algosec

Secure application connectivity.
Anywhere.



Strategic playbook: the AI prompt guide

From manual coding to natural language governance

A note from Iris

If you've been following along, you've already done the hard work of tracing attack paths and finding ghost rules (those forgotten security settings). Now, it's time to let the machine do the heavy lifting. This isn't about an AI chatbot that writes poetry; it's about intent-based security. We're moving away from hunting through thousands of lines of code and toward a world where you manage security by simply stating what you want to achieve. This is Stop #4, where your operational speed truly triples.

The new interface: From code to intent

For years, being a network security engineer required a multilingual expertise. You had to speak different technical languages for different vendors - Cisco in the morning, AWS in the afternoon, and Azure by the end of the day.

We call this the **Syntax Tax**. It's the hours wasted translating a simple business request - like 'Let this app talk to that database' - into the cryptic, manual commands required by three different consoles. We are introducing AI as a productivity accelerator. We aren't replacing the engineer; we are replacing the manual data entry that leads to configuration fatigue. You provide the intent; the AI handles the translation.

The pathway to hybrid security

1. The hybrid manifesto:
   Establishing the architectural truths of hybrid security. Coming soon;
2. Cutting the kill chain:
   Shifting from alerts to visual, cross-estate risk mapping.
3. Attack path blueprint:
   Tactical steps for remediating hybrid vulnerabilities.
4. AI prompt playbook:
   Putting natural language automation to work for your team.
5. The trinity demo:
   A live masterclass in unified execution.
6. Migration mapping blueprint:
   The final framework for secure application mobility.

Handling misconfigurations

Natural language turns repetitive chores into instant actions. Here is how we use simple prompts to solve complex problems:

1. The ghost hunter

- **The problem:** Manually searching through spreadsheets to find misconfigurations. With Horizon you can easily locate misconfigurations and identify sources of internet access and safely disable them.
- **The result:** With AlgoSec's AI ability to name and cross-references your entire network, you can easily locate your relevant misconfigurations and applications allowing you to organize them and put the relevant fixes in place.

2. Lateral move lockdown

- **The problem:** When a new cyber threat makes headlines, you need to know **immediately** where you are exposed. With Horizon, you can identify possible infiltration from the public internet to our private database to identify which points of access are undesirable.
- **The result:** Horizon identifies the gaps enabling you to draft a new, secure policy for you before a breach can occur.

3. The behavioral bridge

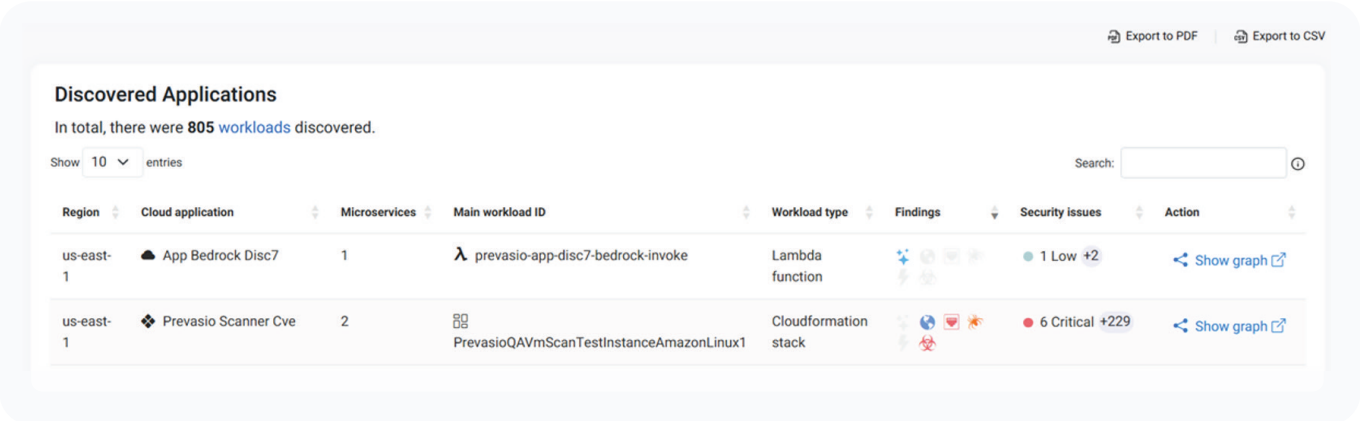
- **The problem:** Unknown TCP - the dark matter of your network. Traffic is moving, but you don't know what it is, so you're afraid to block it. Horizon allows you to easily identify your apps and takes away the mystery.
- **The result:** The AI analyzes patterns to give mystery traffic a name (like Web-Sync-Service), allowing you to secure it with confidence.

Spotlight: Shadow AI discovery

Your developers are likely using AI tools (like ChatGPT or AWS Bedrock) to work faster. If these aren't monitored, they become Shadow AI - unsecured back doors into your data.

How we shine a light on the shadows:

- **Automatic badging:** The system scans your network and places a specific **AI Icon** on your map the moment it detects an AI service being used.
- **Risk scoring:** It automatically flags if an AI tool is leaking data to a non-sanctioned external location or violating privacy regulations (like PCI-DSS).



The hacker's map: Telling the story to leadership

Eventually, you have to explain your work to stakeholders who don't know technical jargon. You need a way to show the danger, not just describe it.

- **Horizon's contribution:** Horizon displays the easiest path an attacker could take to reach your data.
- **The bridge:** This turns a complex network problem into a visual story. It identifies the Point of Least Resistance, making it easy for leadership to see why a specific security update is a top priority.

Summary: Your new routine

The Velocity Framework

AI is a force multiplier, not a navigator. It doesn't set our security objectives; it simply accelerates the speed at which we achieve them and enables us to improve our workflow. Here is a suggested workflow considering our AI capabilities:

Daily: The 24-hour threat pulse

The goal: Rapid situational awareness.

Recommended action: Identify the top three emerging risks from the last 24 hours to ensure our perimeter adapts as fast as the threat landscape.

Weekly: Rulebase optimization

The goal: Precision-engineered security.

Recommended action: Prune redundant and shadowed rules to achieve:

- **Attack surface reduction:** Eliminate the hidden permissions that allow silent lateral movement.
- **Operational excellence:** Boost inspection speeds and lower latency by streamlining firewall processing.
- **Audit readiness:** Reduce compliance noise by **30%**, creating a clear, defensible path to **Zero Trust / Least Privilege** verification.

Monthly: Application trust report

The goal: Total visibility and executive assurance.

The action: Generate a high-fidelity report verifying that our Tier-1 applications are fully shielded:

- **Perimeter status:** Confirm all critical applications are protected .
- **Compliance mapping:** Use automated evidence collection to bridge the gap between raw logs and regulatory frameworks, ensuring we are **audit-ready** 24/7.

Next Stop (Weeks 9-10): We've automated the hygiene; now it's time for the masterclass. Join us for **The trinity demo**, where we show you our three core tools work together in one live, unified execution.

Welcome to the Fabric.

Iris AlgoSec

© AlgoSec Inc. All rights reserved. AlgoSec and the AlgoSec logo are registered trademarks of AlgoSec Inc.
All other trademarks used herein are the property of their respective owners.