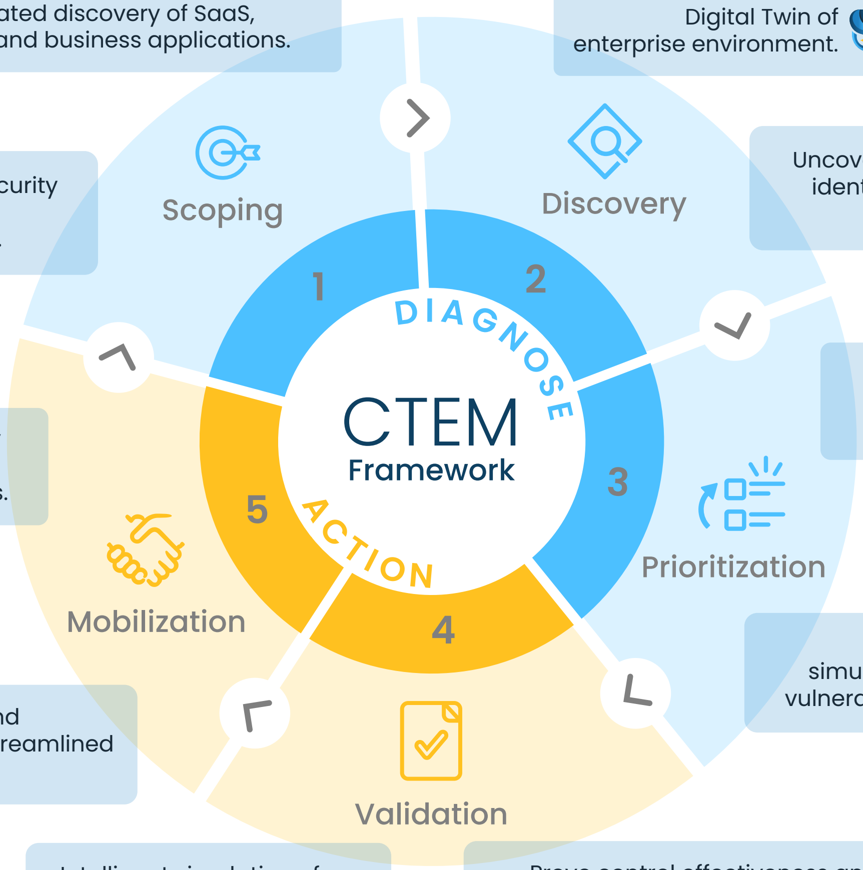
Tuskira

Agentic AI for Security Operations

By aligning with Gartner's CTEM framework and extending it with our AI-driven Digital Twin, attack simulations, exploit validation, and automated mitigations, Tuskira delivers a faster, smarter path to cyber resilience. Here's how our differentiated use cases map directly to each stage of the industry-standard cycle.



Automated discovery of SaaS, cloud, and business applications.

Unify disparate security & asset data from 3rd-party sources.

Digital Twin of enterprise environment.

Uncover exposures and identity-driven attack paths.

Prioritize CVEs by exploitability and defense posture.

Attack-path simulation across vulnerability chains.

Prove control effectiveness and quantify residual risk across exposures.

Intelligent simulation of exploitability, reachability & defensibility.

Map patches and ownership for streamlined remediation.

Automated discovery of SaaS, cloud, and business applications.

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

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.

Key Benefits and Capabilities

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

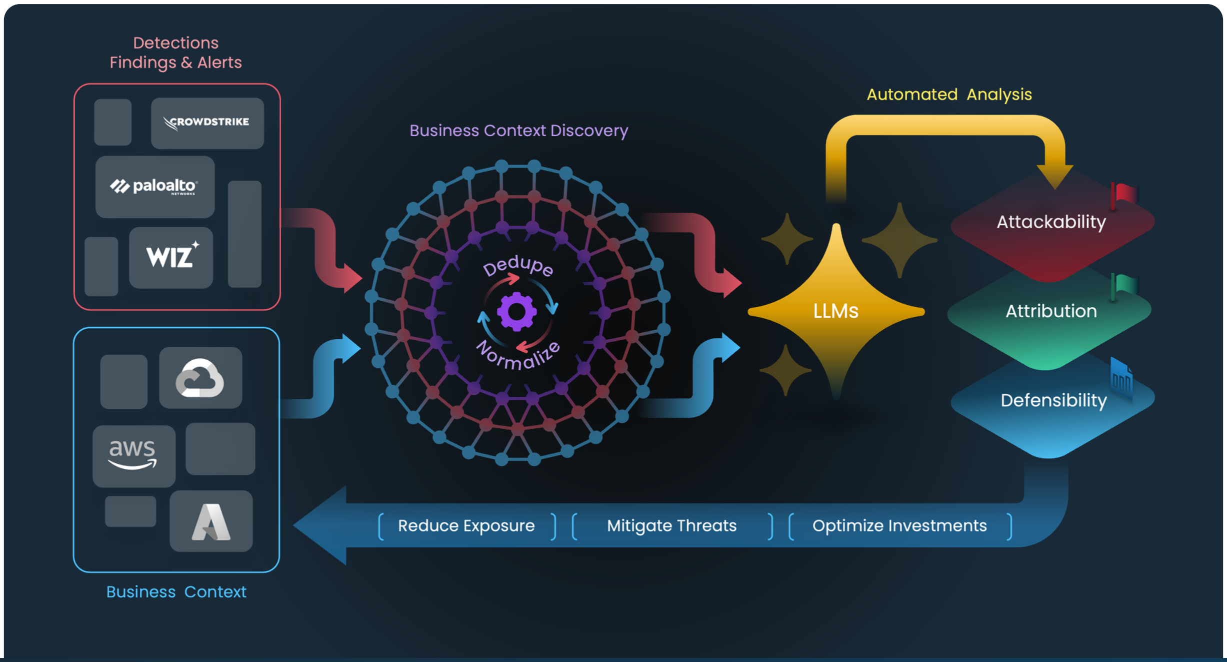
- Identify Policies and settings in existing defense controls to Mitigate Vulnerability Exploitation
- Identify "Mitigations" for Zero-Days with Unavailable Patches

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



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