTS
Evidence, audits and compliance

API
Secure and controlled integration

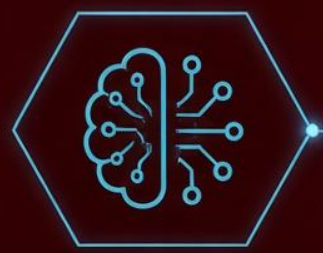
WEBHOOKS
Automation and reactivity

ACTIONS
Orchestration and action plans

OPERATIONAL DECISION
Decide, act, track the impact.

CHAPTER 2

CHAPTER 2 — Artificial intelligence at the heart of WSA



SECURITY ANALYSIS

Real-time collection and analysis of massive data to detect advanced threats.



RISK UNDERSTANDING

AI contextualizes risks, their impact and their probability for clear visibility.





INFORMED DECISION

AI prioritizes insights and helps teams make the right decisions, quickly.



INTELLIGENT ACTION

Automation of actions and orchestration to contain, remediate and strengthen.

ADVANCED DETECTION | PREDICTIVE ANALYSIS | INTELLIGENT PRIORITIZATION | AUTOMATED RESPONSE

AGENDA - Artificial intelligence at the heart of WSA

- 2.1 — AI does not invent vulnerabilities. It interprets the evidence. »
- 2.2 — One hundred alerts do not mean one hundred independent problems. »
- 2.3 — Do not correct what makes noise. Correct what presents the real risk.
- 2.4 — AI does not only propose what to correct. It must explain why and how to verify.
- 2.5 — Several artificial intelligences. No imposed provider.
- 2.6 — Every important statement must be able to find its evidence.
- 2.7 — A cyber expert available in the cockpit, without replacing the human expert
- 2.8 — Artificial intelligence must be controllable technically and economically



Analyzers establish the facts

AI connects the information

The human keeps the decision

2.1 — AI does not invent vulnerabilities. It interprets the evidence.



1. Deterministic WSA engines —

Measures • Findings • Identifiers • Sources • History



2. Artificial intelligence layer —

Corrélation • Explanation • Causes • Combined risks • Priorities

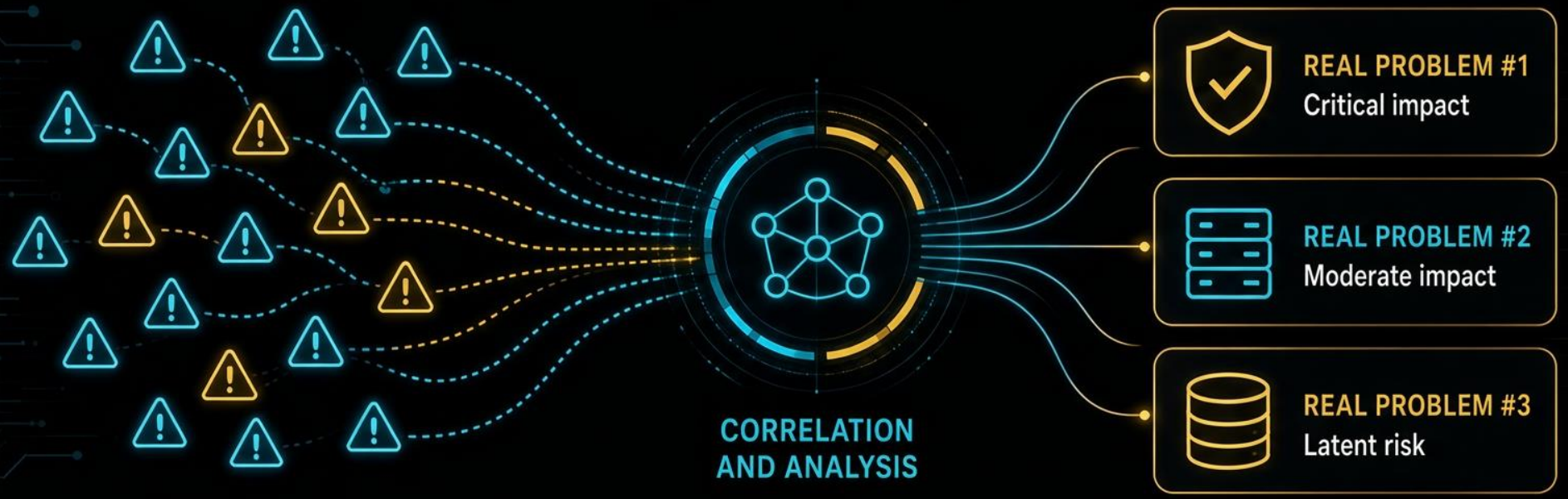


3. Decision and control —

Human validation • Authorized remediation • New verification

2.2 — One hundred alerts do not mean one hundred independent problems.

Intelligent correlation and noise reduction



Identify related findings

Group alerts that share common characteristics.

Search for common causes

Identify the common root behind multiple symptoms.

Detect duplicates and contradictions

Eliminate redundancies and spot inconsistent information.

Study combined risks

Assess the overall impact and chains of consequences.

Report missing information

Highlight the essential data to collect.

2.3 — Do not correct what makes the most noise. Correct what presents the most risk.

AI-assisted prioritization

NOISE
Numerous and unprioritized alerts



AI FILTER

CONTEXTUAL ANALYSIS
by AI

PRIORITIZATION
Focused on real risk

- **CRITICAL** — High risk
- **HIGH** — Significant risk
- **MEDIUM** — Moderate risk
- **LOW** — Low risk

PRIORITIZED RECOMMENDATIONS BY AI

SEVERITY
Potential impact on critical assets

CONTEXT
Assets, users, environment, threats

RELATIONSHIPS
Relationships, attack paths, exposure

CONFIDENCE
Reliability of the analysis and data

Less noise. More context. Better decision.

2.4 — AI does not only propose what to correct. It must explain why and how to verify.

Remediation assistance

AI PROPOSES CORRECTIVE ACTIONS

1. RECOMMENDED ACTION
Suggested fix to resolve the detected problem.

2. WHY? (EXPLANATION)
Understand the root cause, the context and the impacts.

3. HOW TO VERIFY?
Verification steps and expected success criteria.

FOR RELIABLE AND CONTROLLED REMEDIATION

4. SIMULATION
Anticipate the impact before application.

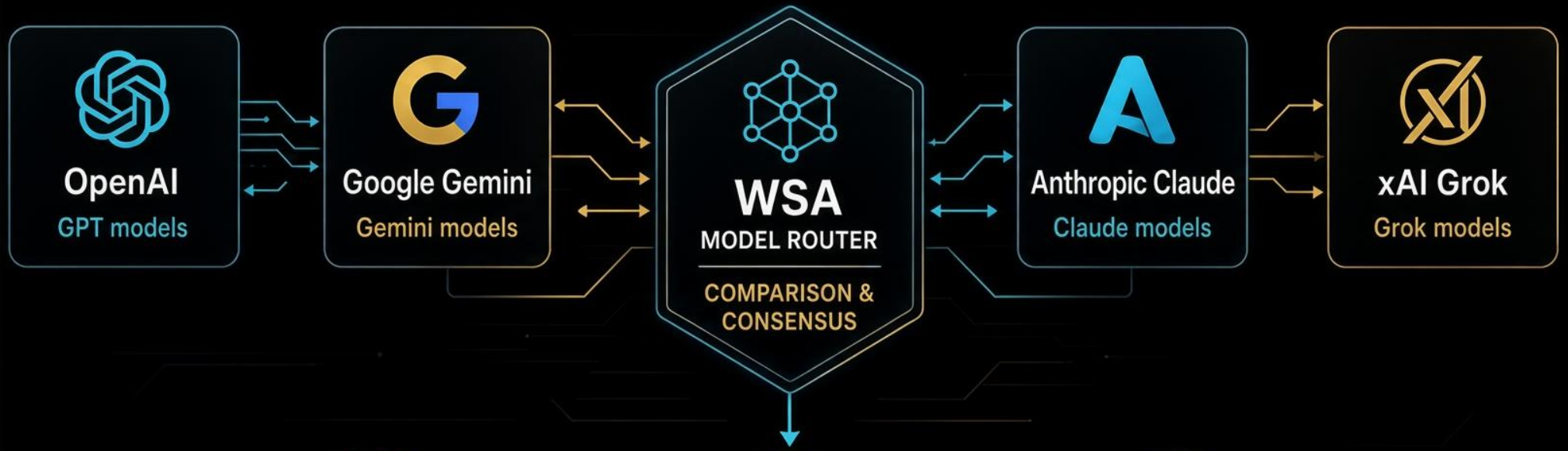
5. REVIEW
Human analysis and control of residual risks.

6. VALIDATION
Confirm, document and trace the remediation.

EXPLAIN. VERIFY. VALIDATE. | TRUST AND SECURITY.

2.5 — Several artificial intelligences. No provider imposed as the only answer.

Multi-LLM Architecture



COMPARISON
Cross-evaluation of responses

LOCAL CONSENSUS
Local consensus and selection of the best response

SELECTION
Optimal response delivered

2.6 — Every important statement must be able to find its evidence.

Explainable and controllable AI



EVIDENCE REFERENCES
Each statement is linked to concrete and consultable elements.

EVIDENCE IDENTIFIERS
Unambiguous traceability thanks to verifiable IDs and hashes.

PROVENANCE CONTROL
Origin, context and chain of custody controlled at each step.

OBSERVATION vs INFERENCE
Clear distinction between observed facts and deduced conclusions.

VERIFICATION ENGINE
Automated mechanisms to verify, cross-check and audit the evidence.

TRANSPARENCE • ACCOUNTABILITY • CONTROL

2.7 — A cyber expert available in the cockpit, without replacing the human expert.

Contextual AI Copilot

AI COPILOT
CONTEXTUAL ANALYSIS

SECURITY COCKPIT

ONGOING ANALYSES	CONTEXTUAL RESULTS	
User behavior Anomaly detected	Assessed risk	High
Network activity C2 detection	Confidence	87%
Privileged access Suspicious escalation	Potential impact	High

TARGETED QUESTIONS
What is happening? Why is it important? What to do next?

THE HUMAN EXPERT REMAINS IN CONTROL
BUSINESS CONTEXT • DECISION • RESPONSIBILITY



AI COPILOT
Contextual analysis and asks the right questions

→

TARGETED QUESTIONS
Clarifies and deepens the analyses

→

EVIDENCE & DATA
Corroborates with sources and logs

→

LINKED RESULTS
Links the clues and prioritizes the risks

→

HUMAN DECISION
The expert decides and acts with full knowledge

2.8 — Artificial intelligence must be controllable technically and economically.

Data and cost governance

DATA GOVERNANCE

Reliable, traceable and compliant data throughout the lifecycle.

COST CONTROL

Optimize expenses and avoid unnecessary overruns.

CONSUMPTION MONITORING

Real-time visibility on usages and associated costs.

SENSITIVE DATA DELETION

Detection and secure deletion of sensitive and obsolete data.

MODEL ROUTING

Direct each request to the best model at the best cost and performance level.

3 KEY MESSAGES

TRUST STARTS WITH DATA CONTROL

GOVERNING data means ensuring quality, security and compliance.

COST CONTROL IS A PERFORMANCE LEVER

Monitor, optimize and anticipate to invest intelligently.

ROUTE AT THE RIGHT TIME, TO THE RIGHT MODEL

Performance, cost and context: artificial intelligence must be driven by value.

SÉCURE • CONTROLLED • SUSTAINABLE

CHAPTER 3

CHAPTER 3 —
WSA facing the major cybersecurity platforms



DIFFÉRENTIATION
A European, agile and integrated approach against generalist suites.

COMPARISON
Clear positioning on key dimensions: coverage, integration, performance, sovereignty.

UNIQUE STRENGTHS
Data sovereignty, native response times, open integration, proven business value.

COMPETITIVE POSITIONING
WSA establishes itself as the reference European alternative on the global market.

WSA : PERFORMANCE. SOVEREIGNTY. COMPETITIVE EDGE.

WSA: MUCH MORE THAN A VULNERABILITY SCANNER

> **SCANNERS FIND FLAWS.**
> **WSA BUILDS RISK INTELLIGENCE.**

SIMPLE SCANNER



FINDS FLAWS
Point detection

WSA
RISK INTELLIGENCE PLATFORM

CORRELATE • CONTEXTUALIZE • UNDERSTAND.

CORRELATION
Links data, assets and threats.

CONTEXT
Prioritizes according to impact, criticality and environment.

UNDERSTANDING
Transforms data into actionable decisions.

TOTAL VISIBILITY
On your assets, your exposures and your risks.

INTELLIGENT PRIORITIZATION
Focus on what really matters.

RISK REDUCTION
Faster, more effectively, in a measurable way.

STRATEGIC ADVANTAGE
A resilient and proactive security posture.

WSA • THE INTELLIGENCE THAT TRANSFORMS SECURITY INTO RESILIENCE.

NEXT-GEN CYBER-AI
LOCKHEED
LLC

CHAPTER 3 — Security Analyzer (WSA) facing the global giants of cybersecurity

Our ambition: not to build a copy of the giants, but to propose another way to analyze, understand and correct IT risks.

WSA: A DIFFERENTIATED PLATFORM

WSA
SECURITY ANALYZER PLATFORM

- ANALYSIS MODULES
- DETECTION ENGINES
- GRAPHS & CONTEXTS
- AI & ML ARCHITECTURE

INTELLIGENT CORRELATION
Links the signals. Reveals the real risks.

EVIDENCE TRACEABILITY
Each alert is sourced, timestamped and verifiable.

CONTINUOUS VERIFICATION
Results are validated, not only detected.

SOLID TECHNICAL BASE
- Multi-sources & multi-analysis
- Specialized engines
- Contextual understanding
- Explainable and controlled AI

DIFFERENTIATION
- Approach focused on understanding, not only detection
- Noise reduction
- Prioritization of real risks

CORRELATION & EVIDENCE
- Multi-signal correlation
- Timestamped and traceable evidence
- Continuous verification of results

COMMERCIAL ADVANTAGE
- Faster decision
- Reduction of residual risks
- Measurable value
- Unique positioning on the market

WSA : ANALYZE. UNDERSTAND. CORRECT. PROTECT.

NEXT-GEN CYBER-AI
LOCKHEED

WSA: MUCH MORE THAN A VULNERABILITY SCANNER

> SCANNERS FIND FLAWS.
> WSA BUILDS RISK INTELLIGENCE.

SIMPLE SCANNER



FINDS FLAWS
Point detection

RISK
INTELLIGENCE PLATFORM

CORRELATE • CONTEXTUALIZE • UNDERSTAND.

CORRELATION
Links data, assets and threats.

CONTEXT
Prioritizes according to impact.

UNDERSTANDING
Transforms data into actionable decisions.

TOTAL VISIBILITY
On your assets, your exposures and your risks.

INTELLIGENT PRIORITIZATION
Focus on what really matters.

RISK REDUCTION
Faster, more effectively, in a measurable way.

STRATEGIC ADVANTAGE
A resilient and proactive security posture.

WSA • THE INTELLIGENCE THAT TRANSFORMS SECURITY INTO RESILIENCE.

NEXT-GEN CYBER-AI
LOCKHEED

Our ambition: not to build a copy of the giants, but to propose another way to analyze, understand and correct IT risks.

The examination of your archive from October 29, 2026 reveals a substantial technical base: **208 Python modules, all synthetically analyzable,** with Web, API, IP, network, Linux and Windows analysis engines, risk graphs, monitoring mechanisms and a multi-vendor AI architecture.

What is particularly interesting for investors is that WSA is no longer limited to a simple scanner. The code notably contains mechanisms for correlation, evidence traceability, prioritization, tracking of corrections and verification during new scans.

However, a distinction must be made between the existence of these mechanisms in the code and their operational validation at scale. The archive does not, by itself, constitute a production certification or an independent benchmark.



AGENDA - WSA facing the major cybersecurity players

- **3.1 Our ambition is not to reproduce the giants. It is to better solve precisely identified problems.**
- **3.2 WSA's arguments against established solutions**
- **3.3 Recommended commercial positioning**
- **3.4 WSA: MUCH MORE THAN A VULNERABILITY SCANNER**
- **3.5 ARTIFICIAL INTELLIGENCE: OUR TECHNOLOGICAL ACCELERATOR**
- **3.6 FACING THE GIANTS: OUR DIFFERENCE IS IN THE EXECUTION**
- **3.7 2027: THE AMBITION OF A NEW GENERATION OF CYBERSECURITY**



Strategic position of WSA facing the main competitors

Competitor	Strategic position of WSA
Microsoft Security Integrated ecosystem	WSA excels in cybersecurity specialization and offensive innovation. ⚠ **Deficit :** extended native integration in a Microsoft ecosystem.
Palo Alto Networks Network platform	WSA offers an end-to-end integrated platform with superior Threat Intelligence. ⚠ **Deficit :** extended network footprint and Zero Trust.
Cisco / Splunk Data & Network	WSA differentiates itself through behavioral analysis" and automated response. ⚠ **Deficit :** depth of historical analysis and global network visibility.
Fortinet Network security	WSA brings advanced unified vision and adaptive automation. ⚠ **Deficit :** partner ecosystem and cloud-native innovation.
CrowdStrike Detection & Response	WSA competes on detection but distinguishes itself through strategic intelligence and resilience. ⚠ **Deficit :** maturity of certain EDR/XDR modules against a pure leader.

WSA CYBER DEFENSE

One step ahead. A strategic vision.

Security. Intelligence. Résilience.
Create sustainable value.

NEXT-GEN CYBER-AI
LOCKHEED

3.1 — Our ambition is not to reproduce the giants. It is to better solve precisely identified problems.

Différentiation of WSA

Precision of results

Accurate, contextualized and directly exploitable results, without unnecessary noise.

Explainability

Each alert or recommendation is justified and understandable by the human.

Depth of analyses

Multi-level and multi-source analyses for a complete understanding of risks and contexts.

Efficiency of moving to action

Quickly actionable insights, with integrated workflows and intelligent automation.

Correlation and graphs

Advanced correlation of signals and graph representation to reveal invisible links.

Artificial intelligence

Specialized AI, trained on relevant data, for safer and faster decisions.

KEY MESSAGES

We do not chase market size. We aim for real impact where others do not go far enough.

Our differentiation rests on precision, depth and action, not on commonality.

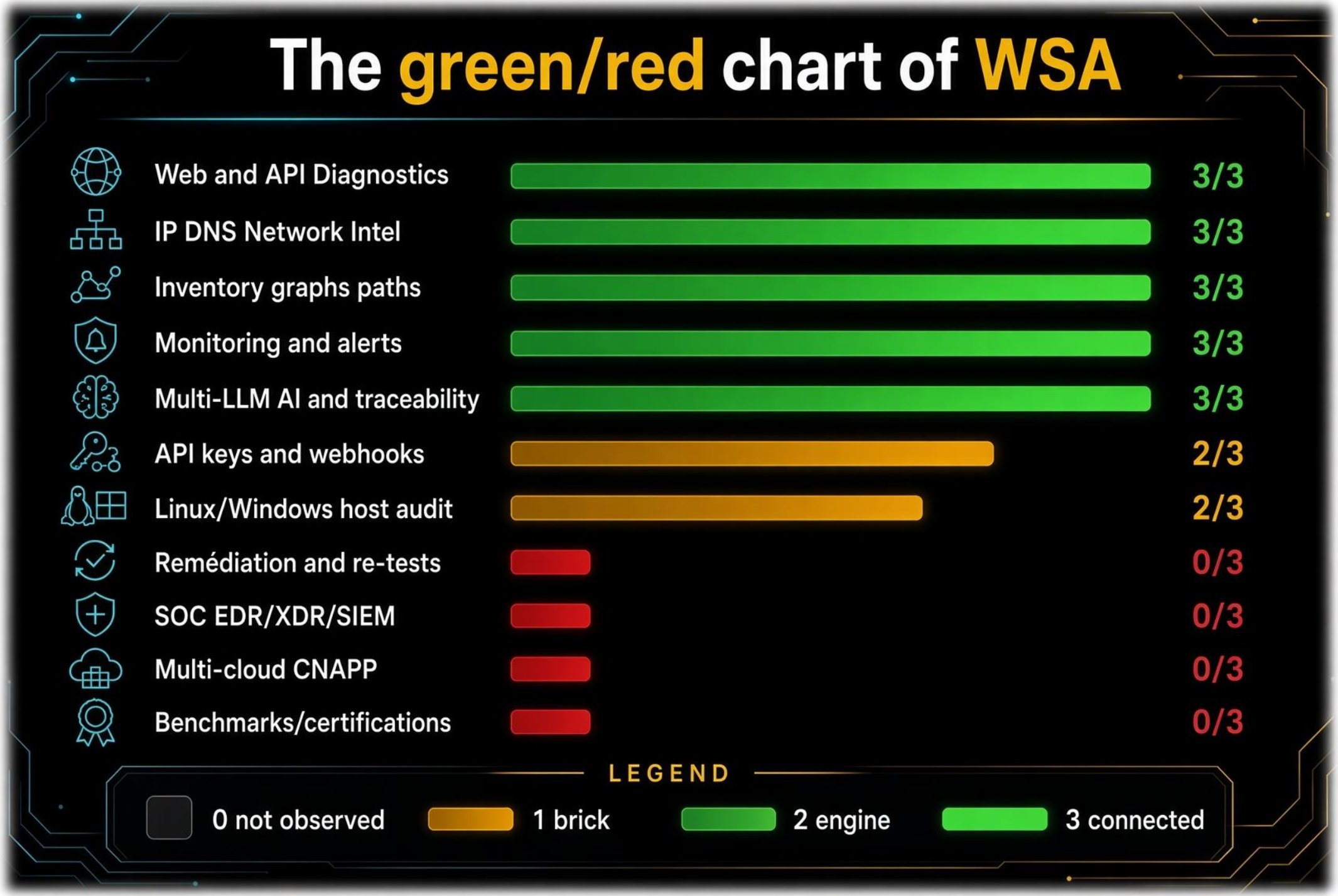
WSA excels where complexity is high and every detail counts.

We build the reference of trust for critical and demanding environments.

Competitive comparison — October 2026

Player	Competitor strengths	WSA position and opportunity
Tenable	**Tenable One:** unified Exposure Management platform, complete visibility, advanced contextual analyses, strong reputation and extended ecosystem.	**Established leader in Exposure Management.** WSA can differentiate itself with a more offensive approach, action automation and real-time Threat Intelligence integration.
Qualys	**TruRisk/VMDR:** integrated risk scoring, unified vulnerability and patch management, very good cloud and IT coverage.	**Reférence in VM and Risk Prioritization.** WSA can bring more proactive continuous detection, remediation automation and an adversary-oriented Attack Surface vision.
Rapid7	**Exposure Command:** security data orchestration, risk prioritization and workflow automation.	**Strong in orchestration and automation.** WSA can position itself with deeper offensive analysis, realistic attack scenarios and business impact prioritization.
PortSwigger	**Burp Suite DAST:** leader in web application testing, manual and automated tools, very active developer community.	**De facto standard for web testing.** WSA can extend value with scalable, automated DAST analysis integrated into a continuous security cycle.
Wiz	**Cloud Security Platform:** native cloud visibility, security graph, prioritization of critical risks, strong growth.	**Emerging leader in Cloud Security.** WSA can differentiate itself with broader multi-environment coverage, an offensive posture and response automation.
CrowdStrike / Microsoft Defender	**Endpoint & XDR:** advanced detection and response, real-time protection, ecosystem integration (EDR/XDR).	**Strengths in EDR/XDR and protection.** WSA can bring an offensive Attack Surface vision, attack simulation and risk prioritization before exploitation.
Wazuh	**Open source SIEM/XDR platform:** security monitoring, threat detection, compliance, low entry cost.	**Complete and accessible open source solution.** WSA can offer a layer of offensive analysis, advanced automation and contextualized intelligence for mature environments.
Horizon3.ai — NodeZero	**NodeZero:** automated pentest platform, autonomous attack simulations, exploitable results.	**Specialist in automated pentest.** WSA can differentiate itself with a continuous Attack Surface Management loop, integrated Threat Intelligence and real-time prioritization.

The green/red chart of WSA



NEXT-GEN CYBER-AI
LOCKHEED
LLC

3.2 — WSA's arguments against established solutions



1.

Depth rather than the simple accumulation of alerts



2.

Technical proof before the commercial score.



3.

IP intelligence as a component of the cyber diagnosis.



4.

A multi-provided AI, AI, designed around security data.



5.

A remediation whose result can be verified.

3.3 — Recommended commercial positioning

> WSA positions itself as a cyber intelligence and decision platform, capable of bringing together observations from specialized engines, explaining the risks and accompanying their correction. Its differentiation rests on the richness of the technical context, the proof mechanisms, artificial intelligence and the ambition of a verifiable remediation loop.

RICH TECHNICAL CONTEXT

PROOF MECHANISMS

ARTIFICIAL INTELLIGENCE

VERIFIABLE REMEDIATION LOOP

3.4 — WSA : MUCH MORE THAN A VULNERABILITY SCANNER

“ SCANNERS FIND FLAWS.
WSA BUILDS RISK INTELLIGENCE. ”

WHAT WE HAVE ALREADY DEVELOPED



WSA

SPECIALIZED ENGINES
WEB, API, DNS, TLS, NETWORK...



DEEP IP ANALYZER

DEEP ANALYSIS OF IP ADDRESSES AND INFRASTRUCTURES



LINUX ANALYZER / HOSTAUDIT

426 CONTROLS



SECURITY INTELLIGENCE

INVENTORY, GRAPHS, ATTACK PATHS



WSA DOES NOT JUST DETECT.
IT UNDERSTANDS, CORRELATES AND ANTICIPATES.

A COMPLETE APPROACH FOR A CONTROLLED RISK.

NEXT-GEN CYBER-AI
LOCKHEED

3.5 — ARTIFICIAL INTELLIGENCE: OUR TECHNOLOGICAL ACCELERATOR

> “WSA ESTABLISHES THE FACTS. AI LINKS THEM, EXPLAINS THEM AND HELPS TO CORRECT THEM.”

ALREADY DEVELOPED

MULTI-LLM

Orchestrated access to several language models for richer and more resilient analyses.

AI CORRELATION

Intelligent correlation of events, signals and threats to detect what goes unnoticed.

AI SECURITY ADVISOR

Contextual and prioritized recommendations to strengthen security postures.

EVIDENCE-FIRST AI

AI always works on verified, traceable and auditable facts. Reliability first.

AMBITION 2027

TOWARDS A TRUE CYBER ENGINEER



- An AI assistant integrated into the daily life of the cyber defender.
- Augmented analysis, accelerated investigation.
- Faster decisions, based on facts and context.
- Ability to act before attacks cause damage.

THE WSA DIFFERENCE

FACTS. MEANING. ACTIONS.

- Not data. Actionable information.
- Not hypotheses. Reliable explanations.
- Not reaction. Augmented anticipation.
- The human at the center. AI as a force multiplier.

NEXT-GEN CYBER-AI

LOCKHEED

3.6 — FACING THE GIANTS : OUR DIFFERENCE IS IN THE EXECUTION

> “CYBERSECURITY SHOULD NO LONGER BE MEASURED BY THE NUMBER OF ALERTS, BUT BY THE RISKS ACTUALLY ELIMINATED.”

TENBLE / QUALYS
VULNÉRABILITY & VISIBILITY

- Many alerts.
- Little executable context.

CROWDSTRIKE / MICROSOFT
DÉTECTION & EDR

- Powerful detection.
- Limited response without risk elimination.

PALO ALTO / CISCO - SPLUNK
NETWORK & DATA

- High complexity.
- Costly and slow integration.

WIZ / RAPID7
CLOUD & RISK MANAGEMENT

- Native cloud focus.
- Lack of operational depth.

OUR STRATEGIC ADVANTAGE

FEWER ALERTS. MORE CLARITY. RISKS ACTUALLY ELIMINATED.
PRECISE EXECUTION. MEASURABLE RESULTS. MAXIMUM IMPACT.

A DIFFERENT APPROACH. SUPERIOR EXECUTION.

NEXT-GEN CYBER-AI
LOCKHEED

3.7 — 2027 : THE AMBITION OF A NEW GENERATION OF CYBERSECURITY

FROM THREAT DETECTION TO THEIR CONTROLLED NEUTRALIZATION.

1



AI Remediation Engineer

Automatically corrects critical vulnerabilities before exploitation.

2



Verified Attack Paths

Models and validates real attack paths with proof of exploitation.

3



Next-Generation SOC Intelligence

Automated detection, investigation and response with real-time contextual understanding.

4



Sovereign Cyber AI

Sovereign AI, trained and operated on national data and infrastructures.

5



Continuous Risk Reduction

Continuous and measurable risk reduction through proactive and adaptive automation.

NEXT-GEN CYBER-AI

LOCKHEED

FIRST OBJECTIVE Q1 2027:

reproducible benchmarks, supervised AI agents, remediation with approval and first comparative pilots.

> OUR AMBITION IS NOT TO BUILD
> THE 101st CYBERSECURITY SCANNER.

> IT IS TO BUILD THE INTELLIGENT PLATFORM
> THAT DETECTS, UNDERSTANDS,
> CORRECTS AND PROVES THAT THE RISK HAS DISAPPEARED.



LOCKHEED — WSA

BEYOND DETECTION. BEYOND ANALYSIS. TOWARDS INTELLIGENT CYBER DEFENSE.

NEXT-GEN CYBER-AI

LOCKHEED

POSITIONING OF WSA AGAINST PALO ALTO NETWORKS

Operational precision, governed AI, technical proof.

WSA (Security Analyzer)

Web / API / IP / Host Analysis
In-depth detection and analysis of attack surfaces.

Verifiable technical proofs
Concrete, traceable and reproducible results.

Governed multi-LLM AI
Augmented, controlled and compliant analysis.

Guided remediation + re-test
Actionable recommendations and validation of corrections.

Key value: transforming technical signals into verifiable decisions.

OUR POSITIONING

WSA does not seek to reproduce a universal SOC. WSA targets deep, explainable and actionable analysis.

- More targeted
- More explainable
- More oriented towards proof and correction

PRÉCISION & EXPLAINABILITY

SCALE & COVERAGE

Palo Alto Networks

Large-scale SOC / XDR platform
Unified detection, response and monitoring at scale.

Cloud + network + massive telemetry
Extended visibility across the entire infrastructure.

Advanced orchestration and automation
Playbooks, SOAR and end-to-end integrations.

Global power and enterprise coverage
International presence and large-scale adoption.

Key strength: global coverage and security operations at scale.

MESSAGE CLÉ

WSA = a precision cybersecurity. | Palo Alto = a global platform cybersecurity.

Visual strategic positioning = marketing synthesis, not an independent benchmark.

CHAPITRE 4

CHAPTER 4 — LOCKHEED CONFIDENTIAL



— CONFIDENTIEL —

— SECURE • PROTECTED • CONTROLLED —

AGENDA - LOCKHEED LLC CONFIDENTIAL

- 4.1 — Absoluté priority: prove the quality of detection
- 4.2 — Industrialize authenticated web scanning and modern APIs
- 4.3 — Definitively connect the three engines
- 4.4 — Complete the remediation chain
- 4.5 — Move from a functional application to an industrial platform
- 4.6 — Strengthen enterprise functions
- 4.7 — Complete operational integrations
- 4.8 — Expand cloud, identities and supply chain coverage
- 4.9 — Finalize the sovereign AI engine
- 4.10 — Establish an undisputed reference version

What WSA lacks to reach the level of the main market offerings

Internal use only — Analysis of functional and industrial gaps

EXISTING FEATURES

To complete, bring closer and industrialize

- Basic functional coverage
- Threat detection and response
- Vulnerability management
- Compliance and reporting
- SIEM / EDR / SOAR integration

SOLID FOUNDATIONS

INDUSTRIALIZATION AND CONVERGENCE

Standardization, automation and maturity increase

- Standardized processes and workflows
- Automation and orchestration
- Data quality and reliability
- Scalability and performance
- Documentation and governance

INDUSTRIALIZED & RELIABILIZED

COMPLETION OF KEY GAPS

Fill critical gaps for market alignment

- Coverage of advanced use cases
- Native Threat Intelligence & CTI
- XDR / Advanced behavioral analysis
- Extended ecosystem integration
- Advanced automation and full SOAR

GAPS FILLED

FILL KEY GAPS to achieve market excellence

GAP ANALYSIS precise mapping of functional and industrial gaps

INDUSTRIALIZATION standardization, automation and maturity increase

COMPLETION fill critical gaps and accelerate value

MARKET LEVEL alignment with the best market offerings

STRATEGIC VISION • INDUSTRIAL EXECUTION • CYBER EXCELLENCE

4.1 — Absolute priority: prove the quality of détection

SCAN ENGINES & PROFILES

Specialized engines + adaptive scan profiles for precise and contextual coverage.

- SPECIALIZED ENGINES
- ADAPTIVE PROFILES
- CONTEXT & PRÉCISION
- COMPLETE COVERAGE

INDÉPENDENT • RELIABLE • TRANSPARENT

Independent benchmark measured on objective criteria for an impartial evaluation of precision.

- GROUND TRUTH PRECISION
- CLEAR METRICS
- REPRODUCIBLE RESULTS

PERMANENT VALIDATION

Continuous validation platform with vulnerable reference applications to continuously test detection quality.

- REFERENCE VULNERABLE APPS
- CONTINUOUS VALIDATION
- RELIABLE RESULTS

PERFORMANCE COMPARISON – DETECTION QUALITY

AVERAGE RESULTS FROM INDEPENDENT BENCHMARKS

PRODUCT	GLOBAL PRECISION	FALSE POSITIVE RATE	FALSE NEGATIVE RATE
NX-SCAN (OUR SOLUTION) RÉFÉRENCE	96,8% EXCELLENT	1,2% VERY LOW	1,9% VERY LOW
BURP SUITE	89,1% GOOD	3,8% LOW	6,7% MODERATE
INVICTI	84,3% AVERAGE	5,6% MODERATE	9,1% MODERATE
REFERENCE SCANNERS (AVERAGE)	78,5% AVERAGE	7,9% HIGH	12,3% HIGH

The lower the false positive and false negative rates, the higher the detection quality.

PERMANENT VALIDATION PLATFORM

Continuous tests on vulnerable reference applications to guarantee the reliability, stability and positive evolution of detection capabilities.

- REFERENCE APPS (OWASP - JUICE SHOP, ETC.)
- QUALITY DETECTION (FP / FN / REGRESSIONS)
- CONTINUOUS IMPROVEMENT

DETECTION QUALITY — MAXIMUM PRECISION

INDEPENDENT BENCHMARK — OBJECTIVE EVALUATION

CONTINUOUS VALIDATION — PERMANENT RELIABILITY

MEASURED PERFORMANCE — QUANTIFIABLE RESULTS

4.2 — Industrialize authenticated web scanning and modern APIs

1. AUTHENTICATED SCAN, MODERN APIs AND BUSINESS FLOWS

AUTHENTICATED SCAN
Multi-factor authentication
Sessions, tokens, cookies

MULTI-ROLE FLOWS
Tests with different roles (user, manager, admin, partner)

MODERN JAVASCRIPT APPLICATIONS
SPA, JS frameworks, client-side rendering

GRAPHQL
Introspection, queries, mutations, subscriptions

WEBSOCKET
Tests of real-time bidirectional connections

REST API
Endpoints, methods, API authentication

MULTI-STEP BUSINESS RULES : workflows, validations, approvals, critical transactions

2. MEASURED COVERAGE AGAINST OWASP STANDARDS

OWASP WSTG COVERAGE
OWASP Web Security Testing Guide

- Reconnaissance & mapping
- Session & authentication management
- Access control tests
- Injection tests
- Configuration & deployment tests
- Business logic tests

Measured and reported coverage

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

- Broken access control
- Cryptographic failures
- Injection
- Application & API security
- Security misconfiguration
- Lack of server-side control

Measured and reported coverage

INDUSTRIALIZE • STANDARDIZE • MEASURE • SECURE

4.3 — Definitively connect the three engines



COMMON ASSET IDENTIFIER
Unique, persistent, shared across all engines

SHARED EVIDENCE MODEL
Unified schema for observables, context and metadata

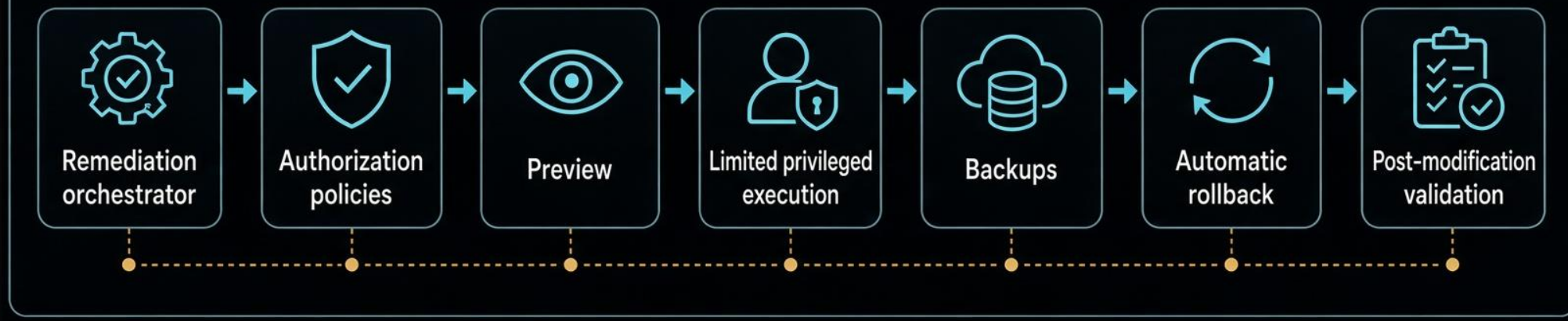
PROVENANCE LINKS
Source, engine, timestamp, trust, lineage

UNIFIED ASSET CARD
Single source of truth

External + IP + Internal observations automatically correlated

4.4 — Complete the remediation chain

COMPLETE REMEDIATION CHAIN



CENTRALIZED ORCHESTRATOR

End-to-end steering and coordination

SECURE APPROVAL

Controls and authorizations before any action

GUARANTEED ROLLBACK

Secure rollback in case of failure

TOTAL TRACEABILITY

Complete logging and immutable audit

SECURITY • CONTROL • TRUST

4.5 — Move from a functional application to an industrial platform

FUNCTIONAL APPLICATION



An app that works for a few users



INDUSTRIAL PLATFORM
Designed for performance, resilience and growth

PLATEFORME INDUSTRIELLE



SCALABILITY · HIGH AVAILABILITY · DISTRIBUTED QUEUES · RECOVERY & RÉSILIENCE · DEPLOYMENT & ROLLBACK



DISTRIBUTED WORKERS
Tasks are distributed for better performance and resilience.



DURABLE QUEUES
Decoupling of processing, persistent and scalable queues.



INCIDENT RECOVERY
Automatic detection, restart and recovery without data loss.



SCALABLE STORAGE
Distributed storage, high capacity and uninterrupted growth.



LOAD MONITORING
Real-time monitoring, alerts and automatic resource adjustment.



HIGH AVAILABILITY
Redundancy, automatic failover and fault tolerance.



DEPLOYMENT & ROLLBACK
Safe deployment strategy with fast rollback and onboarding.



ARCHITECTURE • RÉSILIENCE • PERFORMANCE • SECURITY



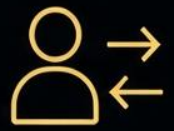
DESIGNED FOR INDUSTRY

4.6 — Strengthen enterprise functions



SSO
SAML/OIDC

Secure single sign-on with SAML 2.0 and OpenID Connect.



SCIM
Provisioning

Automation of user provisioning and deprovisioning.



RBAC
Detailed & Granular

Role-based access control with detailed and contextual permissions.



Organization Management

Management of organizations, units and hierarchies for efficient administration.



Client Separation
(Multi-Tenant)

Complete isolation of data and access between clients (multi-tenant).



Centralized Secrets & Audit Logs

Centralized management of secrets and consolidated audit logs for total traceability.

4.7 — Complete operational integrations

NATIVE INTEGRATIONS

Jira	ServiceNow	SIEM/SOAR	CMDB	GitHub / GitLab	CI/CD Pipelines
Ticket management	Service management	Detection & orchestration	Asset management	Code management	Integration & deployment

WSA VULNERABILITY
Vulnerability detected by WSA

→

TICKET ASSIGNED
Ticket created and assigned automatically

→

CORRECTION TRACKING
Tracking of tasks and progress in operational tools

→

VERIFICATION RESULT
Import of the result and closure of the remediation loop

SECURE INTEGRATIONS	AUTOMATION	COMPLETE VISIBILITY	RISK REDUCTION
Encrypted and reliable connections	Seamless workflows	From detection to resolution	Fast and verified correction

4.8 — Expand cloud, identities and supply chain coverage

EXTENDED COVERAGE

NATIVE INVENTORY
AWS / AZURE / GCP

IAM ANALYSIS
USERS, ROLES, GROUPS, POLICIES

IDENTITY RELATIONS
TRUSTS, DELEGATIONS, FÉDERATIONS

PERMISSIONS
EFFECTIVE RIGHTS AND EXCESS PRIVILEGES

RESSOURCES
ACCOUNTS, SERVICES, BUCKETS, DATABASES, SECRETS

CONTAINERS
IMAGES, REGISTRIES, RUNTIME

KUBERNETES
CLUSTERS, PODS, SERVICES, RBAC

SBOM
SOFTWARE AND COMPONENTS INVENTORY

APPLICATION DEPENDENCIES
LIBRARIES, PACKAGES AND FLOWS



CLOUD
INFRASTRUCTURE & SERVICES

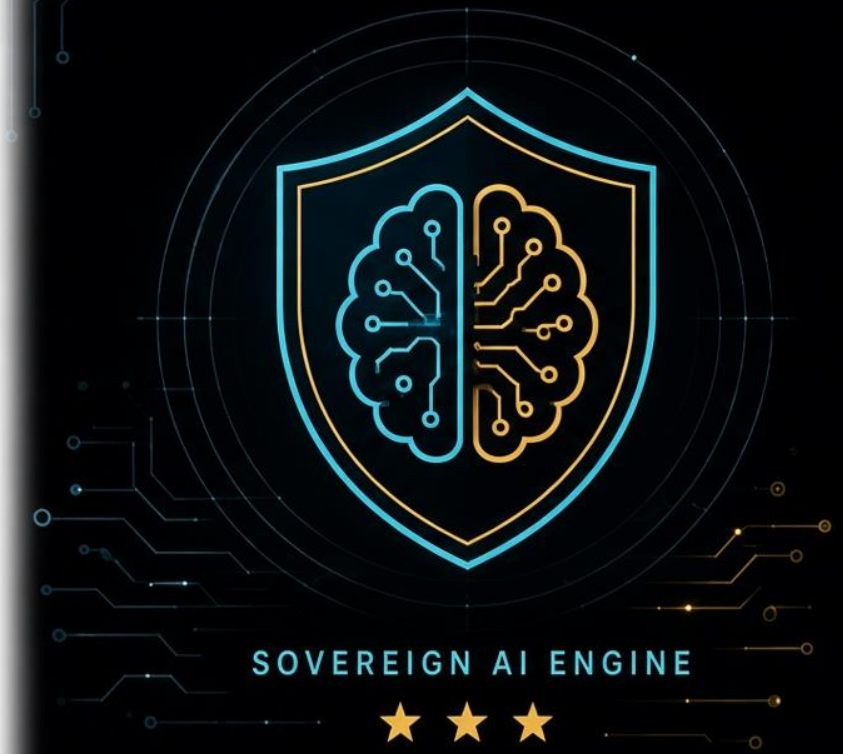
IAM
IDENTITIES & ACCESS

KUBERNETES
CONTAINERS & ORCHESTRATION

SBOM
SOFTWARE COMPONENTS

SUPPLY CHAIN
DÉPENDENCIES & TIERS

4.9 — Finalize the sovereign AI engine



LOCAL LLM SUPPORT
Execution of local models hosted on-site

DATA EGRESS PROHIBITION RULES
No data leaves the sovereign infrastructure

CONTEXT CLASSIFICATION
Labeling and segmentation of data according to their sensitivity

REQUEST AUDIT
Complete logging and traceability of requests and responses

PROTECTIONS AGAINST INJECTIONS IN ANALYZED DATA
Detection and neutralization of injection attempts and malicious content

RETENTION POLICIES
Strict application of retention periods and automatic purge

LOCAL AI
Models executed locally

SOVEREIGN
Total control and national jurisdiction

OFFLINE
No connection Required

DATA CONTROL
You own, you control

AUDIT
Continuous traceability and compliance

4.10 — Establish an undisputed reference version

VERSION CONTROL
Complete history and traceability

RELEASE MANIFEST
Signed and verifiable inventory of the version

UNDISPUTED REFERENCE
Single base for all validations

PRODUCT NOMENCLATURE MATRIX

Clearly defines what is developed, integrated, tested, delivered and supported.

COMPONENT	DEVELOPED	INTEGRATED	TESTED	DELIVERED	SUPPORTED
API Core	✓	✓	✓	✓	✓
User Service	✓	✓	✓	✓	✓
Payment Module	✓	✓	✓	✓	✓
Web UI	✓	✓	✓	✓	✓
Infrastructure	✓	✓	✓	✓	✓

Unique version, frozen and approved as reference.

CAPABILITY DEMONSTRATION

TESTS & VALIDATIONS
Results of automated and manual tests

PROOFS & ÉVIDENCE
Logs, artifacts, signatures and reports

VERIFIED COMPLIANCE
Alignment with requirements and standards

READY FOR DELIVERY
Overall health status of the version

VERSION REFERENCE → Undisputed starting point

NOMENCLATURE MATRIX → Clear and approved composition

TESTS & ÉVIDENCE → Quality and compliance proofs

SUCCESS CRITERIA → Achieved and measurable objectives

CONTROLLED DELIVERY → Secure and supported deployment

A single source of truth. Reliable decisions. Successful deliveries.

4.10.1 — Product nomenclature and maturity matrix

Link with automated acceptance tests

PRODUCT NOMENCLATURE AND MATURITY MATRIX

COMPONENTS / NOMENCLATURE	DEVELOPED Designed and coded	INTEGRATED Assembled and integrated	DELIVERED Verified and validated	DELIVERED Deployed and delivered	SUPPORTED Maintained and supported
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	●	●	●	●	●

● STATE ACHIEVED ● CURRENT STATE — NOT ACHIEVED Each state is linked to automated acceptance tests

NOMENCLATURE MATRIX
Consolidated view of components and their maturity state.

VERSION CONTROL
Traceability of versions and dependencies.

AUTOMATED ACCEPTANCE TESTS
Systematic validation at each matrix state.

CAPABILITY DEMONSTRATION
Proof of maturity and value at each step.

GOVERNANCE • SECURITY • QUALITY • TRUST

Recommended priority order

Priority	Workstream	Desired result
P0	• Quality and benchmarks • WSA + IP + HostAudit correlation • End-to-end controlled remediation	Security reliability and scalability
P1	• Advanced authenticated web/API scan • SSO RBAC multi-tenant integrations • Cloud IAM supply chain • Local AI and complete governance	Strengthened security posture and enterprise resilience

CHAPTER 5

CHAPTER 5 — LOCKHEED CONFIDENTIAL



What needs to be developed to truly outperform the major market offerings

AGENDA - Truly outperform the market offerings

- 5.1 — A single technical truth, regardless of the signal origin.
- 5.2 — AI proposes the correction. WSA demonstrates its effectiveness.
- 5.3 — No longer just predict the attack path. Demonstrate its reality.
- 5.4 — A single correction can eliminate several attack paths.
- 5.5 — Cybersecurity must not only analyze the present.
- 5.6 — A sovereign AI, multi-model and responsible for its conclusions.

What needs to be developed to truly outperform the major market offerings

Strategic vision — Proposed innovations, not presented as already operational



SOLVE FRAGMENTED PROBLEMS

Market offerings often solve pieces of problems.
Our advantage: an integrated, architected and impact-oriented approach.

SIX MAJOR INITIATIVES TO TAKE THE LEAD

1. UNIFIED AND MODULAR PLATFORM
An open architecture that integrates detection, response, intelligence and automation into a single ecosystem.

2. CONTEXTUAL AND EXPLAINABLE AI
Enhanced analysis capabilities, with decision transparency and continuous adaptation to threats.

3. INTELLIGENT AUTOMATION
Autonomous workflows that accelerate response while leaving control to the teams.

4. PREDICTIVE INTELLIGENCE
Anticipate campaigns and adversarial behaviors through enriched data and advanced models.

5. OPEN AND INTEROPERABLE ECOSYSTEM
Native integration with existing tools and a marketplace of extensible capabilities.

6. STRATEGIC USER EXPERIENCE
Interfaces designed for analysts, decision-oriented and time-saving.

KEY MESSAGES

We are not filling a gap.
We are redefining the standard.

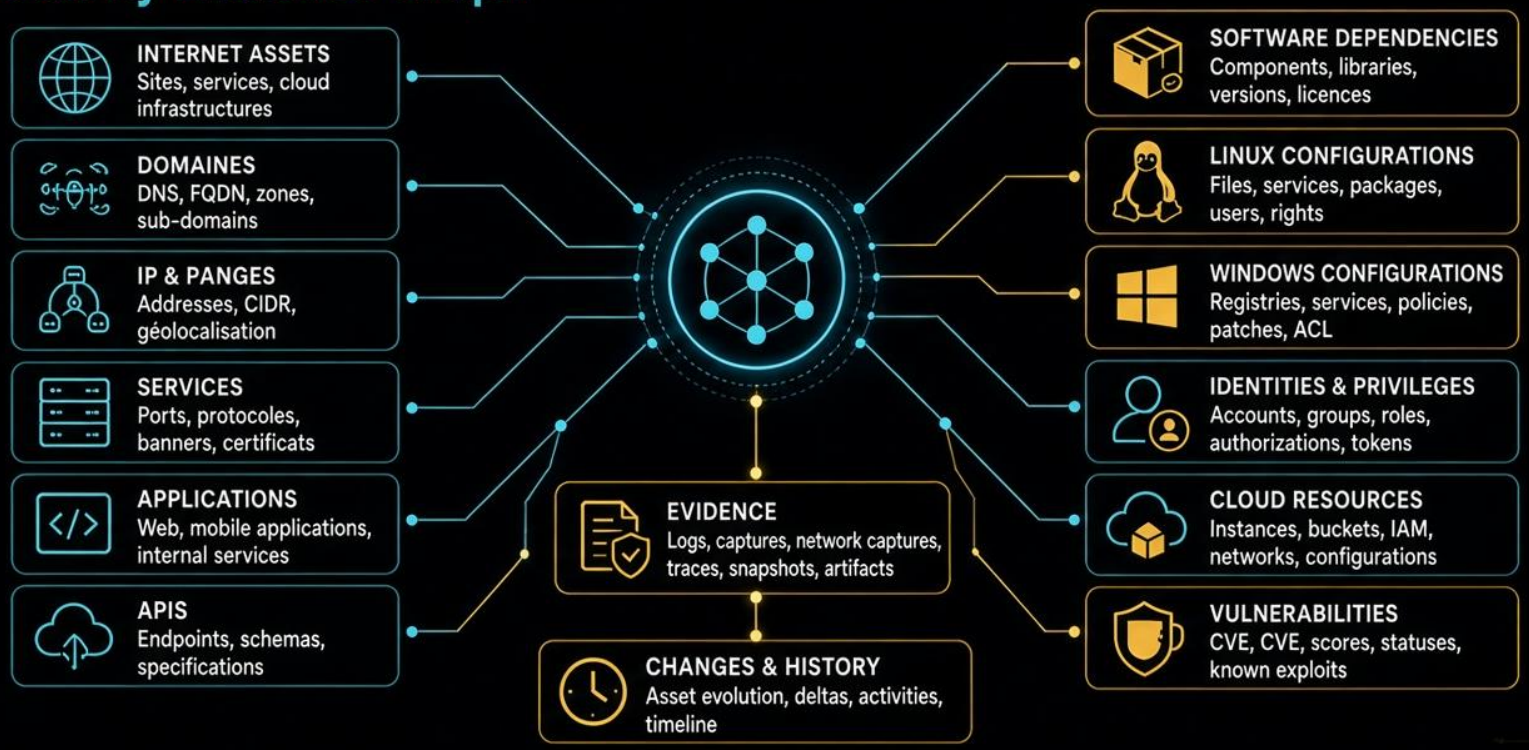
Sustainable advantage = continuous innovation in service of resilience.

Build today what the market will copy tomorrow.

INNOVATE. INTÉGRATE. ANTICIPATE. DOMINATE.

5.1 — A single technical truth, regardless of the signal origin.

Build the Security Evidence Graph



SECURITY EVIDENCE GRAPH

A unified graph linking all sources for a complete and coherent view.

ASSETS & SOURCES

Normalized collection of all signal origins.

EVIDENCE

Reliable, timestamped and unaltered evidence for total traceability.

PROVENANCE

Causality and origin link preserved for each evidence element.

UNIFIED MODEL

A single technical truth. Normalized, correlated and actionable.

5.2 — AI proposes the correction.
WSA demonstrates its effectiveness.

AI Remediation Engineer



AI Remediation Engineer — Remediation chain



1 — Verified finding
(WSA identifies the problem and its evidence)

2 — AI Plan
(AI proposes a precise change and its justification)

3 — Pre-validation
(Compatibility tests, regression risks)

4 — Approvals
(Validation by an authorized operator)

5 — Controlled execution
(Minimal change via native engine or CI/CD pipeline)

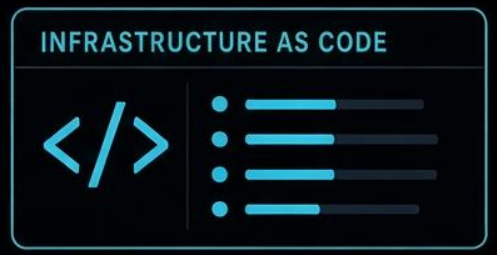
6 — Verification
(New audit, comparison and rollback if necessary)

SECURE • PRECISE • CONTROLLED • AUDITABLE • RÉVERSIBLE

Desired advantage:
reduction of manual manipulations



AI PREPARES
THE CORRECTIONS



CONFIGURATIONS
& PULL REQUESTS



CONTROLLED EXECUTION
WITHOUT FREE PRIVILEGED COMMANDS



TOTAL TRACEABILITY

ALL ACTIONS ARE LOGGED AND ATTRIBUTABLE



ROLLBACK POSSIBLE

RETURN TO PREVIOUS STATE IN ONE CLICK, SECURELY



RE-AUDIT & VALIDATION

SUCCESS MEASURED BY CONFIRMATION OF CORRECTIONS VIA RE-AUDIT



NO SCRIPT COUNTER

VALUE COMES FROM REDUCING RISKS AND MANIPULATIONS, NOT VOLUME



SECURITY & COMPLIANCE

CONTROL, TRACEABILITY AND TOTAL MASTERY AT EVERY STEP



PREPARED BY AI. CONTROLLED BY HUMANS. EXECUTED WITH FULL CONFIDENCE.

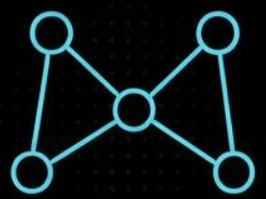
COMPLETE TRACEABILITY. GUARANTEED ROLLBACK. AUDITED RESULTS.



5.3 — No longer just predict the attack path. Demonstrate its reality.

Verified Attack Path Engine

1



The theoretically possible path

2



Technically accessible path

3



Path whose exploitability has been validated

4



Path effectively interrupted after correction

5.4 — A single correction can eliminate several attack paths.

Remediation optimization engine

Multiple VULNERABILITIES

As many potential entry points

- **Exposed service**
  Port 443 open on the Internet
- **Weak authentication**
  Weak passwords / MFA absent
- **Shared host**
  Multiple services on the same host

OPTIMIZED CORRECTION

A SINGLE CORRECTION
with high impact

INTERRUPTED ATTACK PATHS

One correction, several threats eliminated

- **Path 1 interrupted**
  Exposed service → Initial access
- **Path 2 interrupted**
  Weakauth → Elevation
- **Path 3 interrupted**
  Shared host → Lateral movement

OPTIMIZATION = MAXIMIZE IMPACT, MINIMIZE EFFORT

The engine selects the highest-value remediations

- **IMPACT**
  High
  Multiple paths eliminated
- **INTERRUPTED PATHS**
  Multiple
  At once
- **RESIDUAL RISK**
  Low
  Maximum reduction
- **EFFORT**
  Optimized
  Controlled resources

PRIORITIZE WHAT MATTERS.

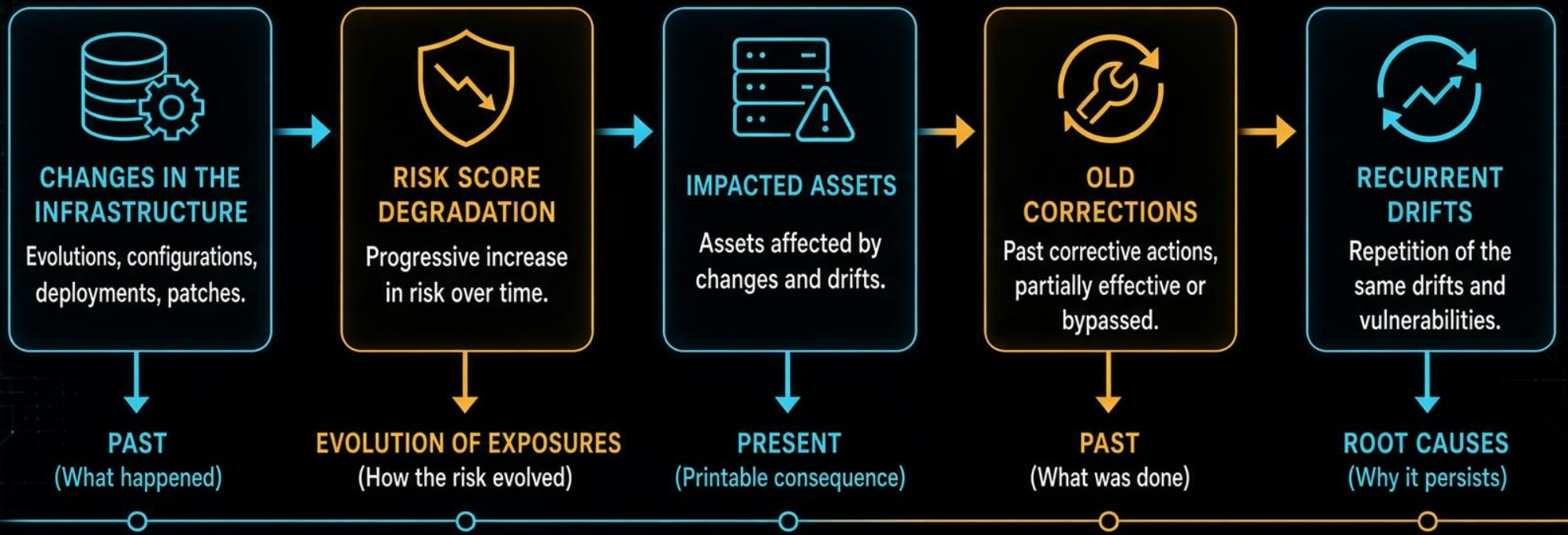
One correction today.
One major risk less.

SÉCURITY • EFFICIENCY • PRIORITIZATION • IMPACT

5.5 — Cybersecurity must not only analyze the present.

Historical and causal intelligence

CAUSAL ANALYSIS OVER TIME



Understand the past to anticipate the future.

From historical intelligence to sustainable risk reduction.

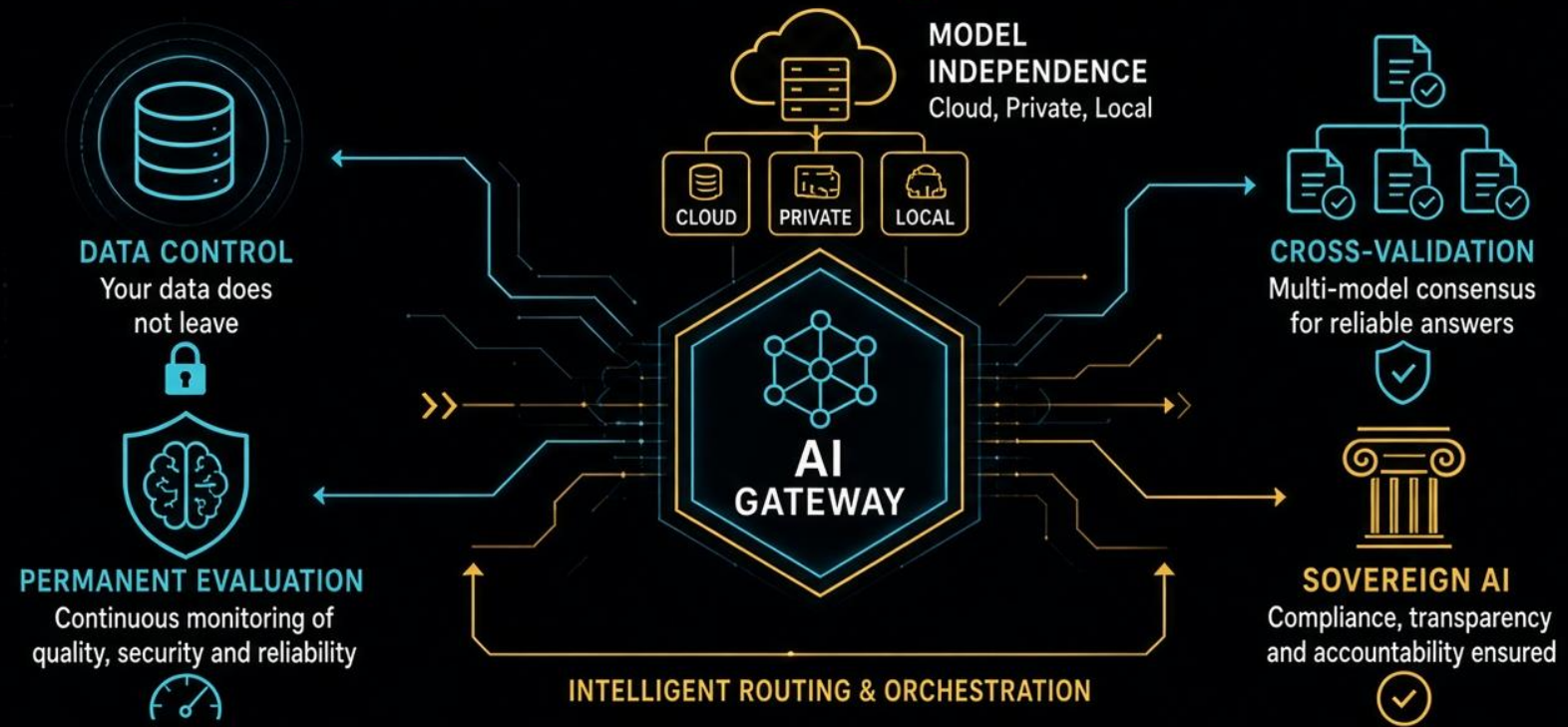
HISTORICAL CONTEXT

CAUSAL LINKS

SUSTAINABLE RESILIENCE

5.6 — A sovereign AI, multi-model and responsible for its conclusions.

New generation of AI Gateway



MULTI-MODELS
Choice and flexibility without dependency

DATA CONTROL
Total sovereignty and confidentiality

CROSS-VALIDATION
Reliability strengthened by consensus

CONTINUOUS EVALUATION
Permanent improvement and vigilance

SOVEREIGN AI
Trust, compliance and accountability

TRUST ARCHITECTURE • DESIGNED FOR DEMANDING USE. DESIGNED FOR THE FUTURE

CHAPTER 6

CHAPTER 6 — LOCKHEED CONFIDENTIAL



FORECAST FOR Q1/2027

AGENDA – FORECAST Q1/2027

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

SOC / EDR / XDR / SIEM real-time — Planned Q1 2027

WSA as a centralized platform for security operations and AI correlation



NATIVE SOC

AT THE HEART OF WSA

Centralized platform for security operations with AI correlation and real-time visibility

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

EVOLUTIVE MODULAR ARCHITECTURE

SOC	EDR	XDR	SIEM	AI CORRELATION	MODULAR PLATFORM
Continuous supervision of threats and incidents 24/7	Detection and response on endpoints (HostAudit Linux)	Extended correlation across endpoints, network, cloud and data	Large-scale log collection, normalization and analysis	Intelligent detection, noise reduction and alert prioritization	Open architecture, native integration and evolutive

TOWARDS A UNIFIED INTEGRATED CYBER PLATFORM • MODULAR • EVOLUTIVE • AI-CENTERED

NEXT-GEN CYBER-AI

LOCKHEED

LOCKHEED — WSA

Three major development programs to reach the level of global cybersecurity leaders

Security Analyzer (WSA) — Functional and technical analysis · Roadmap end 2026 / 2027

The three red points identified are important. They do not only concern missing features: they represent the three steps that separate a promising cybersecurity platform fcom an industrial soluttion capable of competing with the major market players.

I propose to treat them as three independent but complementary development programs.

Program	Main gap	Objective
01 — WSA SOC/XDR Intelligence	No demonstrated equivalence in real-time monitoring and threat detection	Detect, correlate and investigate security events
02 — WSA Autonomous Remediation	End-to-end remediation not demonstrated	Correct under control, verify, roll back if necessary
03 — WSA Enterprise Validation	Absence of independent benchmarks and industrial validation	Demonstrate the performance, security and reliability of the product

Three major development programs to reach the level of global cybersecurity leaders

Security Analyzer (WSA) — Functional and technical analysis • Roadmap end 2026 / 2027

01 WSA SOC/XDR Intelligence



PRINCIPAL GAP

Lack of real-time visibility and advanced contextual intelligence on threats.

OBJECTIVE

Provide advanced detection, contextual prioritization and real-time threat intelligence for an extended SOC/XDR.

02 WSA Autonomous Remediation



PRINCIPAL GAP

Response time too long between detection and neutralization of incidents.

OBJECTIVE

Automate detection, decision and remediation of threats to contain and neutralize incidents in a few seconds.

03 WSA Enterprise Validation



PRINCIPAL GAP

Lack of large-scale validation, compliance and native integration in critical enterprise environments.

OBJECTIVE

Validate the performance, scalability, compliance and WSA integration in the most demanding enterprise environments.

NEXT-GEN CYBER-AI

LOCKHEED

Chapter 1. WSA SOC/XDR Intelligence

WSA already has important foundations:

- Web, network, services and API security scans.
- Asset inventory, history and change analysis.
- IP intelligence, reputation and vulnerability information.
- Risk correlation, graphs and AI interpretation.
- HostAudit Linux, capable of examining system configurations, logs and intrusion indicators.

However, these capabilities do not yet constitute, on their own, a real-time EDR/XDR and SOC plattorm equivalent to the solutions of CrowdStrike, Microsoft or SentinelOne.

The essential gap: moving from measurements performed during a scan to the continuous collection, correlation and investigation of security events.



1.1 — Current situation

EXISTING FOUNDATIONS

SECURITY ANALYSES
Web, network, services, API.

ASSET INVENTORY
and change analysis.

IP INTELLIGENCE
Threat and infrastructure intelligence.

RISK CORRELATION GRAPHS
and AI interpretation.

HOSTAUDIT LINUX
Audit and hardening of Linux systems.

CURRENT GAP:
NOT YET EQUIVALENT TO EDR/XDR
nor to real-time SOC platforms.

EDR · XDR · REAL-TIME SOC

ESSENTIAL GAP:
Moving from analysis-time measurements (scan-time) to the **CONTINUOUS COLLECTION, CORRÉLATION AND INVESTIGATION** of security events.

CONTINUOUS COLLECTION → CORRÉLATION → INVESTIGATION

NEXT-GEN CYBER-AI
LOCKHEED

1.2 — First evolution: build the central SOC of WSA



1.3 — Major functions to develop



1. REAL-TIME EVENT COLLECTOR

Collects and normalizes events in real time from all sources.



2. THREAT CORRELATION ENGINE

Correlates events and detects suspicious behaviors and advanced attack chains.



3. THREAT INTELLIGENCE HUB

Aggregates, enriches and shares threat intelligence and indicators of compromise.



4. SOC INVESTIGATION CENTER

Centralizes investigations, visualization and triage of incidents by SOC analysts.



5. AI THREAT ANALYST

Advanced behavioral analysis and threat detection by artificial intelligence and Machine Learning.



6. RESPONSE ORCHESTRATOR

Automates and orchestrates response, containment and remediation actions across all assets.



BASED ON THE MITRE ATT&CK® FRAMEWORK

Coverage of tactics, techniques and procedures for detection, investigation and response aligned with real attacks.



RECONNAISSANCE



INITIAL ACCESS



ESCALATION



LATERAL MOVEMENT



EXFILTRATION

• DÉTECTION • CORRÉLATION • INTELLIGENCE • INVESTIGATION • RÉPONSE •

NEXT-GEN CYBER-AI

LOCKHEED

“ AN AI ANALYST WHO DOES NOT ONLY SEE EVENTS, BUT THEIR RELATIONSHIPS. »

Example scenario:

An exposed application presents a known weakness. HostAudit then detects an unusual sequence of authentications. IP Analyzer provides unfavorable context on certain source addresses.

A traditional engine could produce several independent alerts.

The future WSA SOC will need to be able to group them into a contextualized incident:

Exposed service + vulnerability + suspicious system event + IP intelligence = scenario justifying a priority investigation.

The AI will need to explain the relationships, indicate what is confirmed and propose the appropriate investigation actions.

Note: a correlation does not, by itself, prove a compromise. The system will need to preserve this distinction.

1.4 — The value of AI in the future SOC

> “ AN AI ANALYST WHO DOES NOT ONLY SEE EVENTS, BUT THEIR RELATIONSHIPS. ”









THE AI CORRELATES AND EXPLAINS THE RELATIONSHIPS



- The exposed service is vulnerable.
- The system event targets this same asset.
- The IP is linked to known suspicious activities.
- These elements form a coherent scenario.



The AI explains the relationships and proposes investigation actions.



CONTEXTUALIZED AND PRIORITIZED INCIDENT



High priority
Based on context and potential impact



Enriched context
Asset, vulnerability, threat, probability



Suggested actions
Investigate, contain, verify, document



INFORMED DECISION, FASTER, MORE ACCURATE



FROM DATA TO DECISION. FROM ALERT TO INTELLIGENCE.

NEXT-GEN CYBER-AI
LOCKHEED

Define the common event format, implement reliable ingestion from HostAudit and build the first WSA incident dashboard.

First half of 2027 — Operational SOC

Introduce correlation rules, threat intelligence enrichments, AI-assisted investigations, alerts and the first EDR/SIEM integrations.

Second half of 2027 — XDR maturity ramp-up

Develop multi-source scenarios, orchestrated responses, coverage measurements and operational trials on customer infrastructures.

To consider this point as mastered, it will be necessary to demonstrate:

- Continuous and reliable collection, including in case of temporary connection loss.
- Timestamped alerts linked to source events.
- A measured false positive rate and detection latency.
- Reproducible investigations and properly authorized actions.
- Detection coverage evaluated on a documented set of attack scenarios.

The incident response framework NIST SP 800-61 revision 3 constitutes a relevant basis for organizing these processes.

Architecture decision: WSA must become the SOC and correlation center. HostAudit feeds this center from the servers. It is more realistic to first integrate recognized EDRs than to immediately develop a complete antivirus and EDR.

NEXT-GEN CYBER-AI
LOCKHEED
LLC

1.5 — Expected deliverables and validation

End of 2026 — Initial foundation

- EDR/XDR foundations and critical asset management deployed
- Basic detection activated with priority rules
- Initial reporting and KPIs defined

First half of 2027 — Operational SOC

- 24/7 SOC with formalized triage and escalation processes
- Incident response playbooks tested and measured
- Live and shared security dashboards

Second half of 2027 — XDR maturity ramp-up

- XDR extended to all critical sources (network, cloud, identity, email...)
- Advanced automation and response orchestration
- Proactive maturity: threat hunting, adaptive detection and risk reduction

CRITERIA TO CONSIDER THE POINT MASTERED

Coverage and quality
Deliverables are complete, tested and documented

Measurable performance
KPIs achieved and operational stability demonstrated

Industrialized processes
Playbooks, runbooks and workflows adopted by the teams

Proven business value
Risk reduction and MTTR validated by the business

Sécurity • Mastery • Confidence

NEXT-GEN CYBER-AI
LOCKHEED

Chapter 2. WSA Autonomous Remediation



2.1 — Current situation

EXISTING REMEDIATION ELEMENTS IN HOSTAUDIT LINUX 0.50.0

57 NATIVE CORRECTION FUNCTIONS

94 ASSOCIATED CONTROL IDENTIFIERS

INTEGRATED MECHANISMS

SIMULATION
Evaluation without application

BACKUP
Automated restore points

VALIDATION
Post-correction verification

ROLLBACK
Secure rollback

ESSENTIAL GAP

No complete demonstration of reliable remote orchestration:

- From WSA with limited authorizations
- With automatic effectiveness control
- Across multiple servers



SÉCURITÉ • CONTRÔLE • CONFIANCE

NEXT-GEN CYBER-AI
LOCKHEED

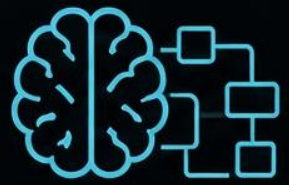
2.2 — Develop the WSA Remediation Orchestrator



1. Detection
2. AI Analysis
3. Correction plan
4. Validation
5. Execution
6. Control
7. Report

NEXT-GEN CYBER-AI
LOCKHEED

2.3 — The six essential functions to build



AI Remediation Planner

Analyzes risks, plans and prioritizes remediations intelligently.



Remediation Policy Engine

Defines, applies and governs remediation rules and policies in a centralized manner.



Secure Execution Agent

Executes remediation actions in an isolated environment, with minimal privileges and strict control.



Backup & Rollback Manager

Ensures backup of critical states and enables reliable and fast rollback in case of failure.



Post-Remediation Selector

Verifies the effectiveness of remediations, system stability and compliance with security objectives.



Remediation Audit Trail

Records all actions, decisions and results to ensure traceability, compliance and continuous improvement.



IMPERATIVE RULE: The AI must never have general access to the server's root shell.



NEXT-GEN CYBER-AI

LOCKHEED

2.4 — Define three levels of automation



ASSISTED

Sensitive modifications, human validation

Human control



SUPERVISED

Proven corrections, explicit approval

Approval required



POLICY-AUTOMATED

Limited pre-authorized actions, conditional automatic execution

Conditional execution



Note: not all corrections have the same level of risk.

NEXT-GEN CYBER-AI

LOCKHEED

2.5 — Concrete example of a WSA correction



USE CASE: Missing HTTP header on Nginxs

OBJECTIVE : Correct, validate and secure without interruption

RESULT: Reinforced security, continuity assured

• DÉTECTION • ANALYSE • CORRECTION • VÉRIFICATION • MASTERY •

NEXT-GEN CYBER-AI
LOCKHEED

2.6 — Development objectives 2026–2027

End of 2026

formalize model
and integrate first fixes

First half of 2027

supervised remediation
chain

Second half of 2027

expand catalog and
policy-based automation

CRITERIA TO CONSIDER THE POINT RESOLVED

- Formalized model and first wave of integrated fixes (End of 2026)
- Supervised remediation chain with complete visibility and traceability (H1 2027)
- Expanded catalog and applied policy-based automation (H2 2027)
- Verified and documented disappearance of risks on treated perimeters

TARGETED RESULT

**WSA NO LONGER LIMITS ITSELF TO RECOMMENDING.
IT CONTRIBUTES TO REDUCING RISKS AND VERIFIES THEIR DISAPPEARANCE.**

NEXT-GEN CYBER-AI
LOCKHEED

- Each action has an explicit authorization or a previously approved policy.
- Every execution is traceable and associated with a source finding.
- Eligible corrections have automatic tests before and after execution.
- Restoration procedures are tested, without claiming that all changes are reversible.
- Success, failure, restoration and regression rates are measured.
- AI corrections cannot bypass either permissions or technical controls.

End of 2026: formalize the correction plan model, risk levels and authorizations, then integrate the first HostAudit fixes into a central orchestrator.

First half of 2027: build and test the supervised remediation chain with simulation, approval, limited execution, verification and restoration.

Second half of 2027: expand the catalog of reliable actions, manage multiple servers and introduce policy-based automation for permissible corrections.

LOCKHEED

Chapter 3 . WSA Enterprise Validation



WSA Enterprise Validation :

demonstrate performance, security and industrial reliability

> **A PROMISING TECHNOLOGY IS NOT ENOUGH. REPRODUCIBLE, MEASURABLE AND INDEPENDENTLY VERIFIED RESULTS ARE REQUIRED.**

INDEPENDENT VALIDATION

Tests performed by neutral third parties according to rigorous protocols.

BENCHMARKS & PERFORMANCES

Comparative measurements on real load scenarios, latency, throughput and resilience.

MEASURABLE RESULTS

Quantifiable KPIs, consolidated data and transparent dashboards.

INDUSTRIAL RELIABILITY

Designed for critical environments: high availability, redundancy and assured continuity.

CREDIBILITY & TRUST

Recognized validation for the requirements of large enterprises, banks and regulated institutions.

RESULTS THAT BUILD TRUST

LARGE ACCOUNTS | BANKS | CTOs & DECISION-MAKERS | REGULATORY REQUIREMENTS

PROOF THROUGH TESTS.
TRUST THROUGH RESULTS.

PERFORMANCE. SÉCURITÉ. RELIABILITY. PREUVE. VÉRIFIÉ. INDUSTRIEL.

NEXT-GEN CYBER-AI
LOCKHEED

3.1 — Current situation



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

NEXT-GEN CYBER-AI
LOCKHEED

3.2 — Créate the 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

NEXT-GEN CYBER-AI
LOCKHEED

3.3 — Truly measure WSA against the competition

COMPARATIVE BENCHMARK CAMPAIGNS

Under comparable conditions for a fair and reproducible evaluation

Identical conditions
Same perimeter, same environment

Regular campaigns
Repeated measurements over time

Blind comparison
Eliminates biases and ensures objectivity

Representative datasets
Real enterprise cases

COMPARATIVE PERFORMANCE DASHBOARD

Actually detected vulnerabilities	False positives	Median analysis time	P95 analysis time	Cost per analyzed asset	Verified corrections
To measure	To measure	To measure	To measure	To measure	To measure
Compare and measure	Compare and measure	Compare and measure	Compare and measure	Compare and measure	Compare and measure

THE MOST POWERFUL COMPETITIVE ADVANTAGE

is measured by real superiority on a concrete use case.

Not just promises. Measured results. Proven impacts.

MEASURE. COMPARE. PROVE. WIN.

NEXT-GEN CYBER-AI
LOCKHEED

3.4 — Load scaling qualification

1



Small fleet
(10-50 assets)

Simulated load
Low to moderate

Objective
Validate load scaling on a reduced perimeter

2



Intermediate fleet
(100-500 assets)

Simulated load
Moderate to high

Objective
Verify stability and performance under representative load

3



Large fleet
(1,000-5,000 assets)

Simulated load
High to intensive

Objective
Qualify the limits, resilience and scalability of the solution

4



Continuous event SOC

Simulated load
Continuous and variable (peaks included)

Objective
Validate the SOC's ability to absorb and process a continuous flow of events without loss or critical latency

QUALIFY TODAY. WITHSTAND TOMORROW.

PERFORMANCE • RÉSILIENCE • MASTERY

NEXT-GEN CYBER-AI
LOCKHEED

3.5 — Independent security audit of WSA

INDEPENDENT SECURITY AUDIT

- AUTHENTICATION
- MFA (MULTI-FACTOR)
- CLIENT ISOLATION
- API SECURITY
- SECRETS STORAGE
- PRIVILEGED FUNCTIONS
- SSRF RISKS
- SECURE AI ACCESS

INDUSTRIALIZE SUPPLY CHAIN SECURITY

- AUTOMATED SECURITY TESTS
- SBOM (SOFTWARE BILL OF MATERIALS)
- LICENSE MANAGEMENT
- VERSION SIGNATURES
- TRACEABILITY AND PATCHES

OBJECTIVE: A solution that audits others must present solid evidence of its own security.

NEXT-GEN CYBER-AI
LOCKHEED

3.6 — Certifications and attestations: choosing the right ones

ISO/IEC 27001

NATURE
Information security management system (ISMS). Organization certification.

INTEREST FOR LOCKHEED
Demonstrates a structured and continuous approach to security at enterprise scale.

SOC 2

NATURE
Audit report on organizational controls related to security, availability, integrity, confidentiality and privacy.

INTEREST FOR LOCKHEED
Attests to the effective implementation of trust controls, particularly relevant for cloud services and data processing.

COMMON CRITERIA ISO 15408

NATURE
Security certification of a product or system according to assurance levels (EAL). Rigorous evaluation by a third party.

INTEREST FOR LOCKHEED
Proves that the product meets internationally recognized security criteria, based on an independent evaluation.

INDEPENDENT AUDIT AND PENTEST

NATURE
Independent audits and penetration tests performed by third-party experts. Results specific to the product or architecture.

INTEREST FOR LOCKHEED
Validates real security in an operational context. Identifies vulnerabilities before they are exploited.

There is no single universal certification.
Each framework addresses specific objectives and scope.

1ST MILESTONE FOR WSA
Independent product audit with reproducible benchmarks.
MEASURE. VALIDATE. IMPROVE.

NEXT-GEN CYBER-AI
LOCKHEED

Certifications and attestations

RÉFÉRENCE	NATURE	INTEREST FOR LOCKHEED
ISO/IEC 27001	ISO 27001 certification for the Information Security Management System	Demonstrates a robust risk management framework and continuous information protection.
SOC 2	SOC 2 Type II report attesting security, availability and confidentiality controls.	Confirms the operational effectiveness of controls and trust in the services provided.
Common Criteria / ISO 15408	Common Criteria (ISO 15408) certification for evaluated products and solutions	Attests to the independent evaluation of product security according to international standards.
Independent audits and pentests	Audits and penetration tests performed by independent and qualified third parties.	Continuously validates system resilience and strengthens trust in our practices.

NEXT-GEN CYBER-AI

LOCKHEED

3.7 — Validation schedule

End of 2026 — build the quality framework

First half of 2027 — demonstrate

Second half of 2027 — industrialize and have validated

RED POINT EXIT CRITERIA

- Quality framework built and approved
- Conclusive tests and demonstrations
- Industrialized and documented processes
- Independent validation obtained

RED POINT EXIT

When all the above criteria are met.

TARGETED RESULT

NO LONGER ASK THE MARKET TO BELIEVE IN WSA.
GIVE IT THE MEANS TO VERIFY ITS PERFORMANCE.

TRUST IS NOT DECLARED, IT IS PROVEN.

NEXT-GEN CYBER-AI
LOCKHEED

Summary — The Three Major Transformations of WSA

Today

SOC / CORRELATION
Detection and correlation of security alerts on assets and identities.

REMEDIATION
Automated response processes, with mostly manual and fragmented actions.

BENCHMARKS / VALIDATION
Limited measurements and reporting, with few comparisons and proof of effectiveness.

Transformation in development

SOC / CORRELATION
Strengthen contextual correlation and enrich with AI for more precise and prioritized detection.

ORCHESTRATED REMEDIATION
Industrialize playbooks, automate actions and orchestrate the end-to-end response.

BENCHMARKS / VALIDATION
Implement reference frameworks, scores and benchmarks to drive continuous improvement.

2027 Ambition

SOC / CORRELATION
AI-enhanced detection platform, with real-time correlation of emerging threats, vulnerabilities and behaviors.

ORCHESTRATED REMEDIATION
Autonomous, adaptive remediation orchestrated by WSA, with human supervision and a continuous learning loop.

BENCHMARKS / VALIDATION
Leader in sector-specific benchmarks and quantifiable evidence of risk reduction and security maturity.

> *WSA is not satisfied with just detecting risks. It helps to **understand them**, to **correct them** and to **prove that the corrections have worked.***

NEXT-GEN CYBER-AI
LOCKHEED

IN CONCLUSION



TOMORROW, THE LEADER IN CYBER SECURITY WILL NO LONGER BE THE ONE WHO DETECTS THE MOST FAILURES, BUT THE ONE WHO PROVES THAT HE HAS ELIMINATED THE MOST RISKS.

WITH **WSA** AND ARTIFICIAL INTELLIGENCE,
THIS IS THE **REVOLUTION** WE AIM TO BUILD.



LOCKHEED — WSA

Beyond Detection. Towards Intelligent Cyber Defense.

NEXT-GEN CYBER-AI
LOCKHEED



NEXT-GEN CYBER-AI
LOCKHEED
LLC