CISO FIELD GUIDE · 2026

The CISO’s Checklist for the Agentic Supply Chain

Four prerequisites every security leader needs to check before AI agents start shipping code autonomously.

SEVERITY SCORECARD

LOW	MEDIUM	HIGH	CRITICAL
Governed & contained. Controls are working as designed.	Systemic governance gap. Risk grows over time without remediation.	Active governance failure. Adversaries can already exploit blind spots.	Immediate exploitation risk. Stop, contain, then re-architect.

☐

DISCOVERY & VISIBILITY

Detect every AI agent, model, and skill operating in your environment.

Severity · High

You can’t protect yourself from the Shadow AI assets you can’t see.

☐

SUPPLY CHAIN INTEGRITY

Verify every artifact, dependency, and tool the agent consumes.

Severity · Critical

If an attacker manages to run the code on a developer’s machine or a server, they’ve already breached your perimeter.

☐

GRANULAR GOVERNANCE

Bind every agent to least-privilege, with policy enforced at runtime.

Severity · Critical

Least privilege principle: even vetted agents can make mistakes, so you want to limit the potential blast radius.

☐

UNIFIED PLATFORM MANAGEMENT

Manage models, artifacts, policy, and evidence on one platform.

Severity · Medium

To ensure long-term protection, avoid a fractured approach; without unified governance, you face uncontrollable risk and a total loss of business-level visibility.

Ready to secure your agentic supply chain?

Get the full CISO's checklist for securing the agentic supply chain — automate policy guardrails, enforce granular permissions on AI assets and tools, and prevent unauthorized access across production environments.

Get Full Checklist