



Shedding Light to Uncovered Vulnerabilities with the Defender Vulnerability Management Add-on

Microsoft 365 Security & Compliance User Group

Michalis Michalos, June 25th 2025

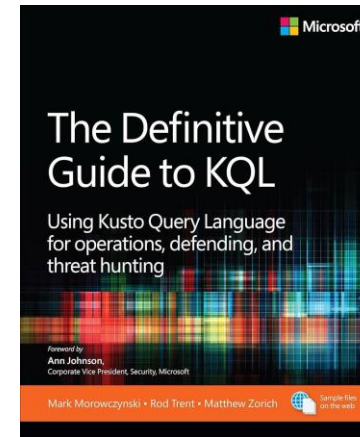
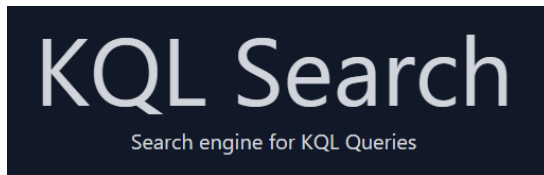
About me

- Currently working as Cyber Resilience & Intelligence Manager
- Over 12 years of experience in ICT
- Working in Cybersecurity since 2019
- Electrical Engineer BSc, MSc, MBA
- Father of 2, lifetime Scout, own a wine cooler, and a watch enthusiast



Projects

- Blogging at michalos.net
- github.com/cyb3rmik3/KQL-threat-hunting-queries
- github.com/cyb3rmik3/MDE-DFIR-Resources
- github.com/christosgalano/sKaleQL
- Featured in:



Agenda

- What is MDVM
- MDVM Flavors
- MDVM Licensing
- Deep dive in add-on capacity
- KQL tables available
- Closing remarks



What is MDVM?

Microsoft Defender Vulnerability Management (MDVM) is a comprehensive security solution that helps organizations **discover, assess, prioritize, and remediate** vulnerabilities and misconfigurations across their environment.

It provides real-time **asset visibility, intelligent assessments**, and built-in **remediation tools** to **reduce cyber risk**.



MDVM Flavors



MDVM Premium



MDVM Core

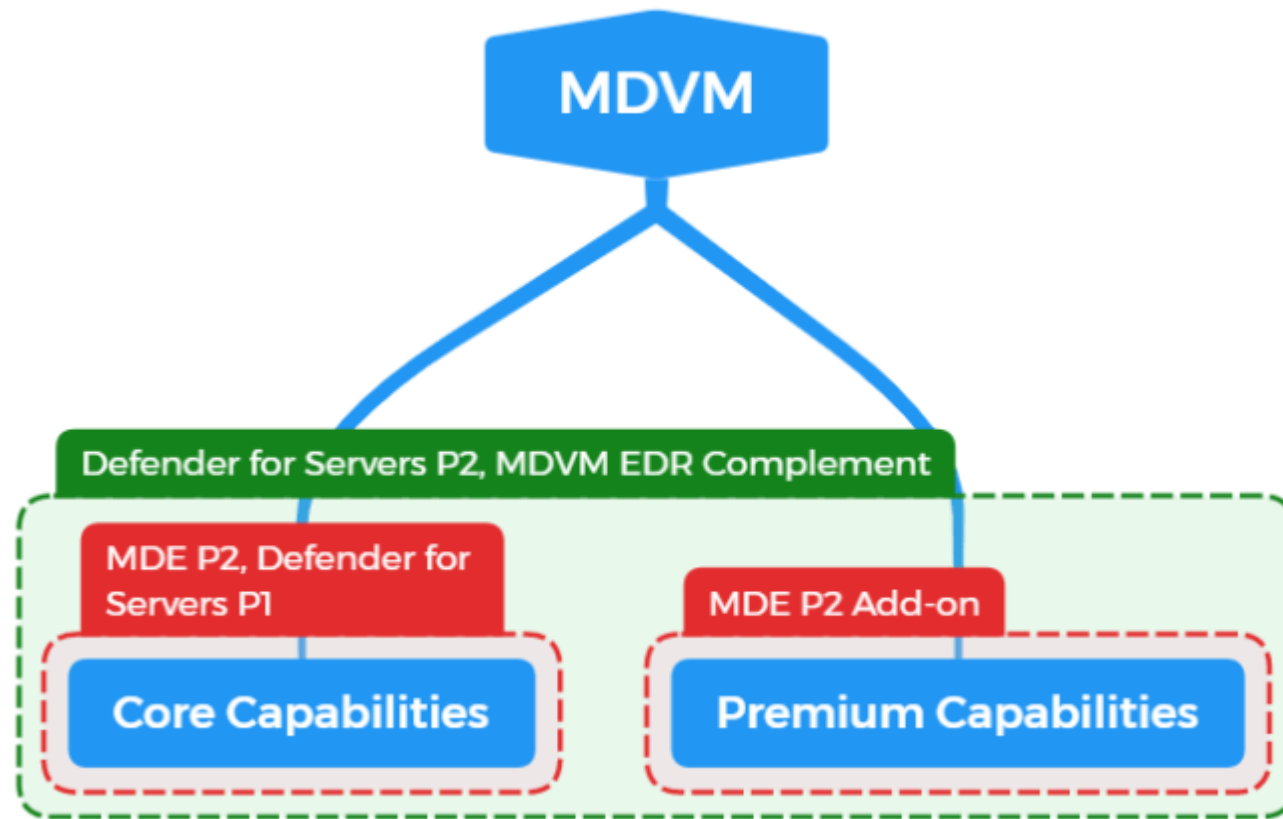
MDVM Core

- Device discovery & Inventory
- Vulnerability & Configuration Assessment
- Risk based prioritization
- Continuous monitoring and remediation tracking
- Software inventory & usage insights

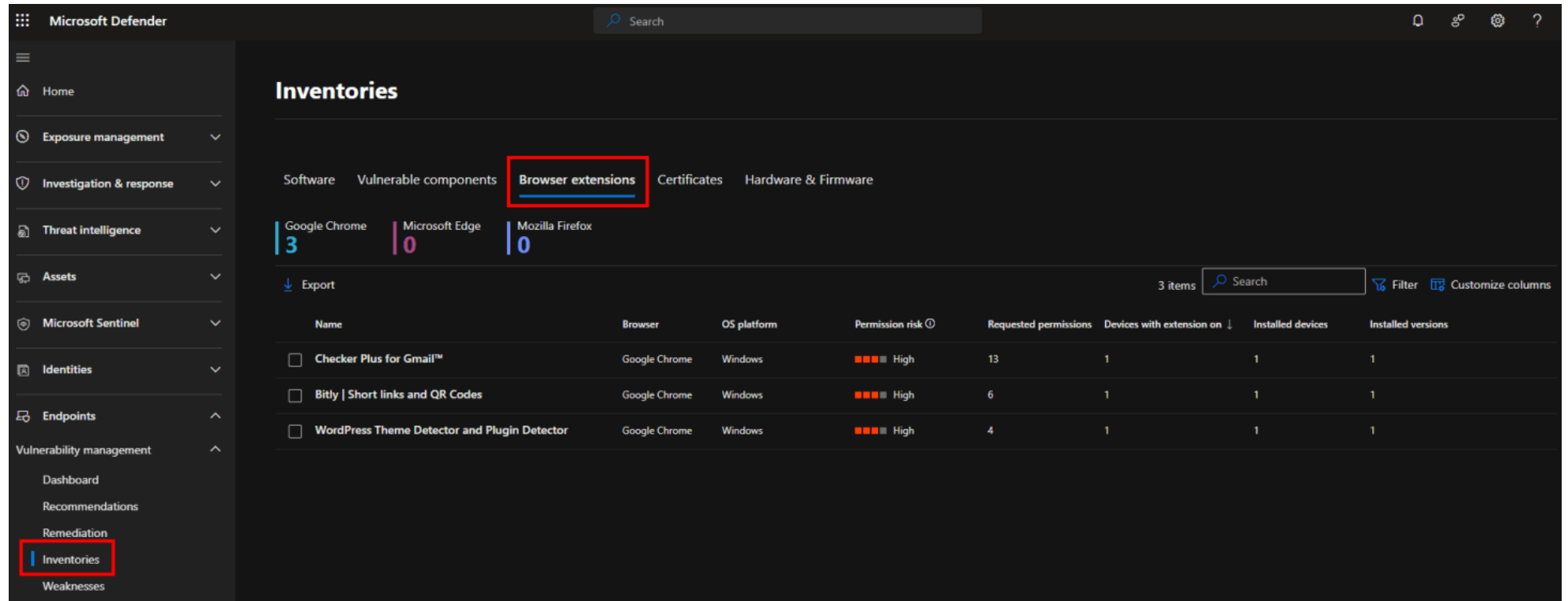
MDVM Premium

- Security baselines assessment
- Block vulnerable applications
- Browser extensions assessment
- Digital certificate assessment
- Network share analysis
- Hardware and firmware assessment

MDVM Licensing



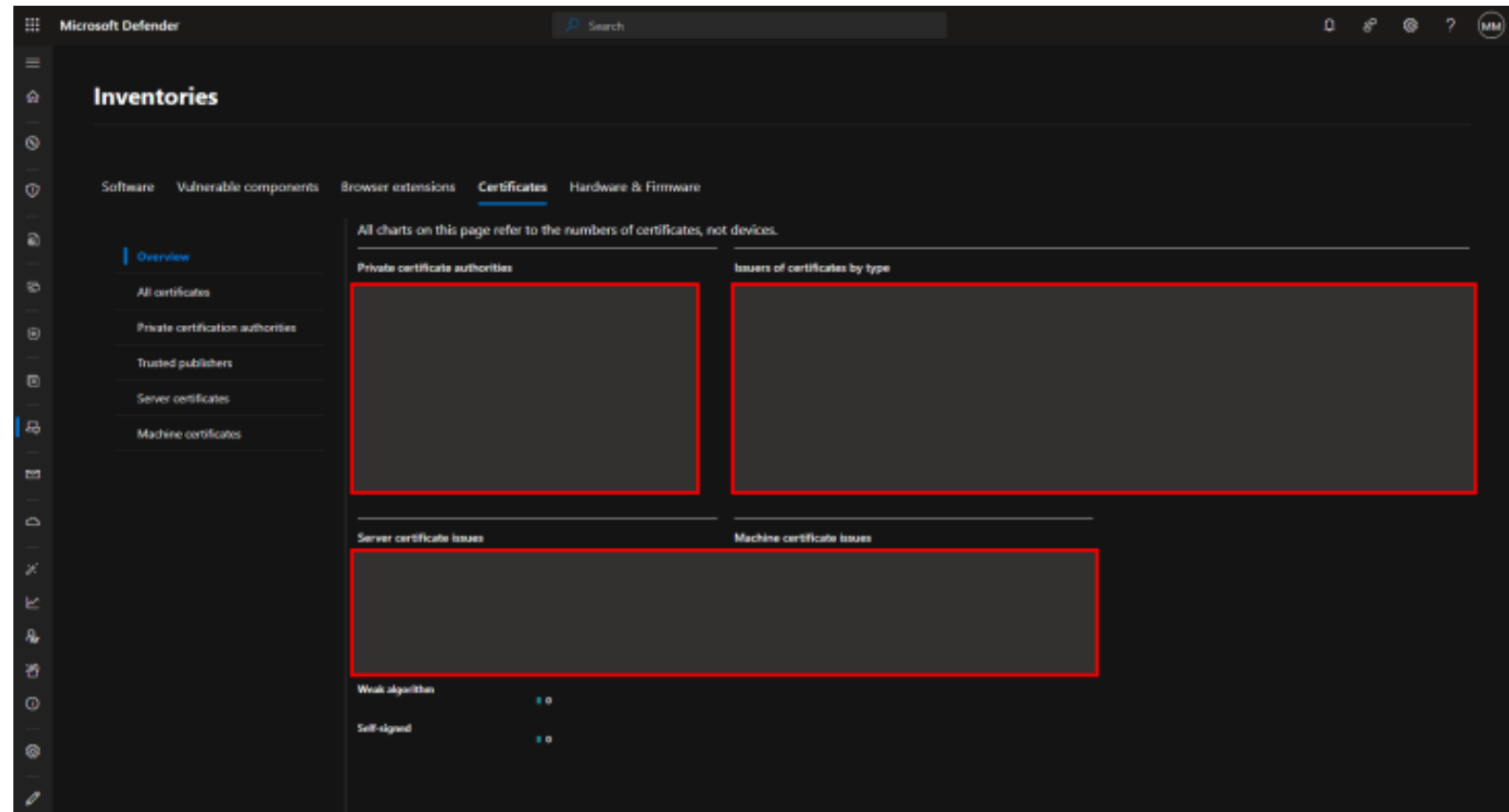
MDVM – Browser extensions



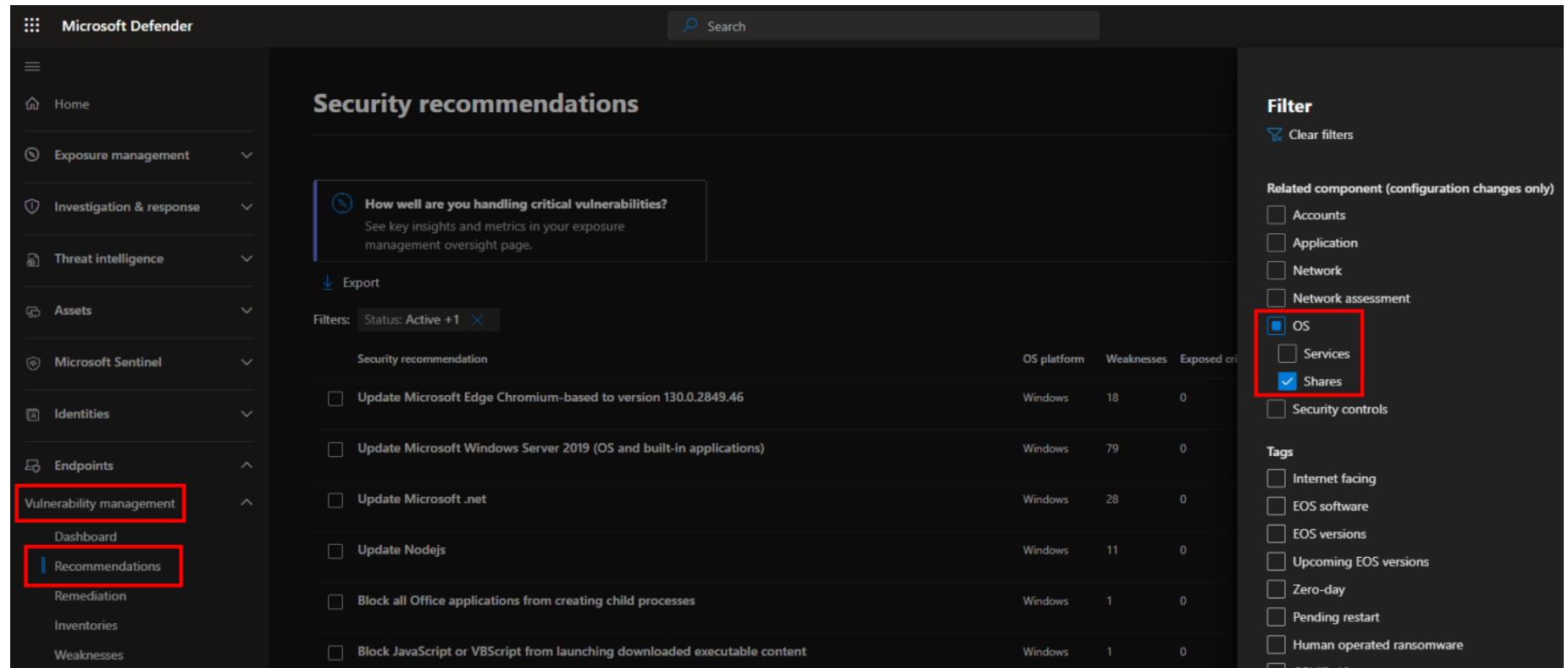
The screenshot displays the Microsoft Defender web interface. On the left, a navigation sidebar lists various security tools, with 'Inventories' highlighted. The main content area, titled 'Inventories', shows tabs for 'Software', 'Vulnerable components', 'Browser extensions' (which is selected and highlighted with a red box), 'Certificates', and 'Hardware & Firmware'. Below the tabs, there are counts for Google Chrome (3), Microsoft Edge (0), and Mozilla Firefox (0). A table below lists the installed browser extensions, with columns for Name, Browser, OS platform, Permission risk, Requested permissions, Devices with extension on, Installed devices, and Installed versions. Three extensions are listed: 'Checker Plus for Gmail™', 'Bitly | Short links and QR Codes', and 'WordPress Theme Detector and Plugin Detector', all with a 'High' permission risk.

Name	Browser	OS platform	Permission risk ⓘ	Requested permissions	Devices with extension on ↓	Installed devices	Installed versions
<input type="checkbox"/> Checker Plus for Gmail™	Google Chrome	Windows	High	13	1	1	1
<input type="checkbox"/> Bitly Short links and QR Codes	Google Chrome	Windows	High	6	1	1	1
<input type="checkbox"/> WordPress Theme Detector and Plugin Detector	Google Chrome	Windows	High	4	1	1	1

MDVM – Digital certificates



MDVM – Network Shares



The screenshot displays the Microsoft Defender Security Center interface. The left-hand navigation pane shows the 'Vulnerability management' section selected, with the 'Recommendations' sub-section highlighted. The main content area is titled 'Security recommendations' and displays a list of security recommendations. The right-hand pane shows the 'Filter' section, where the 'Shares' filter is selected under the 'Related component (configuration changes only)' category.

Security recommendations

How well are you handling critical vulnerabilities?
See key insights and metrics in your exposure management oversight page.

Export

Filters: Status: Active +1

Security recommendation	OS platform	Weaknesses	Exposed cri
<input type="checkbox"/> Update Microsoft Edge Chromium-based to version 130.0.2849.46	Windows	18	0
<input type="checkbox"/> Update Microsoft Windows Server 2019 (OS and built-in applications)	Windows	79	0
<input type="checkbox"/> Update Microsoft .net	Windows	28	0
<input type="checkbox"/> Update Nodejs	Windows	11	0
<input type="checkbox"/> Block all Office applications from creating child processes	Windows	1	0
<input type="checkbox"/> Block JavaScript or VBScript from launching downloaded executable content	Windows	1	0

Filter

Clear filters

Related component (configuration changes only)

- ☐ Accounts
- ☐ Application
- ☐ Network
- ☐ Network assessment
- ☒ OS
- ☐ Services
- ☒ Shares
- ☐ Security controls

Tags

- ☐ Internet facing
- ☐ EOS software
- ☐ EOS versions
- ☐ Upcoming EOS versions
- ☐ Zero-day
- ☐ Pending restart
- ☐ Human operated ransomware
- ☐ CVE ID: 10

MDVM – Hardware & Firmware

Inventories

Software

Vulnerable components

Browser extensions

Certificates

Hardware & Firmware

Laptop, desktop and server models

Processors

Bios

Lenovo BIOS1

HP BIOS-

Dell BIOS-

Microsoft BIOS-

Export

1 of 1 selected

Search

Filter

Customize columns

Name	OS platform	Vendor	Weaknesses	Threats	Exposed devices
<input checked="" type="checkbox"/> <input type="text"/>	Windows	Insyde	0		0 / 1

Introduced KQL tables

DeviceTvmBrowserExtensions

DeviceTvmBrowserExtensionsKB

DeviceTvmCertificateInfo

DeviceTvmHardwareFirmware

DeviceTvmSecureConfigurationAssessmentKB (for network shares)

Closing remarks

Co-existing with Microsoft Security Exposure Management

Make sure to engage with vulnerabilities that are relevant

Prioritize, or die trying to assess, monitor and remediate

Automate as much as you can





Thank you

michalos.net

x.com/cyb3rmik3

linkedin.com/in/mmihalos