

Session 5 | KQL



Session 5 | KQL – The Scan

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/>

Show | Agenda

Welcome

What's new in KQL

Working with IOCs

Learning KQL

KQL Tools

Our KQL Guest

What did you do with KQL this month?

Show | Agenda

Welcome

What's new in KQL

~~Working with IOCs~~

Learning KQL

~~KQL Tools~~

Our KQL Guest

What did you do with KQL this month?

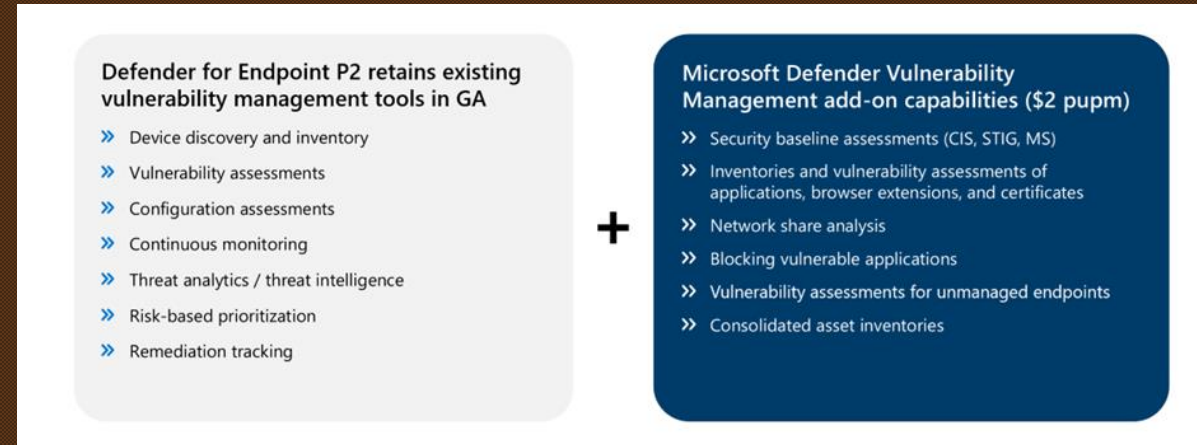
Microsoft Defender Vulnerability Management

DeviceBaselineComplianceProfiles
DeviceBaselineComplianceAssessment
DeviceBaselineComplianceAssessmentKB

DeviceTvmSecureConfigurationAssessment
DeviceTvmSecureConfigurationAssessmentKB

DeviceTvmCertificateInfo

DeviceTvmBrowserExtensions
DeviceTvmBrowserExtensionsKB



Guest Speaker

Mehmet Ergene

Today's | Guest Mehmet Ergene



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

<https://twitter.com/Cyb3rMonk>

<https://posts.bluraven.io/>

What did you do with KQL

File Share auditing

What did you do with KQL

Create Data Collection Rule

Data collection rule management

Basics Resources Collect Review + create





Select which events to stream. ⓘ

☐ All Security Events ☐ Common ☐ Minimal ☒ Custom

Each box can contain up to 20 expressions

Add

Event logs

| | |
|---|---|
| Security!*[System[(EventID=4663)]] and *[EventData[Data[@Name='AccessMask']='0x2']] |  |
| Security!*[System[(EventID=4663)]] and *[EventData[Data[@Name='AccessMask']='0x4']] |  |
| Security!*[System[(EventID=4663)]] and *[EventData[Data[@Name='AccessMask']='0x6']] |  |
| Security!*[System[(EventID=4907)]] |  |

Questions?

Thanks for attending

