



SECURITY OPERATIONS USER GUIDE

LeakData Exposure Triage

A practical guide to installing, authorizing, running, and safely interpreting the LeakData investigation agent for Microsoft Security Copilot and Microsoft Sentinel.

SUBMISSION GUIDE | VERSION 1.1 | 19 SEPTEMBER 2026

READ-ONLY

No mutation actions

2 SOURCES

LeakData and Sentinel

1-168 H

Configurable lookback

What this guide covers

- Prerequisites and access checks before installation.
- OAuth authorization without sharing passwords or client secrets.
- Validated inputs and the expected five-section investigation output.
- False-positive controls, privacy limits, troubleshooting, and removal.

Availability status

This document supports preview and certification preparation. The agent must not be described as publicly available until Microsoft approval and publication are complete.

Publisher: CYBERVISIR SOLUTIONS LTD

Product: LeakData | Offer: LeakData Exposure Triage

SECTION 1

Product overview

LeakData Exposure Triage correlates an authorized LeakData exposure summary with matching delivery telemetry in the customer's Sentinel workspace.

Purpose

The agent checks only the linked account's verified primary email. Domain and phone searches are not supported. After one successful LeakData search, it checks the authorized Microsoft Sentinel workspace for matching records in **LeakDataAlerts_CL** and produces conservative recommendations for human review.



What the agent returns

Output section	What it contains	What it does not claim
Scope	The linked account's verified primary email and lookback window.	Authorization for domain, phone, or third-party email searches.
LeakData exposure summary	Minimized exposure counts and categories returned by the authorized search.	Raw leak rows, plaintext passwords, or complete hashes.
Workspace evidence	Matching event count, first and last seen times, and sample event IDs.	Independent proof that a compromise occurred.
Correlation and confidence	High, Medium, None, or unavailable for data correlation, with supporting evidence.	A compromise-confidence or risk score.
Recommended analyst actions	Read-only next steps that require analyst judgment.	Automatic reset, block, isolation, notification, or incident creation.

Core interpretation rule

Matching rows in LeakDataAlerts_CL confirm delivery and data consistency because those rows originate from LeakData. They are not an independent source of compromise evidence.

SECTION 2

Before you begin

Complete this readiness check before importing, acquiring, or authorizing the agent. Capacity and ingestion choices can create charges.

Publication boundary

Use Partner Center preview links or an approved private test package until certification is complete. Do not use this guide as proof that the offer is publicly listed.

Readiness checklist

Area	Required state	How to verify
LeakData account	Signed in to the linked account, with its primary email verified.	Open LeakData account settings and confirm the primary email is verified.
Security Copilot	An authorized workspace and a user who can install or use the agent.	Confirm the user can open Security Copilot and access the intended workspace.
Microsoft Sentinel	An authorized workspace available to the user.	Confirm the workspace appears when Sentinel workspaces are listed.
LeakData connector	The LeakData Sentinel solution is installed when correlation is expected.	Check that the custom table LeakDataAlerts_CL exists.
Cost approval	Any required Security Copilot capacity and Sentinel ingestion are approved by the organization.	Confirm budget, capacity, retention, and test-workspace decisions before activation.

Permission map

Task	Typical permission
Install or preview the solution	A role allowed to acquire and deploy the Security Store solution in the target environment.
Authorize LeakData	The individual LeakData account owner; search consent applies only to that account's verified primary email.
Query Sentinel	Read access to the selected Sentinel workspace and relevant data.
Revoke access	The LeakData account owner or an administrator with authority to remove the enterprise application grant.

Test safely

Use synthetic events and an explicitly approved test workspace for certification runs. Do not ingest production data solely to demonstrate the solution.

SECTION 3

Install and authorize

After a preview or public listing is available, acquire the solution in Security Store and complete LeakData OAuth from Security Copilot.

1

Open the approved listing

Use the Partner Center preview link supplied for testing, or search Security Store only after the offer is public. Confirm the publisher is CYBERVISIR SOLUTIONS LTD and the product is LeakData.

2

Acquire and deploy

Select the permitted plan and target environment. Review the plan terms before confirming. Deployment and licensing behavior depend on the approved listing.

3

Open My solutions

In Security Store, open My solutions and follow the setup action for LeakData Exposure Triage. The solution should become visible to the intended Security Copilot workspace.

4

Start LeakData authorization

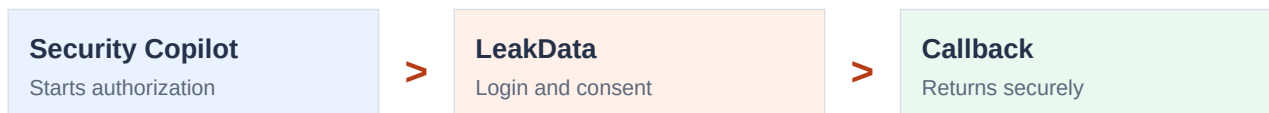
From the solution setup or agent connection flow, choose Connect or Sign in. Security Copilot sends the browser to LeakData using OAuth authorization code flow.

5

Sign in and consent

Authenticate directly on leakdata.io. Confirm that the requested scope is search. Approve only for the intended LeakData account, then allow the browser to return to Security Copilot.

Authorization flow



Secret-handling rule

Enter passwords only on their official sign-in pages. Do not paste a LeakData password, OAuth client secret, access token, or raw credential into a prompt, ticket, screenshot, or agent input.

Successful connection checks

- The connection returns to Security Copilot without an OAuth error.
- The agent appears in the intended Security Copilot workspace.
- A search can access only the linked account's verified primary email.
- An unrelated email is rejected without data; domain and phone inputs never trigger a search.

SECTION 4

Configure and run

Provide the three validated inputs, select the intended workspace, and review the resulting five-section report.

Inputs

Input	Accepted value	Example	Validation behavior
AssetType	Exactly email, after lowercasing. Setting name retained for compatibility.	email	Any other value stops the run before a tool call.
Asset	The linked account's verified primary email.	analyst@example.com	Empty or unrelated third-party scope is rejected.
TimeRangeHours	A whole number from 1 through 168.	24	Values outside the range or non-integers are rejected.

Run sequence

1

Open the agent

In Security Copilot, select LeakData Exposure Triage from the agent or solution experience.

2

Enter the scope

Set AssetType to email, enter the linked account's verified primary email, and set the lookback window. Do not substitute another address.

3

Check the LeakData result

The agent makes one email search. If LeakData denies or fails the check, stop before any Sentinel tools run. Report an incomplete check, never zero exposure.

4

Confirm the workspace

Only after a successful authorized result, select the permitted Sentinel workspace. The agent checks LeakDataAlerts_CL and correlates exact email matches. Do not query another tenant.

5

Review the complete report

Read Scope, LeakData exposure summary, Workspace evidence, Correlation and confidence, and Recommended analyst actions before deciding any response.

Example input

AssetType: email
Asset: analyst@example.com
TimeRangeHours: 24

No Sentinel table is still a valid outcome

After a successful LeakData check, a missing LeakDataAlerts_CL table means delivery telemetry is unavailable. Keep the authorized summary and state the gap; missing or failed checks never establish no exposure.

SECTION 5

Interpret results safely

The confidence value measures agreement between data sources. It never establishes that an account was compromised.

Data-correlation confidence

Level	When it applies	Required wording and action
High	The current authorized LeakData result and an exact matching Sentinel delivery agree.	High data-correlation confidence. State clearly that this is not compromise confidence; require analyst review.
Medium	Only one source contains evidence, or records are stale, partial, or mismatched.	Name the missing or conflicting evidence and recommend validation before response.
None	Successful checks of both sources find no evidence for the validated scope and time window.	Report no observed evidence in the checked sources and time range; do not claim universal absence.
Unavailable	LeakData fails or denies the check, or corroboration is unavailable and no positive evidence remains.	State the incomplete check. A LeakData failure stops Sentinel tools and must never be reported as zero exposure.

The report can support

- A decision to investigate the verified primary email further.
- A delivery-quality check between LeakData and Sentinel.
- Prioritization based on explicit evidence and stated gaps.
- A human-reviewed remediation plan.

The report cannot prove

- That credentials were used by an attacker.
- That a mailbox, identity, endpoint, or tenant is compromised.
- That a duplicate Sentinel event is independent evidence.
- That no exposure exists outside the checked sources and window.

Severity rule

Critical means Severity 9 only

The native LeakData analytic rule alerts only when Severity equals 9. Do not label a lower severity as critical, and do not create an incident automatically.

Analyst decision checklist

- Confirm the email is the linked account's verified primary email.
- Confirm timestamps, event type, severity, and normalized asset match exactly.
- Distinguish LeakData-originated delivery evidence from independent identity, endpoint, or network evidence.
- Document missing, stale, partial, or conflicting data before escalating.
- Require the appropriate owner to approve any notification, reset, block, isolation, or incident action.

SECTION 6

Security, privacy, and data handling

The agent is designed for minimized, read-only investigation of the linked account's verified primary email, enforced by instructions and the LeakData service.

Data-handling map

Data	Used for	Displayed or retained in the report
Verified primary email	Scope validation and exact matching.	Displayed as the investigation scope.
Minimized LeakData summary	Exposure context for the authorized asset.	Summary fields only; no raw leak rows.
Sentinel event metadata	Delivery and consistency correlation.	Counts, time bounds, event type, severity, and limited sample event IDs.
RawData	Only to derive the normalized alert asset during the workspace query.	Not projected or reproduced in the report.
Passwords and secrets	Not required for agent input or output.	Never accepted, requested, displayed, or inferred.

Security controls

Built-in controls

- One authorized LeakData search per run.
- Linked account email ownership enforced by the LeakData service.
- Read-only LeakData and Sentinel operations.
- Exact normalized-asset correlation and bounded results.
- Explicit gaps instead of generated assumptions.

Prohibited handling

- Plaintext passwords or complete password hashes.
- Raw leak rows or unrelated personal data.
- Cross-tenant workspace enumeration or querying.
- Automatic deletion, reset, block, isolation, or notification.
- Secrets in source control, prompts, screenshots, or support tickets.

OAuth grant hygiene

Use a dedicated organizational account where appropriate, review grants periodically, and revoke the LeakData connection when the user no longer needs the agent. Do not share one user's OAuth connection with another user.

Operational responsibility

Your organization remains responsible for authorization, data-retention choices, Sentinel access, incident decisions, and compliance with its own policies. LeakData findings should be combined with independent security evidence before a response action is approved.

SECTION 7

Troubleshooting

Use the symptom table first. Keep diagnostics free of passwords, tokens, client secrets, and raw exposure records.

Symptom	Likely cause	Safe resolution
Offer or agent is not visible	The offer is not public, the user is outside the preview audience, or deployment has not completed.	Confirm the correct preview link, tenant, audience, and My solutions status. Do not claim publication until approved.
OAuth returns an error	The connection was interrupted, consent was denied, or the callback/configuration does not match.	Restart connection from Security Copilot. Sign in only at leakdata.io. Record the error ID and time without including secrets.
Asset is rejected	The value is empty, the type is not email, or the address is not the linked account's verified primary email.	Set AssetType to email and confirm the linked account's primary email. Do not query Sentinel to bypass a rejection.
LeakData search fails	Authorization, rate limits, availability, or a missing valid summary prevented the check.	Stop before Sentinel tools. Report the check as incomplete, never as zero exposure or confidence None.
No Sentinel workspace	The user lacks access or selected the wrong tenant/workspace context.	Confirm read permission and the intended tenant. Do not query another tenant to work around access.
LeakDataAlerts_CL is missing	The LeakData Sentinel solution is not installed, has not delivered data, or the wrong workspace is selected.	Validate connector installation and synthetic delivery in an approved test workspace. The agent may still return the LeakData summary.
Results disagree	Time ranges, normalized asset values, delivery delay, or partial data differ.	Treat confidence as Medium, compare timestamps and event metadata, and document the mismatch before action.

Diagnostic sequence

1

Record non-sensitive context

Capture UTC time, workspace name, input type, lookback hours, and the visible error ID. Redact the asset if it is personal data.

2

Recheck authorization

Confirm the input matches the linked LeakData account's verified primary email and the selected Sentinel workspace is authorized.

3

Separate sources

Determine whether the issue is LeakData search, Sentinel table availability, Sentinel query, or the correlation stage.

4

Retry once after correction

Correct the identified setting and run again. Avoid repeated retries that could obscure timing or usage evidence.

5

Escalate with safe evidence

Contact support with the error ID, UTC time, product version, and sanitized reproduction steps. Never attach credentials or raw leak records.

Certification testing note

Measure Security Compute Unit usage from three to five representative successful runs only after access and capacity are approved. Do not estimate or publish an SCU value from theory.

SECTION 8

Remove access and get help

Remove the deployed solution and revoke its OAuth connection when access is no longer required. Verify that both sides are disconnected.

Removal sequence

1

Stop active use

Finish or cancel any current investigation and record only the sanitized case notes required by your organization.

2

Remove the solution

Use Security Store My solutions or the approved administrative flow to remove LeakData Exposure Triage from the intended environment.

3

Revoke LeakData authorization

In LeakData connected applications or the authorized identity administration flow, revoke the Security Copilot connection for the user.

4

Verify disconnection

Confirm the agent can no longer call LeakData and is no longer available to the intended workspace. Do not rely only on the browser session being closed.

5

Review downstream retention

Apply the organization's approved Sentinel retention and case-record policies. Removing the agent does not automatically delete customer workspace data.

Support

Email support@leakdata.io. Include UTC time, product and guide version, sanitized reproduction steps, workspace name, and any non-sensitive error ID. Never send passwords, tokens, client secrets, or raw leak rows.

Policies and product references

[LeakData Privacy Policy](#) - leakdata.io/privacy

[LeakData Terms](#) - leakdata.io/terms

[Microsoft Security Store documentation](#) - learn.microsoft.com

[Microsoft Security Copilot documentation](#) - learn.microsoft.com

Document control

Document	Value
Guide version	1.1
Guide date	19 September 2026
Offer	LeakData Exposure Triage
Publisher	CYBERVISIR SOLUTIONS LTD
Release status	Submission preparation; certification and public availability pending