SECURITY COPILOT AGENT: **SIGN-IN INVESTIGATOR**

water
IT Security & Defense

Stop chasing sign-in alerts. Start closing them.

Sign-In Investigator turns a Microsoft Defender incident into **a structured, evidence-backed investigation report** in under 2 minutes – with risk classification, IOC enrichment, and ranked containment actions ready for the analyst to execute.

The Problem

A typical identity incident touches **seven Microsoft surfaces**: Defender, Entra sign-in logs, Entra audit logs, risky users, conditional access, threat intelligence, and the user's mailbox. Tier-1 analysts spend **20–40 minutes per incident** pivoting between them, wasting valuable time before containment can even begin.

Sign-In Investigator: What it delivers

~2 min

Typical time to report

From incident ID to a complete, evidence-backed investigation report. No tab-switching, no copy-paste.

1 workflow

Repeatable risk classification

Correlates Microsoft security signals into one standardized workflow for faster, defensible decisions.

<1 SCU

Per investigation

Predictable costs that scale with the number of suspicious IPs and the size of the user's recent sign-in history.

How it works

Resolve the incident

Pulls the Defender incident, extracts the affected user, suspicious IPs, and any flagged URLs.

Reconstruct the sign-in story

Anomaly detection across Entra logs – new locations, weak MFA, conditional access misses, legacy auth, VPN use.

Enrich the evidence

Roles, audit log changes, IP reputation from Microsoft Defender TI, email and URL click correlation.

Report & recommend

Single Markdown report, risk-classified findings, ranked containment actions referencing actual evidence.

Built for your stack

REQUIRED

- Microsoft Entra ID P2 – sign-in retention & risk signals
- Microsoft Defender for Office 365 P1 (P2 recommended) - mail & URL telemetry
- Microsoft Defender Threat Intelligence – IP reputation
- Security Reader role – minimum for read-only use

OPTIONAL, EXPANDED COVERAGE

- Microsoft Defender for Identity - on-premises Active Directory context
- Microsoft Sentinel UEBA – expanded role context

PRIVACY POSTURE

- No data leaves your Microsoft tenant boundary
- No third-party APIs, no external credentials

Built for these moments

SOC tier-1 triage – an Entra sign-in alert lands at 03:00. Get a complete picture before paging tier-2.

Identity admin audit – an HR-flagged user account needs a 7-day rear-view of activity.

Threat intel enrichment – pull every IOC from an incident, enrich with first-party Microsoft Defender TI.

Executive briefing – a one-paragraph summary for the post-incident review meeting at 10:00.

Setup in minutes

1. Install → 2. Assign identity → 3. Choose mode → 4. Run investigation

1. Install

Install Sign-In Investigator from the Microsoft Security Store, and set it up in the Security Copilot portal.

2. Assign identity

Sign in with the account that should act as the agent identity and make sure it has the required permissions, at least Security Reader.

3. Choose mode

Use "Chat with agent" for open-prompt interaction, or "Go to agent" to run a guided investigation.

4. Run investigation

Provide an incident ID or UPN. The agent returns an incident summary, user sign-in activity, and, where available, related risky email activity.

Ready to close sign-in incidents faster?

Scan the QR code to book a free 30-minute demo!

Philipp Kretz
Lead Partner Management & Marketing
philipp.kretz@wtrsecurity.de
www.water-security.de