seemplicity

Seema: Your Exposure Management AI Assistant

DATA SHEET

Talk to Your Data. Get Answers Instantly.

Seema is your AI-powered Security Data Agent built directly into the Seemplicity platform. Unlike generic chatbots, Seema has full, real-time context of your entire security ecosystem: findings, resources, SLA statuses, and cross-team scopes. She eliminates manual data mining, allowing you to move from complex silos to actionable insights using only plain English.

Welcome I'm Seema,
Seemplicity's data agent

I can explore your findings, tickets and configurations.
You can ask me to assess risk, track remediation progress, analyze trends,
or answer questions about your security posture across all environments

Am I affected by Log4j vulnerabilities?

Compare the SLA perfomance of my scope groups

Show me "Exploited in the Wild" vulnerabilities without tickets

Give me a remediation plan for my most risky asset

Ask me anything...

Advanced Analytical Capabilities

Stop digging through filters and start asking questions. Seema crunches your security data in real-time to provide precise,human readable breakdowns.

Multidimensional Finding Deep-Dives
Filter by priority, CVE, CWE, data source, or SLA status. Whether you need to see "all critical SQL injections in production" or "overdue vulnerabilities by package," Seema slices the data exactly how you need it.

Granular Resource Intelligence
Instant lookups by resource type, tags, cloud account, or specific department. Seema can even identify findings that don’t fall into any of your officially tracked areas. Seema understands a full map of your environment so you never have to guess where a risk is hiding.

KPI & Metric Tracking
Understand MTTR, SLA compliance rates, and remediation velocity without building a single report. Just ask for the metric, and Seema will show the trends.

Comparative Team Analysis
Benchmark performance across the organization. Compare Team A’s remediation speed against Team B, or see which business units are driving your highest risk concentrations.

Instant Visualizations
Transform raw data into clarity. Specify your preferred format, such as pie charts, bar graphs, heatmaps, or structured tables, and Seema will generate it for you instantly.

Proactive Risk Prioritization
Seema doesn't just list findings; she surfaces what matters. Seema highlights exploitable CVEs, high-EPSS scores, and reachable assets to ensure you're tackling the "head of the spear" first.

> “I’m usually pretty skeptical of AI 'chatbots,' but Seema is different because she actually knows our environment. I don't have to explain what a 'production tag' is or why something matters to us since she already has the context. It’s like having an extra analyst on the team who just handles the data-crunching."
>
> **Senior AppSec Engineer,**
> Global SaaS Organization

Maximizing Your ROI

You do not need to be formal or technical, but providing specific context helps Seema deliver the sharpest results.

Zero Learning Curve
There is no need to learn SQL or internal data models; you simply ask questions in plain English

Provide Strategic Context
Mention specific priorities (P0, P1), severities (Critical, High), or team names to focus the search.

Define Your Output
Specify if you want to see a table, a trend over time, or multiple views at once.

Iterative Discovery
Seema maintains contextual memory. Start broad and then drill in by asking to "break that down by datasource" or "zoom into the broken SLA group".

Precision First Identification
Use industry standard CVE IDs (e.g., CVE-2021-44228) to ensure 1 to 1 mapping with your unique vulnerability findings.

Contextual Clarity
Start a fresh chat when switching to a completely different subject to keep answers clean and accurate.

Strategic Time Range Analysis

Time is a critical factor in security. Seema tracks multiple timestamps to provide a complete picture of your remediation lifecycle.

Timestamp	What It Means	Strategic Use Case
Discovered Time	When a scanner first detected the finding.	*Identifying new findings and discovery trends.*
Last Reported Time	When a scanner last confirmed the finding exists.	*Distinguishing between stale and active findings.*
Resolved Time	When the finding was marked as fixed.	*Measuring remediation speed and MTTR.*
SLA Due Date	The deadline for fixing a finding per policy.	*Monitoring SLA compliance and upcoming breaches.*
Resource First Seen	When a resource first appeared in your environment.	*Identifying new assets or recognizing inventory growth.*
Resource Last Seen	When a resource was last reported by a scanner.	*Identifying stale assets or decommissioned resources.*

Conversational Blueprints for Smarter Decisions

Harness the logic of a world-class security analyst to meet any objective. Seema's conversational memory allows you to drill into SLAs, risk trends, and resource health with zero learning curve.

Objective	Example Prompt
Risk Prioritization	*"Show me the most critical findings (P0) in AWS with broken SLA"*
Visual Reporting	*"Create a pie chart of open findings by severity"*
Asset Exposure	*"List resources tagged 'production' with critical CVEs"*
Efficiency Metrics	*"What is the mean time to remediation for P1 findings in Q4?"*
Vulnerability Response	*"Show me open findings for CVE-2021-44228"*
Security Posture	*"Give me a high-level overview of our current security posture"*
Status Reporting	*"What improved and what worsened in the last 90 days?"*

✦ Show Thinking

Top 5 open vulnerabilities in “Exposed to the Internet” that are RCE and/or KEV

Finding	Priority	CVE(s)	EPSS (Score/ Percentile)	Affected asset (Type/cloud account)	RCE	KEV	Active Remediation Ticket
					✓	✓	✗
					✓	✓	✗
					✓	✓	✗
					✓	✓	✗
					✗	✓	✗

✦ For findings that are Exposed to the internet, show me the top 5 open vulnerabilities that are RCE and/ or Exploited in the Wild(KEV). Include for each: Priority, CVE, EPSS score/ percentile, affected asset (name + type + cloud account), and whether there’s an active remediation ticket (and the ticket ID if exists). Also summarize how many of these are currently overdue on SLA.

Built for Accuracy and Integrity

To ensure the highest level of data reliability, Seema operates as a dedicated Read-Only Intelligence Layer.

Grounded In Reality
Seema provides insights backed exclusively by your environment's data rather than generic security advice.

Secure By Design
She focuses on analysis rather than making unauthorized configuration changes or external system calls.

Focused Expertise
If a query falls outside her data scope, Seema will transparently pivot to a relevant, data-backed alternative.

Default Precision
Seema defaults to showing open, active findings to ensure you are always looking at what currently matters.