Autonomous CTEM

To Manage Exposure Risk

SAFE CTEM shifts exposure management from tracking *what's vulnerable* to focusing on *what's exploitable.*

SAFE CTEM focuses on the three most critical pieces: continuous visibility, risk-driven prioritization, and remediation that actually reduces exposures. By aggregating and de-duplicating asset and vulnerability data across tools, SAFE isolates the 1–5% of exposures that actually increase attack risk, keeping priorities stable long enough for remediation teams to act with confidence.

The result is a CTEM program security and IT trust; built for speed, scale, and measurable exposure reduction.

From Chaos to Clarity with SAFE CTEM

It is the market's only autonomous CTEM platform that ties exposures directly to business risk – enabling a complete CTEM lifecycle management using Agentic AI:

✅ Continuous Attack Surface Visibility
✅ Risk-Based Vulnerability Prioritization
✅ KEV & Zero-Day Response
✅ Targeted Remediation and Exposure Reduction
✅ Vulnerability & Patch Governance
✅ Security-IT Remediation Alignment

SAFE CTEM Highlights

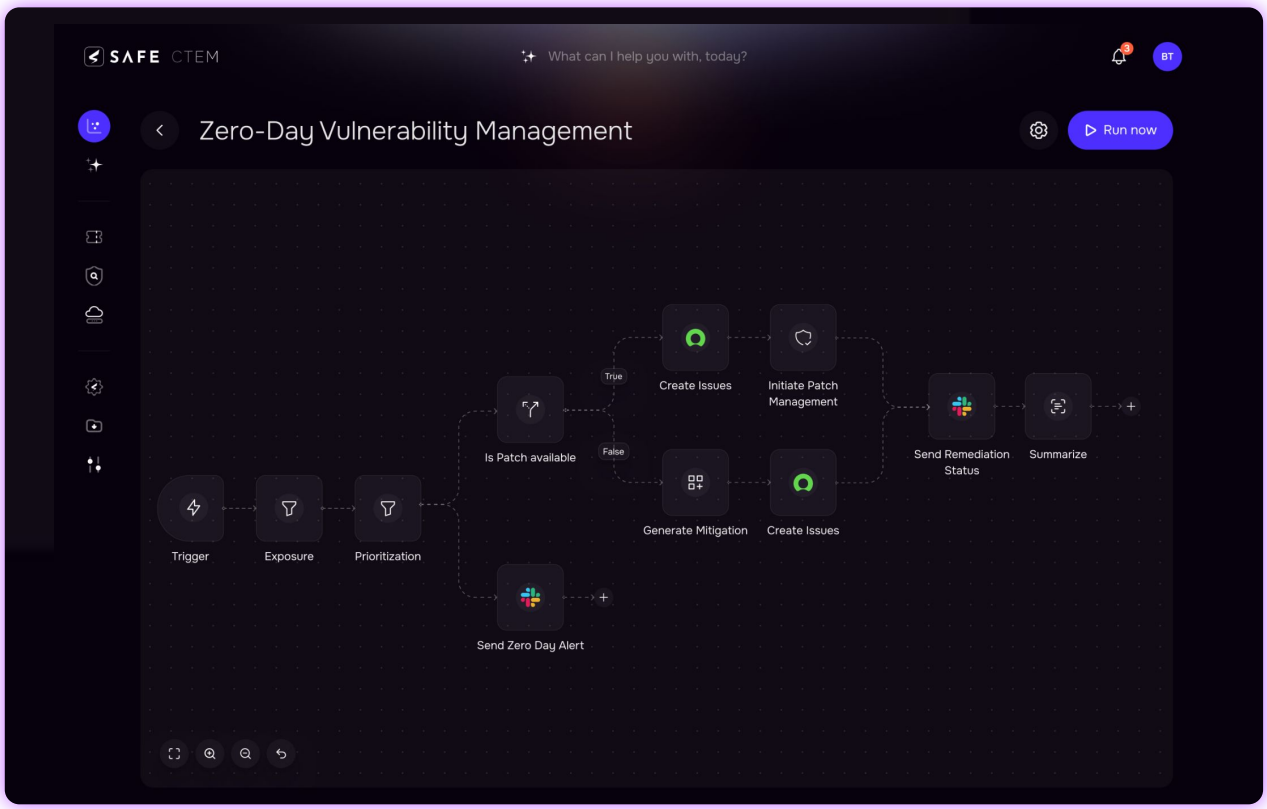
💡 **Unified Attack Surface and Exposure Visibility**
Continuous, comprehensive visibility that cuts through noise by connecting findings, assets, configurations, & threat signals into a single, enriched exposure picture

💡 **Exposure-First Prioritization That Holds**
Prioritize exposures based on real-world exploitability, environment context, and business impact, so teams can focus on what attackers are most likely to use

💡 **Measurable Exposure Burndown and Remediation**
Automate remediation with clear, defensible priorities that IT teams trust. Measure isk reduction over time, not just tickets closed

💡 **Agentic Execution Across the CTEM Lifecycle**
Leverages Agentic workflows to autonomously drive analysis, prioritization, and response; keeping CTEM running with minimal manual effort

💡 **Automation That Scales Your CTEM Program**
Automate correlation, reasoning, prioritization, and tracking across hybrid environments — scaling CTEM through intelligence, not more analysts.



Autonomous Workflows at Your Fingertips with 40+ AI Agents

SAFE CTEM powers agentic workflows that run continuously and autonomously. **Security teams can build their own AI agents or leverage out-of-the-box workflow templates**, while 40+ specialized Agents automatically correlate data, infer exposure, re-prioritize risk, and orchestrate remediation across the CTEM lifecycle. The result is a CTEM program that adapts in real time with minimal manual effort, so teams stay focused on reducing exposure, not managing workflows.

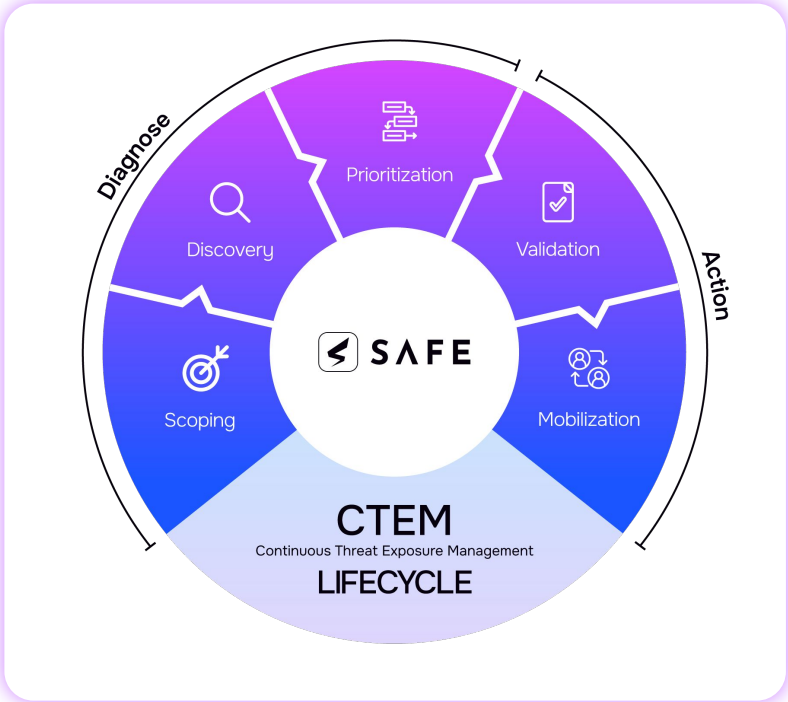
Agentic Exposure Management with SAFE CTEM

1. Context-Driven CTEM Scoping

SAFE CTEM defines scope dynamically by aligning assets, environments, and exposure domains to business-critical systems and operational priorities. Agentic AI continuously classifies and tags assets based on ownership, environment, business function, and risk impact—ensuring CTEM efforts focus on what matters most.

2. Continuous Discovery

SAFE CTEM continuously discovers assets and exposures across cloud, on-prem, and hybrid environments by ingesting telemetry from scanners, EDR, cloud control planes, SaaS platforms, and CMDBs. Agentic AI normalizes and de-duplicates this data in real time to create a single authoritative exposure inventor for effective prioritization.



3. Risk-Based Prioritization

Agentic AI continuously correlates threat intelligence, asset criticality, reachability, control posture, and attack path context to identify the exposures most likely to be exploited. As environmental conditions and threat signals change, SAFE dynamically adjusts prioritization, so teams can focus on what materially reduces risk.

4. Agentic Exposure Validation

SAFE CTEM uses agentic AI to validate exploitability using live environmental signals rather than static scan results. It determines whether a vulnerability is reachable, if compensating controls mitigate the risk, if runtime activity indicates active use, and whether the asset sits on an exposed attack path.

5. Autonomous Mobilization

SAFE CTEM uses agentic workflows to orchestrate remediation campaigns, while AI agents continuously track exposure state as fixes are applied, assets evolve, or controls improve. Autonomous measurement calculates true exposure burn-down independent of ticket closure, ensuring progress reflects real risk reduction.

Want to see SAFE CTEM in action? Schedule your 1:1 demo with a SAFE cyber risk expert today.

VISIONARY IN EXPOSURE MANAGEMENT
GARTNER MAGIC QUADRANT, 2025

CATEGORY LEADER IN CRQ
FORRESTER CRQ WAVE Q2, 2025

LEADER IN THIRD PARTY RISK MANAGEMENT
LIMINAL LINK INDEX™ REPORT, 2025

RESEARCH SPONSOR
MITRE ATT&CK, TOP CONTRIBUTOR

www.safe.security | getintouch@safe.security