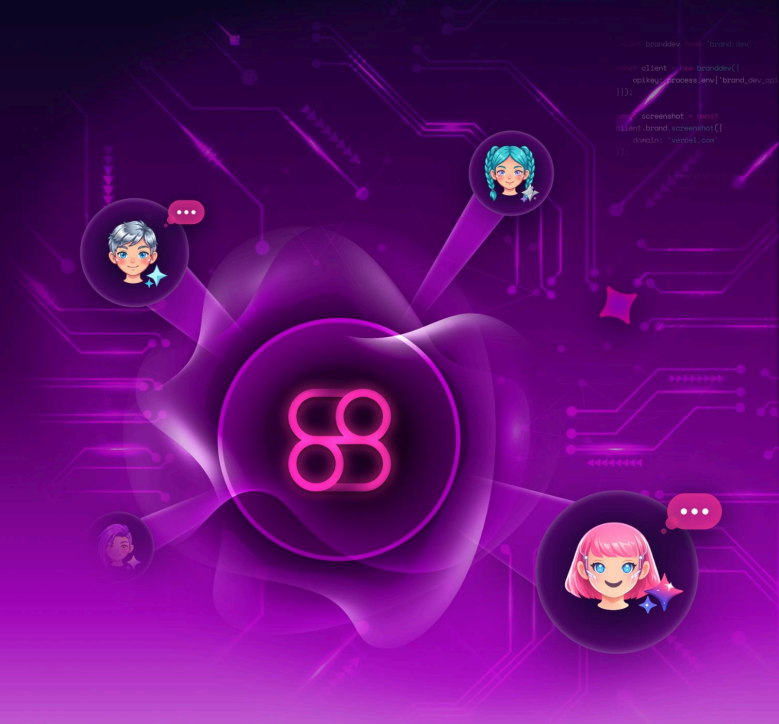
seemplicity

/solution brief

Faster, Smarter Risk Reduction with Seemplicity AI



Insight without context is just noise. Most security tools surface findings, but leave your team to figure out what actually matters, why, and what to do next. Seemplicity's AI capabilities close that gap, transforming vulnerability and exposure data into clear, contextual guidance that accelerates decisions and action across your exposure management lifecycle.

As attackers increasingly use AI to find and exploit weaknesses faster than ever, defenders can't afford to rely on manual processes alone. Fighting AI with AI is no longer optional. It's the only way to keep pace.

From automating insight generation to powering smarter workflows, Seemplicity AI is designed to help you reduce noise, save time, and act faster, without compromising on data control or trust.

BUILT ON TRUST

Your Data Stays Yours

When Seemplicity AI is active, it operates entirely within the Seemplicity platform, without exposing your data to external tools or vendors.

Your data is:

- **Not used to train AI models**
- **Not stored in the AI engine**
- **Not used for automated decision making**

SEEMA

From Questions to Answers

Seema is Seemplicity's AI powered chat assistant, with direct access to your live exposure management data. Instead of navigating dashboards to find simple answers, your team asks questions in plain language and gets clear, data backed responses across findings, assets, scopes, queues, and SLAs.

- **Natural Language Queries**
  Ask direct questions about exposure data and progress, and get straightforward answers grounded in your environment.
- **Unified Security Context**
  Connect findings, resources, and ownership in a single, explainable response that draws on the full picture of your data.
- **Clear Summaries and Visuals**
  Get concise explanations and visual insights grounded in your live Seemplicity data.

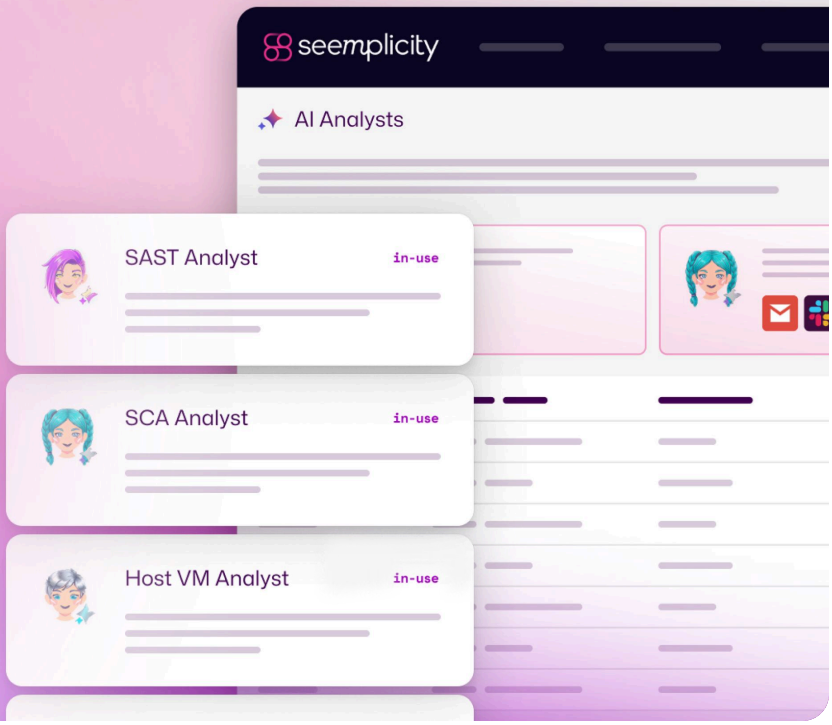
RESULT

Faster understanding, quicker decisions, and less time spent searching for insight.

AI ANALYSTS

From Scanner Noise to Confirmed Exploitability

AI Analysts are a set of autonomous agents that replace manual triage with structured, evidence-based exploitability investigations. Seemplicity's AI Analysts research real world exploit prerequisites, inspect live runtime configurations, check network reachability, and confirm whether vulnerabilities are actually exploitable on specific assets.



Host / VM Analyst

Confirms real world exploitability for infrastructure and host findings.

- **Threat Intelligence Research**
  Pulls exploit prerequisites from GitHub, Metasploit, and Exploit-DB
- **Runtime Exploitability Verification**
  Analyzes system configurations such as kernel flags, process states, and runtime parameters to verify if exploitation is actually possible.
- **Network Reachability Analysis**
  Checks reachability by inspecting security groups, public IP presence, active connections, and access patterns, with no full network modeling required.
- **Remediation Complexity Scoring**
  Flags operations that carry business risk, such as kernel updates that require a reboot, so teams can plan remediation without creating new incidents.
- **Automated Fixer Identification**
  Reviews historical Jira and ServiceNow tickets, git logs, and assignment records to surface who owns assets or components.

SAST / Code Analyst

Confirms whether code level vulnerabilities are actually reachable before they reach a developer.

- **Deep Code Validation**
  Reads source code from repositories to confirm whether a vulnerability is reachable given how the application is actually built, not just whether a vulnerable function exists in a dependency.
- **Dependency Reachability**
  Checks whether vulnerable library functions are imported and called before putting a finding in front of a developer.
- **PR Ready Fix Generation**
  Scopes the blast radius of each fix, whether a single file or a broader refactor, and produces remediation recommendations developers can act on immediately.

SCA Analyst

Validates third party and dependency findings across the build chain.

- **Software Composition Analysis Validation**
  Confirms actual function usage and dependency reachability across the build chain before flagging third party library vulnerabilities.
- **SBOM Powered Zero Day Response**
  Runs single query lookups across Artifactory, Aquasec, and GitHub to find every instance of a vulnerable component the moment a zero day drops, before scanner signatures catch up.

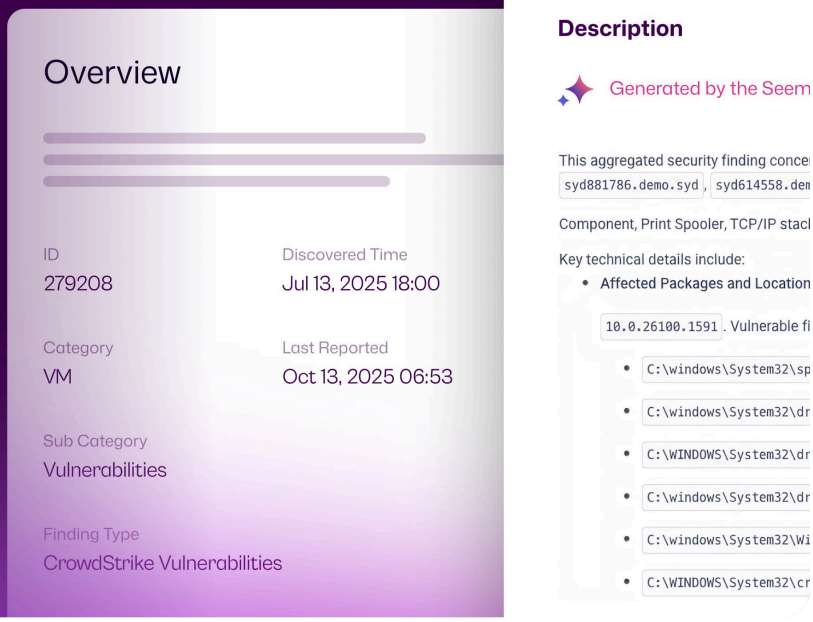
RESULT

A shorter, verified shortlist of findings that genuinely need action, with the evidence to back up every one.

AI ENHANCED FINDING DESCRIPTIONS

Readable, Relevant, Ready to Act

Scanner output is not always presented in the most readable format. Seemplicity uses large language models to turn complex findings into clear, concise, and actionable summaries.



- **Single Findings**
  Use the AI powered toggle to instantly generate digestible descriptions and remediation steps for individual issues.
- **Aggregated Findings**
  When grouping multiple issues, AI generates a unified description and fix plan tailored to the full scope. You can preview, regenerate, and edit freely.

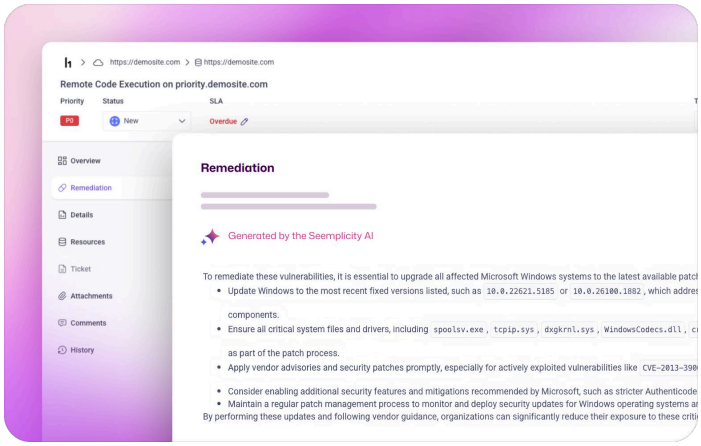
RESULT

Whether your team is reading one issue or many, they get the context they need without the technical fog.

REMEDIATION STEPS

From Assigned to Resolved

Stop wasting time deciphering vague remediation instructions. Seemplicity AI embeds precise, asset specific guidance into each finding.



- **Asset Specific Fixes**
  Tailored for containers, web servers, libraries, and more.
- **Step by Step Instructions**
  Clear, actionable fixes mapped to real world workflows.
- **Consistency Across Teams**
  Standardized guidance improves resolution quality.

RESULT

Engineering teams resolve faster, with confidence and consistency.

AI INSIGHTS

From Data to Decisions

Seemplicity uses AI to transform dense dashboards into prioritized, shareable insights.

- **Automated Insight Generation**
  Highlights critical insights based on your real-time data.
- **Prioritized Intelligence**
  See what matters most.
- **Collaborative Sharing**
  Share insights directly inside workflows for faster alignment.

RESULT

Visualize less, understand more, act faster.

AI can analyze a finding

Seemplicity knows which findings matter, who should fix them, whether the fix actually happened, and can prove all of it to your auditor.

Visit seemplicity.ai to learn more.

Please enter your sub heading in this text box

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