Admin Guard Insight Security Copilot Agent Requirements Document Template

1. Purpose of the Agent (Customer benefit)

The Admin Guard Insight Security Copilot Agent helps organizations strengthen their privileged identity security posture by analyzing administrative activity, privileged role exposure, risky sign-ins, identity risk signals, and protection controls aligned to Zero Trust principles.

The agent is designed to produce an executive-grade posture report for security leaders and IT management. It focuses on the Identity pillar of Zero Trust and helps customers answer practical questions such as:

- Which critical and non-critical privileged roles are currently exposed or highly concentrated
- What suspicious privileged sign-ins or risky administrative behaviors require attention
- Whether MFA, Conditional Access, and PIM governance are strong, mixed, weak, or not yet fully confirmed
- Which privileged identities, roles, or governance gaps should be prioritized first by leadership

Customer benefits:

- Provides a unified, CISO-friendly view of privileged identity exposure and administrative risk
- Improves visibility into direct role assignment, governance discipline, and potential PIM gaps
- Supports Zero Trust maturity improvement for the Identity pillar through evidence-based recommendations

Products used:

- Microsoft Entra ID and related identity/policy data retrieved through Security Copilot Entra capabilities
- Microsoft Defender XDR incident data through the M365 skillset
- Microsoft Security Copilot for orchestration, reasoning, and final report generation

- Microsoft Defender XDR Advanced Hunting tables when available and supported, to provide deterministic metrics for sign-ins, administrative activity, and privileged governance snapshots

2. Functional Design

The Admin Guard Insight agent follows a layered evidence model designed to balance precision, resilience, and readability.

Core functional behavior:

- Builds a privileged identity scope using AskNL2API as the primary Entra retrieval path, focusing on critical roles first while still considering other privileged roles that materially affect exposure
- Uses deterministic KQL skills when supported in the customer environment to calculate privileged sign-in metrics, privileged administrative activity metrics, and privileged governance / PIM visibility metrics
- Uses AskNL2API as the fallback and enrichment path when Advanced Hunting is unavailable, incomplete, or not populated
- Collects administrative audit evidence, risky user evidence, and Defender incidents involving privileged identities
- Evaluates MFA, Conditional Access, and PIM governance based on explicit evidence rather than broad inference
- Generates a markdown-formatted executive report through the GenerateAdminInsightReport skill

The agent intentionally avoids hallucinated numbers. Deterministic counts are only surfaced when the underlying KQL path is available and returns valid data. When deterministic telemetry is not available, the report remains useful by presenting compact qualitative evidence and clearly bounded conclusions rather than estimated counts.

3. Triggers for Agent Activation

- The agent is configured to run through a scheduled trigger once every 7 days.
- Trigger details:
- Trigger Name: WeeklyRun
- Type: Timer-based
- Frequency: 604800 seconds (7 days)

The agent can also be executed manually through the Security Copilot interface for on-demand privileged identity reviews, governance validation, or follow-up analysis after suspicious administrative activity.

4. Plugins or Data Signals

The following skillsets, skills, and data signals are used by the current design.

Required skillsets / integrated capabilities:

- Entra
- M365
- AdminGuardInsight

Core skills and data signals:

- AskNL2API — primary Entra retrieval path for privileged role scope, sign-in evidence, MFA/Conditional Access posture, and PIM / governance interpretation
- GetEntraAuditLogs — administrative audit evidence for privileged changes and control changes
- GetEntraRiskyUsers — identity risk evidence for privileged users when available
- GetDefenderIncidents — Microsoft Defender incident evidence involving privileged identities
- GetAdminSignInDeterministicMetricsKql — deterministic privileged sign-in metrics when Advanced Hunting is available and populated
- GetAdminActivityDeterministicMetricsKql — deterministic privileged administrative activity metrics focused on real change operations
- GetPrivilegedRoleGovernanceKql — deterministic governance and PIM visibility snapshot using supported identity telemetry
- GenerateAdminInsightReport — final executive report generation

Important deployment note: Advanced Hunting is treated as optional. Customers without Advanced Hunting, or without the required tables populated, can still use the agent. In those cases, the agent falls back to AskNL2API and native Entra evidence to preserve report quality without inventing deterministic numbers.

5. Customer Onboarding/Deployment

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

- The tenant administrator must enable the agent package and ensure the required skillsets (AdminGuardInsight, Entra, and M365) are enabled
- Authorized users can access the agent through the Agents experience in Security Copilot
- The agent can run automatically through the weekly timer trigger or be executed manually on demand
- For deterministic metrics, the customer environment should support the relevant Advanced Hunting data path; if not, the agent will continue to operate through AskNL2API fallback and supported Entra evidence

The output is available in the Copilot session view as a structured, markdown-formatted privileged identity posture report. The report is intended for security leadership, identity administrators, and IT management teams that need a concise but evidence-based understanding of privileged role exposure, governance discipline, protection posture, and administrative risk.