Simbian®

AI CTEM Agent: Exposure Management That Thinks Before It Acts

Overview

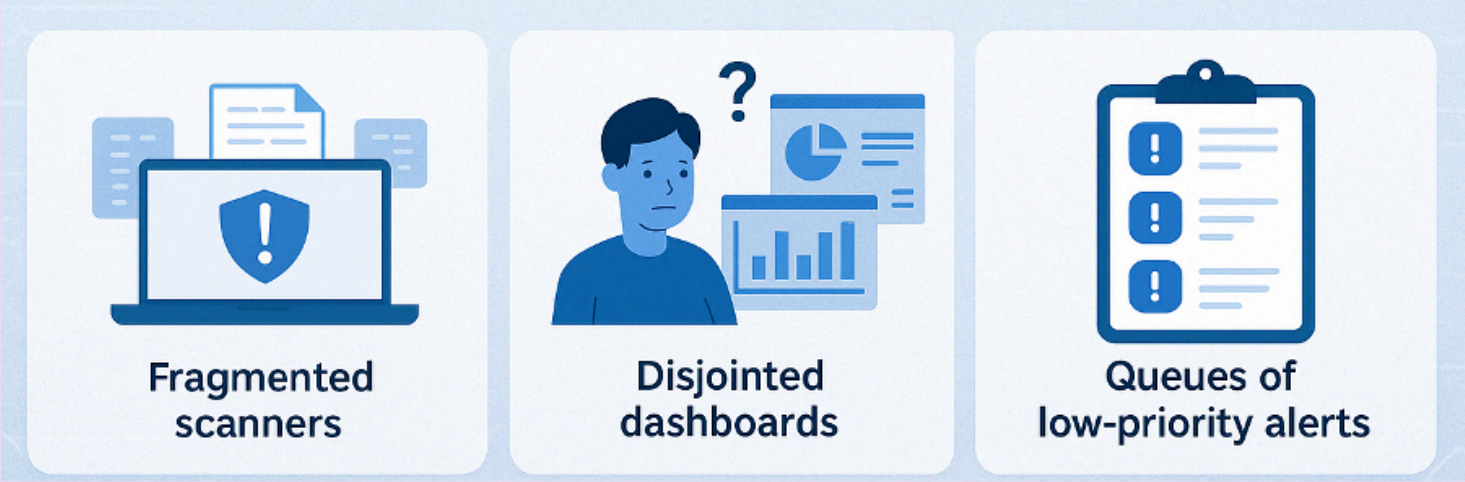
According to a recent study by Gartner, by 2026, organizations that prioritize their security investments based on a continuous exposure management program will be three times less likely to suffer a breach.

Between unpatched systems, misconfigurations, and third-party risks, exposure has become a moving target that can't be managed in bursts. Yet most organizations still treat it episodically—jumping from scan to spreadsheet to sprint—battling low priority alerts and struggling to assess which exposures actually matter, or what to fix first.

The problem isn't lack of tooling—it's too much of it. Fragmented scanners, disjointed dashboards, and long queues of low-priority alerts flood the queue. It's operationally messy and strategically blind.

Security teams are overwhelmed. IT and Devs are frustrated. And risk keeps piling up.
Worse, remediation often sits with teams outside security—so what's critical to one team often lands at the bottom of the backlog for another.

But that dynamic is changing. AI Agents are making it possible to move beyond episodic response—toward a continuous, intelligent, and judgment-driven approach to exposure management.

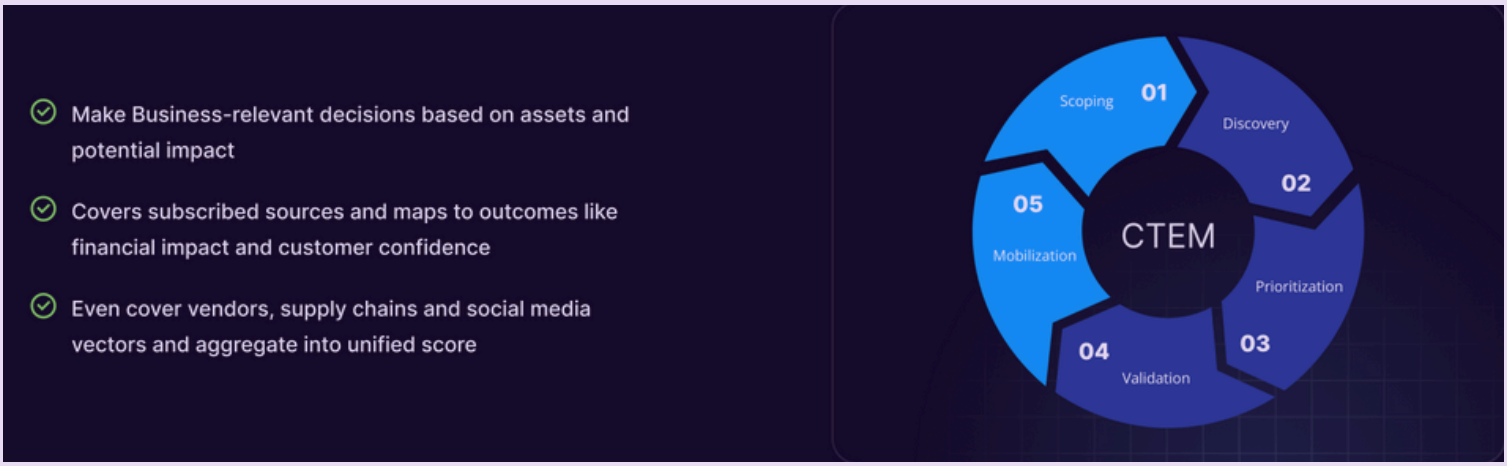


+1 650-695-0740 sales@simbian.ai www.simbian.ai

Simbian AI CTEM: From Noise to Impact Based Surgical Remediation

Simbian AI CTEM Agent gives security teams a faster, smarter way to manage exposure—like a risk analyst who never sleeps and never misses the context.

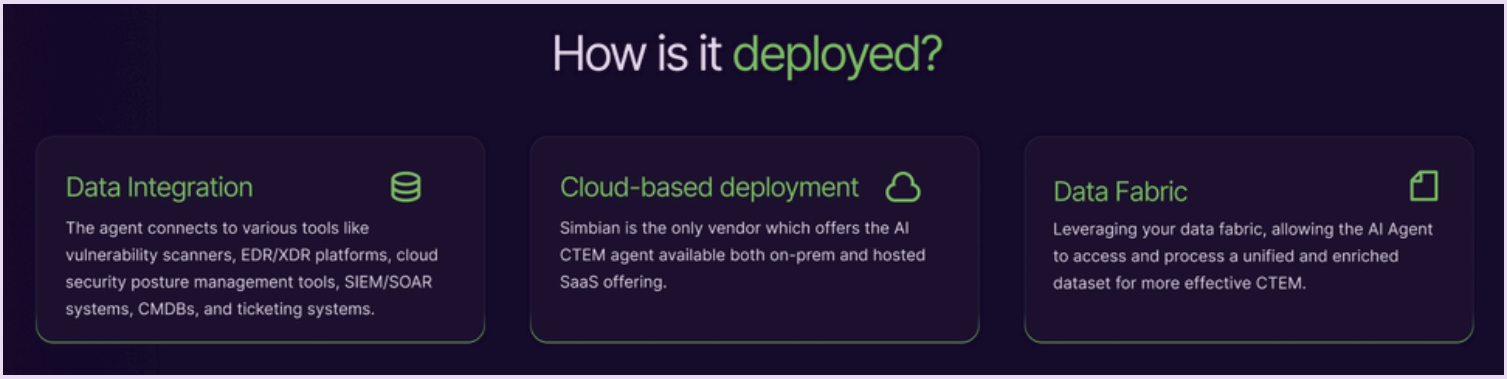
From automated penetration testing and attack simulations to API security testing and vulnerability detection, the Agent continuously validates your defenses—flagging what's exploitable, not just what's present.
It performs live security control validation, assesses exposure across your infrastructure, and delivers an aggregated risk view that reflects real-world attack paths and urgency with prescriptive, developer-ready remediation.



By integrating real-time attack simulations into your CTEM program, it replaces episodic, point-in-time assessments with real-time, continuous validation, sharpening the signal-to-noise ratio—making it clear which vulnerabilities matter, where they live, and what to patch first.

Its reports are PCI DSS–ready and accepted by auditors—helping customers meet compliance requirements without manual overhead.

The result: a more efficient patching strategy, streamlined communication with IT and dev teams, and less friction when driving remediation across large, distributed environments.



+1 650-695-0740 sales@simbian.ai www.simbian.ai

Built to Operate Across Your Infrastructure

Key Features

TrustedLLM™ Defense Layer- Eliminates GenAI risks (hallucinations, prompt injections, PII exposure)

Penetration testing: Regular penetration testing to identify vulnerabilities that may have been missed by other security measures.

Zero-Noise Prioritization- Surfaces only exposures that require immediate action

Prescriptive Remediation Guidance- Clear, environment-specific fix instructions

Live Feedback Loop- Continuously adjusts based on changing threat conditions

Rapid Deployment – Agent-based and agentless options deploy in hours, not weeks

Unified Platform Architecture – Built to work across hybrid environments with a single control plane

Vendor-neutral / cross-platform

- Cloud: AWS, Azure, GCP
- Identity: Okta, Entra, AWS IAM
- Infra: Containers, workloads, config drift

Understands organizational nuances

- Personalizes output for your teams and systems
- Tailors action paths based on policy and tooling

Integrates with your remediation engines

- Issue trackers, orchestration tools, collaboration platforms

Guided actions, not just alerts

- Step-by-step recommendations aligned to real-world exploitability

Benefits

+1 650-695-0740 sales@simbian.ai www.simbian.ai