KQL Café | June 2024

Your | hosts

Alex Verboon

https://twitter.com/alexverboon

https://www.linkedin.com/in/verboonalex/

https://github.com/alexverboon

https://www.verboon.info/

Gianni Castaldi

https://twitter.com/castello_johnny

https://www.linkedin.com/in/giannicastaldi/

https://github.com/KustoKing

https://www.kustoking.com/

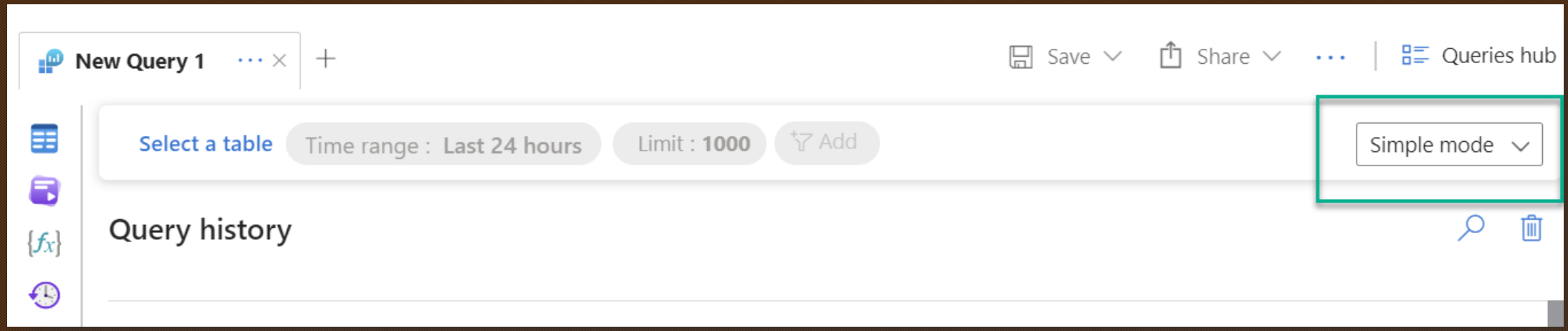

KQL|Cafe

Show | Agenda

Welcome
What is new/updates for KQL
Our guest: Nicola Suter
Learning KQL
What did you do with KQL this month?

News

Analyze data using Log Analytics Simple mode (Preview)
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-simple-mode



News

Definitive Guide to KQL Book - Microsoft Employee Submitted Queries

https://github.com/KQLMSPress/definitive-guide-kql/tree/main/Extra%20Microsoft%20Employee%20Submitted%20Queries

Monitoring Cosmos DB's request unit consumption.
Identifying top N queries by consumption in Cosmos DB.
Checking for requests that are throttled in Cosmos DB.
Checking for antivirus exclusions.
Identifying applications using auto proxy (WPAD).
Detecting changes to evade detection.
Analyzing Microsoft Graph API usage patterns.
Analyzing traffic patterns to Microsoft Graph APIs.
Monitoring ID Governance in Microsoft Entra for usage patterns.
Visualizing authentication method use over time.
Understanding administrative activities.
Monitoring short-lived connections in PostgreSQL.
Monitoring failed login attempts in PostgreSQL.
Resource utilization monitoring in PostgreSQL.
Summarizing sign-ins via iOS and macOS SSO Extensions.
Searching for MFA phone number changes using regex.
Tracking dynamic group membership changes.
Session breakdown by legacy vs modern TLS.
Understanding email authentication patterns for security.
Monitoring token protection impact and managing conditional access.
Analyzing Intune device management events and enrollments.
Monitoring failed operations and sign-in events.
Network traffic monitoring.
Identity governance operations.
Detecting suspicious activities and anomalies.
Identifying vulnerabilities and attack surfaces via IP range and CVE ID tracking.
Detecting administrative actions and user re-enabling.
High-risk sign-in patterns detection.
Reporting on antimalware versions.
Detecting email anomalies.
Performance troubleshooting for SQL servers.
Monitoring conditional access policy applications and failures.

News

Definitive Guide to KQL Book - Microsoft Employee Submitted Queries

https://github.com/KQLMSPress/definitive-guide-kql/tree/main/Extra%20Microsoft%20Employee%20Submitted%20Queries

Estefani Arroyo
Michael Barbush
Kristopher Bash
Bailey Bercik
Keith Brewer
Chad Cox
Varun Dhawan
Michael Epping
Marius Folling
Cosmin Guilman
Tim Haintz
Franck Heilmann
Mark Hopper
Laura Hutchcroft
Jef Kazimer
Corissa Koopmans
Gloria Lee
Michael Lindsey
Rudnei Oliveira
Razi Rais
Yong Rhee
Sravani Salura
Krishna Venkit

News

Microsoft Defender for Endpoint Advanced Hunting and Application Control for Business – WDACConfig

https://www.youtube.com/watch?app=desktop&si=tJbFbzRJNy79lUo7&v=oyz0jFzOOGA&feature=youtu.be

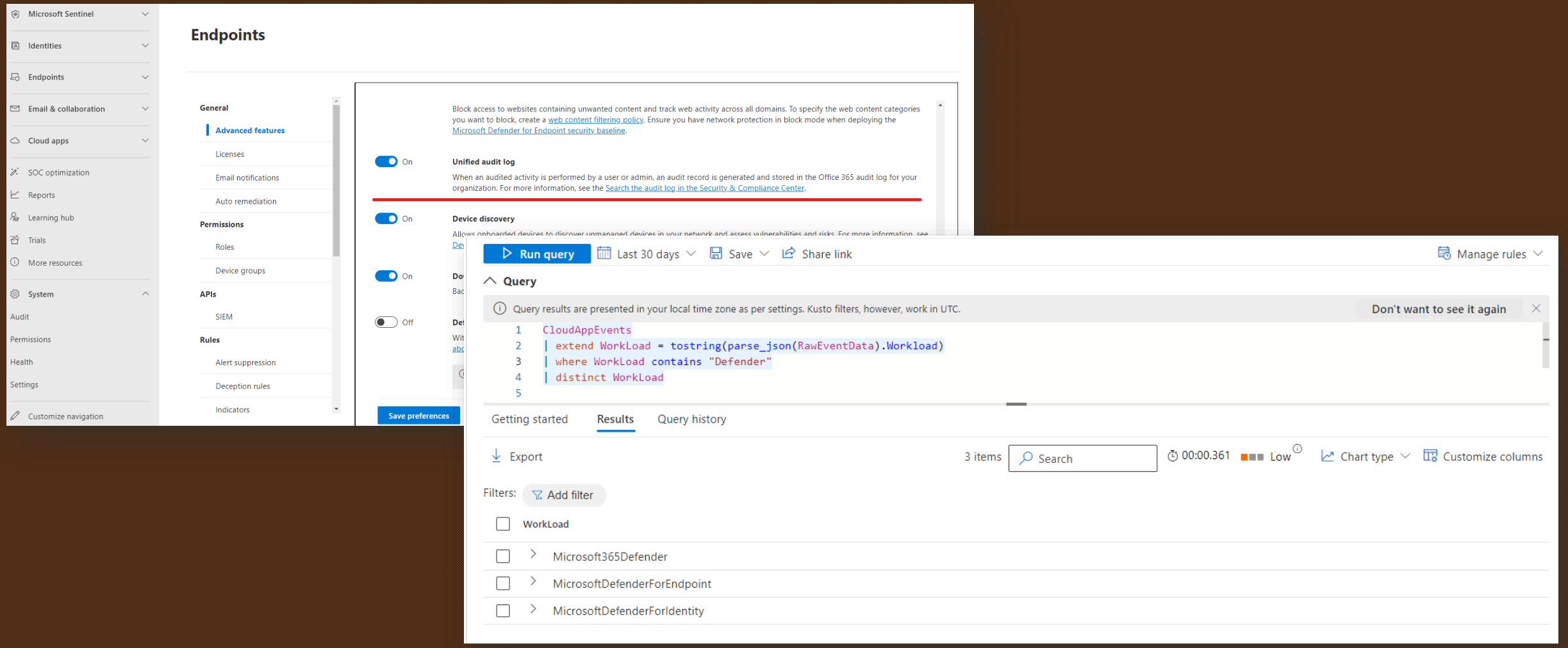
https://github.com/HotCakeX/Harden-Windows-Security

How to Use Microsoft Defender for Endpoint Advanced Hunting With WDAC App Control - SpyNetGirl Blog

News

Audit Defender XDR Activities

https://kqlquery.com/posts/audit-defender-xdr/



News

Detect suspicious processes running on hidden desktops
https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/detect-suspicious-processes-running-on-hidden-desktops/ba-p/4072322

Our Guest: Michalis Michalos

https://www.linkedin.com/in/mmihalos/

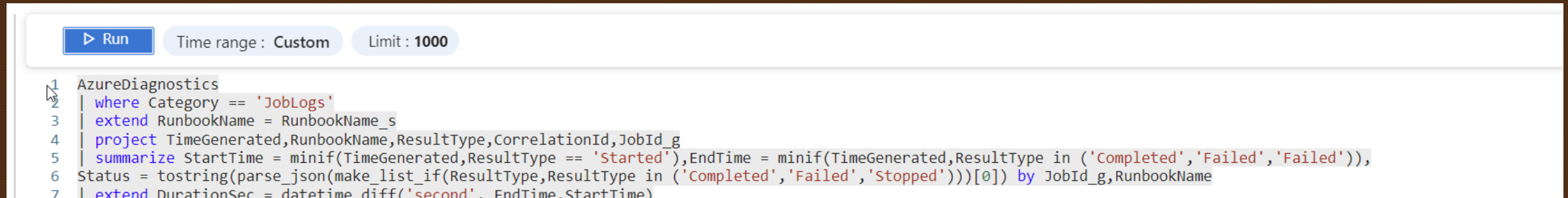
Learn KQL

- * in project

What did you do with KQL this month?

- Automation Account Runbook logs

```
AzureDiagnostics
| where Category == 'JobLogs'
| extend RunbookName = RunbookName_s
| project TimeGenerated,RunbookName,ResultType,CorrelationId,JobId_g
| summarize StartTime = minif(TimeGenerated,ResultType == 'Started'),EndTime =
minif(TimeGenerated,ResultType in ('Completed','Failed','Failed')),
Status = tostring(parse_json(make_list_if(ResultType,ResultType in ('Completed','Failed','Stopped')))[0])
by JobId_g,RunbookName
| extend DurationSec = datetime_diff('second', EndTime,StartTime)
| join kind=leftouter (AzureDiagnostics
| where Category == "JobStreams"
| where StreamType_s == "Error"
| summarize TotalErrors = dcount(StreamType_s) by JobId_g, StreamType_s)
on $left. JobId_g == $right. JobId_g
| extend HasErrors = iff(StreamType_s == 'Error',true,false)
| project StartTime, EndTime, DurationSec,RunbookName,Status,HasErrors,TotalErrors,JobId_g
```



What did you do with KQL this month?

- JA3

What did you do with KQL this month?

- | where InternetFacingReason == "ExternalNetworkConnection“

https://github.com/alexverboon/Hunting-Queries-Detection-Rules/blob/main/Defender%20For%20Endpoint/MDE-InternetFacing.md

Thanks for attending