Security Copilot Agent — Scenario

L1 SOC Triage Agent

1) Purpose of the Agent (Customer benefit)

The **L1 SOC Triage Agent** performs the initial triage of Microsoft Sentinel incidents in a fast, standardized way. It aggregates essential context (entities, severity, MITRE ATT&CK tactics, related alerts and signals) and classifies the next action (close, escalate, contain). It produces a single Markdown report with an executive summary, correlated evidence, analyst reasoning, and actionable recommendations—formatted for easy paste into ticketing systems.

Customer value

- Speeds up L1 time-to-respond with incident-centric correlation (no hopping across multiple panes).
- Standardizes the "true positive / benign / needs investigation" decision to reduce analyst variance.
- Delivers a single executive-ready output (evidence + prioritized recommendations), ready for SNOW/Jira.
- Operates with data that already exists (Sentinel/Defender) and handles missing data gracefully.

2) Functional Design

1. **Incident Ingestion**
    a. Receives the parameter Incident (GUID, number, or URL).
    b. Retrieves the incident details and entities using:
        i. GetIncident
        ii. GetIncidentEntities
2. **Contextual Enrichment**
    a. **Defender:**
        i. EnrichIncidentWithDeviceContext
        ii. EnrichIncidentWithFileContext
    b. **Purview:**
        i. GetDataRiskSummary
        ii. GetUserRiskSummary
        iii. ZoomIntoPurviewDataRisk
        iv. ZoomIntoPurviewUserRisk

c. **Threat Intelligence (DTI):**
    i. FindThreatIntelligence
    ii. GetSummaryForIndicators
d. **Sentinel:**
    i. GetSentinelIncidents for related or similar alerts.
e. **NL2KQLDefenderSentinel:**
    i. Enables natural-language query generation to validate hypotheses.

3. **L1 Analysis and Decision**
    a. Consolidates and correlates findings across all enabled skillsets.
    b. Determines the L1 verdict and corresponding recommendation:
        i. **Close – Benign/False Positive**
        ii. **Remediate – Action Required**
        iii. **Escalate – Further Investigation Needed (Tier 2)**
    c. Uses objective evidence such as MITRE ATT&CK mapping, IOC correlations, device exposure, and user risk signals.
4. **Report Generation**
    a. Produces a concise **Markdown report** with:
        i. Executive Summary
        ii. Incident Context and Entities
        iii. Correlated Evidence
        iv. Analyst Reasoning
        v. Recommended Actions
        vi. Coverage & Limitations
    b. Clearly identifies the **data sources and reasoning** for the verdict.

3) Triggers for Agent Activation

Trigger: Default

Type: Manual (no schedule/recurrence)

ProcessSkill: SentinelDataLeak.SentinelDataLeakInvestigator

Invocation: Analyst provides Incident (GUID / number / URL).

4) Plugins or Data Signals

Required Skillsets.

- Sentinel
- Defender *(via NL2KQLDefenderSentinel)*
- Purview
- Fusion
- ThreatIntelligence.DTI
- M365

- SOCTriageAgent *(Agent's own group)*

Child Skills (as declared in manifest):

- GetIncident
- GetIncidentEntities
- GetSentinelIncidents
- EnrichIncidentWithDeviceContext
- EnrichIncidentWithFileContext
- GetDataRiskSummary
- GetUserRiskSummary
- ZoomIntoPurviewDataRisk
- ZoomIntoPurviewUserRisk
- FindThreatIntelligence
- GetSummaryForIndicators
- NL2KQLDefenderSentinel

Data Sources and Correlation:

- **Sentinel** – Incident base data and entity extraction.
- **Defender** – Endpoint and device posture correlation.
- **Purview** – Data and user risk insights.
- **Threat Intelligence (DTI)** – IOC and actor enrichment.
- **Fusion / MCP** – Advanced correlation across signals.
- **M365** – Supporting identity and activity context.

5) Customer Onboarding/Deployment

Pre-requisites:

- Microsoft Sentinel workspace with required permissions to read incidents and entities.
- The following skillsets enabled and configured:
  Sentinel, Defender, Purview, ThreatIntelligence.DTI, NL2KQLDefenderSentinel, M365, Fusion.

Deployment Steps:

1. Setup **L1 SOC Triage Agent** the secure store
2. Enable all required skillsets listed above.
3. Ensure the Security Copilot plugin permissions include access to these data sources.