Security Copilot Agent – Scenario

Login Investigator

Version: v1

1) Purpose of the Agent (Customer Benefit)

Agent Name: Login Investigator

The Login Investigator agent validates whether a user's recent sign-ins are legitimate by orchestrating global Microsoft skills in Microsoft Entra and Defender. It builds a 30-day (configurable) user baseline (IPs, regions, devices, client apps), evaluates the latest relevant interactive sign-in, checks IP reputation, device management status, user risk, Conditional Access (CA) evaluation outcomes, and lists related Defender XDR incidents. The agent then produces a concise Markdown report with a checklist, evidence (including tool Sources), and prioritized actions.

Why customers will find this valuable:

- Faster triage: single-run validation across Entra, ID Protection, Intune, XDR, and TI.
- Lower false positives: per-user baseline clarifies normal IPs/regions/devices.
- Traceable decisions: standardized evidence with explicit tool Sources for audit/tickets.
- No Sentinel dependency: works fully with global skills (no KQL fallback).
- Actionable outcomes: prioritized recommendations (e.g., MFA prompts, password reset, CA tuning).

Products in scope: Microsoft Defender XDR (MDE/MDI/MDO), Microsoft Entra ID, Microsoft Intune, Microsoft Threat Intelligence (DTI).

2) Functional Design

Input & validation:

Receive UPN, LookbackDays (default 30), IncidentLookbackDays (default 30), Strictness, OutputLanguage.

- User profile: fetch user details by UPN (Entra Users).

- Sign-ins: retrieve recent interactive sign-ins; build baseline (IPs, countries/cities, devices, client apps) and select the current sign-in (latest relevant).
- Threat intelligence: check reputation for the current sign-in IP via DTI (or alternate TI global skill).
- Devices: get user's devices and compliance/ownership (Intune) to determine known/managed status.
- Risk: obtain risky user state and detections (Entra ID Protection).
- Conditional Access: evaluate CA outcomes for the current sign-in; list evaluated policies and results (MFA/blocked/etc.).
- Incidents: list related Defender XDR incidents within IncidentLookbackDays (severity, status, category, title).
- Anomaly logic: compare current sign-in vs baseline (new IP/region/device, impossible travel, unusual client app, failure spikes).
- Scoring & narrative: derive a concise Risk Assessment (Low/Medium/High) with rationale.
- Output: generate a Markdown report (Summary, Checklist with Evidence+Source, Evidence section, Related Incidents table, Recommended Actions).

3) Triggers for Agent Activation

Manual (v1): Analysts run the agent on demand by providing a UPN (Mandatory). Optional inputs: Look back days (default 30), Strictness (default balanced), Language (default en-US), Incident Look Back Days (default 30).

4) Plugins or Data Signals

- **M365**
    - M365.GetDefenderIncidents
    - M365.GetDefenderIdentitySummary
- **Entra**
    - GetEntraUserDetailsV1
    - GetEntraSignInLogsV1
    - GetEntraRiskyUsers
    - CAPolicyAnalysisAgent
    - CAPolicyReviewRecommenderStandalone

- **Intune**
    - GetIntuneDeviceGroupMemberships
    - GetIntuneDevices
- **ThreatIntelligence.DTI**
    - ThreatIntelligence.DTI.GetReputationsForIndicators
    - ThreatIntelligence.DTI.FindThreatIntelligence (as a fallback)
- **Local (GPT renderer)**
    - ProcessLoginAnalysis

Data Signals (ingested/queried)

- **Defender XDR**
- **Identity (Entra)**
- **Device/Endpoint (Intune/Defender)**
- **Threat Intelligence (DTI)**

5) Customer Onboarding / Deployment

1. In the **Security Copilot Agents gallery**, locate **Login Investigator** and enable it.
2. When prompted, consent to the required plugins:
    - M365 (Defender XDR)
    - Entra
    - ThreatIntelligence.DTI
    - Intune
3. Confirm Required Skillsets in the extension: M365, Entra, Intune, ThreatIntelligence.DTI, and Local Login Investigator
4. Validate triggers

How to run

- **On demand**: provide a UPN to analyze a specific user login.
    - Optional parameters:
        - LookbackDays (default 30)
        - Strictness (default balanced)
        - Language (default en-US)
        - Incident Look Back Days (default 30).