Evaluating native-AI solutions

in cyber security

	GPTs & Generic LLMs	MCPs you build	sola
What it is	Text model that generates answers and code - about any subject.	Protocol to let a model call your tools and APIs	Security platform that provides security answers in your organization's context, and in natural language.
Primary strength	Fast ideation, explanations and experiments.	Structured access to real systems.	Full-picture answers across systems, built for security work
Access to your data	Paste-in snippets, ad hoc access.	Tooling you expose via schemas and scopes.	Direct, scoped for security, with read-only integrations
Handling data at scale	Limited by tokens, for manual context only.	Limited by API rate limits and affected by slow pipelines.	Platform-managed collection at scale, while ensuring current context.
Org context	None by default.	Only what you design and maintain.	Modeled across identities, repos, cloud and data as a single view.
Cross-system picture	None.	Limited. You stitch it, and up to you to maintain.	Yes, platform-level view across sources.
Monitoring	Query time only.	Query time, unless you build more.	Continuous, tracks drift and new exposures.
Security posture	Prone to insecure defaults.	Depends on your guardrails and scopes.	Security-first, with no agents in production.
Typical failure modes	Confident wrong answers and hallucinations, skipped controls.	Over or under scoping, prompt injection, schema drift and blind spots.	No general-purpose AI, supporting security use cases only.
Maintenance burden	Low: the review is on you, though.	High: ongoing schemas and prompts, requires stitching and audits.	Low: connect sources, build your app using the co-pilot and tweak any time.
Output quality	Useful drafts, unreliable for production security.	For basic, and limited questions - possibly good enough. Beyond that, you will struggle to even get answers.	Higher-quality, current answers shaped by security knowledge, and at a larger scale.
Best use	Learning, prototypes, quick refactors	When you want DIY control and can manage the ongoing maintenance	When you want practical, cross-stack security answers without wiring everything yourself.

sola