Tuskira

Case Study:

Global Financial Services Company

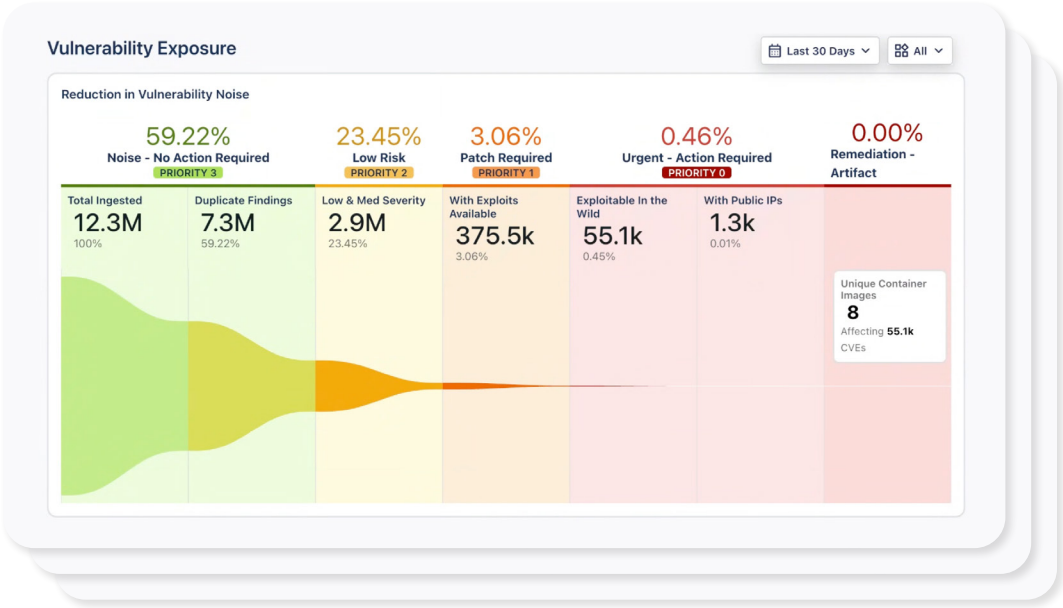
Industry:
Global Financial Services

Use Case:
Unified Threat Exposure Reduction, Triage Automation, Control Validation

Environment:
Wiz, Tenable, Veracode, CrowdStrike, Proofpoint, AWS IAM

From 12.3 Million Vulnerabilities to 0.46% Actionable Risk

A global financial services enterprise faced an overwhelming volume of signals across vulnerability, misconfiguration, and policy telemetry. With over 12.3 million findings across 10+ tools, the security team struggled to separate actionable risk from noise. Within weeks of deployment, Tuskira's AI-driven exposure management platform distilled this chaos into clarity, reducing triage by 99.5%. It narrowed focus to just 0.46% of threats requiring action and validated defense posture across IAM, WAF, container, and EDR controls.



The Challenges

- 12.3M total findings across VM, cloud misconfigurations, policy violations, and settings.
- Overwhelmed security operations and remediation teams were unable to triage at scale.
- No way to correlate known exploits, defense gaps, or simulate attacker behavior.
- Control misconfigurations in IAM and WAF created hidden exposures.

The Tuskira Approach

1. Agentic AI for De-duplication & Risk Suppression

- Removed 7.3M duplicate issues (59.22%) across tools like Wiz, Tenable, and Veracode.
- Tagged 2.9M low/medium severity issues (23.45%) for suppression.

2. Exploit & Exposure Correlation

- Flagged 375.5K vulnerabilities with known exploits.
- Identified 55.1K actively exploited in the wild.
- Surface-level scan uncovered 1.3K internet-exposed risks.

3. Defense Simulation & Control Validation

- Ran continuous attack simulations using Tuskira's digital twin.
- Verified coverage across EDR, WAF, IAM, and runtime controls.
- Prescribed prioritized IAM and WAF mitigations.

4. Outcome-Based Prioritization & Escalation

- Assigned true Priority 0 to 1.3K vulnerabilities with public exposure + active exploitation.
- Focused remediation on just 8 container images responsible for all 55.1K critical CVEs.

Results

Category	Findings	% of Total	Action	Priority
Total Findings	12.3M	100%	Ingested	—
Noise / Duplicates	7.3M	59.22%	Suppressed	P3
Low/Med Severity	2.9M	23.45%	Suppressed	P2
Exploitable	431K	3.5%	Analyzed	P1
Urgent + Internet-Exposed	1.3K	0.46%	Remediated	P0

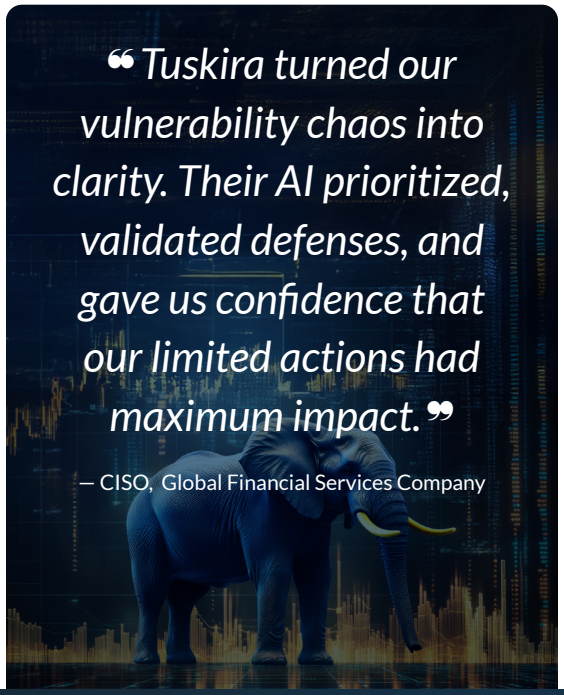
Measurable Business Outcomes

- 99.5% reduction in triage workload
- Triage time dropped from 3 weeks down to 30 minutes
- Focus narrowed from 12.3M down to 0.46% actionable threats
- Validated defense readiness with attack simulation
- Measurable ROI across Wiz, IAM, WAF, container security

Why Tuskira

Tuskira unifies telemetry, simulates attacks, validates defenses, and guides real mitigation. In this deployment, the platform did what no legacy tool could:

- Remove 10M+ non-actionable findings
- Map threats to control gaps in IAM and WAF
- Deliver a true signal-to-action ratio of 0.46%

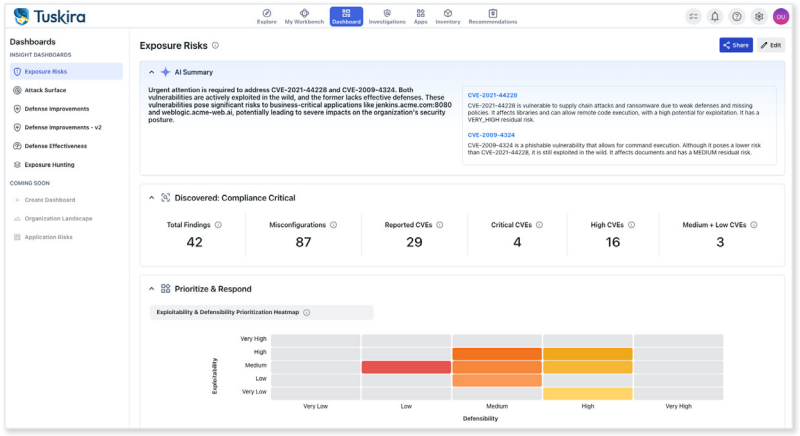


Unique Insight

Just 8 container images accounted for all 55.1K actively exploited CVEs. By validating base images through simulation, the team rebuilt images with signed, hardened versions, thereby eliminating risk at the source.

Tuskira in Action

- Vulnerability Exposure Dashboard with AI-driven triage funnel
- Remediation Workbench showing ticket impact, exposure score reduction, and time saved by AI Analysts



Final Takeaway

Tuskira translates risks into threats by simulating, suppressing the noise, and orchestrating defense. For security leaders seeking to stay ahead of attackers, reduce analyst burden, and maximize ROI from existing tools, Tuskira demonstrates what’s possible when AI becomes part of your security operations workforce.

Request a Demo

Streamline your security operations and enhance threat defense! Go to tuskira.ai/demo to schedule a personalized demo of Tuskira and see how our platform can optimize your security stack.

Website: www.tuskira.ai
Email: contact@tuskira.ai

Tuskira

