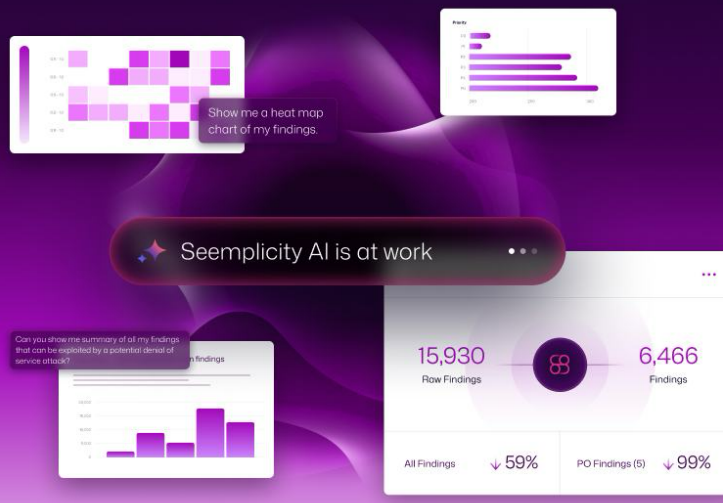
seemplicity

/datasheet

Seemplicity Agentic Exposure Action Platform™

Apply deep context and speed across the exposure management and response lifecycle to outpace AI-driven attack velocity, before attackers can act on what they find.

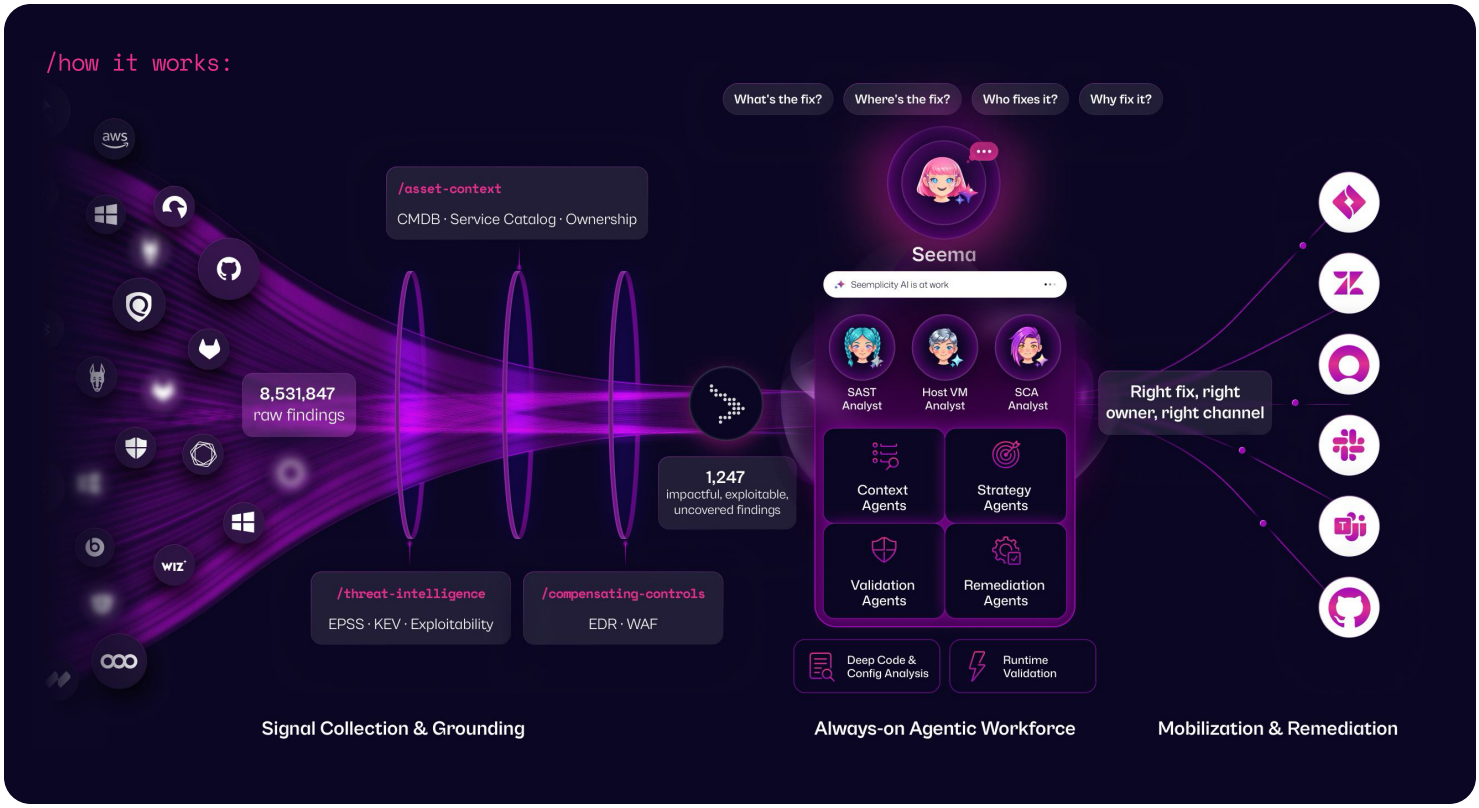


In the AI-driven world we live in, detection is easy, but context-aware action at speed is what defines resilience. Attackers now use AI to find and exploit weaknesses faster than any manual process can track. Security teams that rely on fragmented signals and slow coordination are not just behind, they are exposed.

Seemplicity is the Agentic Exposure Action Platform™ that closes the gap between finding an exposure and resolving it. Our Agentic Workforce, including Seema, our conversational AI assistant, and specialized AI Analysts for code, dependencies, and infrastructure, moves beyond static rules to power a high-velocity exposure management and response engine.

By linking exposure data, threat intelligence, and business context, Seemplicity delivers the right tasks to the right people, in the tools they already use, with the evidence needed to act with confidence.

> “Within a few hours we were receiving data from our tools in Seemplicity. Within a few days, we had already had tickets assigned.
>
> Senior Director of Cyber Operations



/agentic workforce

Autonomous Validation at Every Layer

SEEMA

AI Assistant

Ask questions in plain language across findings, assets, queues, and SLAs and get data-backed answers instantly.

SAST ANALYST

Code Reachability

Confirms whether a vulnerability is reachable in your codebase before it ever reaches a developer backlog.

SCA ANALYST

Dependency Validation

Validates third-party library reachability across the build chain and runs instant zero-day lookups when a CVE drops.

HOST / VM ANALYST

Infrastructure Exploitability

Checks runtime configurations, kernel state, and network reachability to confirm whether exploitation is actually possible.

With Seemplicity, organizations have achieved:

4x

improvement in number of exposures remediated

90%

reduction in unknown asset ownership

6-figure

annual cost savings with tool rationalization

/capabilities

Driving Exposure Management & Response Through Agentic Action

Eliminate Friction and Force-Multiply Your Fixes

- **Shrink the Noise:** Synthesize hundreds of alerts into single Root Cause Fixes, reducing alert volume by up to 90% so teams focus on what moves the needle.
- **Accelerate MTTR:** Eliminate manual research by delivering step-by-step, asset-specific instructions directly to the right developer backlog with no interpretation required.
- **Contextual Reachability:** Analyze network paths and runtime configurations to ensure teams focus only on exposures an attacker can actually reach.

Clear Ownership For Better Execution

- **Determine Asset Ownership:** Identify the technical team responsible for unclaimed assets, even as org structures evolve, reducing unknown ownership by 90%.
- **Drive Autonomous Accountability:** Operationalize the transition from overwhelming signals to autonomous, verified action with clear SLA tracking and escalation paths.
- **Expose Toxic Combinations:** Surface hidden exploit chains where independent, low-severity issues merge into high-risk attack paths before attackers connect the dots.

> “What stood out to me about Seemplicity most was their use of artificial intelligence, bringing the issue to the end user that can actually solve the problem.”
>
> VP of Security Architecture & Engineering

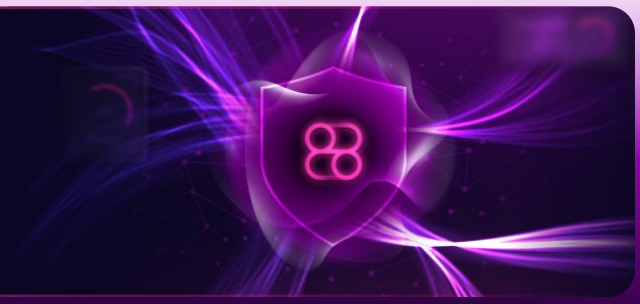
Turn Fragmented Data into Decisive Action

- **Agent-Ready Grounding:** Normalize fragmented security data from every tool into a unified, AI-consumable format that powers high-confidence routing at speed.
- **Real-Time Conversational Intelligence:** Generate executive summaries or get instant status updates via the Seema AI Assistant with no dashboard navigation required.
- **Quantifiable Risk Reduction:** Transition from reactive operations to a high-velocity exposure management and response program with measurable, reportable results.

Strategic Alignment Across Crossfunctional Teams

- **High-Confidence Routing:** Route requests with high confidence, providing developers with clear, consistent fixes and reducing back-and-forth between security and engineering.
- **Simplify Complex Narratives:** AI translates scanner outputs into summaries for non-technical stakeholders so leadership understands risk without a decoder.
- **Full Lifecycle Partnership:** Apply deep context and prioritization to every finding across the entire exposure management and response lifecycle, from discovery through verified closure.

Learn more about Agentic Exposure Action Platform™ at seemplicity.ai



Trusted by the World’s Leading Enterprises

Carlsberg Group · MORNINGSTAR · SoFi · Graphic Packaging International · NTT · WEST BEND · Hertz · OpenWeb