


M365 SATURDAY BANGALORE 2022



 @m365blr #M365BLR

 www.m365event.com

3 December, 2022

Quest

PENTHARA
TECHNOLOGIES

JPOWER4



Microsoft

Athen.



RAPID CIRCLE

SOHO
DRAGON

ATNA
TECHNOLOGIES

A One Day In Person Event

- Hands on sessions by experts and community leaders
- Deep-dive into Microsoft 365 Services
- Focus on:
 - Microsoft Teams
 - Power Platform
 - SharePoint

Win exiting prizes!



Lenovo M10 FHD
Plus (2nd Gen)



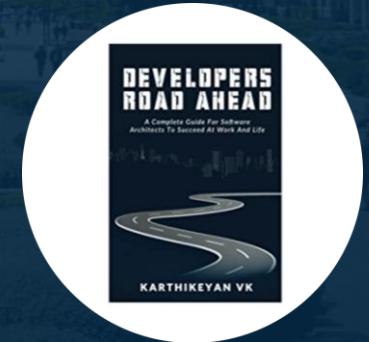
JBL Tune 125TWS



boAt Blaze Smart Watch



Cool Water Bottle



Developer Road Ahead

SUPPORT A CAUSE



“Giving is Receiving”



Support 'Scope for Change' to create more impact and touch the lives of more underprivileged students.

DONATE NOW!

Quest

PENTHARA
TECHNOLOGIES

JPOWER4

 Microsoft

Athen.

 RAPID CIRCLE

SOHO
DRAGON

ATNA
TECHNOLOGIES

Session 3

Advance Hunting with Defender Portal

10:00 AM – 10:45 AM IST

SPEAKERS PANEL



Samik Roy

MCT, Lead Cloud Developer

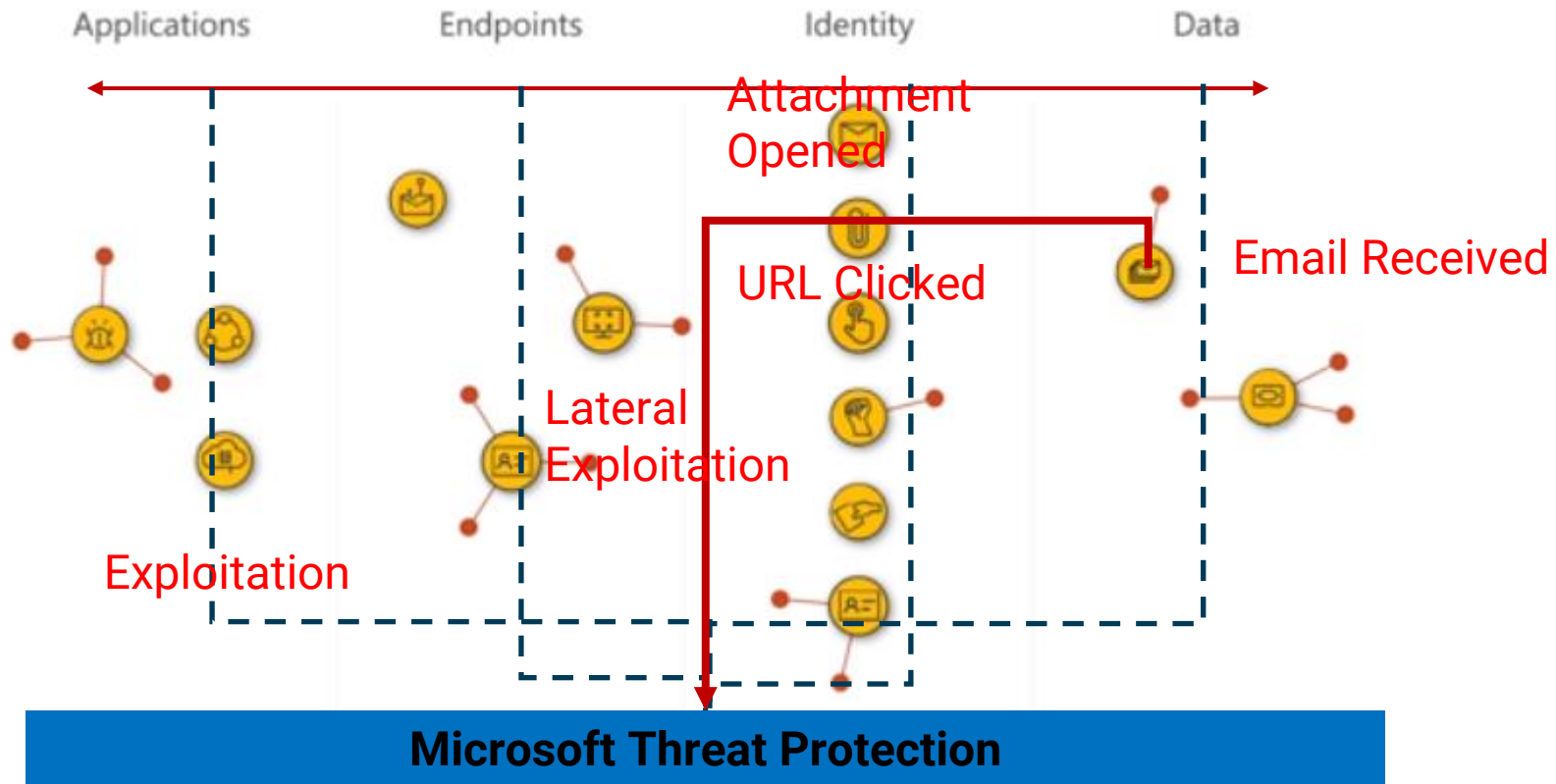
<https://github.com/samikroy>

<https://www.linkedin.com/in/roysamik/>

Agenda

- Why Defender
- How to use the portal for hunting
- Demo
- Where to go for more
- QnA

Why Defender



The Portal

Advance
Hunting

The screenshot shows the Microsoft 365 Defender portal. The left sidebar contains a navigation menu with options like Home, Incidents & alerts, Hunting, Advanced hunting, Custom detection rules, Actions & submissions, Threat analytics, Secure score, Learning hub, Trials, Partner catalog, Assets, Endpoints, Email & collaboration, Cloud apps, Reports, Audit, Health, Permissions, and Settings. The 'Incidents & alerts' and 'Hunting' options are highlighted with a red box, and a red arrow points to them from the text 'Advance Hunting'. The main content area is titled 'Advanced Hunting' and includes a 'New query' button and a 'Create new' dropdown. Below this, there are sections for Alerts, Apps & identities, Email & collaboration, and Devices, each with a list of event types. The right sidebar contains a 'Query' section with a 'Run query' button and a 'Save' button. Below this, there are sections for 'Getting Started' and 'Results', each with a 'Run basic queries' and 'Run advanced queries' button. The bottom of the page features a dark blue banner with the SPS EVENTS logo, the text 'M365 SATURDAY BANGALORE 2022', and the website 'www.m365event.com'.

The Portal

Left
Navigation

The screenshot displays the Microsoft Sentinel Advanced Hunting console. On the left, a 'Left Navigation' pane is highlighted with a red box, showing a tree view of data sources under the 'Advanced Hunting' header. The tree includes categories like 'Alerts', 'Apps & identities', 'Email & collaboration', and 'Devices', each with expandable sub-items. A red arrow points from the 'Left Navigation' text to this pane. The main area is the 'Query Console', also highlighted with a red box and labeled with a red arrow. It features a top bar with 'Run query', 'Save', and 'Share link' buttons, along with a 'Last 30 days' filter and a 'Create detection rule' button. Below this is a 'Query' input area with a placeholder message: 'Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.' and a 'Don't want to see it again' button. The bottom of the console shows a 'Getting Started' section with 'Run basic queries' and 'Run advanced queries' links, and a 'Results' section with 'Basic queries' and 'Advanced queries' links. A table at the bottom provides details for these queries, including a 'Limit' of 10 rows and a 'Summarize' option for daily event counts over 7 days.

Advanced Hunting

New query + Create new

Schema Functions Queries

Alerts

- AlertInfo
- AlertEvidence

Apps & identities

- IdentityInfo
- IdentityLogonEvents
- IdentityQueryEvents
- IdentityDirectoryEvents
- CloudAppEvents
- AADSpnSignInEventsBeta
- AADSignInEventsBeta

Email & collaboration

- EmailEvents
- EmailAttachmentInfo
- EmailUrlInfo
- EmailPostDeliveryEvents
- UrlClickEvents

Devices

- DeviceInfo

Query Console

Run query Save Share link Last 30 days Create detection rule

Query

Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC. Don't want to see it again

1

Getting Started Results

Run basic queries

Basic queries

Limit Shows 10 rows from the specified table

Run advanced queries

Advanced queries

Summarize Shows the number of events each day in the past 7 days

Why Defender



The Page

Advanced Hunting

[Help resources](#) [Query resources report](#) [Schema reference](#) [Try the new Hunting page](#)

[New query](#) [+ Create new](#)

[Schema](#) [Functions](#) [Queries](#) [...](#)

Alerts

- AlertInfo
- AlertEvidence

Apps & identities

- IdentityInfo
- IdentityLogonEvents
- IdentityQueryEvents
- IdentityDirectoryEvents
- CloudAppEvents
- AADSpnSignInEventsBeta
- AADSignInEventsBeta

Email & collaboration

- EmailEvents
- EmailAttachmentInfo
- EmailUrlInfo
- EmailPostDeliveryEvents
- UrlClickEvents

[Run query](#) [Save](#) [Share link](#)

[Last 7 days](#) [Create detection rule](#)

Query

Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.

[Don't want to see it again](#)

1




[Getting Started](#) [Results](#)


[Run basic queries](#)


[Run advanced queries](#)


The Left Nav


Advanced Hunting


 New query  Create new 


Schema Functions Queries ... 

Alerts 




Apps & identities 


Email & collaboration 



Devices 



Threat & Vulnerability Management 



Advanced Hunting



 New query  Create new 

Schema **Functions** Queries ... 




  AssignedIPAddresses


  DeviceFromIP


  FileProfile




  SeenBy


Advanced Hunting

 New query  Create new 


Schema Functions **Queries** ... 

Shared queries 

  Suggested 

My queries 

Save a query in this folder so you can quickly access it later.

Community queries 

Demo

Query Builder

▶ Run query

Save

Share link

Sample size: 10k

Last 7 days

Endpoints

Remote administration from public IPs

All filters

Filter

Clear all

AND

Network events: **SourceIpType** equals Public

AND

OR

Remove subgroup

Network events: **DestinationP...** equals 22

OR

Network events: **DestinationP...** equals 3889

OR

Network events: **DestinationP...** equals 2900

OR

Network events: **DestinationP...** equals 23

OR

Network events: **DestinationP...** equals 161

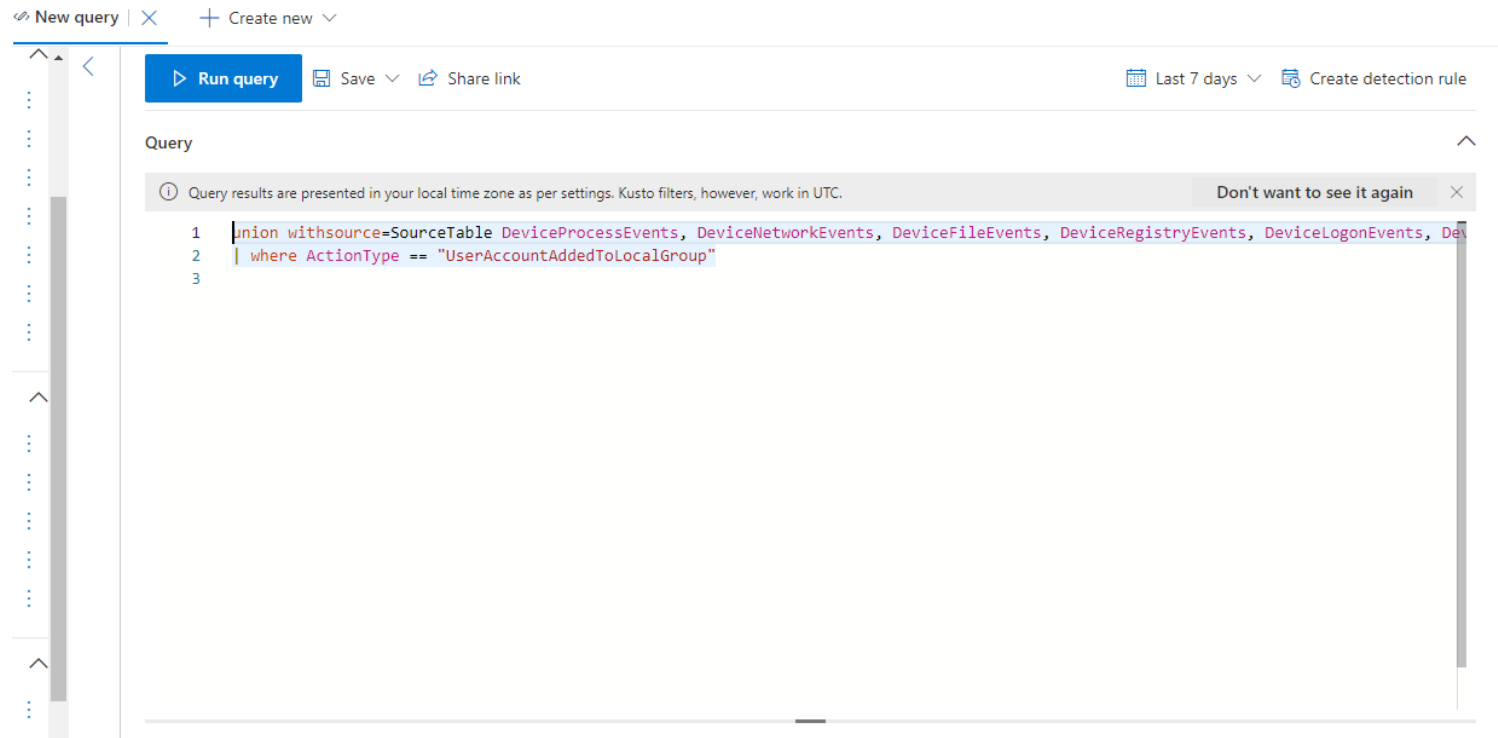
+ Add filter

Add subgroup

+ Add filter

Add subgroup

Query Editor



Questions



Thank You



Where To Go for More

- GitHub - <https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries>
- Webinars - <https://techcommunity.microsoft.com/t5/security-compliance-and-identity/recordings-security-community-webinars/ba-p/2865990>
- Licenses - <https://learn.microsoft.com/en-us/microsoft-365/security/defender/prerequisites?view=o365-worldwide>

A Big Thank You to all the Sponsors!

Diamond:

Quest

PENTHARA
TECHNOLOGIES

Platinum:

JPOWER4

Gold:

 Microsoft

 **RAPID CIRCLE**

Athen.

**SOHO
DRAGON**

ATNA
TECHNOLOGIES

Learning Partner:



Next Session

How to configure data loss prevention (DLP) policies in Power Platform

11:00 AM – 11:45 AM

SPEAKERS PANEL



Aakash Maurya

Sr SharePoint Developer &
Team Lead