**Demo Guide: Integrate Microsoft Sentinel with Power Platform (SOC)**

# Overview & Architecture

Goal: Connect Microsoft Power Platform telemetry to Microsoft Sentinel, visualize and detect risks, and automate response using low-code tools.

**What you will build:**

* Ingest Power Platform admin and activity logs into Sentinel
* Verifying ingestion with KQL queries
* Create an alert and an automated response
* Optional: Power BI report and Copilot Studio chatbot for incident intake

# Prerequisites

* Azure subscription with a Log Analytics workspace and Microsoft Sentinel enabled
* Permissions: Microsoft Sentinel Contributor (workspace) and rights to create Data Collection Rules/Endpoints
* Microsoft Purview (Unified Audit) enabled; Dataverse auditing enabled for production environments
* Power Platform environment(s) where you can enable auditing and generate activity
* Docs: See official Microsoft Learn articles referenced in chat.

# Step-by-Step Integration

**Step 1 — Install the solution**

• Azure portal → Microsoft Sentinel

A screenshot of a computer

AI-generated content may be incorrect.

* Create your Sentinel workspace

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

* Content hub → Search “Microsoft Business Applications” → Install

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

• Adds data connectors, analytics rules, workbooks, and hunting queries for Power Platform & Dataverse.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Note:

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Step 2 — Enable data connectors**

• Sentinel → Configuration → Data connectors → Open connector page → Connect:

Example Open – Dataverse

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

* Microsoft Power Platform Admin Activity → Table: PowerPlatformAdminActivity
* Microsoft Power Automate → Table: PowerAutomateActivity
* Microsoft Dataverse → Table: DataverseActivity

A screenshot of a computer

AI-generated content may be incorrect.

**Step 3 — Turn on auditing**

* Microsoft Purview: Enable unified auditing for your tenant.

A screenshot of a computer

AI-generated content may be incorrect.

* Dataverse: Enable auditing globally and per-entity (single & multiple record auditing for production envs).

A screenshot of a computer

AI-generated content may be incorrect.

**Step 4 — Generate sample activity**

* Create/edit/delete a test app, update a DLP policy, run/disable a test flow, create/bulk-delete Dataverse records.

**Step 5 — Verify ingestion with KQL**

* Sentinel → Logs (or Defender portal → Advanced hunting) → Run the KQL below.

# Sample KQL Queries

1. Quick check: return latest Power Platform admin logs

|  |
| --- |
| PowerPlatformAdminActivity | take 50 |
|  |

1. Monitor DLP policy changes (create/update/delete)

|  |
| --- |
| PowerPlatformAdminActivity | where TimeGenerated > ago(24h) | where Operation in ("DlpPolicyCreated","DlpPolicyUpdated","DlpPolicyDeleted") | extend Props = parse\_json(Properties) | project TimeGenerated, Operation, Actor=Identity, EnvironmentName, PolicyName=tostring(Props.policyName) | order by TimeGenerated desc |

1. Detect potential mass deletion of Power Apps (threshold-based)

|  |
| --- |
| PowerPlatformAdminActivity | where TimeGenerated > ago(24h) | where Operation == "DeleteApp" | summarize Deletes=count() by Actor=Identity, EnvironmentName, bin(TimeGenerated, 1h) | where Deletes > 5 | order by TimeGenerated desc |

1. Power Automate flows disabled or deleted by user

|  |
| --- |
| PowerAutomateActivity | where TimeGenerated > ago(24h) | where Operation in ("TurnOffFlow","DeleteFlow") | project TimeGenerated, Operation, Actor=Identity, FlowName=tostring(parse\_json(Properties).flowDisplayName), EnvironmentName | order by TimeGenerated desc |
|  |

1. Unusual flow run volume per user (spike over baseline)

|  |
| --- |
| let lookback = 7d; let recent = 1d; let baseline = PowerAutomateActivity | where TimeGenerated between (ago(lookback) .. ago(recent)) | where Operation == "FlowRun" | summarize baseline\_count = count() by User=Identity; let current = PowerAutomateActivity | where TimeGenerated > ago(recent) | where Operation == "FlowRun" | summarize current\_count = count() by User=Identity; current | join kind=leftouter baseline on User | extend baseline\_count = coalesce(baseline\_count, 0) | extend increase = current\_count - baseline\_count | where current\_count > baseline\_count \* 2 and current\_count >= 50 | order by increase desc |

1. Dataverse bulk deletes in short window

|  |
| --- |
| DataverseActivity | where TimeGenerated > ago(24h) | where Operation == "Delete" | summarize Deletes=count() by UserId, EntityName=tostring(parse\_json(Properties).entity), bin(TimeGenerated, 15m) | where Deletes > 100 | order by TimeGenerated desc |

# Create an Analytic Rule (Alert)

Example: Alert on Power App mass deletions > 5 per hour.

* Sentinel → Analytics → Create → Scheduled query rule.

A screenshot of a computer

AI-generated content may be incorrect.

* Query: use sample (C), adjust threshold & window; map Actor to Account entity.
* Frequency: every 5–15 minutes; set severity High; configure suppression as needed.

# Automate Response (Playbook)

* Sentinel → Automation → Create playbook (Logic App) triggered on incident creation.
* Actions: Post to Teams, create Planner task, update Dataverse incident table, or call a Power Automate flow via HTTP.
* Test by simulating mass delete or disabling flows in a test environment.

# Optional Enhancements

* Power BI: Connect to Log Analytics (Kusto) and build visuals on PowerPlatformAdminActivity/DataverseActivity.
* Copilot Studio: Build an incident intake bot writing to Dataverse and triggering a Power Automate flow to notify SOC.
* Power Apps: Simple app that lists Sentinel incidents via API and links to Dataverse records.

# Test Scenarios Checklist

* Scenario 1 — DLP Policy Change → Query (B) should show activity and optionally trigger alert.
* Scenario 2 — Mass App Deletion → Query (C) surfaces actor & environment; alert + playbook execute.
* Scenario 3 — Disable/Delete Flows → Query (D) lists operations; Teams notification received.
* Scenario 4 — Dataverse Bulk Deletes → Query (F) catches spike; incident created.
* Scenario 5 — Unusual Flow Run Spike → Query (E) flags spike > baseline.

# Troubleshooting

* Wait up to 60 minutes for ingestion; confirm auditing and connector status.
* Verify permissions (Sentinel/Workspace RBAC, Dataverse admin).
* Tune thresholds and add allowlists to reduce noise.

## CLEAN UP

* Disable/delete rules and playbooks; remove test artifacts in non‑production.