GitHub - microsoft/Microsoft-365-Defender-Hunting-Queries: Sample queries for Advanced hunting in Microsoft 365 Defender

By tali-ash

Archived: 2026-04-06 00:08:07 UTC

page_type	sample
languages	kusto
products	Microsoft 365 Defender
description	Microsoft 365 Defender repository for Advanced Hunting

Deprecated

We moved to **Microsoft threat protection community**, the unified Microsoft Sentinel and Microsoft 365 Defender repository.

Microsoft SIEM and XDR Community provides a forum for the community members, aka, Threat Hunters, to join in and submit these contributions via GitHub Pull Requests or contribution ideas as GitHub Issues. Hunting queries for Microsoft 365 Defender will provide value to both Microsoft 365 Defender and Microsoft Sentinel products, hence a multiple impact for a single contribution. These contributions can be just based on your idea of the value to enterprise your contribution provides or can be from the GitHub open issues list or even enhancements to existing contributions.

- **Contribute** your queries to the **Microsoft 365 Defender folder** in the Hunting Queries section.
- Specifics on what is required for Hunting queries is in the **Query Style Guide**.
- Webcasts content can be found in the **Tutorials folder**.
- Power BI example can be found in the **Tools folder**.
