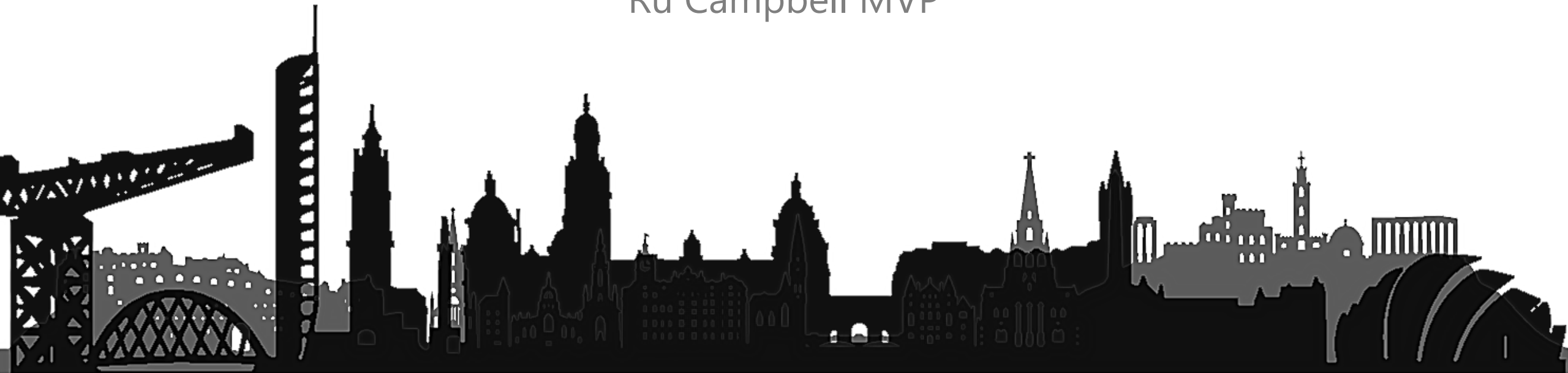




Become a Defender for Endpoint Black Belt in 30 Minutes

Ru Campbell MVP



About me

Decade+ in IT

2x Microsoft MVP

Author, Mastering Microsoft 365 Defender (2023)

Microsoft 365 Security & Compliance User Group

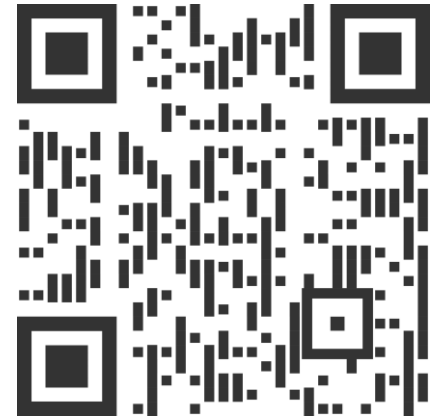
Microsoft Security Solutions Architect, Threatscape



@rucam365



Ru Campbell



Show of hands...

Who knows EDR is?

Who knows XDR is?

Who uses Microsoft Defender for Endpoint?

Who uses another EDR/XDR?



Part of a bigger picture

Microsoft 365 Defender

security.microsoft.com

Microsoft
Defender for
Endpoint

MDE

Microsoft
Defender
Vulnerability
Management

MDVM

Microsoft
Defender for
Office 365

MDO

Microsoft
Defender for
Identity

MDI

Microsoft
Defender for
Cloud Apps

MDA

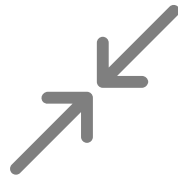


Layered approach to endpoint protection

Next generation
protection
and
firewall



Attack surface
reduction



EDR
and
advanced hunting



Auto investigation
and
remediation



Threat and
vulnerability
management



Windows, macOS, Linux servers, Android phones, iOS/iPadOS



Different SKUs

Plan 2	The whole shebang	E5, E5 Security, Standalone
Plan 1	Limited capabilities	E3
Defender for Business	Very close to Plan 2	Business Premium, Standalone



Different SKUs: Plan 2

Next generation
protection
and
firewall



Attack surface
reduction



EDR
and
advanced hunting



Auto investigation
and
remediation



Threat and
vulnerability
management

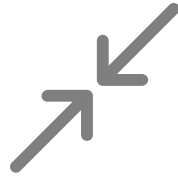


Different SKUs: Defender for Business

Next generation
protection
and
firewall



Attack surface
reduction



EDR
without
advanced hunting



Auto investigation
and
remediation



Threat and
vulnerability
management



Different SKUs: Plan 1

Next generation
protection
and
firewall



Attack surface
reduction
without telemetry



Deploying to clients

Decentralised – uses your existing management tool

Intune > ConfigMgr > GPO

Endpoint settings vs. service settings



<<

Home > Endpoint security



Endpoint security | Antivirus

...

<<

Overview

- Overview
- All devices
- Security baselines
- Security tasks

Manage

- Antivirus
- Disk encryption
- Firewall
- Endpoint detection and response
- Attack surface reduction
- Account protection
- Device compliance
- Conditional access

Monitor

- Assignment failures

Summary

Unhealthy endpoints

Active malware

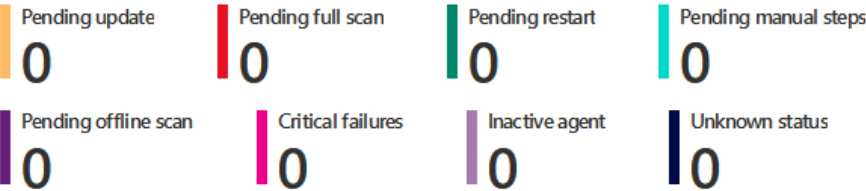
Reusable settings (preview)



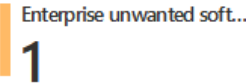
Refresh

Last refreshed on: 29/11/2022, 19:23:18

Unhealthy endpoints



Active malware across categories (Top 8)



AV policies

+ Create Policy Refresh Export

Deploying to clients

Decentralised – uses your existing management tool

Intune > ConfigMgr > GPO

Endpoint settings vs. service settings

Running modes – passive and active



Deploying to servers

Not included in user license - CSP must use Defender for Cloud (Arc!)

Microsoft Defender
for Cloud

MDC

Microsoft Defender
for Servers P1 / P2

MDS

Microsoft Defender
for Endpoint P2

MDE

You can still manage policy using Intune... with limitations



Black belt practices – deployment and config














Black belt practices – deployment and config

Cloud delivered protection
with block at first sight





-  Home
-  Dashboard
-  All services
-  Devices
-  Apps
-  Endpoint security
-  Reports
-  Users
-  Groups
-  Tenant administration
-  Troubleshooting + support

Edit profile



- 1 Configuration settings
- 2 Review + save

Settings

 Search for a setting

^ Cloud protection

Turn on cloud-delivered protection ⓘ

Yes

⌵

Cloud-delivered protection level ⓘ

High

⌵

Defender Cloud Extended Timeout In Seconds ⓘ

50

✓

⌵ Microsoft Defender Antivirus Exclusions

⌵ Real-time protection

⌵ Remediation

Black belt practices – deployment and config

Cloud delivered protection
with block at first sight

Tamper protection + disable
local admin merge





Settings > Endpoints

Endpoints

General

Advanced features

Licenses

Email notifications

Auto remediation

Permissions

Roles

Device groups



On

Tamper protection

Stop unwanted changes to your security solution and its essential functions. With tamper protection, malicious apps are prevented from turning off security features like virus & threat protection, behavior monitoring, cloud-delivered protection, and more. [Learn about tamper protection requirements](#)



On

Show user details

Enables displaying user details: picture, name, title, department, stored in Azure Active Directory.



On

Skype for business integration

Enables 1-click communication with users.



Pending

Microsoft Defender for Identity integration

Retrieves enriched user and device data from [Microsoft Defender for Identity](#) and forwards Microsoft Defender for Endpoint signals, resulting in better visibility, additional detections, and efficient

Save preferences



Black belt practices – deployment and config

Cloud delivered protection
with block at first sight

Tamper protection + disable
local admin merge

EDR in block mode





Settings > Endpoints

Endpoints

General

Advanced features

Licenses

Email notifications

Auto remediation

Permissions

Roles

Device groups



On

Enable EDR in block mode

When turned on, Microsoft Defender for Endpoint leverages behavioral blocking and containment capabilities by blocking malicious artifacts or behaviors observed through post-breach endpoint detection and response (EDR) capabilities. This feature does not change how Microsoft Defender for Endpoint performs detection, alert generation, and incident correlation. To get the best protection, make sure to apply [security baselines in Intune](#). See [EDR in block mode](#) for more details.



On

Automatically resolve alerts

Resolves an alert if Automated investigation finds no threats or has successfully remediated all malicious artifacts.



On

Allow or block file

Make sure that Windows Defender Antivirus is turned on and the cloud-based protection feature is enabled in your organization to use the allow or block file feature.

Save preferences



Black belt practices – deployment and config

Cloud delivered protection
with block at first sight

Update hourly

Tamper protection + disable
local admin merge

EDR in block mode





Edit profile ...



- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

^ Updates

Enter how often (0-24 hours) to check for security intelligence updates ⓘ ✓

Define file shares for downloading definition updates ⓘ 0 items ▾

Define the order of sources for downloading definition updates ⓘ 2 items ▴

+ Add Delete

☐ Order of sources for downloading definition updates

☐ Microsoft update server ...

☐ MMPC ...

▽ User experience

Black belt practices – deployment and config

Cloud delivered protection
with block at first sight

Update hourly

Tamper protection + disable
local admin merge

EnableFileHashComputation

EDR in block mode



- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Settings picker

Use commas "," among search terms to lookup settings by their keywords

Search

+ Add filter

Browse by category

Administrative Templates\Windows Components\Microsoft Defender Antivirus\MpEngine

1 results in the "MpEngine" subcategory

Select all these settings

Setting name

<input checked="" type="checkbox"/>	Enable file hash computation feature	
-------------------------------------	--------------------------------------	--

Black belt practices – deployment and config

Cloud delivered protection
with block at first sight

Tamper protection + disable
local admin merge


EDR in block mode


Update hourly


EnableFileHashComputation


Improve telemetry with audit
settings





- <<
-  Home


 Dashboard


 All services


 Devices


 Apps


 Endpoint security

 Reports

 Users

 Groups

 Tenant administration

 Troubleshooting + support

... > Windows | Configuration profiles > ALL - Improve MDE Telemetry >

Edit profile - ALL - Improve MDE Telemetry



Settings catalog

Audit Security Group Management ⓘ	Success+Failure	⌵	⊖
Audit Security System Extension ⓘ	Success+Failure	⌵	⊖
Audit User Account Management ⓘ	Success+Failure	⌵	⊖
Detailed Tracking Audit PNP Activity ⓘ	Success+ Failure	⌵	⊖
Object Access Audit File System ⓘ	Success+ Failure	⌵	⊖
Object Access Audit Filtering Platform Connection ⓘ	Failure	⌵	⊖
Object Access Audit Filtering Platform Packet Drop ⓘ	Failure	⌵	⊖

Black belt practices – deployment and config

Cloud delivered protection
with block at first sight

Tamper protection + disable
local admin merge

EDR in block mode

Update hourly

EnableFileHashComputation

Improve telemetry with
undocumented audit settings

Consider tiering implications





Settings > Endpoints

Endpoints

General

Advanced features

Licenses

Email notifications

Auto remediation

Permissions

Roles

Device groups



On

Live Response

Allows users with appropriate RBAC permissions to investigate devices that they are authorized to access, using a remote shell connection.



On

Live Response for Servers

Allows users with Live Response privileges to connect remotely to servers (Windows Server or Linux devices) that they are authorized to access.



On

Live Response unsigned script execution

Enables using unsigned PowerShell scripts in Live Response.



Off

Restrict correlation to within scoped device groups

When this setting is turned on, alerts are correlated into separate incidents based on their scoped device group. By default, incident correlation happens across the entire tenant scope.

Save preferences



Black belt practices – operations

Exclusions: minimal as possible, specific as possible



Black belt practices – operations

Exclusions: minimal as possible, specific as possible

Audit > warn > block





- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Edit profile



Attack Surface Reduction Rules

Block persistence through WMI event subscription ⓘ

Block

▼

Block credential stealing from the Windows local security authority subsystem (lsass.exe) ⓘ

Warn

▼

Block Adobe Reader from creating child processes ⓘ

Warn

▼

Block Office applications from injecting code into other processes ⓘ

Warn

▼

Block Office applications from creating executable content ⓘ

Warn

▼

Block all Office applications from creating child processes ⓘ

Warn

▼

Black belt practices – operations

Exclusions: minimal as possible, specific as possible

Audit > warn > block

Troubleshooting mode





Devices >



Active

Device summary

Tags

No tags found

Security Info

Open incidents

2

Active alerts ①

4

Exposure level ①

⚠ Medium

Overview

Alerts

Timeline

Security recommendations

Active alerts

180 days

Risk level:
Medium

4 active alerts

in 2 incidents



■ Medium (2) ■ Low (1) ■ Informational (1)

Security assessments

Exposure level:
Medium

65 active security recommendations

Discovered vulnerabilities

■ High (4) ■ Medium (1)

See all recommendations

See all users

Manage device

- Report device inaccuracy
- Restrict app execution
- Run antivirus scan
- Collect investigation package
- Initiate Live Response Session
- Initiate Automated Investigation
- Ask Defender Experts
- Device value
- Action center
- Exclude device
- Turn on troubleshooting mode

Black belt practices – operations

Exclusions: minimal as possible, specific as possible

Audit > warn > block

Troubleshooting mode

Performance analyser



```
PS C:\WINDOWS\system32> Get-MpPerformanceReport -Path .\Recording.ETL -TopFiles 3 -TopScansPerFile 10
```

TopFiles

=====

Count	TotalDuration	MinDuration	AverageDuration	MaxDuration	MedianDuration	Path
1	2463.5300ms	2463.5300ms	2463.5300ms	2463.5300ms	2463.5300ms	C:\Program Files\Google\Chrome\Application\107.0.5304.122\chrome.dll

Scans:

ScanType	Duration	Reason	SkipReason	Path
UfsFileScan	2463.5300ms		Not skipped	C:\Program Files\Google\Chrome\Application\107.0.5304.122\chrome.dll

Count	TotalDuration	MinDuration	AverageDuration	MaxDuration	MedianDuration	Path
9	1711.0047ms	1.2871ms	190.1116ms	499.9462ms	165.3723ms	C:\Program Files\Google\Chrome\Application\chrome.exe

Scans:

ScanType	Duration	Reason	SkipReason	Path
UfsFileScan	499.9462ms		Not skipped	C:\Program Files\Google\Chrome\Application\chrome.exe
UfsFileScan	447.6776ms		Not skipped	C:\Program Files\Google\Chrome\Application\chrome.exe
UfsFileScan	191.6241ms		Not skipped	C:\Program Files\Google\Chrome\Application\chrome.exe
UfsFileScan	178.3432ms		Not skipped	C:\Program Files\Google\Chrome\Application\chrome.exe
StreamScan	165.3723ms	OnOpen	Not skipped	C:\Program Files\Google\Chrome\Application\chrome.exe
UfsFileScan	163.8453ms		Not skipped	C:\Program Files\Google\Chrome\Application\chrome.exe
UfsFileScan	60.8138ms		Not skipped	C:\Program Files\Google\Chrome\Application\chrome.exe

Black belt practices – operations

Exclusions: minimal as possible, specific as possible

Custom hunting queries


Audit > warn > block


Troubleshooting mode

Performance analyser




 [Share link](#)

 Create detection rule \wedge


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

```
1 DeviceEvents
2     | where ActionType == "PowerShellCommand"
3     | project PowershellCommand=extractjson("$.Command", AdditionalFields, typeof(string)), InitiatingProcessCommandLine, InitiatingProcessParentFileName
4 // exceptions
5     | where InitiatingProcessParentFileName != "Deploy-Application.exe"
6 // monitored cmdlets
7     | where PowershellCommand has "Set-ExecutionPolicy"
8         or PowershellCommand has "Invoke-WebRequest"
9         or PowershellCommand has "Invoke-Shellcode"
```


 Export

2 items

🕒 0:0.125  Low ⓘ

 Customize columns

<input type="checkbox"/>	Timestamp	DeviceId	PowershellCommand	InitiatingProcessParentFile...	InitiatingProcessCommandL...	ReportId
<input type="checkbox"/>	30 Nov 2022 09:07:44	 3ee2fb289dbd7d25cf...	Invoke-WebRequest	explorer.exe	"powershell.exe"	521364
<input type="checkbox"/>	30 Nov 2022 08:12:55	 3ee2fb289dbd7d25cf...	Set-ExecutionPolicy	cmd.exe	powershell	518658



Advanc

Monitored

Query



Gett

↓ E

☐☐☐☐☐

- Alert details
- Impacted entities
- Actions
- Scope
- Summary

Provide the name of the alert and the information displayed with it.

Detection name *

Monitored cmdlets

Frequency *

Every hour

Alert title *

A monitored cmdlet was executed

Severity *

Info

Category *

Suspicious activity

Threat analytics report

Select Threat

Next


Cancel




Monitored


- ✓ Alert details
- ✓ Impacted entities
- Actions**
- Scope
- Summary

Choose an applicable action to take on entities found by your query.

- Devices** 

 - ☐ Isolate device
 - ☐ Collect investigation package
 - ☐ Run antivirus scan
 - ☒ Initiate investigation
 - ☐ Restrict app execution

Files 

Users 



Black belt practices – operations

Exclusions: minimal as possible, specific as possible

Custom hunting queries

Security recommendations

Audit > warn > block

Troubleshooting mode

Performance analyser



Security recommendations

The new Microsoft Defender Vulnerability Management add-on has been turned on for all devices, including servers, in your organization. [Learn more about this change](#)

Filter by device groups (3/3)

Export

83 items

Search

Filter

Customize columns

Filters: Status: Active +1

Security recommendation	OS platfo...	Weaknesses	Related component	Threats	Exposed devices	
<input type="checkbox"/> Update Microsoft Edge Chromium-based	Windows	7	Microsoft Edge Chromium-based		2 / 3	
<input type="checkbox"/> Update Rarlab Winrar to version 6.11.0.0	Windows	5	Rarlab Winrar		1 / 2	
<input type="checkbox"/> Update Microsoft Windows 10 (OS and built-in applications)	Windows	44	Microsoft Windows 10		1 / 2	
<input type="checkbox"/> Update Microsoft Windows 11 (OS and built-in applications)	Windows	264	Microsoft Windows 11		1 / 2	
<input type="checkbox"/> Uninstall Adobe Flash Player	Windows	506	Adobe Flash Player		1 / 1	
<input type="checkbox"/> Update Oracle Jre	Windows	140	Oracle Jre		1 / 1	
<input type="checkbox"/> Block JavaScript or VBScript from launching downloaded executable content	Windows	1	Security controls (Attack Surface Redu...		2 / 3	
<input type="checkbox"/> Block executable files from running unless they meet a prevalence, age, or trus...	Windows	1	Security controls (Attack Surface Redu...		2 / 3	
<input type="checkbox"/> Block process creations originating from PSEXEC and WMI commands	Windows	1	Security controls (Attack Surface Redu...		2 / 3	

Black belt practices – operations

Exclusions: minimal as possible, specific as possible

Audit > warn > block

Troubleshooting mode

Performance analyser

Custom hunting queries

Security recommendations

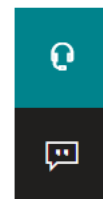
Device discovery



Configure how devices are discovered in your network. Device discovery improves your visibility over all the devices in your network so you can take action to protect them. Discovered devices appear in the device list.

Select the discovery mode being used by your onboarded devices. This controls the level of visibility you can get for unmanaged devices in your corporate network. [Learn more about it](#)

- ### Select which devices to use for Standard discovery
- ☒ All devices (recommended)
Enable Standard discovery for supported devices that have been onboarded.
 - ☐ Select tags
Enable Standard discovery on device or device groups based on selected tags.



Black belt practices – operations

Exclusions: minimal as possible, specific as possible

Audit > warn > block

Troubleshooting mode

Performance analyser

Custom hunting queries

Security recommendations

Device discovery

Threat analytics



Threat analytics

Ransomware

52

Phishing

20

Vulnerability

69

Activity group

70

 Email notification settings

 Help resources

Latest threats







High-impact threats ⓘ




Highest exposure threats



 Search

1-30 < >  Choose columns ▾  30 items per page ▾  Filter

Threat	Alerts	Impacted assets ⓘ	Threat exposure level ⓘ
Threat Insights: Black Basta ransomware attackers leverage Qakbot access	0 active /...		15 - Low
Threat Insights: CVE-2022-41128 vulnerability in JScript9 engine	0 active /...		39 - Medium
CVE-2022-41073 Windows print spooler vulnerability	0 active /...		15 - Low

Call to action

Deploy in passive mode to pilot group; gradually move to active

Not leaving current AV/EDR? At least get recommendations, device discovery, advanced hunting data

Already deployed? Consider the tips in this session

Remember: MDE is just part of overall defence

Not licensed? Get a free trial

Ninja Training:
aka.ms/mdatpninja



Thanks!



@rucam365



Ru Campbell

