THE CISO SYSTEM PROTOCOL

How product-focused companies replace the unicorn CISO with a system that actually runs.

IF THIS SOUNDS FAMILIAR

You have been looking for a CISO for months. The good ones cost $300K+ and still want to build a team beneath them. The affordable ones are project managers with a security title.

Meanwhile, the board keeps asking about security posture. Compliance deadlines are approaching. Your engineering team is shipping without guardrails. And the last security assessment produced a 200-page PDF that no one opened twice.

You do not have a people problem. You have a model problem.

THE INSIGHT

> *Security leadership is not a role to fill. It is a function to install.*

The traditional CISO model asks one person to set strategy, communicate with the board, build programs across AppSec, cloud security, and GRC, execute under compliance pressure, and scale with the business. That model does not fail because of bad leadership. It fails because the scope is structurally unscalable for a single hire.

The CISO System Protocol replaces that assumption with an operating model: a team of specialists delivering named security programs, producing visible results every cycle, and reporting evidence — not anxiety — to your board.

WHAT THIS IS NOT

- **Not a CISO-as-a-Service.** You are not renting a fractional person. You are installing a system.
- **Not a consulting engagement.** There is no 300-page deliverable. Every cycle produces controls, automation, and documentation that reflects reality.
- **Not a security person as a service.** You get a team of domain experts operating as a unified security function — not a contractor filling a seat.

WHAT YOU GET: THE MACHINE

The CISO System Protocol distributes the entire CISO function across four layers. Each layer has clear ownership, defined outcomes, and produces evidence you can see.

LAYER	WHAT HAPPENS	WHAT YOU SEE
Strategic Leadership	Executive-level security leader accountable to the board. Sets direction, communicates risk, aligns security to business goals.	Board-ready reporting. Risk language your CFO can use. No translation needed.
Named Programs	Security delivered through defined programs: AppSec Foundations, GRC Foundations, Cloud Security Posture. Each has outcomes, metrics, and timelines.	A program roadmap with measurable milestones. Not a backlog of findings — a plan with progress.
Iterative Execution	Every cycle delivers something tangible. Automation. Processes. Controls. Documentation tied to real system artifacts.	You can see what changed this month. Controls deployed. Pipelines hardened. Policies that map to configs, not slide decks.
Continuous Governance	Compliance produced from evidence. Exceptions are time-bounded. Metrics track exploitability and response time, not checkboxes.	Three trend lines your board cares about. Audit evidence generated from operations, not assembled in panic.

WHAT CHANGES

WITHOUT THE PROTOCOL	WITH THE PROTOCOL
Months spent searching for a unicorn hire	Security function running within the first cycle
Compliance creates panic every quarter	Compliance evidence produced from operations continuously
Board meetings driven by anxiety and vague assurances	Board receives three metrics that correlate with actual risk reduction
Security progress resets every time someone leaves	Knowledge lives in the system, not in any single person
200-page reports no one reads or acts on	Tangible controls, automation, and documentation you can point to
Risk register that catalogs problems without solving them	Named programs with defined outcomes and visible iteration

THIS PROTOCOL IS DESIGNED FOR COMPANIES THAT

- Are hiring or trying to hire a CISO and finding the market impossible
- Are under board or compliance pressure and need execution, not just leadership optics
- Want predictable security outcomes without growing headcount
- Are tired of security engagements that produce documents instead of progress

THE BELIEF BEHIND THE PROTOCOL

The security industry has spent two decades selling the same model: hire a person, hope they can do everything, replace them when they burn out or leave. The result is a cycle of rebuilding from scratch that no other business function would tolerate.

Asgard Security exists because we believe security leadership should be measured by what actually changed — not by what was documented. The CISO System Protocol is how we deliver on that belief: a team, a system, and visible evidence of progress every single cycle.

Security is not a checkbox.
It is a capability you build and run.

Ready to see how the protocol works for your company?

asgardsec.com · hello@asgardsec.com