Automate Defender for Endpoint

Fabian Bader

WP NINJAS NL

CONNECT

Thank you Sponsors

Gold

robopack

SUPER VISION

AvePoint®

controlUP

inforcer

Recast

Silver

PATCH MY PC

Technical Partners

CONSULTEQ

PROXSYS

SecMinds SOLUTIONS

Secure At Work

Intro – Fabian Bader

glueckkanja

- Lives in Hamburg, Germany
- Cyber Security Architect @ glueckkanja AG
- Microsoft MVP (Security / Azure)
- Organizer of "Purple Elbe Security User Group"
- Author of
  - maester
  - TokenTacticsV2
  - entrascopes.com
  - SentinelARConverter

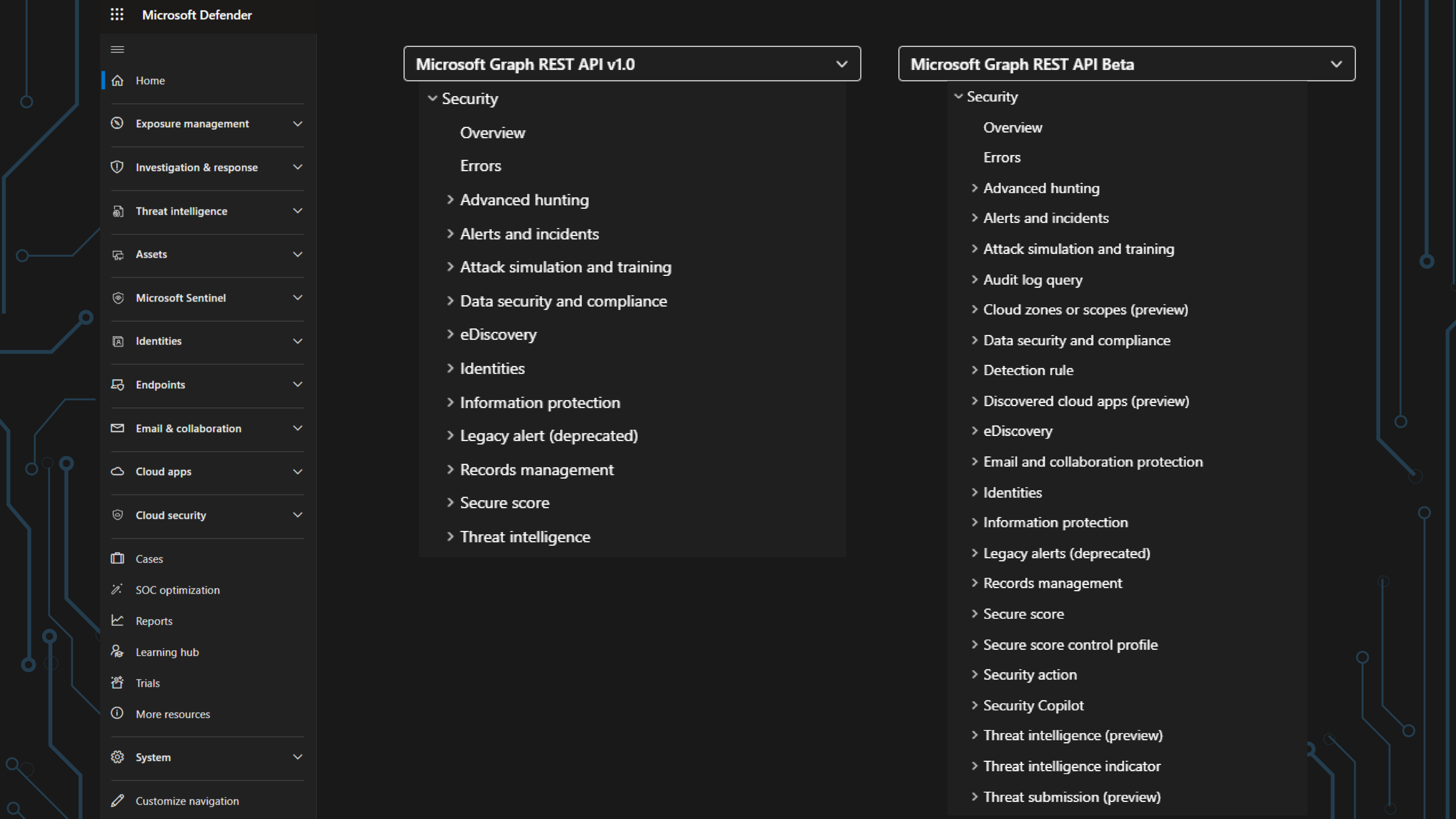
Socials	
Blog/talks:	cloudbrothers.info
Twitter/X:	@fabian_bader
BlueSky:	@fabian.bader.cloud

Agenda

- Why we can't have nice things - ClickOps in 2026
- Solving the mystery - API Proxy
- Bring it all together - The solution

Why we can't have nice things

ClickOps in 2026

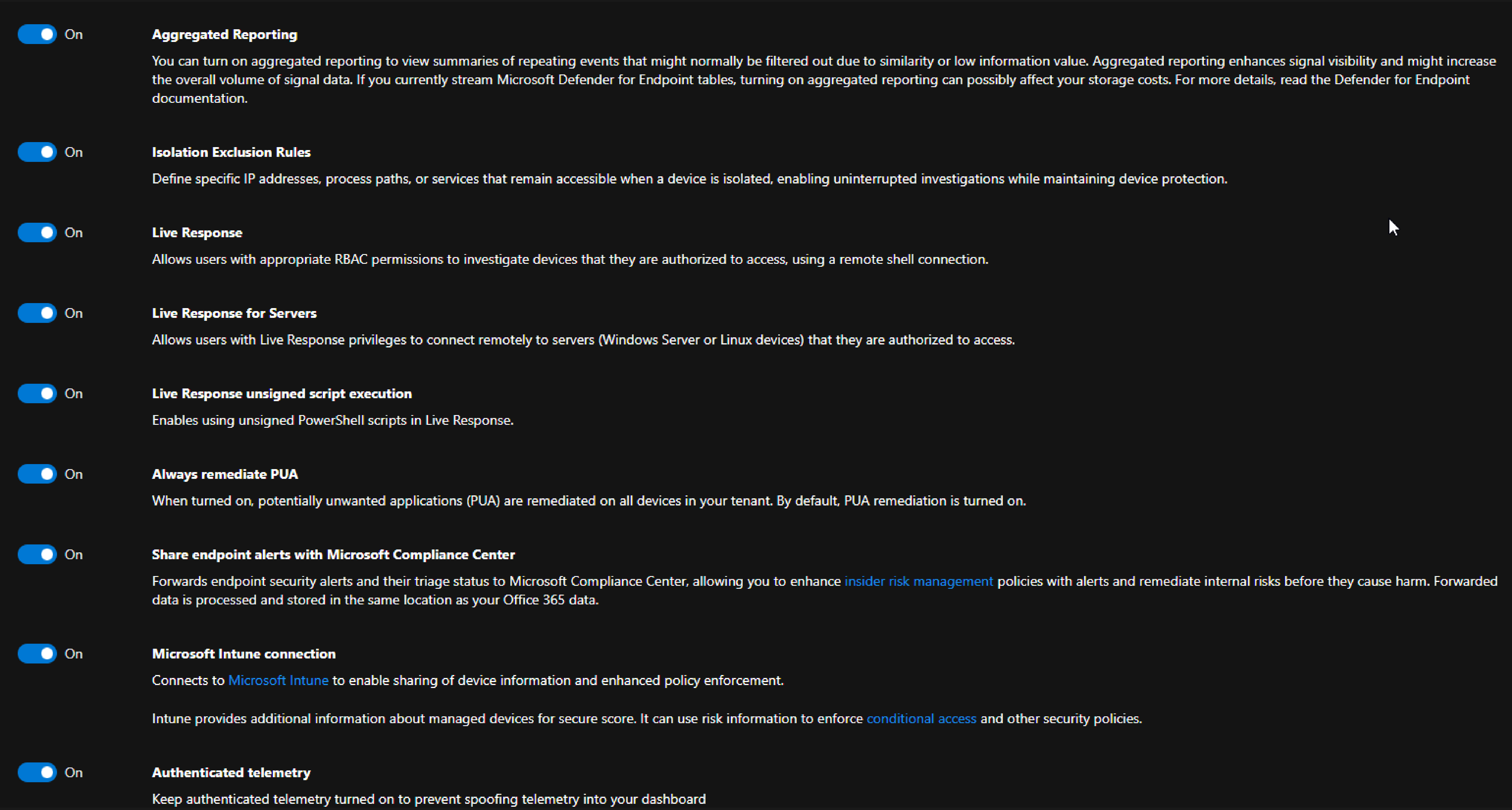


Microsoft Graph REST API v1.0

- Security
  - Overview
  - Errors
  - Advanced hunting
  - Alerts and incidents
  - Attack simulation and training
  - Data security and compliance
  - eDiscovery
  - Identities
  - Information protection
  - Legacy alert (deprecated)
  - Records management
  - Secure score
  - Threat intelligence

Microsoft Graph REST API Beta

- Security
  - Overview
  - Errors
  - Advanced hunting
  - Alerts and incidents
  - Attack simulation and training
  - Audit log query
  - Cloud zones or scopes (preview)
  - Data security and compliance
  - Detection rule
  - Discovered cloud apps (preview)
  - eDiscovery
  - Email and collaboration protection
  - Identities
  - Information protection
  - Legacy alerts (deprecated)
  - Records management
  - Secure score
  - Secure score control profile
  - Security action
  - Security Copilot
  - Threat intelligence (preview)
  - Threat intelligence indicator
  - Threat submission (preview)



● On **Aggregated Reporting**

You can turn on aggregated reporting to view summaries of repeating events that might normally be filtered out due to similarity or low information value. Aggregated reporting enhances signal visibility and might increase the overall volume of signal data. If you currently stream Microsoft Defender for Endpoint tables, turning on aggregated reporting can possibly affect your storage costs. For more details, read the Defender for Endpoint documentation.

● On **Isolation Exclusion Rules**

Define specific IP addresses, process paths, or services that remain accessible when a device is isolated, enabling uninterrupted investigations while maintaining device protection.

● 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.

● On **Always remediate PUA**

When turned on, potentially unwanted applications (PUA) are remediated on all devices in your tenant. By default, PUA remediation is turned on.

● On **Share endpoint alerts with Microsoft Compliance Center**

Forwards endpoint security alerts and their triage status to Microsoft Compliance Center, allowing you to enhance insider risk management policies with alerts and remediate internal risks before they cause harm. Forwarded data is processed and stored in the same location as your Office 365 data.

● On **Microsoft Intune connection**

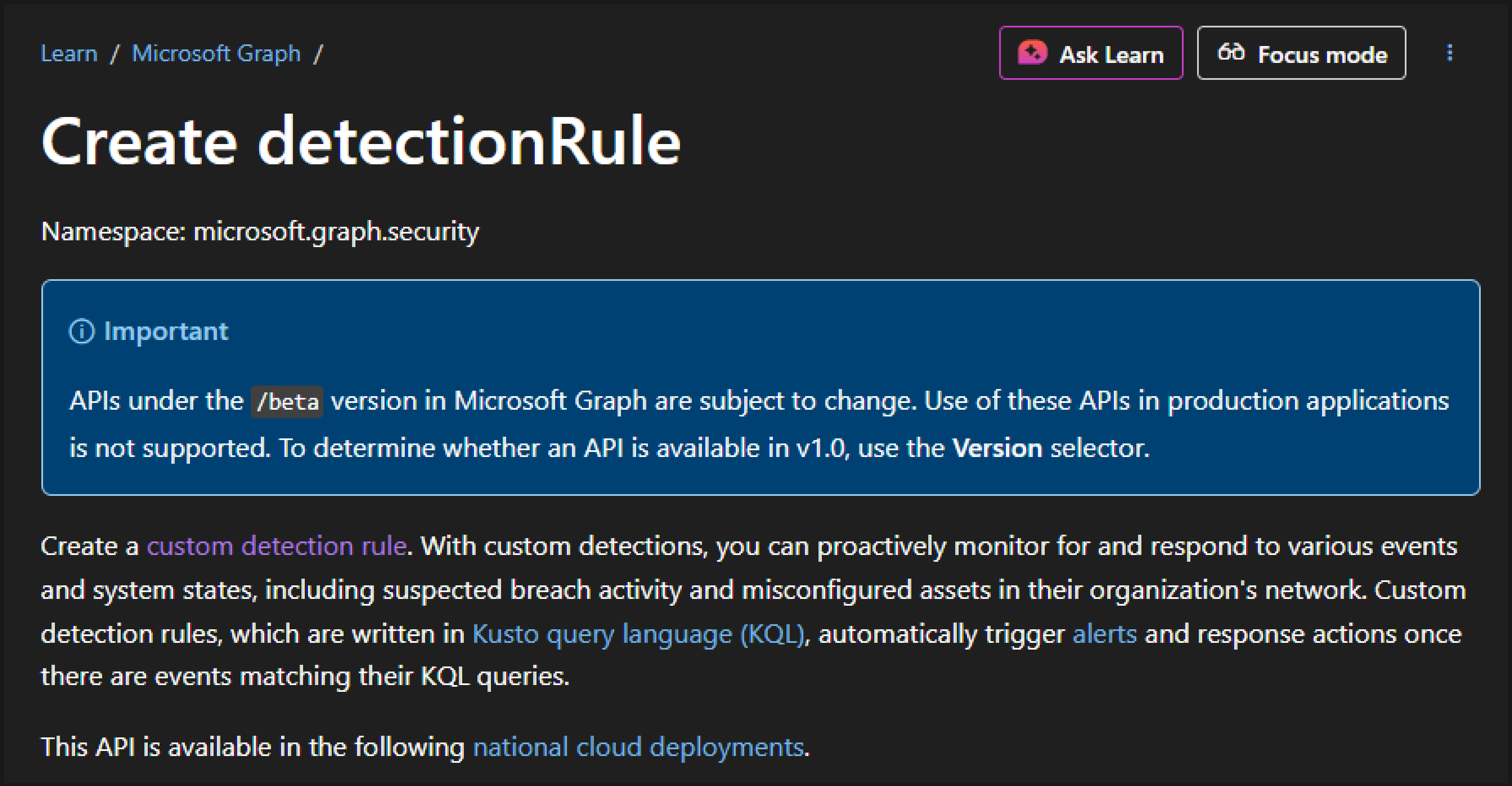
Connects to Microsoft Intune to enable sharing of device information and enhanced policy enforcement.

Intune provides additional information about managed devices for secure score. It can use risk information to enforce conditional access and other security policies.

● On **Authenticated telemetry**

Keep authenticated telemetry turned on to prevent spoofing telemetry into your dashboard

Detection as Code



Create detectionRule

Namespace: microsoft.graph.security

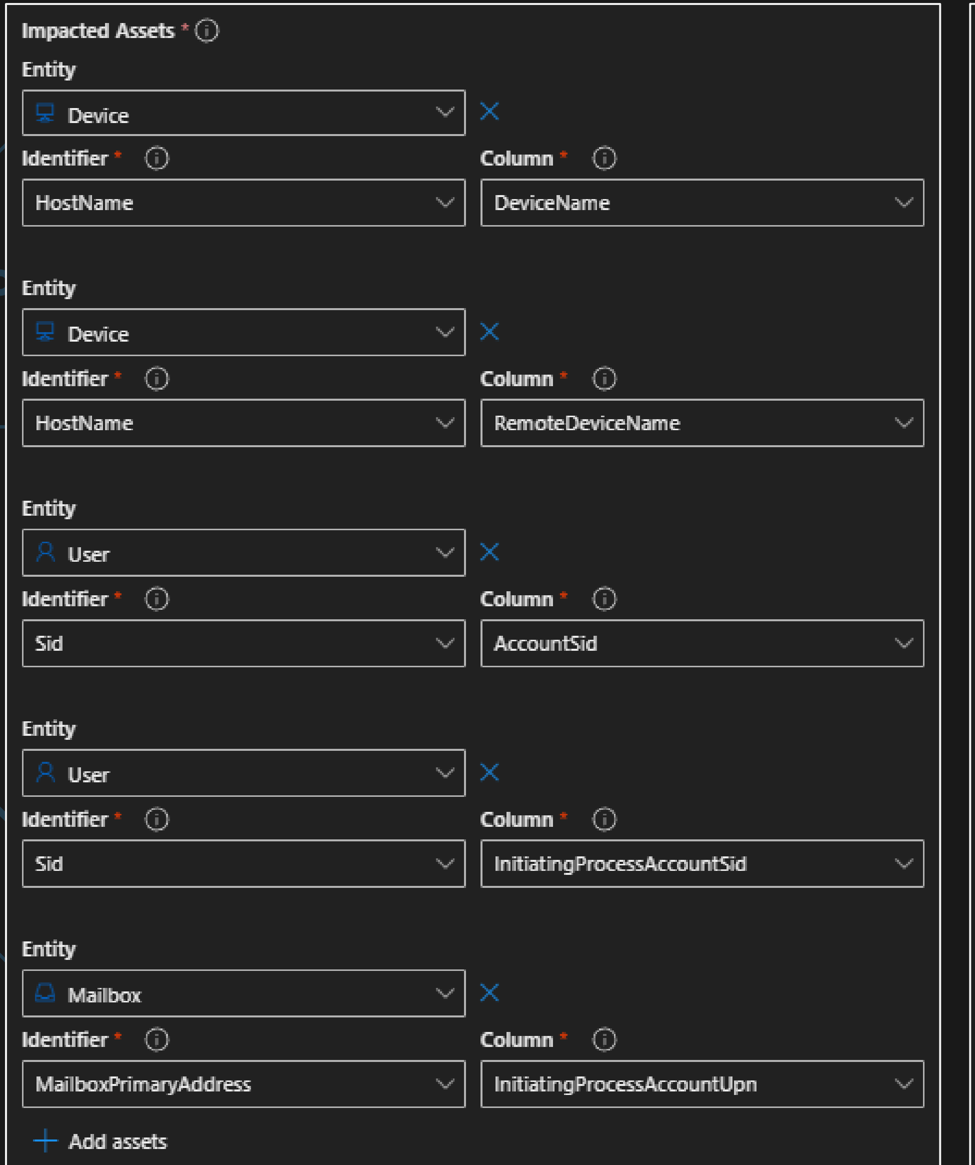
ⓘ **Important**

APIs under the `/beta` version in Microsoft Graph are subject to change. Use of these APIs in production applications is not supported. To determine whether an API is available in v1.0, use the **Version** selector.

Create a custom detection rule. With custom detections, you can proactively monitor for and respond to various events and system states, including suspected breach activity and misconfigured assets in their organization's network. Custom detection rules, which are written in Kusto query language (KQL), automatically trigger alerts and response actions once there are events matching their KQL queries.

This API is available in the following national cloud deployments.

Detection as Code



Impacted Assets *

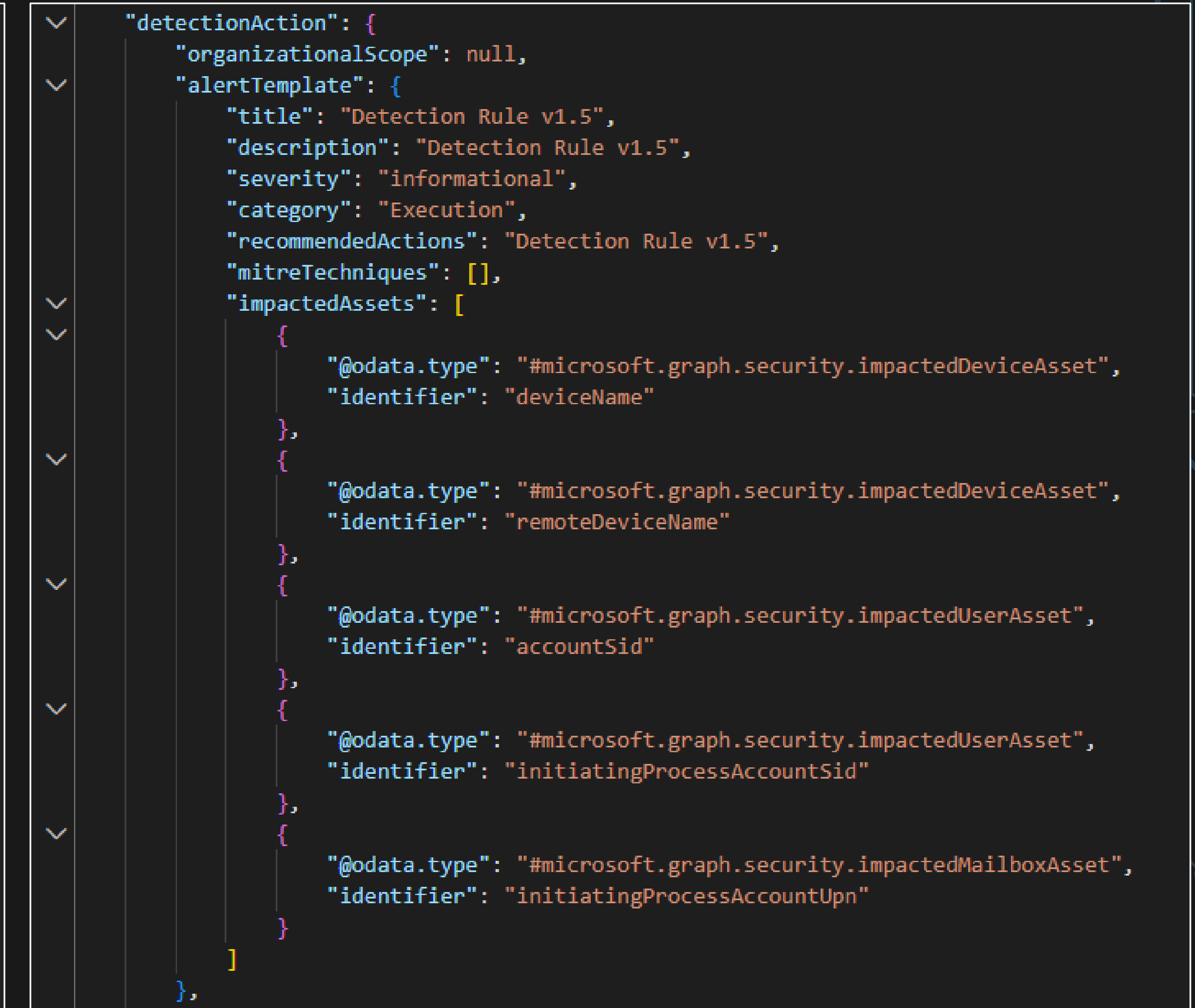
Entity: Device
Identifier *: HostName
Column *: DeviceName

Entity: Device
Identifier *: HostName
Column *: RemoteDeviceName

Entity: User
Identifier *: Sid
Column *: AccountSid

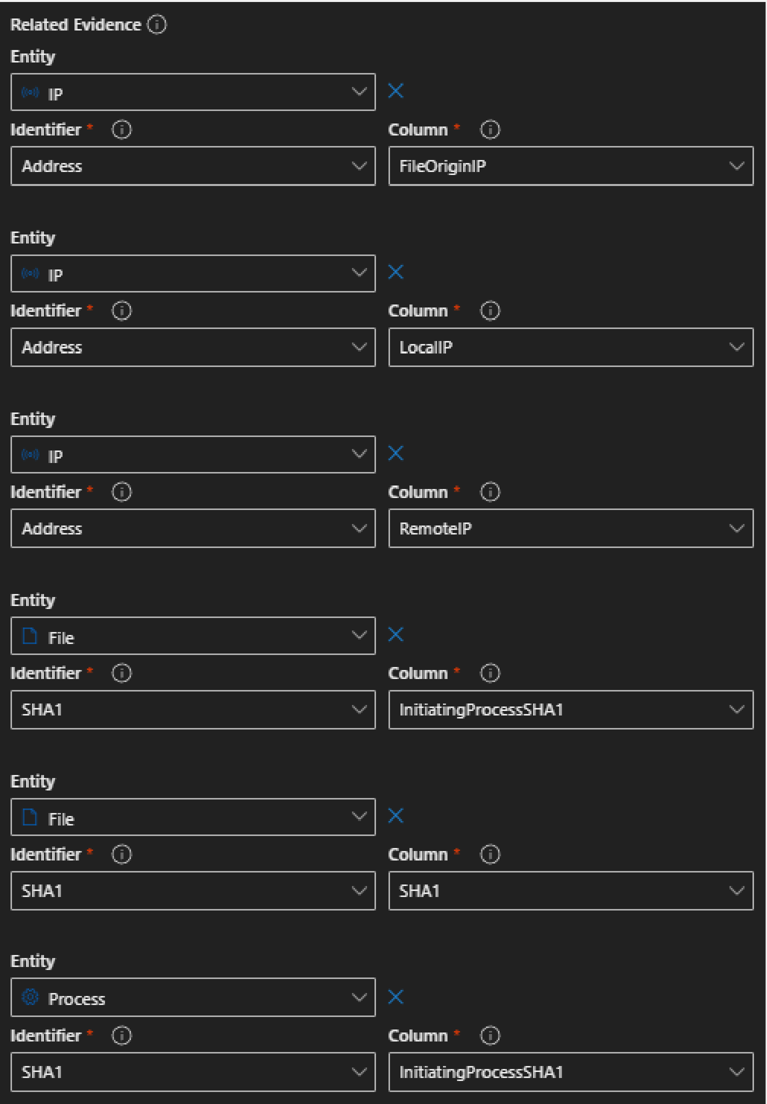
Entity: User
Identifier *: Sid
Column *: InitiatingProcessAccountSid

Entity: Mailbox
Identifier *: MailboxPrimaryAddress
Column *: InitiatingProcessAccountUpn



```
"detectionAction": {
    "organizationalScope": null,
    "alertTemplate": {
        "title": "Detection Rule v1.5",
        "description": "Detection Rule v1.5",
        "severity": "informational",
        "category": "Execution",
        "recommendedActions": "Detection Rule v1.5",
        "mitreTechniques": [],
        "impactedAssets": [
            {
                "@odata.type": "#microsoft.graph.security.impactedDeviceAsset",
                "identifier": "deviceName"
            },
            {
                "@odata.type": "#microsoft.graph.security.impactedDeviceAsset",
                "identifier": "remoteDeviceName"
            },
            {
                "@odata.type": "#microsoft.graph.security.impactedUserAsset",
                "identifier": "accountSid"
            },
            {
                "@odata.type": "#microsoft.graph.security.impactedUserAsset",
                "identifier": "initiatingProcessAccountSid"
            },
            {
                "@odata.type": "#microsoft.graph.security.impactedMailboxAsset",
                "identifier": "initiatingProcessAccountUpn"
            }
        ]
    },
```

Detection as Code



Related Evidence

Entity: IP
Identifier *: Address
Column *: FileOriginIP

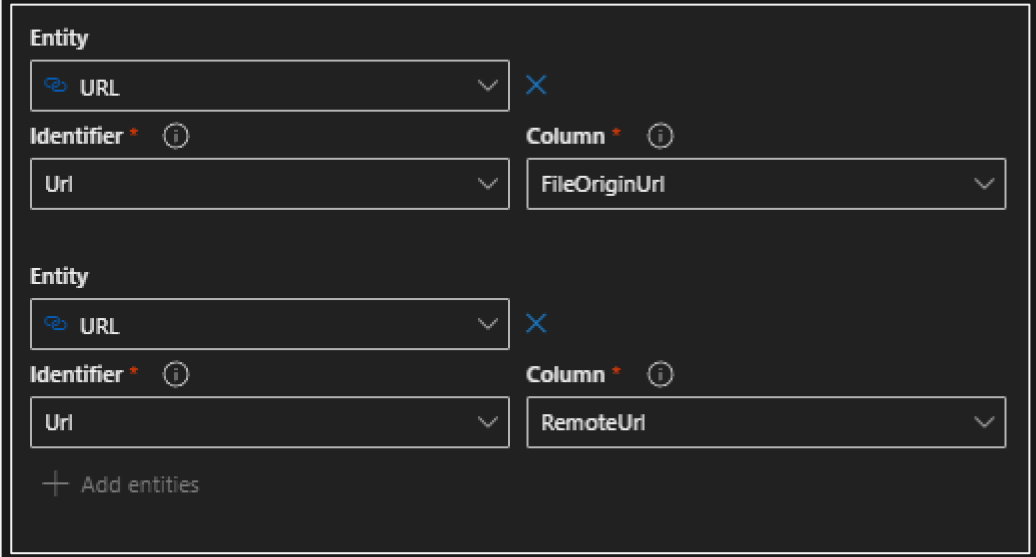
Entity: IP
Identifier *: Address
Column *: LocalIP

Entity: IP
Identifier *: Address
Column *: RemoteIP

Entity: File
Identifier *: SHA1
Column *: InitiatingProcessSHA1

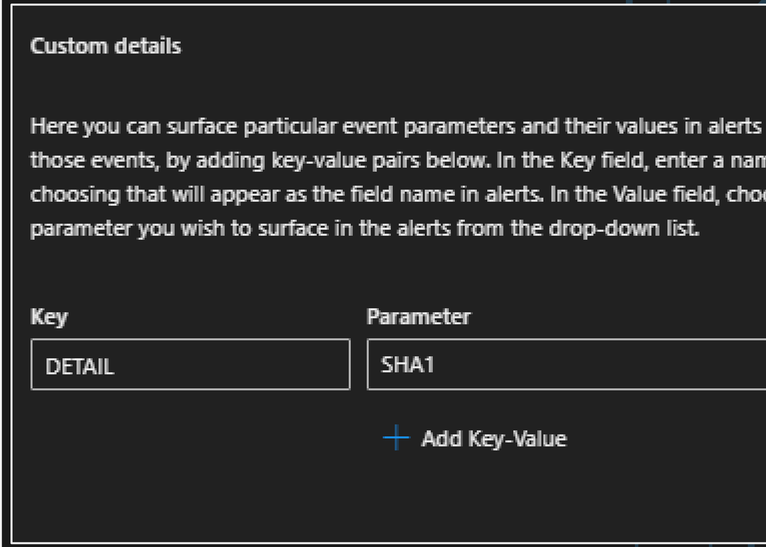
Entity: File
Identifier *: SHA1
Column *: SHA1

Entity: Process
Identifier *: SHA1
Column *: InitiatingProcessSHA1



Entity: URL
Identifier *: Url
Column *: FileOriginUrl

Entity: URL
Identifier *: Url
Column *: RemoteUrl



Custom details

Here you can surface particular event parameters and their values in alerts
those events, by adding key-value pairs below. In the Key field, enter a nam
choosing that will appear as the field name in alerts. In the Value field, choo
parameter you wish to surface in the alerts from the drop-down list.

Key	Parameter
DETAIL	SHA1

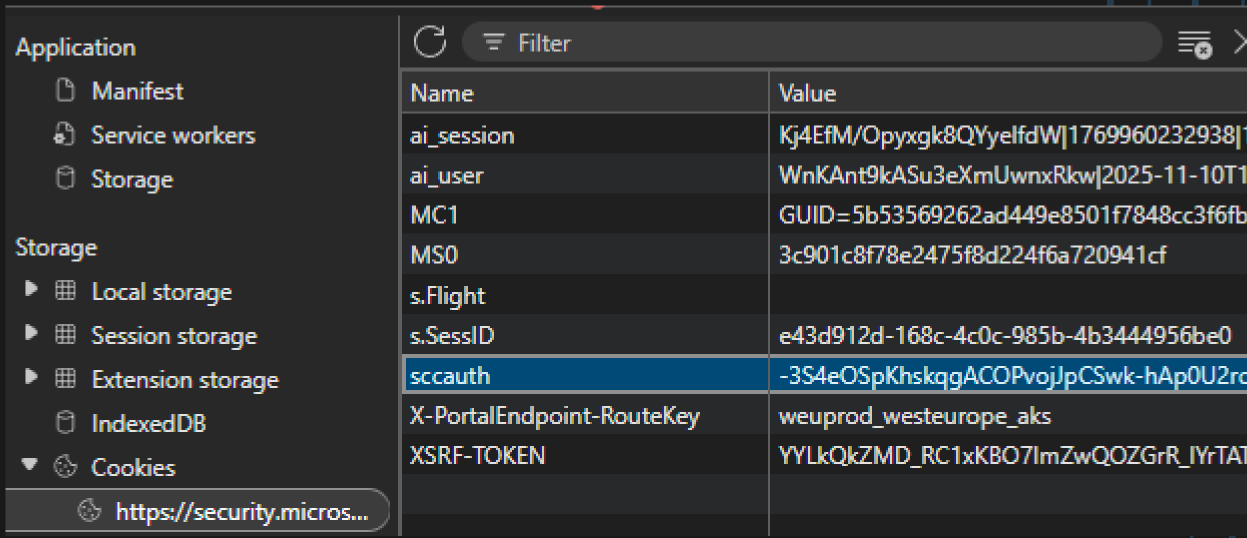
Solving the mystery

The API Proxy unraveled

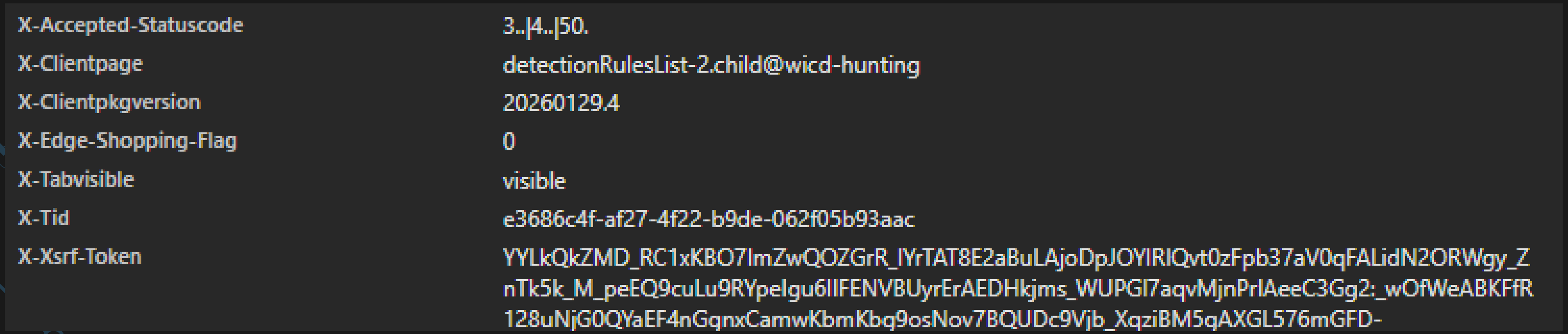
Demo

API Authentication

- Sccauth Cookie
- x-xsrf-token Cookie and API
- X-Tid for multi-tenant support



Name	Value
ai_session	Kj4EfM/Opyxgk8QYyelfdW|1769960232938|
ai_user	WnKAnt9kASu3eXmUwnxRkw|2025-11-10T1
MC1	GUID=5b53569262ad449e8501f7848cc3f6fb
MS0	3c901c8f78e2475f8d224f6a720941cf
s.Flight	
s.SessID	e43d912d-168c-4c0c-985b-4b3444956be0
sccauth	-3S4eOSpKhskqgACOPvojJpCSwk-hAp0U2r
X-PortalEndpoint-RouteKey	weuprod_westeurope_aks
XSRF-TOKEN	YYLkQkZMD_RC1xKBO7ImZwQOZGrR_IYrTAT



X-Accepted-Statuscode	3..|4..|50.
X-Clientpage	detectionRulesList-2.child@wicd-hunting
X-Clientpkgversion	20260129.4
X-Edge-Shopping-Flag	0
X-Tabvisible	visible
X-Tid	e3686c4f-af27-4f22-b9de-062f05b93aac
X-Xsrf-Token	YYLkQkZMD_RC1xKBO7ImZwQOZGrR_IYrTAT8E2aBuLAjoDpJOYIRIQvt0zFpb37aV0qFALidN2ORWgy_ZnTk5k_M_peEQ9cuLu9RYpeIgu6lIFENVBUyrErAEDHkjms_WUPGI7aqvMjnPrlAeeC3Gg2:_wOfWeABKFfR128uNjG0QYaEF4nGqnxCamwKbmKbq9osNov7BQUDc9Vjb_XqziBM5qAXGL576mGFD-

Demo

Bring it all together

The solution - XDRInternals

XDRInternals

XDRInternals

- Open Source PowerShell Module
  - MIT License
- Initially built by
  - Nathan McNulty
  - Fabian Bader
- Our guidelines
  - Only build what's not there
  - Be nice to the API

- https://github.com/MSCloudInternals/XDRInternals

XDRInternals

- 93 cmdlets as of 04.02.2026
- Mostly GET cmdlets, all supporting caching
- ~ 20 change cmdlets e.g.
  - Change Advanced Features
  - Create/Update Advanced Hunting Functions
  - Merge incidents
  - Remove alert from incident
  - New device RBAC groups
- Quality of live
  - Run multi-tenant advanced hunting query
  - Run XSPM Hunting queries

Demo

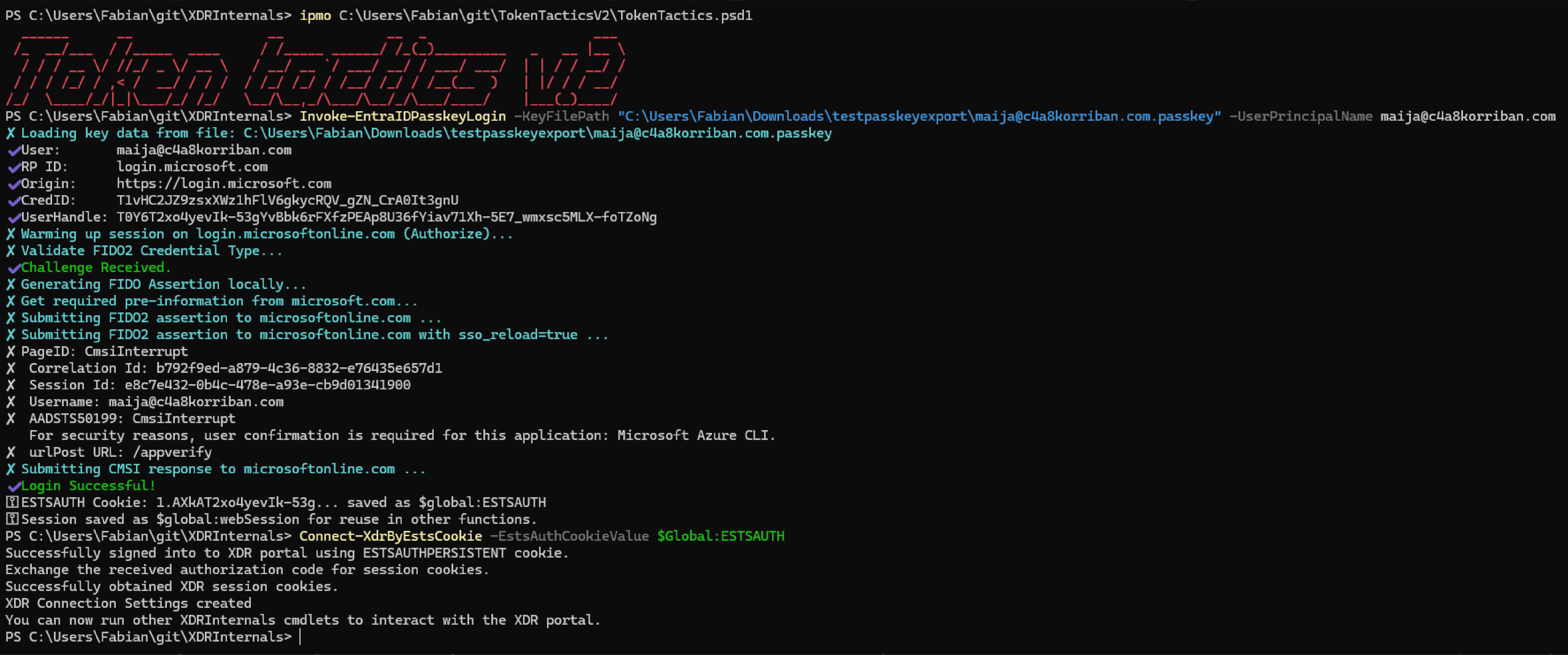
XDRInternals and XDRay

Download and test today

https://github.com/MSCloudInternals/XDRInternals

One last thing

TokenTactics 💖 XDRInternals



```
PS C:\Users\Fabian\git\XDRInternals> ipmo C:\Users\Fabian\git\TokenTacticsV2\TokenTactics.psd1
  ______      __                 __             __  _                    ___
 /_  __/___  / /_____  ____     / /_____ ______/ /_(_)________   _   __ |__ \
  / / / __ \/ //_/ _ \/ __ \   / __/ __ `/ ___/ __/ / ___/ ___/  | | / / __/ /
 / / / /_/ / ,< /  __/ / / /  / /_/ /_/ / /__/ /_/ / /__(__  )   | |/ / / __/
/_/  \____/_/|_|\___/_/ /_/   \__/\__,_/\___/\__/_/\___/____/    |___(_)____/
PS C:\Users\Fabian\git\XDRInternals> Invoke-EntraIDPasskeyLogin -KeyFilePath "C:\Users\Fabian\Downloads\testpasskeyexport\maija@c4a8korriban.com.passkey" -UserPrincipalName maija@c4a8korriban.com
✗ Loading key data from file: C:\Users\Fabian\Downloads\testpasskeyexport\maija@c4a8korriban.com.passkey
✓User:       maija@c4a8korriban.com
✓RP ID:      login.microsoft.com
✓Origin:     https://login.microsoft.com
✓CredID:     T1vHC2JZ9zsxXWz1hFlV6gkycRQV_gZN_CrA0It3gnU
✓UserHandle: T0Y6T2xo4yevIk-53gYvBbk6rFXfzPEAp8U36fYiav71Xh-5E7_wmxsc5MLX-foTZoNg
✗ Warming up session on login.microsoftonline.com (Authorize)...
✗ Validate FIDO2 Credential Type...
✓Challenge Received.
✗ Generating FIDO Assertion locally...
✗ Get required pre-information from microsoft.com...
✗ Submitting FIDO2 assertion to microsoftonline.com ...
✗ Submitting FIDO2 assertion to microsoftonline.com with sso_reload=true ...
✗ PageID: CmsiInterrupt
✗  Correlation Id: b792f9ed-a879-4c36-8832-e76435e657d1
✗  Session Id: e8c7e432-0b4c-478e-a93e-cb9d01341900
✗  Username: maija@c4a8korriban.com
✗  AADSTS50199: CmsiInterrupt
   For security reasons, user confirmation is required for this application: Microsoft Azure CLI.
✗  urlPost URL: /appverify
✗ Submitting CMSI response to microsoftonline.com ...
✓Login Successful!
⚿ESTSAUTH Cookie: 1.AXkAT2xo4yevIk-53g... saved as $global:ESTSAUTH
⚿Session saved as $global:webSession for reuse in other functions.
PS C:\Users\Fabian\git\XDRInternals> Connect-XdrByEstsCookie -EstsAuthCookieValue $Global:ESTSAUTH
Successfully signed into to XDR portal using ESTSAUTHPERSISTENT cookie.
Exchange the received authorization code for session cookies.
Successfully obtained XDR session cookies.
XDR Connection Settings created
You can now run other XDRInternals cmdlets to interact with the XDR portal.
PS C:\Users\Fabian\git\XDRInternals>
```

xdrinternals.com

Up to date advanced hunting schema
Powered by XDRInternals and TokenTactics

Important notice

- MDE and XDR Advanced Hunting APIs retiring
    - https://mc.merill.net/message/MC1220762
- After February 1, 2027, the MDE and XDR APIs will no longer function.
- Migrate as soon as possible

Thank you