REDACTED SAMPLE

Agent Action BOM

Scan Scope

Repo / workflow	Redacted engineering repo
Source mode	Local scan
Raw source retained	No
Artifact type	Agent Action BOM
Purpose	Identify AI-assisted engineering and automation paths that can take meaningful actions

Summary

4 AI/automation paths found	**2** With write or deploy reachability	**2** Using standing credentials	**3** Missing explicit owner
4 Missing approval evidence	**4** Missing policy coverage	**4** Missing proof coverage	

Example Control-First Path

GitHub Action running AI coding assistant	
Introduced by	.github/workflows/agent-pr-review.yml
Credential	GitHub PAT referenced from repository secret
Access type	**Standing privilege**
Reachable actions	**Read, write, comment, modify PR branch**
Reachable targets	Repo contents, pull requests, workflow context
Owner	**Not declared**
Approval evidence	**Missing**
Policy coverage	**Missing**
Proof coverage	**Missing**

Why it matters

> This is not just AI usage. The workflow gives an AI-assisted process standing access to interact with source code and PR state. If the credential is broad, compromised, or reused, the workflow can become an unreviewed privileged actor in the software delivery path.

Recommended action

- Assign owner
- Confirm credential scope
- Replace broad PAT with scoped GitHub App or brokered credential
- Require approval for write actions
- Record proof for approval, credential use, and action outcome

Additional Governable Paths

1. Release workflow with durable credential	Priority: HIGH
Location	.github/workflows/release.yml
Credential	Package registry token / signing key reference
Access type	**Standing or durable**
Reachable actions	**Build, publish, release**
Missing	**Approval evidence, policy coverage, proof coverage**

2. MCP tool configuration	Priority: REVIEW
Location	.cursor/mcp.json
Tool / server	Internal tool server
Credential	Environment variable reference
Reachable actions	**Read, egress, tool call**
Missing	**Owner, approval evidence, policy coverage**

3. Agent framework dependency	Priority: INVENTORY
Location	apps/support-agent/package.json
Framework	LangChain / agent orchestration package
Reachable actions	Unknown from dependency alone
Missing	**Owner, usage validation, policy coverage**

What The Agent Action BOM Answers

- Which AI-assisted workflows or automations exist?
- Where were they introduced?

- Which credentials or identities do they use?
- Is access standing, inherited, static, delegated, or just-in-time?
- What actions are reachable: read, write, deploy, delete, execute, egress?
- Which systems or data targets are reachable?
- Is there an owner?
- Is approval required?
- Is policy coverage present?
- Is proof coverage present?
- Which path should be governed first?

Note: *This sample is illustrative and redacted. It is meant to show the shape of the artifact, not disclose a real customer environment.*