Security Copilot Agent – Scenario

Ransomware Kill Chain Investigator (RKCI)

Version: v2
Owner: adaQuest
Last Updated: 2025-09-17

1) Purpose of the Agent (Customer Benefit)

Agent Name: Ransomware Kill Chain Investigator (RKCI)

Goal: Reduce MTTD/MTTR for ransomware by automatically ingesting Microsoft Defender incidents, enriching users/devices/IOCs (via Entra/Intune/Threat Intelligence), correlating the ATT&CK kill chain, and guiding response with a clear, human-readable plan.

- Faster triage: stitch alerts into a single narrative across ATT&CK phases.
- Higher confidence: identity/device posture and threat-intel context on every entity and IOC.
- Operational scale: repeatable guided response, less analyst toil, consistent quality.

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

2) Functional Design

Operating model — "Agent-as-Process"

RKCI (the Agent) directly orchestrates global skills + local KQL hunts and calls one GPT skill only to render the final brief.

Inputs (defaults)

- IncidentId *(optional)*, LookbackHours=72, IncludeHunts="yes", TopN=50, MinSeverity="High".

Flow

1. **Ingest**
    - If IncidentId given → M365.GetDefenderIncidentReport.

- Else → M365.GetDefenderIncidents (Category=Ransomware, Severity≥High, CreatedAfter=Now-72h) then loop incidents.

2. **Parse incident**

   - Extract timeline, alerts, entities (users/devices/files/IOCs), determinations, severity, impacted assets.

3. **Enrichment**

   - **Identity:** M365.GetDefenderIdentitySummary, Entra.GetEntraUserDetailsV1, Entra.GetEntraSignInLogsV1 (risky sign-ins, impossible travel, CA outcomes).
   - **Device:** Intune.GetDefenderDeviceSummary, Intune.GetIntuneDevices (risk, compliance, ownership, groups).
   - **Threat Intel (per IOC):** ThreatIntelligence.DTI.GetSummaryForIndicators, …GetReputationsForIndicators, …GetWhoisRecordsForIndicators (domains).
   - **File analysis:** M365.GetFileAnalysis when hash/file is available.

4. **Targeted hunting (Microsoft Defender Advanced Hunting only)** — run when IncludeHunts="yes"

   - RKCI_HuntCFA – Controlled Folder Access blocks.
   - RKCI_HuntRansomOps – vssadmin/wbadmin/bcdedit/cipher & wipe/shadowcopy phrases.
   - RKCI_HuntMassRename – bursts of rename/modify (5-minute bins; threshold).
   - RKCI_HuntRansomNotes – common ransom-note filenames.
   - RKCI_HuntPsEncoded – encoded/obfuscated PowerShell execution.
   - RKCI_HuntLateralMovement – PsExec/WMI/Schtasks/SC/AT patterns.
   - Merge only relevant hits; dedupe by (DeviceName, Process/IOC, time bin).

5. **Guided response**

   - M365.GetIncidentGuidedResponse → build prioritized plan (containment → eradication → recovery) with owners and pre-checks.

6. **Executive brief (rendering)**

   - Agent composes a compact ExecutiveContext and calls RKCI_ExecutiveBrief (GPT) to output a **polished Markdown brief** with:
     Executive Summary → Kill Chain (ATT&CK) → Affected Assets → IOCs & TI table → Recommended Actions → Timeline.

Guardrails

- No raw JSON to users.
- Retries: up to 2 per tool call with brief backoff.
- Respect LookbackHours and TopN caps.
- If a data source denies/omits info, state the gap and proceed.
- Least privilege access; avoid unnecessary scopes.

3) Triggers for Agent Activation

Manual (v1): Analysts run the agent on demand by providing a Defender IncidentId. Optional inputs: Lookbackhours (default 72), IncludeHunts (Default yes), MinSeverity (default High)

4) Plugins or Data Signals

- **M365**
  - M365.GetDefenderIncidents
  - M365.GetDefenderIncidentReport
  - M365.GetIncidentGuidedResponse
  - M365.GetDefenderIdentitySummary
  - M365.GetFileAnalysis
- **Entra**
  - Entra.GetEntraUserDetailsV1
  - Entra.GetEntraSignInLogsV1
- **Intune**
  - Intune.GetDefenderDeviceSummary
  - Intune.GetIntuneDevices
- **ThreatIntelligence.DTI**
  - ThreatIntelligence.DTI.GetSummaryForIndicators
  - ThreatIntelligence.DTI.GetReputationsForIndicators
  - ThreatIntelligence.DTI.GetWhoisRecordsForIndicators
  - ThreatIntelligence.DTI.FindThreatIntelligence

- **Local (this project — Defender AH KQL)**
    - RKCI_HuntCFA
    - RKCI_HuntRansomOps
    - RKCI_HuntMassRename
    - RKCI_HuntRansomNotes
    - RKCI_HuntPsEncoded
    - RKCI_HuntLateralMovement
- **Local (GPT renderer)**
    - RKCI_ExecutiveBrief

Data Signals (ingested/queried)

- **Defender XDR:** incidents, alerts, entities (users/devices/files/network/IOCs), determinations, severity.
- **Identity (Entra):** user attributes/roles; sign-in telemetry (risk events, CA outcomes, geo anomalies).
- **Device/Endpoint (Intune/Defender):** device risk/AV-EDR posture; compliance, ownership, group membership.
- **Threat Intelligence (DTI):** reputation/summaries, WHOIS, related intel links/profiles.
- **Advanced Hunting (Defender):** DeviceEvents, DeviceProcessEvents, DeviceFileEvents patterns used by the KQL skills acima.

5) Customer Onboarding / Deployment

Prerequisites
Reader-level (or equivalent least-privilege) permissions for:

- **Microsoft Defender XDR** — to access incidents, alerts, timeline evidence, and device context.
- **Microsoft Entra ID** — to access user details, sign-in logs, risky sign-ins, Conditional Access outcomes.
- **Microsoft Threat Intelligence (DTI)** — to retrieve indicator reputation, WHOIS, and related intel profiles.
- **Microsoft Intune** — to access device compliance, ownership, and group membership.
- **Advanced Hunting access in Defender** — must be able to query DeviceEvents, DeviceProcessEvents, and DeviceFileEvents tables for the KQL hunts.

Additional requirements:

- Security Copilot license + extension enabled in Visual Studio Code.
- Skillset project created as RansomwareKillChainInvestigator (this name is required for namespaces).

- Global skills enabled and consented: M365, Entra, Intune, ThreatIntelligence.DTI.

Enable the agent

1. In the **Security Copilot Agents gallery**, locate **Ransomware Kill Chain Investigator (RKCI)** and enable it.
2. When prompted, consent to the required plugins:
    - M365 (Defender XDR)
    - Entra
    - ThreatIntelligence.DTI
    - Intune (recommended if device compliance posture is in scope)
3. Confirm Required Skillsets in the extension: M365, Entra, Intune, ThreatIntelligence.DTI, and local RansomwareKillChainInvestigator.
4. Validate triggers: default schedule every 30 minutes (DefaultPollPeriodSeconds=1800), with ProcessSkill = RansomwareKillChainInvestigator.RKCI.

How to run

- **On demand**: provide a Defender IncidentId to analyze a specific case.
    - Optional parameters:
        - LookbackHours (default 72)
        - IncludeHunts (yes/no, default yes)
        - TopN (default 50, caps list/table sizes)
        - MinSeverity (default High)

What to expect

- The agent **analyzes full incidents**: timeline, alerts, entities (users, devices, IOCs, files).
- Each entity is enriched with:
    - **Identity**: Entra sign-ins, risky signals, Conditional Access.
    - **Devices**: Defender risk posture, Intune compliance/ownership.
    - **IOCs**: TI summaries, reputation scores, WHOIS (domains), file analysis (hashes).
- Targeted **hunts** run via Defender Advanced Hunting for:
    - Controlled Folder Access (CFA) blocks
    - Ransomware utilities (vssadmin, wbadmin, bcdedit, cipher)
    - Mass file rename/modify bursts
    - Ransom note creation/modification
    - Encoded PowerShell activity
    - Lateral movement patterns (PsExec, WMI, Schtasks, SC, AT)
- Output is a **clear Markdown report** with:
    - **Executive Summary** (what happened, severity, impact)
    - **ATT&CK Kill Chain correlation**
    - **Affected assets** (users, devices)
    - **IOCs & Threat Intel** (table)

    - **Recommended Actions** (containment → eradication → recovery)
    - **Appendix: key timeline events**

Operational guidance

- Only incidents flagged as **ransomware** are considered; other categories are ignored by design.
- Hunts add coverage for early-stage and late-stage ransomware TTPs but respect the defined lookback window.
- Results are capped (TopN) to prevent noise; the brief favors high-signal findings.
- Use the output as an **accelerator for triage** — confirm key findings, and apply recommended containment steps.
- Output is suitable for both **SOC hand-off** and **executive readout**; analysts can export/share directly.
- Gaps are explicitly called out (e.g., "No Intune compliance data available" or "No IOC reputation returned").