Tuskira

GenAI Powered Preemptive Cyber Defense and Response

How Prepared Are Your Defenses?

Organizations grapple with alert fatigue, tool sprawl, and limited resources, hindering effective defense. Tuskira's Agentic AI Security Mesh integrates data from over 150 tools, streamlining operations and enhancing existing defenses. This unified approach empowers security teams to transition from reactive measures to proactive strategies, ensuring continuous protection against evolving cyber threats.

Top Use Cases

Digital Twin & Adversarial Validation

- Discover Business Applications & establish business context
- Discover Network Topology, identity relationships
- Discover exposure based on internet, application, supply chain

Attackpath Simulation & Identify Vulnerability Chain

- Vulnerability Exploit Analysis Over Digital Twin
- Cross-Control Attack Path Simulation
- Identify vulnerability chains across low -> high-grade vulnerabilities

Risk Classification of Vendor-Reported Vulnerabilities

- Reclassify Vendor CVEs Based on Exploitability & Defense Posture
- Reclassify SAST, SCA & DAST vulnerabilities (CVEs, & CWEs) based on runtime defense posture
- Residual Risk for CVEs, CWEs & Misconfigurations

Proactive Risk Mitigation

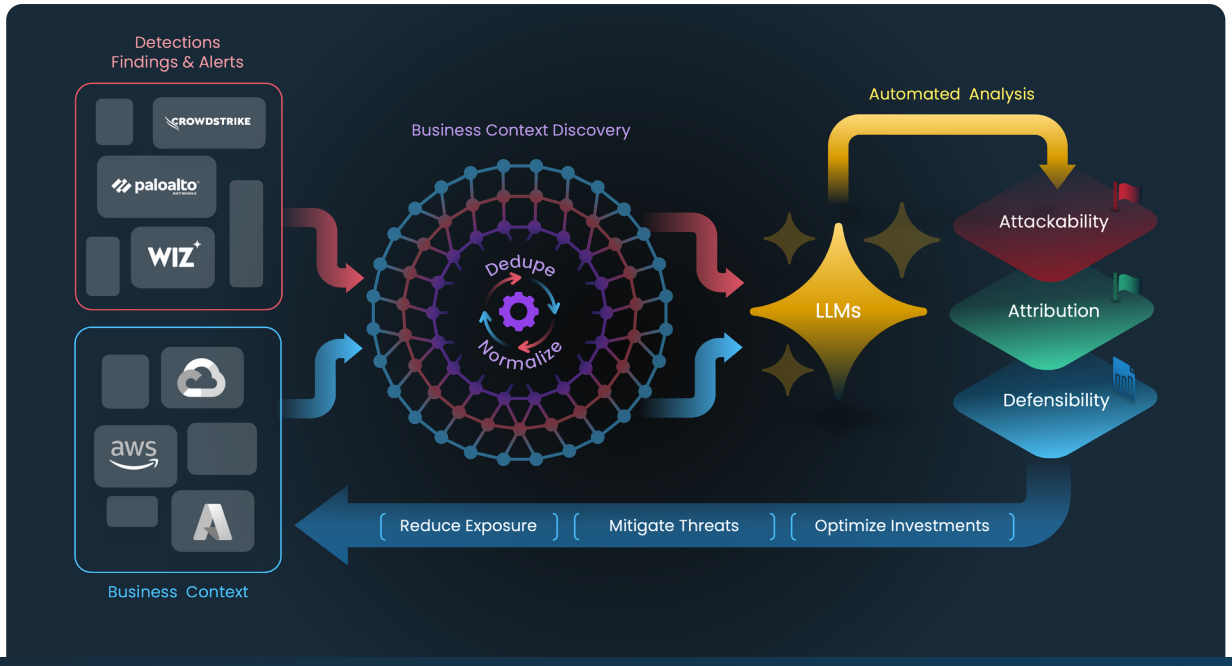
- Identify Policies and settings in existing defense controls to Mitigate Vulnerability Exploitation
- Identify "Mitigations" for Zero-Days with Unavailable Patches

Improve Vulnerability Detection

- Enhance Scan Hygiene and validate "Time To Detect"
- Identify Zero-Day Detection Blind Spots & recommend tool policies & settings

Agentic AI Curated Process Workbench

- Contextualize CVEs Based on Analyst-to-Application Attribution
- Automate Response and Track Gaps in Critical Mitigation Implementation
- Facilitate vulnerability "Risk" exception workflow by defensibility evidence
- Generate Playbooks for Vulnerabilities Mitigations



Key Benefits and Capabilities

Unified Security Data Collection & Aggregation

Collects, normalizes, and de-duplicates security data from over 150+ tools across cloud, hybrid, and on-prem environments.

Business Application and Network Discovery

Automatically maps business applications and network topology, enabling security teams to correlate risks with business operations.

Threat Simulation and Vulnerability Assessment

Employs GenAI-driven exploit validation techniques to evaluate vulnerabilities based on exploitability and prioritize them effectively.

Defensibility Analysis

Analyzes the effectiveness of existing security controls, providing actionable insights into which vulnerabilities are defensible and which require immediate attention.

Programmatic Optimization of Security Controls

Continuously optimizes existing security controls based on AI insights, maximizing tool effectiveness, ROI, and operational efficiency.

> *"It's not just about reacting faster—Tuskira has fundamentally changed how we manage security across our financial infrastructure."*
>
> — CISO, Financial Institution

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