Admin Guard Insight Security Copilot Agent Requirements Document Template

Instructions for Completing Each Section

Each section includes both a description of what is needed, and an example answer that you can reference. When you have completed each section, please delete the blue example text.

1. Purpose of the Agent

The Admin Guard Insight Security Copilot Agent is designed to enhance the security visibility and governance over privileged identities in Microsoft 365 environments. It provides a structured and executive-grade report that summarizes administrative activity, flags suspicious or high-risk behaviors, and identifies protection gaps related to MFA and Conditional Access enforcement.

The primary goals of the agent are:

- To monitor and summarize privileged user actions across the environment.
- To detect and correlate identity-based risks, including risky sign-ins and role changes.
- To assess coverage of Zero Trust identity controls such as MFA and Conditional Access.
- To generate weekly executive-level insights and recommendations.
- To support security administrators and CISOs with actionable intelligence for hardening identity posture.

2. Functional Design

The Admin Guard Insight agent operates in the following stages:

1. Data Collection
   It uses plugins to retrieve audit logs, sign-in logs, directory role assignments, Defender incidents, and risk signals from Microsoft Entra and Defender for Identity.
2. Data Enrichment
   It Invokes reasoning skills (GPT-based) to interpret this raw data into categorized summaries such as risk breakdowns, policy coverage, anomaly detection, and role analysis.
3. Report Generation
   Using structured prompts, the agent generates a markdown-based weekly report with sections including admin activity summaries, risk exposures, unresolved incidents, and prioritized recommendations.
4. Feedback Loop (Optional)
   It allows users to submit qualitative feedback via a rating and comment interface to help evolve future iterations of the agent.

3. Triggers for Agent Activation

The agent is configured to run via a **scheduled trigger** once every 7 days.

Trigger details:

- **Trigger Name:** WeeklyAdminCheck
- **Type:** Timer-based
- **Frequency:** 604800 seconds (7 days)
- **Fetch Skill:**
- **Process Skill:** AdminGuardInsight.FetchAdminData

It can also be manually executed for on-demand investigations via the Security Copilot interface.

4. Plugins or Data Signals

The following plugins and skillsets are required for the agent to function effectively:

Plugins:

- GetEntraAuditLogs
- GetEntraSignInLogsV1
- GetEntraRiskyUsers
- GetDefenderIncidents
- GetEntraUserDetailsV1

GPT Skills:

- EvaluateAdminProtectionPolicies
- SummarizeAdminAuditLogs
- SummarizeAdminSignIns
- SummarizeRiskyAdmins
- SummarizeCriticalAdminRoles
- SummarizeAdminIncidents
- GenerateAdminInsightReport

These skills ensure full coverage of privileged identity activity, risk, protection posture, and response summary.

5. Customer Access Process

Customers will access the agent through the Security Copilot interface. To enable and use the agent:

1. The tenant administrator must enable the agent via the Security Copilot plugin management console.
2. Required permissions and skillsets (AdminGuardInsight, Entra, M365) must be enabled.
3. Once enabled, the agent will be available in the “Agents” tab for all authorized contributors.
4. Execution can occur automatically based on the defined trigger or manually on-demand.
5. Output is accessible in the Copilot session view and exportable as markdown-formatted report.

Documentation and onboarding walkthrough will be available via the Microsoft Partner Center and Security Copilot developer portal.

6. Timeline of Engineering Milestones

Instructions: We have provided a timeline of key engineering milestones leading to the private and public previews of the agent targeted for May 16th.

NOTE: Please start with this table. We have supplied some milestone dates that are critical for the May 16th target. You may add additional interim milestone dates as needed.

Date	*Deliverables*	*Owner - Name and Email*
March 25	*Workshop*	
April 1 to April 15	*1. Updated plan* *a. Value Prop Description* *2. ISV UX for Agent* *3. Build prototype* *4. Share demo*	
April 23	*Private preview ready*	
May 16	*Public preview ready*	