NIC REBEL EDITION

Detection as Code

Microsoft Defender XDR and Microsoft Sentinel

NIC REBEL EDITION

Truls Thorstad Dahlsveen

Security Architect @ Sopra Steria
Microsoft MVP Security – SIEM & XDR

infernux.no

Anders Kristiansen

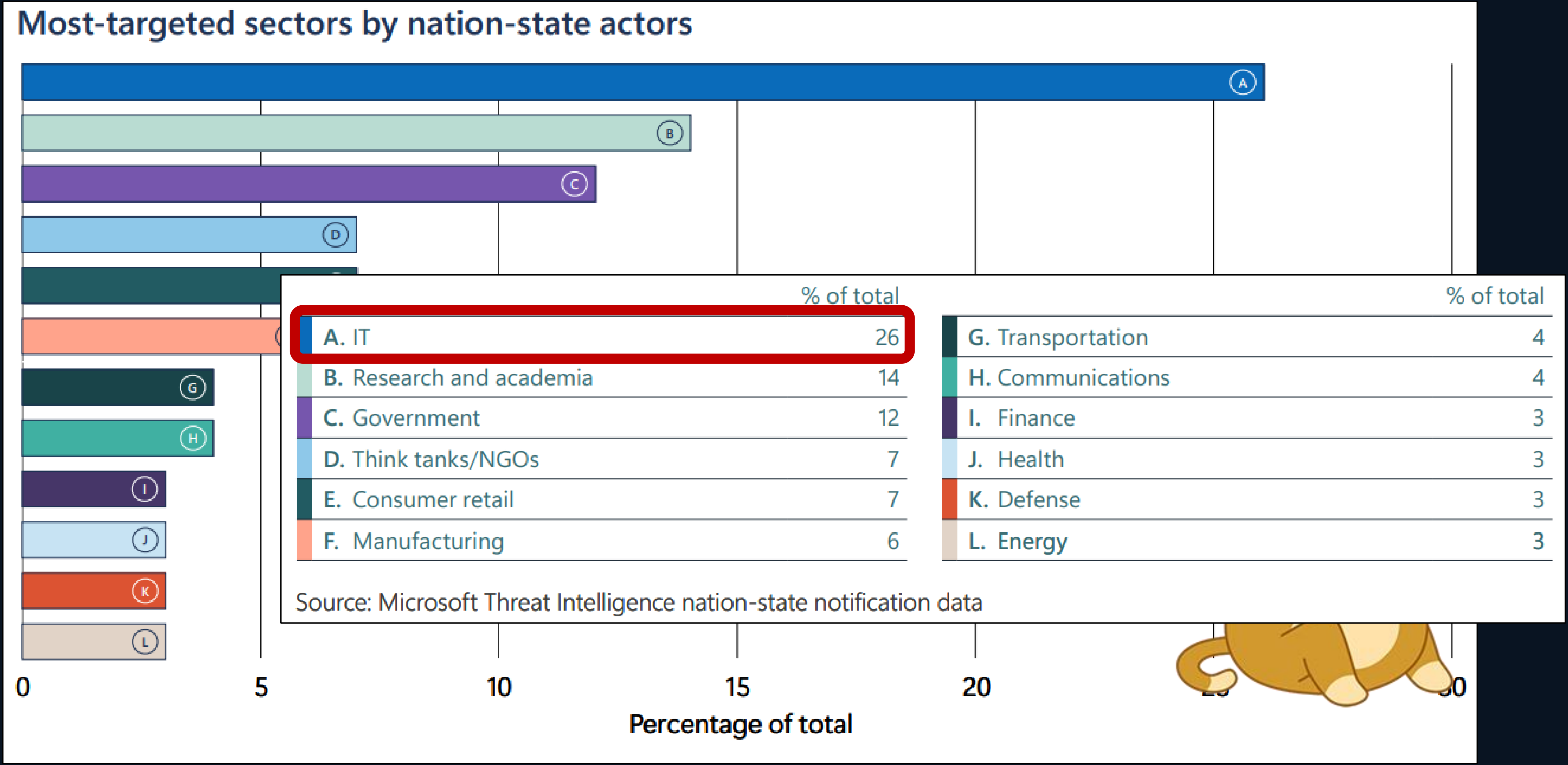
Lead Security Architect @ Storebrand
Microsoft MVP Security – SIEM & XDR
Identity & Access

anderskristiansen.com

Trust is Not Enough: Why Your Current Detections Are Too Late

- **You must manage detection and response at the speed and scale the modern attack demands.**

Detection is needed in every layer



Most-targeted sectors by nation-state actors

	% of total		% of total
A. IT	26	G. Transportation	4
B. Research and academia	14	H. Communications	4
C. Government	12	I. Finance	3
D. Think tanks/NGOs	7	J. Health	3
E. Consumer retail	7	K. Defense	3
F. Manufacturing	6	L. Energy	3

Source: Microsoft Threat Intelligence nation-state notification data

Alert fatigue

Trust, but verify

Speed and reliability

Detection engineering is much more than code

Think like a threat actor/hacker

Do it yourself - No Threat Intelligence available

Use existing frameworks:

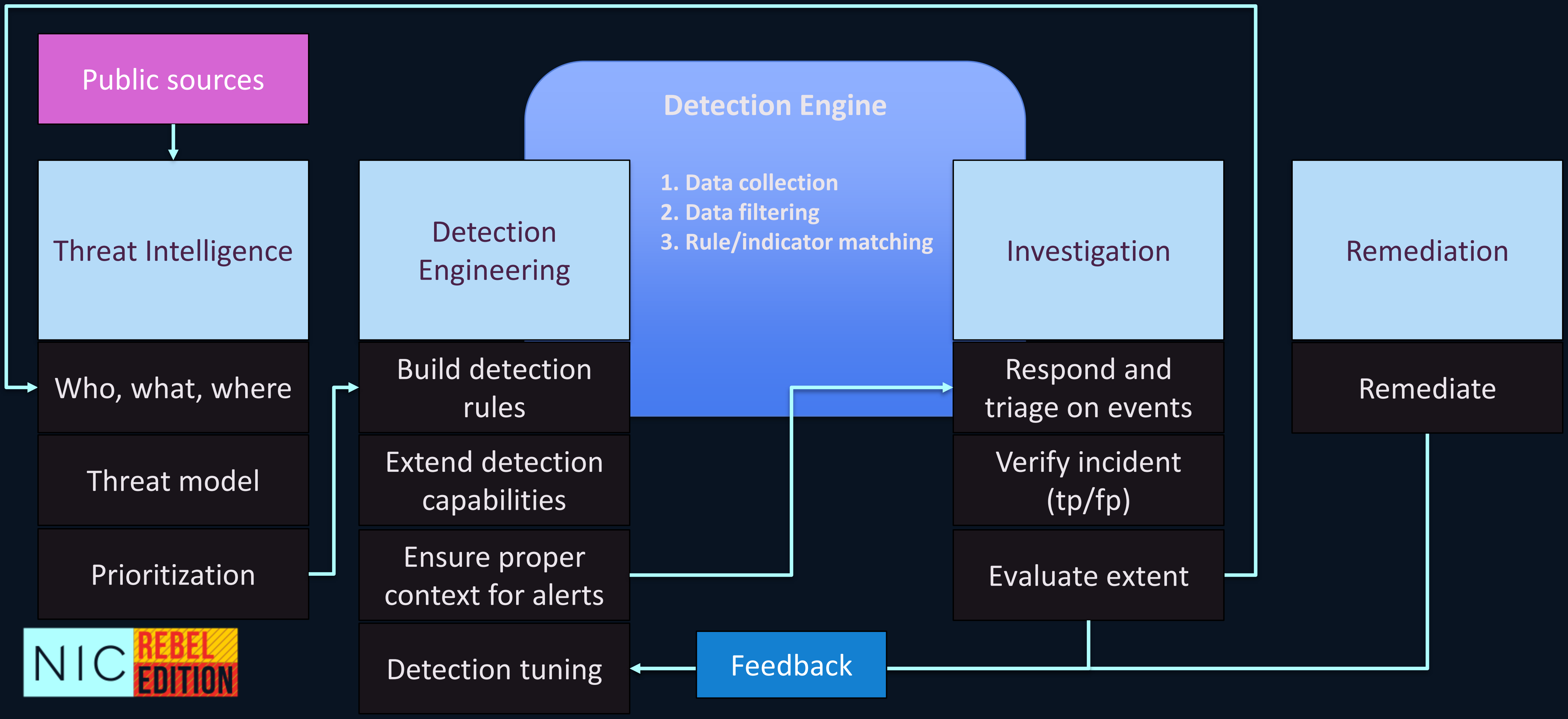
-MITRE ATT&CK®

-Palantir Alert and Detection framework

-NIST

NIC REBEL EDITION

Detection and response roles overview



Public sources

Threat Intelligence

Who, what, where

Threat model

Prioritization

Detection Engineering

Build detection rules

Extend detection capabilities

Ensure proper context for alerts

Detection tuning

Detection Engine

1. Data collection
2. Data filtering
3. Rule/indicator matching

Investigation

Respond and triage on events

Verify incident (tp/fp)

Evaluate extent

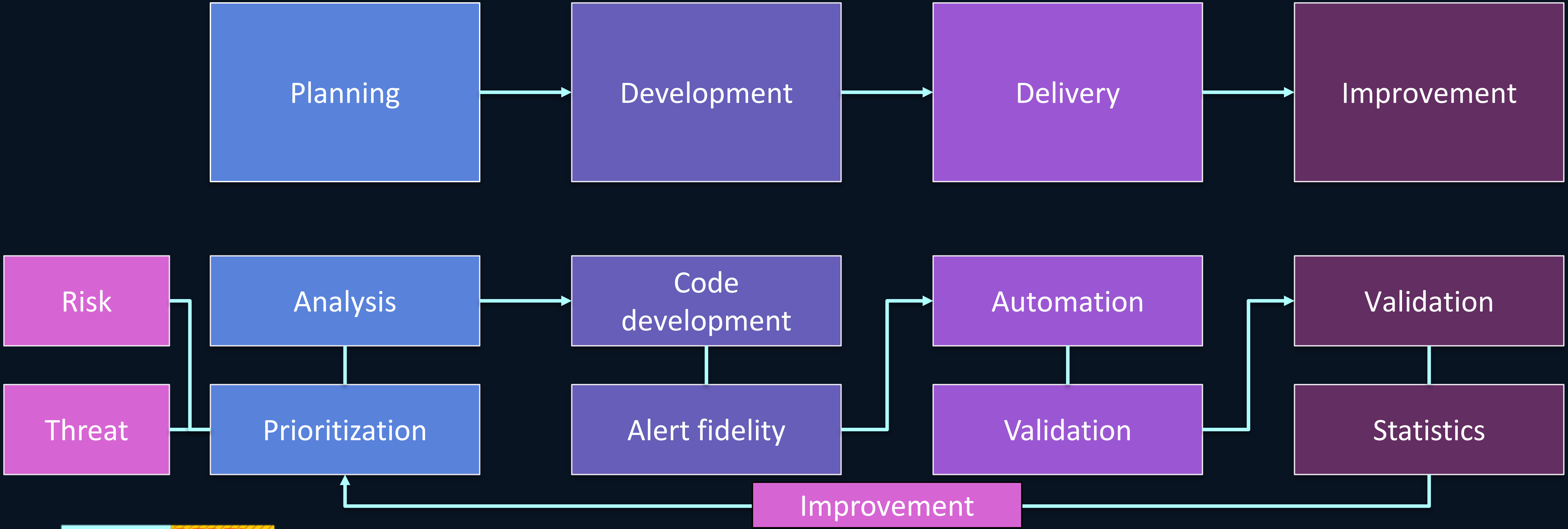
Remediation

Remediate

Feedback

NIC REBEL EDITION

Detection engineering lifecycle



Planning

Development

Delivery

Improvement

Risk

Threat

Analysis

Prioritization

Code development

Alert fidelity

Automation

Validation

Validation

Statistics

Improvement

Automation & Structure

- Adoption and speed is crucial
- Technical is often much easier than human processes
- We need to work as a team
- Detection engineers needs to be in the loop

NIC REBEL EDITION

Start with what you have

- Logs
- Sentinel instance
- CI/CD

NIC REBEL EDITION

OK, I got all this - I'm sold.

- Start with what you got (learn methodology, its free)
- Are you mature enough?
- Don’t just do code if for the coding's sake
- Define your goals, your team needs to be aligned

NIC REBEL EDITION

Building your folder structure

- Use what makes sense for your team
- Use well known frameworks for folder pattern
- AI assisted
- Be flexible and be ready to change

Flowchart

Demo

Scenario 1: Self Managed

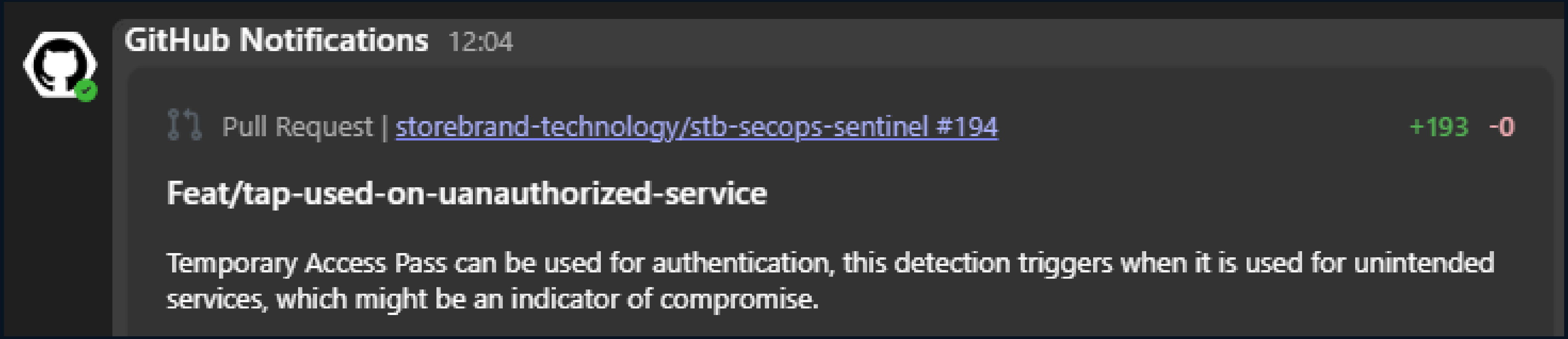
- Only production – that's fine
- Look at the alerts - please
- Fail fast

Scenario 2: Customer with MSP

- You need to cater for both internal SOC and MSP
- Challenges :
  - Visibility in detection rules
  - Tuning of rules can be a challenge
  - RBAC for both parties
  - Align who does what

CI/CD Tips

- Set Codeowners so PR
- Subscribe to the repository in teams, slack..



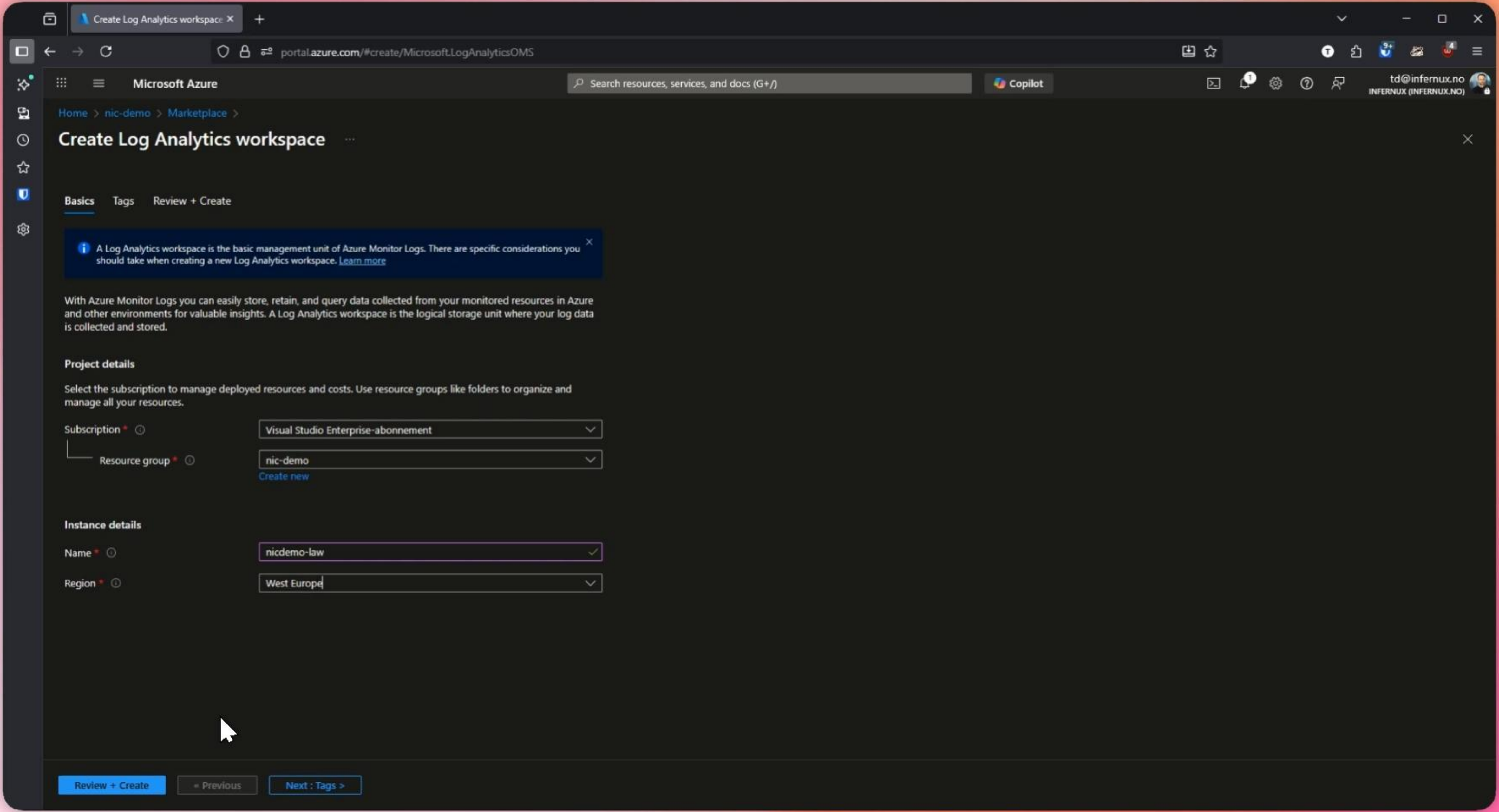
GitHub Notifications 12:04

Pull Request | storebrand-technology/stb-secops-sentinel #194 +193 -0

Feat/tap-used-on-uanauthorized-service

Temporary Access Pass can be used for authentication, this detection triggers when it is used for unintended services, which might be an indicator of compromise.

Microsoft Sentinel introduction


Create Log Analytics workspace
portal.azure.com/#create/Microsoft.LogAnalyticsOMS
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
td@infernux.no
INFERNUX (INFERNUX.NO)
Home > nic-demo > Marketplace >

Create Log Analytics workspace

Basics
Tags
Review + Create

A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. Learn more

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Visual Studio Enterprise-abonnement

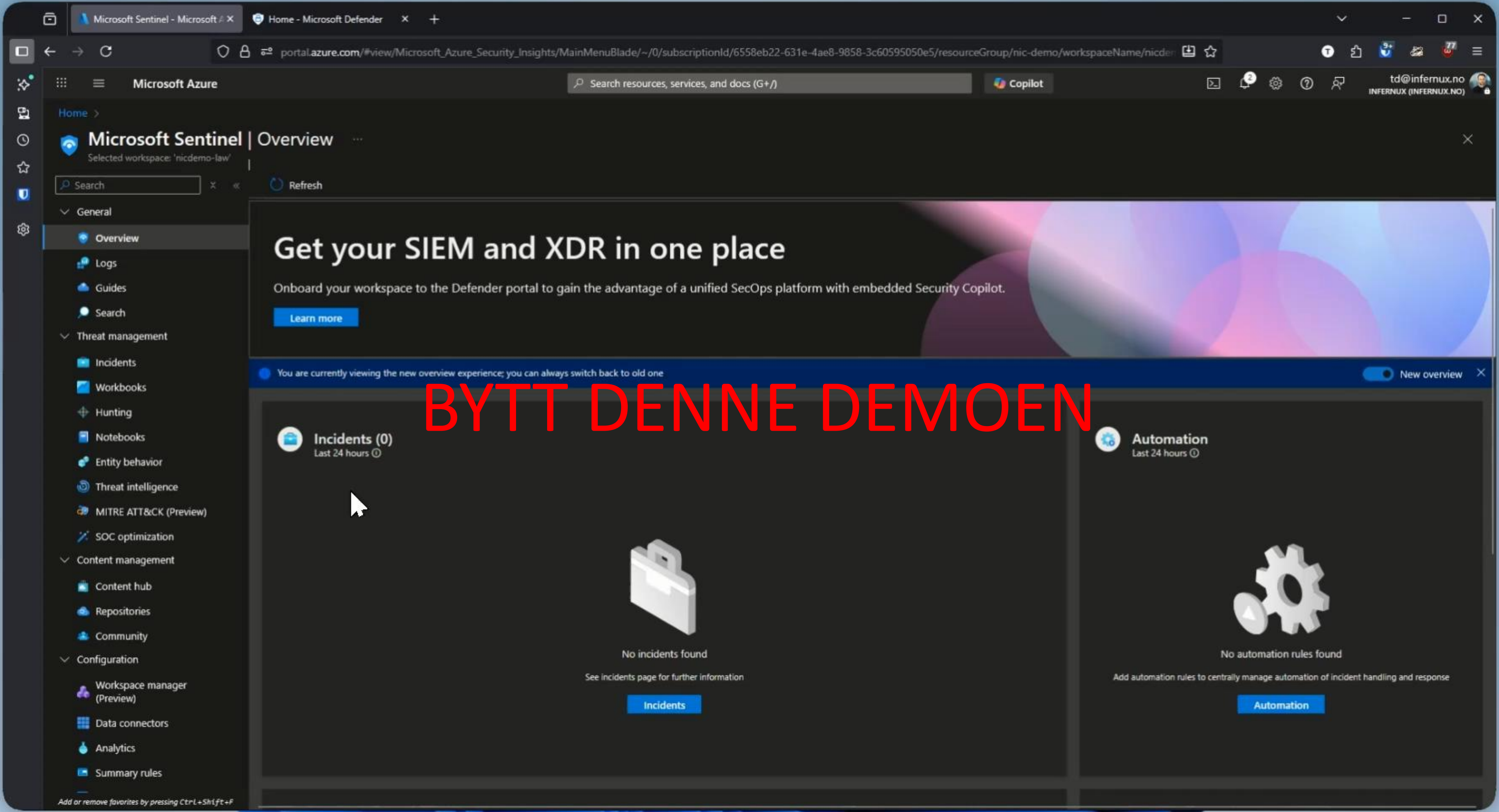
Resource group * : nic-demo

Create new

Instance details

Name * : nicdemo-law

Region * : West Europe



Get your SIEM and XDR in one place

Onboard your workspace to the Defender portal to gain the advantage of a unified SecOps platform with embedded Security Copilot.

You are currently viewing the new overview experience; you can always switch back to old one

No incidents found

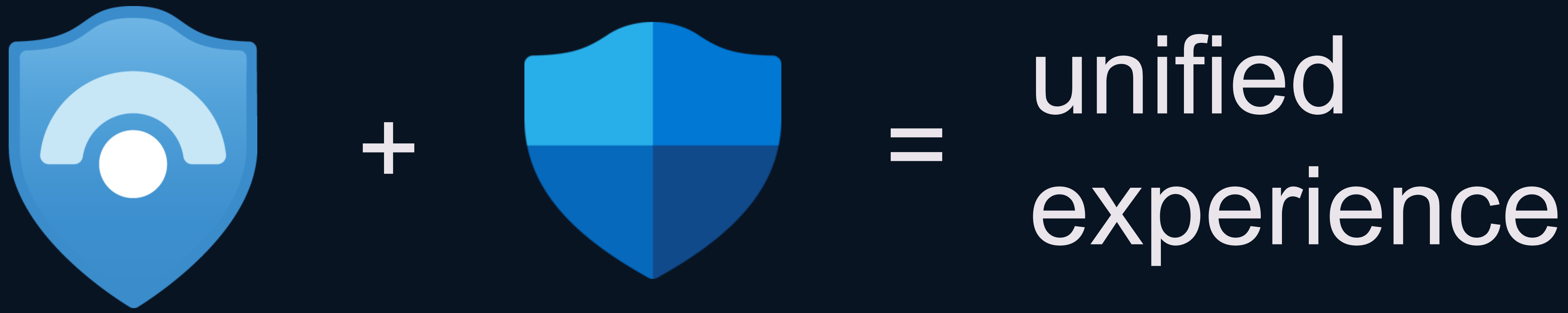
See incidents page for further information

No automation rules found

Add automation rules to centrally manage automation of incident handling and response

BYTT DENNE DEMOEN

Unified Experience



+ =

unified experience

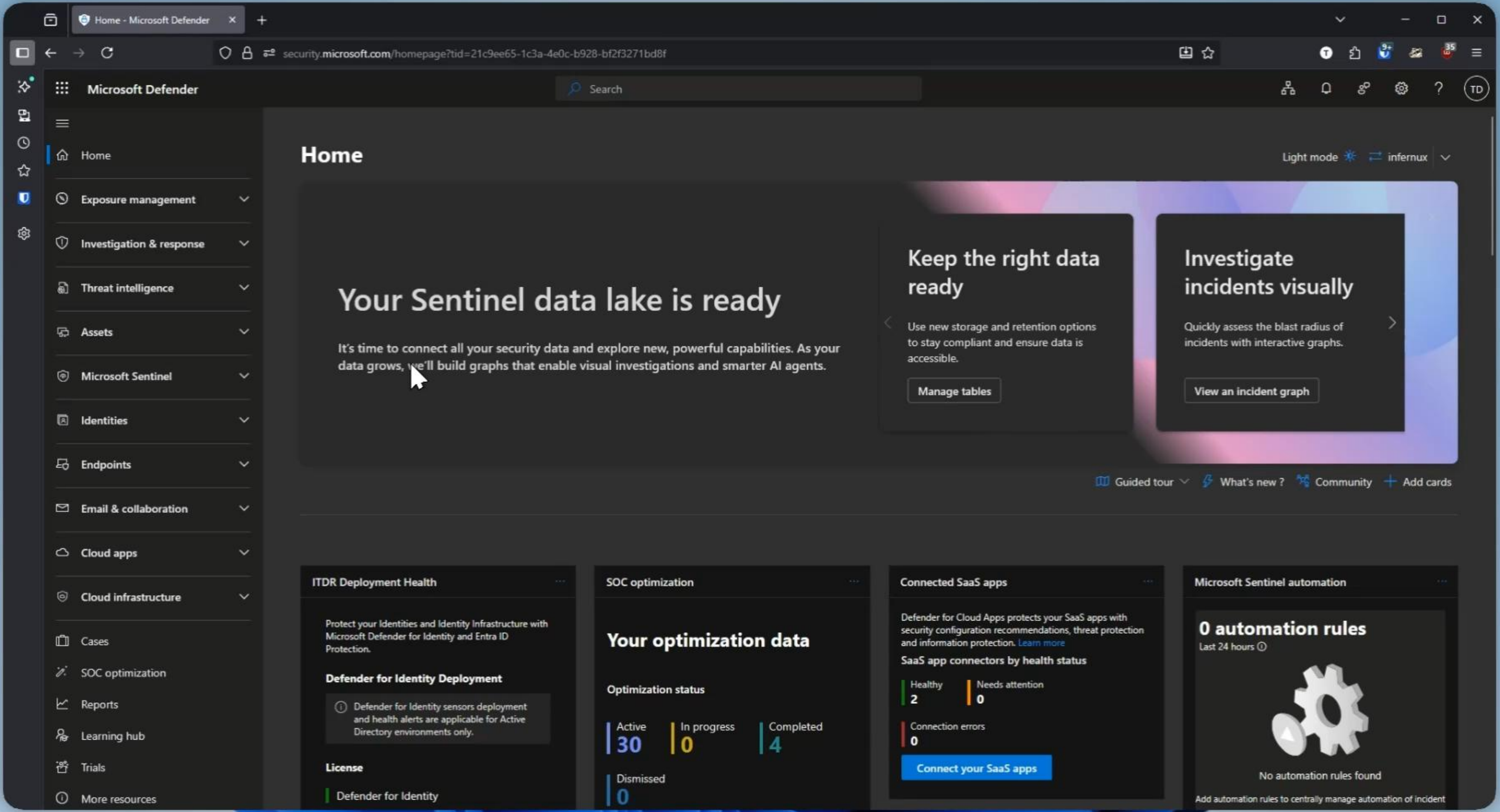
Roadmap

- **Important Update: Custom Detections to be the unified experience for creating detections in Microsoft Defender**

Microsoft is transitioning from Analytics Rules to Custom Detections as the unified experience for the creation of rules. This change is designed to support the unified SOC platform vision, to eliminate fragmented experience, and unify everything that the SOC needs into one portal with unified experiences across all available data.

Defender XDR introduction

NIC REBEL EDITION



Home

Your Sentinel data lake is ready

It's time to connect all your security data and explore new, powerful capabilities. As your data grows, we'll build graphs that enable visual investigations and smarter AI agents.

Keep the right data ready

Use new storage and retention options to stay compliant and ensure data is accessible.

Investigate incidents visually

Quickly assess the blast radius of incidents with interactive graphs.

ITDR Deployment Health

Protect your Identities and Identity Infrastructure with Microsoft Defender for Identity and Entra ID Protection.

Defender for Identity Deployment

Defender for Identity sensors deployment and health alerts are applicable for Active Directory environments only.

License

Defender for Identity

SOC optimization

Your optimization data

Optimization status

Active 30

In progress 0

Completed 4

Dismissed 0

Connected SaaS apps

Defender for Cloud Apps protects your SaaS apps with security configuration recommendations, threat protection and information protection. Learn more

SaaS app connectors by health status

Healthy 2

Needs attention 0

Connection errors 0

Microsoft Sentinel automation

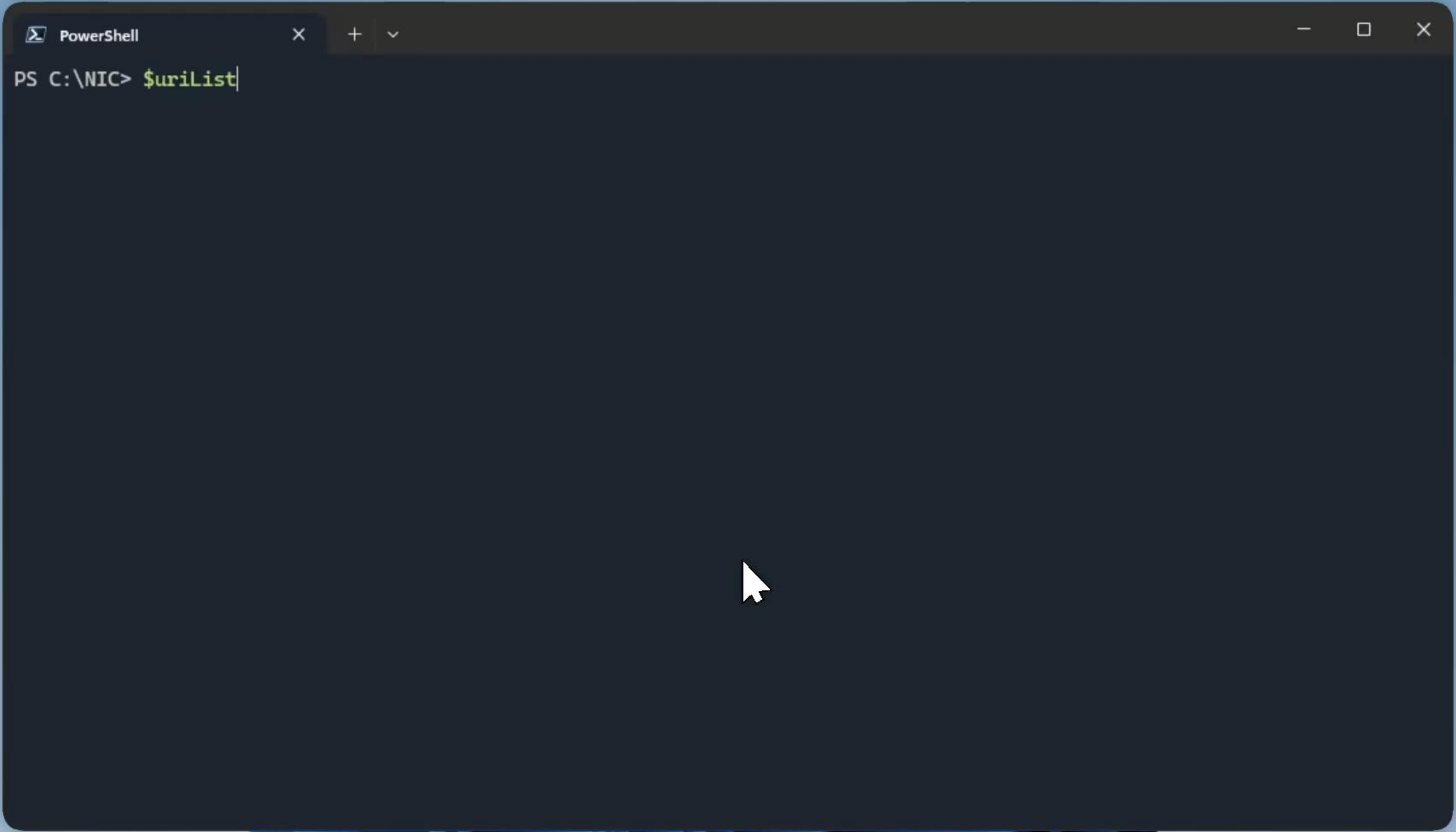
0 automation rules

Last 24 hours

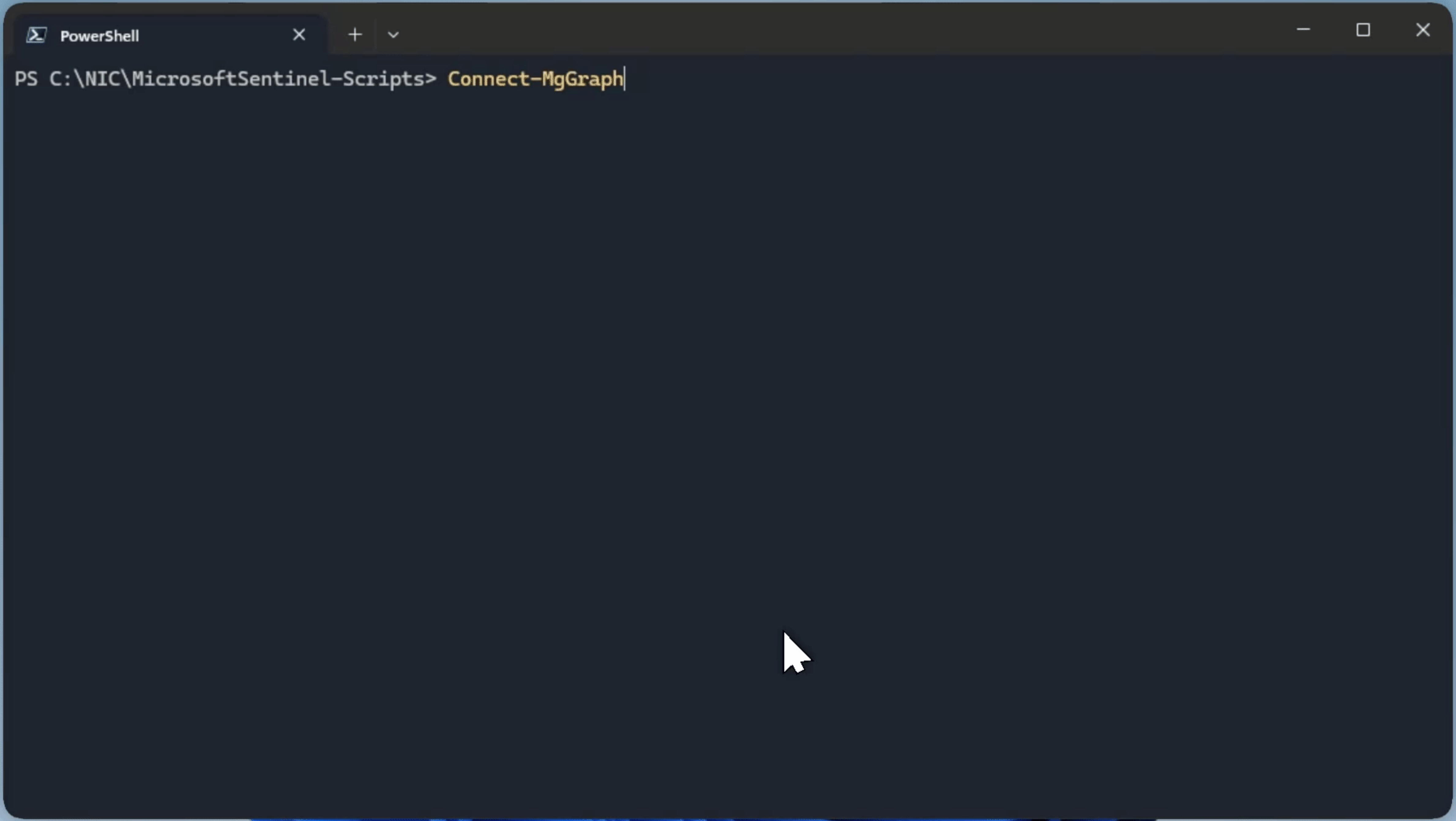
No automation rules found

Add automation rules to centrally manage automation of incident

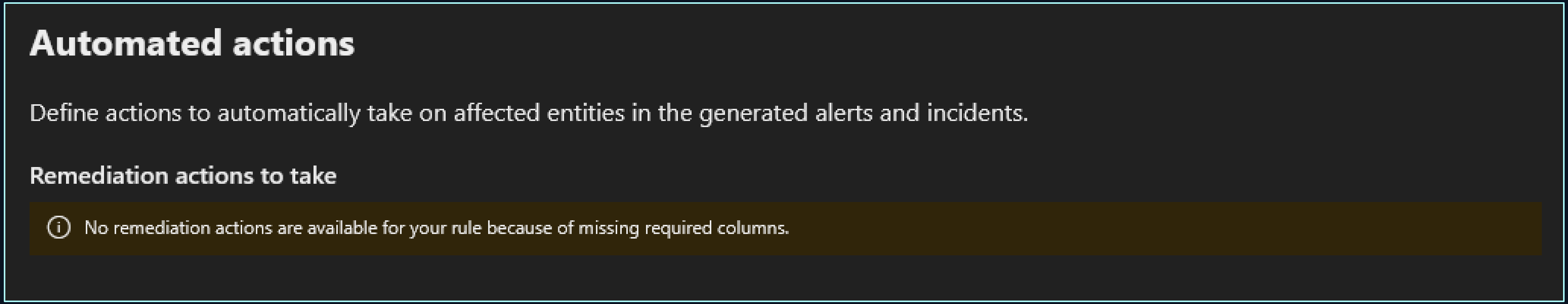
API support for detection queries



```
PS C:\NIC> $uriList
```



```
PS C:\NIC\MicrosoftSentinel-Scripts> Connect-MgGraph
```

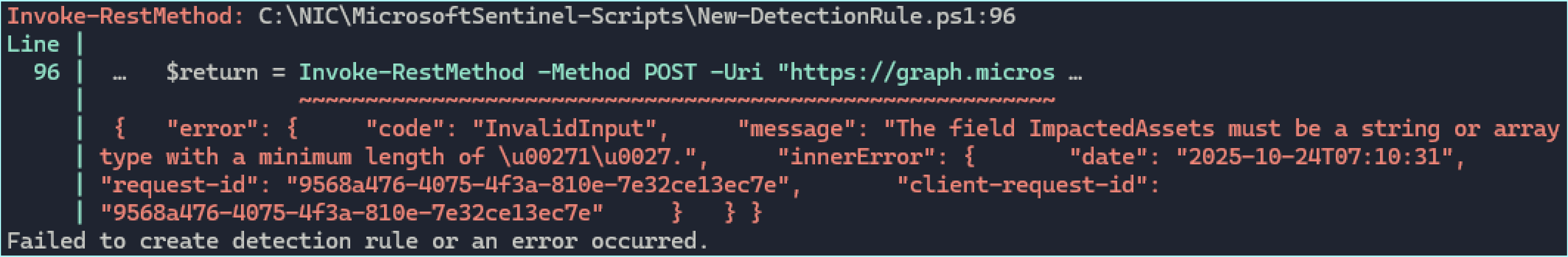


Automated actions

Define actions to automatically take on affected entities in the generated alerts and incidents.

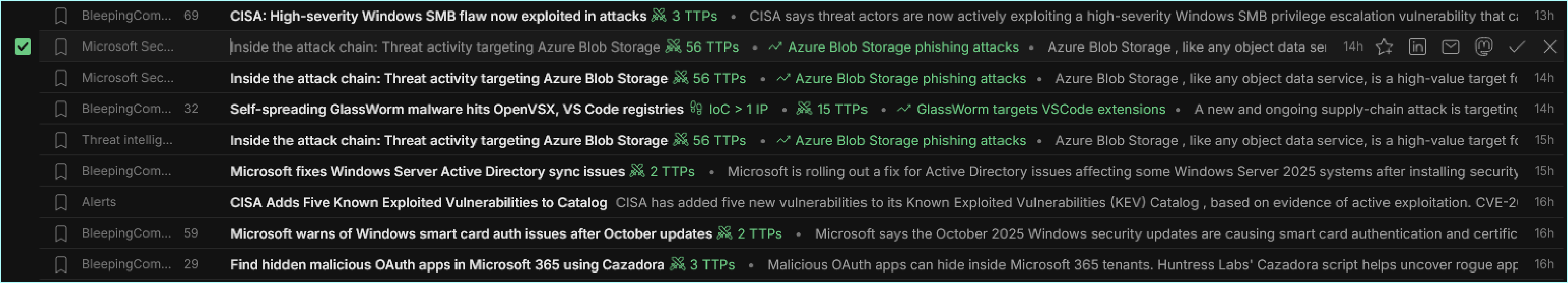
Remediation actions to take

ⓘ No remediation actions are available for your rule because of missing required columns.



```
Invoke-RestMethod: C:\NIC\MicrosoftSentinel-Scripts\New-DetectionRule.ps1:96
Line |
  96 |  …   $return = Invoke-RestMethod -Method POST -Uri "https://graph.micros …
     |                ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
     |  {   "error": {     "code": "InvalidInput",     "message": "The field ImpactedAssets must be a string or array
     | type with a minimum length of \u00271\u0027.",     "innerError": {       "date": "2025-10-24T07:10:31",
     | "request-id": "9568a476-4075-4f3a-810e-7e32ce13ec7e",       "client-request-id":
     | "9568a476-4075-4f3a-810e-7e32ce13ec7e"     }   } }
Failed to create detection rule or an error occurred.
```

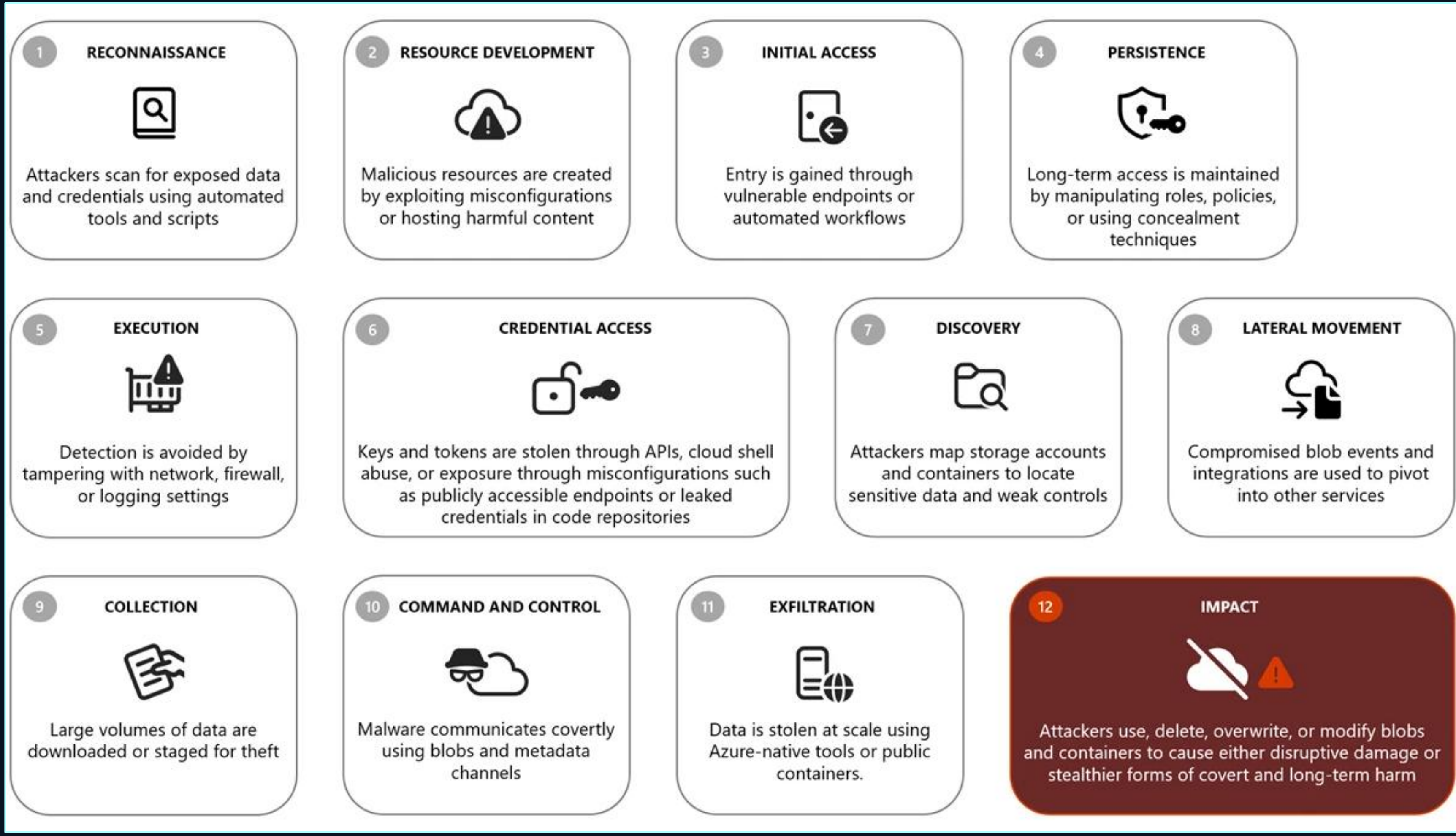
Building a new detection from A to Z



	BleepingCom...	69	CISA: High-severity Windows SMB flaw now exploited in attacks 3 TTPs •	CISA says threat actors are now actively exploiting a high-severity Windows SMB privilege escalation vulnerability that ca	13h
☑	Microsoft Sec...		Inside the attack chain: Threat activity targeting Azure Blob Storage 56 TTPs • Azure Blob Storage phishing attacks •	Azure Blob Storage , like any object data ser	14h
	Microsoft Sec...		Inside the attack chain: Threat activity targeting Azure Blob Storage 56 TTPs • Azure Blob Storage phishing attacks •	Azure Blob Storage , like any object data service, is a high-value target fo	14h
	BleepingCom...	32	Self-spreading GlassWorm malware hits OpenVSX, VS Code registries IoC > 1 IP • 15 TTPs • GlassWorm targets VSCode extensions •	A new and ongoing supply-chain attack is targeting	14h
	Threat intellig...		Inside the attack chain: Threat activity targeting Azure Blob Storage 56 TTPs • Azure Blob Storage phishing attacks •	Azure Blob Storage , like any object data service, is a high-value target fo	15h
	BleepingCom...		Microsoft fixes Windows Server Active Directory sync issues 2 TTPs •	Microsoft is rolling out a fix for Active Directory issues affecting some Windows Server 2025 systems after installing security	15h
	Alerts		CISA Adds Five Known Exploited Vulnerabilities to Catalog	CISA has added five new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog , based on evidence of active exploitation. CVE-20	16h
	BleepingCom...	59	Microsoft warns of Windows smart card auth issues after October updates 2 TTPs •	Microsoft says the October 2025 Windows security updates are causing smart card authentication and certific	16h
	BleepingCom...	29	Find hidden malicious OAuth apps in Microsoft 365 using Cazadora 3 TTPs •	Malicious OAuth apps can hide inside Microsoft 365 tenants. Huntress Labs' Cazadora script helps uncover rogue app	16h

https://www.microsoft.com/en-us/security/blog/2025/10/20/inside-the-attack-chain-threat-activity-targeting-azure-blob-storage/

Attack Chain



1 RECONNAISSANCE

Attackers scan for exposed data and credentials using automated tools and scripts

2 RESOURCE DEVELOPMENT

Malicious resources are created by exploiting misconfigurations or hosting harmful content

3 INITIAL ACCESS

Entry is gained through vulnerable endpoints or automated workflows

4 PERSISTENCE

Long-term access is maintained by manipulating roles, policies, or using concealment techniques

5 EXECUTION

Detection is avoided by tampering with network, firewall, or logging settings

6 CREDENTIAL ACCESS

Keys and tokens are stolen through APIs, cloud shell abuse, or exposure through misconfigurations such as publicly accessible endpoints or leaked credentials in code repositories

7 DISCOVERY

Attackers map storage accounts and containers to locate sensitive data and weak controls

8 LATERAL MOVEMENT

Compromised blob events and integrations are used to pivot into other services

9 COLLECTION

Large volumes of data are downloaded or staged for theft

10 COMMAND AND CONTROL

Malware communicates covertly using blobs and metadata channels

11 EXFILTRATION

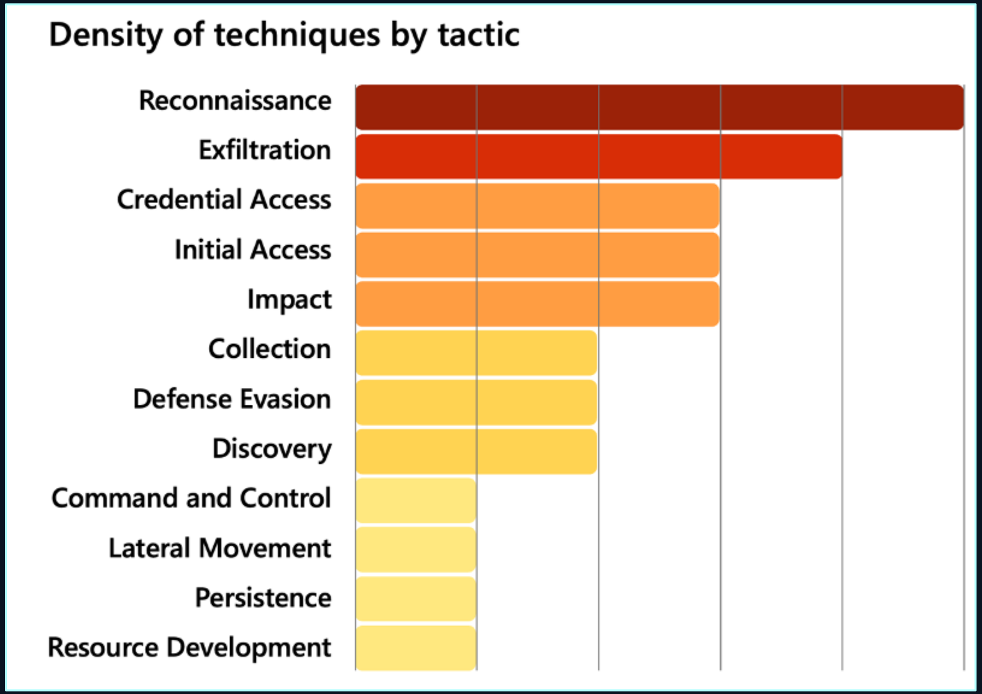
Data is stolen at scale using Azure-native tools or public containers.

12 IMPACT

Attackers use, delete, overwrite, or modify blobs and containers to cause either disruptive damage or stealthier forms of covert and long-term harm

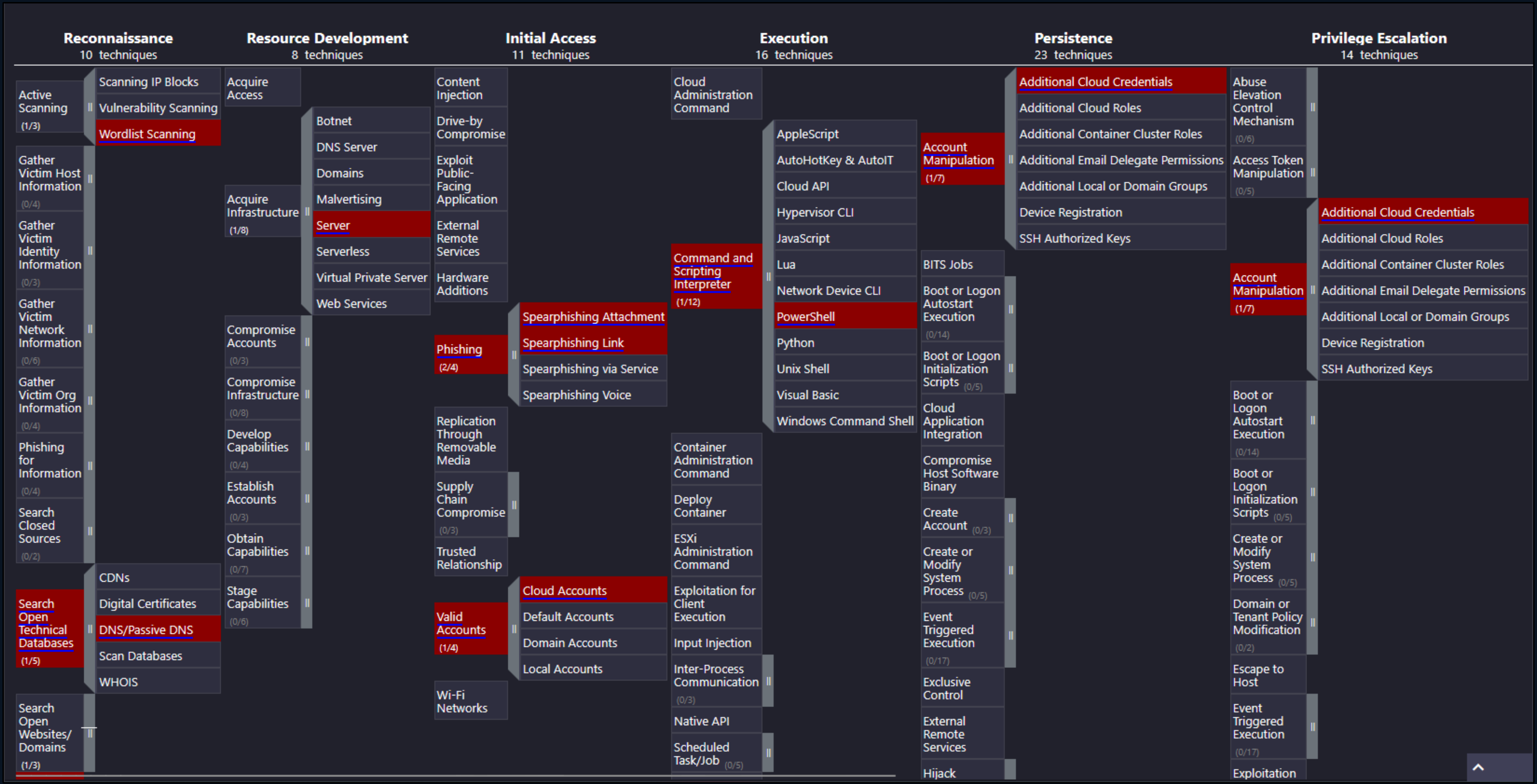
Detection gap analysis

- In this case, we are lacking detections against the entire attack chain
- We want to prioritize early warnings and initial access vectors



Density of techniques by tactic

https://security.microsoft.com/threatanalytics3/8d8a9fa0-4408-47be-8a07-7ce3d21eb827/analystreport



Reconnaissance
10 techniques

- Active Scanning (1/3)
  - Scanning IP Blocks
  - Vulnerability Scanning
  - Wordlist Scanning
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/4)
- Search Closed Sources (0/2)
- Search Open Technical Databases (1/5)
  - CDNs
  - Digital Certificates
  - DNS/Passive DNS
  - Scan Databases
  - WHOIS
- Search Open Websites/ Domains (1/3)

Resource Development
8 techniques

- Acquire Access
- Acquire Infrastructure (1/8)
  - Botnet
  - DNS Server
  - Domains
  - Malvertising
  - Server
  - Serverless
  - Virtual Private Server
  - Web Services
- Compromise Accounts (0/3)
- Compromise Infrastructure (0/8)
- Develop Capabilities (0/4)
- Establish Accounts (0/3)
- Obtain Capabilities (0/7)
- Stage Capabilities (0/6)

Initial Access
11 techniques

- Content Injection
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (2/4)
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing via Service
  - Spearphishing Voice
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (1/4)
  - Cloud Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
- Wi-Fi Networks

Execution
16 techniques

- Cloud Administration Command
- Command and Scripting Interpreter (1/12)
  - AppleScript
  - AutoHotKey & AutoIT
  - Cloud API
  - Hypervisor CLI
  - JavaScript
  - Lua
  - Network Device CLI
  - PowerShell
  - Python
  - Unix Shell
  - Visual Basic
  - Windows Command Shell
- Container Administration Command
- Deploy Container
- ESXi Administration Command
- Exploitation for Client Execution
- Input Injection
- Inter-Process Communication (0/3)
- Native API
- Scheduled Task/Job (0/5)

Persistence
23 techniques

- Account Manipulation (1/7)
  - Additional Cloud Credentials
  - Additional Cloud Roles
  - Additional Container Cluster Roles
  - Additional Email Delegate Permissions
  - Additional Local or Domain Groups
  - Device Registration
  - SSH Authorized Keys
- BITS Jobs
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Cloud Application Integration
- Compromise Host Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/5)
- Event Triggered Execution (0/17)
- Exclusive Control
- External Remote Services
- Hijack

Privilege Escalation
14 techniques

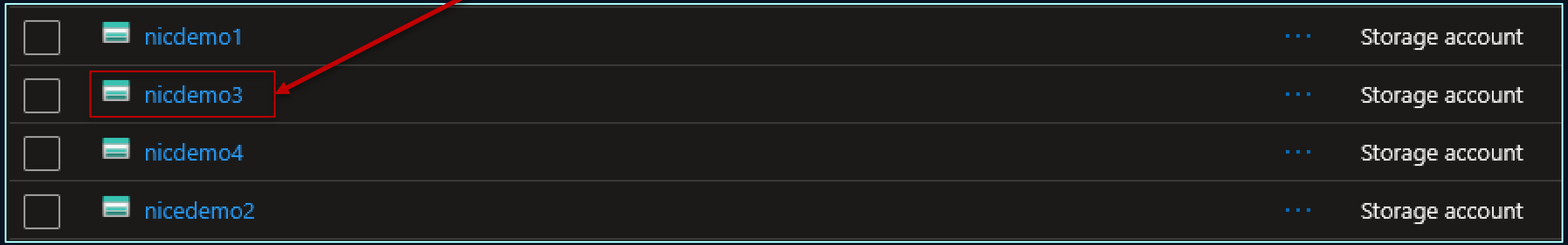
- Abuse Elevation Control Mechanism (0/6)
- Access Token Manipulation (0/5)
- Account Manipulation (1/7)
  - Additional Cloud Credentials
  - Additional Cloud Roles
  - Additional Container Cluster Roles
  - Additional Email Delegate Permissions
  - Additional Local or Domain Groups
  - Device Registration
  - SSH Authorized Keys
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/5)
- Domain or Tenant Policy Modification (0/2)
- Escape to Host
- Event Triggered Execution (0/17)
- Exploitation

NIC REBEL EDITION

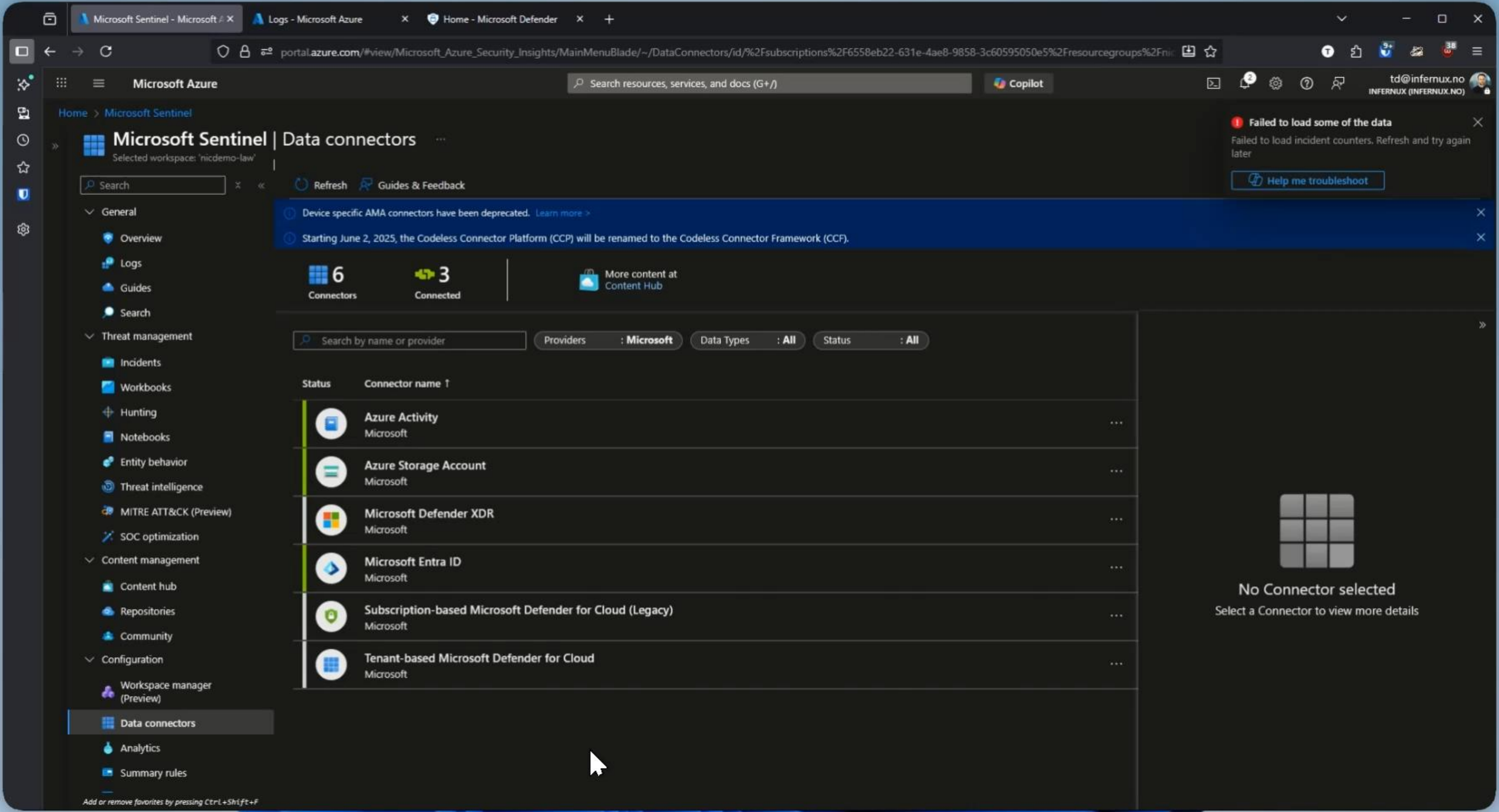
https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fexports.feedly.com%2Fattacks%2F244b0f639c283960c49d6ce51d48cb65%2Ffeedly-ai-inside-the-attack-chain-threat-activity-targeting.json&leave_site_dialog=false

Public network access (default)

Anonymous access for blobs



□	nicdemo1	···	Storage account
□	nicdemo3	···	Storage account
□	nicdemo4	···	Storage account
□	nicedemo2	···	Storage account



Microsoft Sentinel | Data connectors

Selected workspace: 'nicdemo-law'

Failed to load some of the data

Failed to load incident counters. Refresh and try again later

Device specific AMA connectors have been deprecated. Learn more >

Starting June 2, 2025, the Codeless Connector Platform (CCP) will be renamed to the Codeless Connector Framework (CCF).

6 Connectors

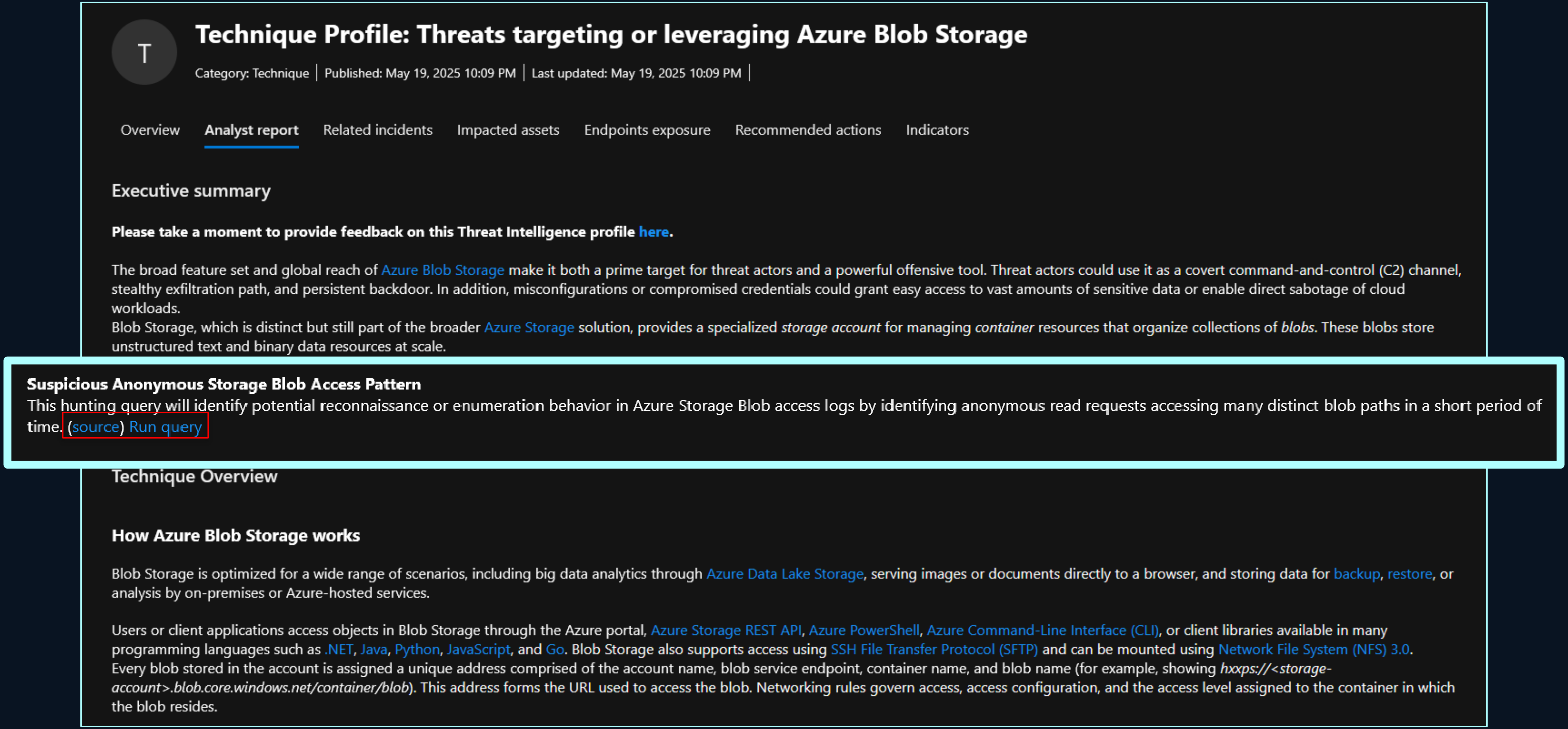
3 Connected

More content at Content Hub

Status	Connector name ↑
	Azure Activity Microsoft
	Azure Storage Account Microsoft
	Microsoft Defender XDR Microsoft
	Microsoft Entra ID Microsoft
	Subscription-based Microsoft Defender for Cloud (Legacy) Microsoft
	Tenant-based Microsoft Defender for Cloud Microsoft

No Connector selected

Select a Connector to view more details



Technique Profile: Threats targeting or leveraging Azure Blob Storage

Category: Technique | Published: May 19, 2025 10:09 PM | Last updated: May 19, 2025 10:09 PM |

Executive summary

Please take a moment to provide feedback on this Threat Intelligence profile here.

The broad feature set and global reach of Azure Blob Storage make it both a prime target for threat actors and a powerful offensive tool. Threat actors could use it as a covert command-and-control (C2) channel, stealthy exfiltration path, and persistent backdoor. In addition, misconfigurations or compromised credentials could grant easy access to vast amounts of sensitive data or enable direct sabotage of cloud workloads.
Blob Storage, which is distinct but still part of the broader Azure Storage solution, provides a specialized *storage account* for managing *container* resources that organize collections of *blobs*. These blobs store unstructured text and binary data resources at scale.

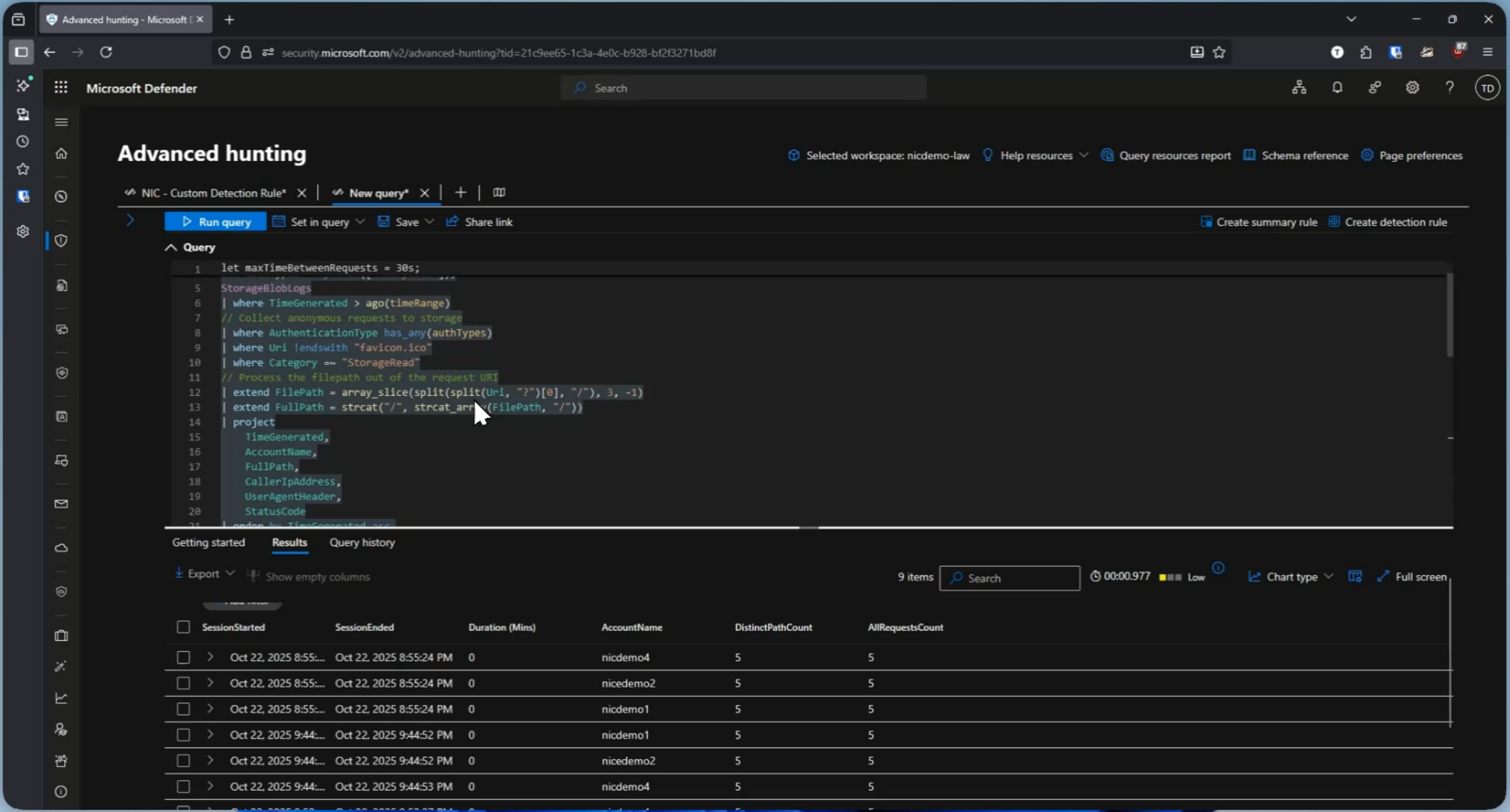
Suspicious Anonymous Storage Blob Access Pattern
This hunting query will identify potential reconnaissance or enumeration behavior in Azure Storage Blob access logs by identifying anonymous read requests accessing many distinct blob paths in a short period of time. (source) Run query

Technique Overview

How Azure Blob Storage works

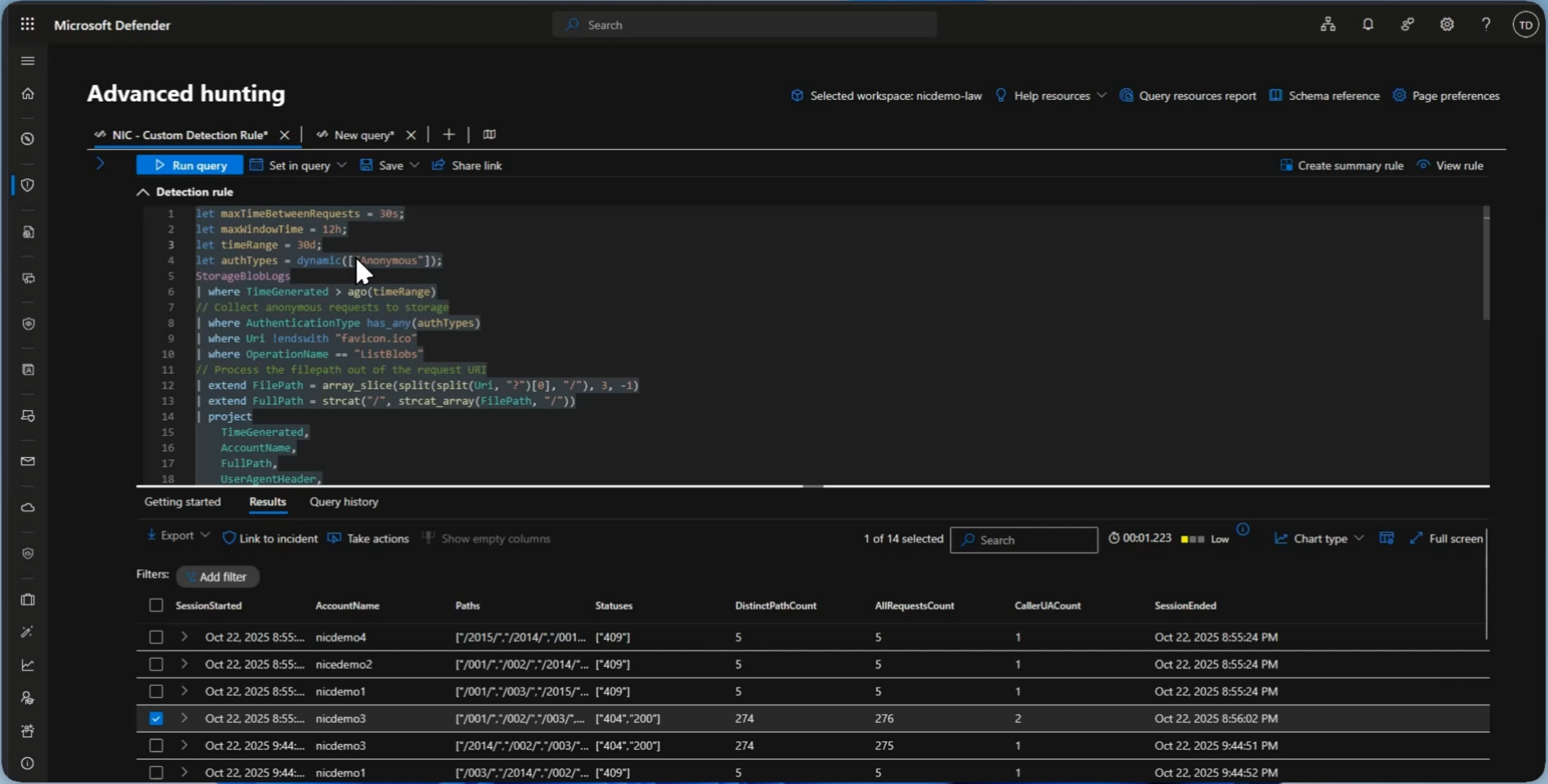
Blob Storage is optimized for a wide range of scenarios, including big data analytics through Azure Data Lake Storage, serving images or documents directly to a browser, and storing data for backup, restore, or analysis by on-premises or Azure-hosted services.

Users or client applications access objects in Blob Storage through the Azure portal, Azure Storage REST API, Azure PowerShell, Azure Command-Line Interface (CLI), or client libraries available in many programming languages such as .NET, Java, Python, JavaScript, and Go. Blob Storage also supports access using SSH File Transfer Protocol (SFTP) and can be mounted using Network File System (NFS) 3.0.
Every blob stored in the account is assigned a unique address comprised of the account name, blob service endpoint, container name, and blob name (for example, showing *hxxps://<storage-account>.blob.core.windows.net/container/blob*). This address forms the URL used to access the blob. Networking rules govern access, access configuration, and the access level assigned to the container in which the blob resides.



```
let maxTimeBetweenRequests = 30s;
StorageBlobLogs
| where TimeGenerated > ago(timeRange)
// Collect anonymous requests to storage
| where AuthenticationType has_any(authTypes)
| where Uri !endswith "favicon.ico"
| where Category =~ "StorageRead"
// Process the filepath out of the request URI
| extend FilePath = array_slice(split(split(Uri, "?")[0], "/"), 3, -1)
| extend FullPath = strcat("/", strcat_array(FilePath, "/"))
| project
    TimeGenerated,
    AccountName,
    FullPath,
    CallerIpAddress,
    UserAgentHeader,
    StatusCode
| order by TimeGenerated asc
```

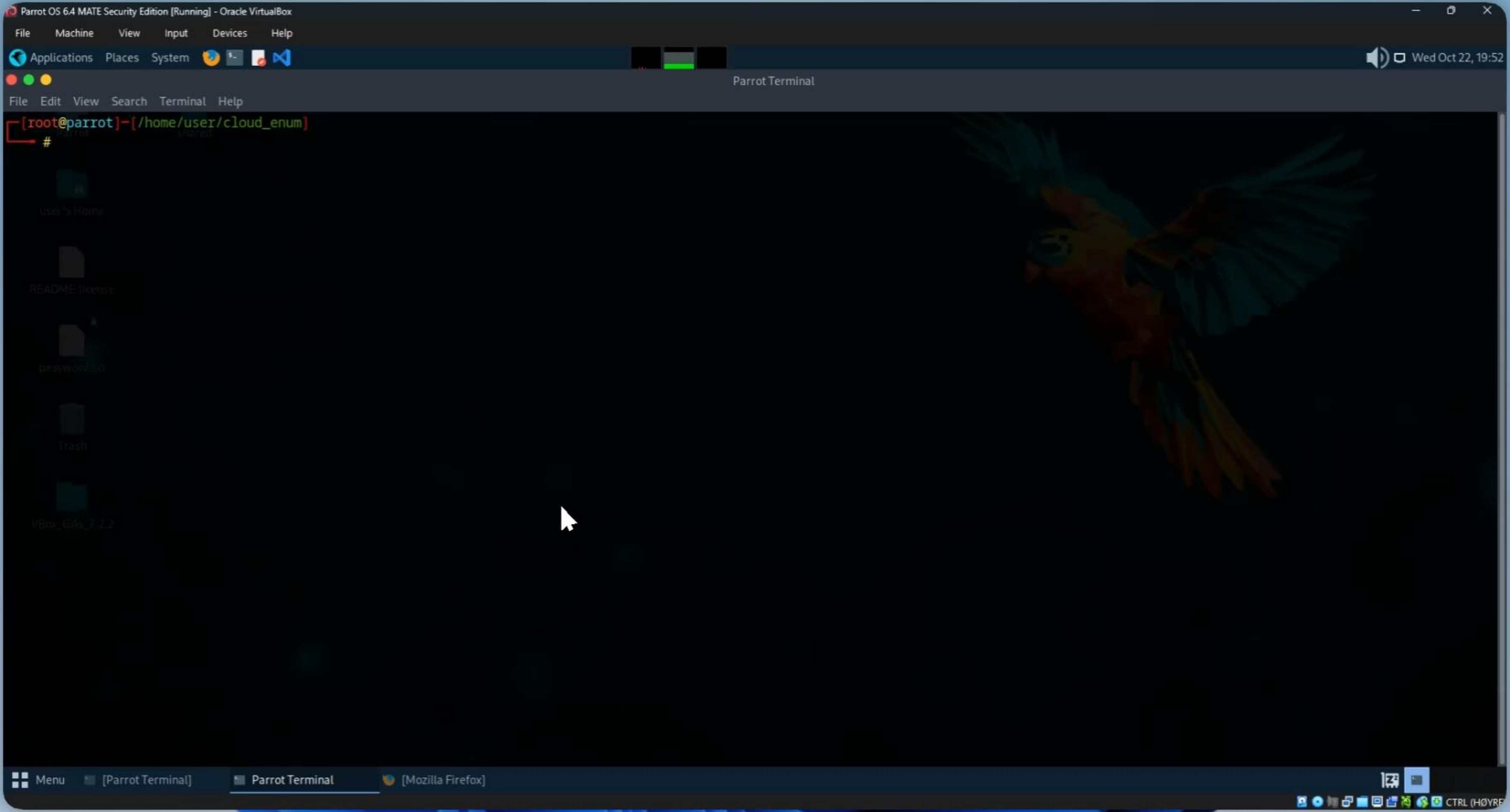
SessionStarted	SessionEnded	Duration (Mins)	AccountName	DistinctPathCount	AllRequestsCount
Oct 22, 2025 8:55:...	Oct 22, 2025 8:55:24 PM	0	nicdemo4	5	5
Oct 22, 2025 8:55:...	Oct 22, 2025 8:55:24 PM	0	nicedemo2	5	5
Oct 22, 2025 8:55:...	Oct 22, 2025 8:55:24 PM	0	nicdemo1	5	5
Oct 22, 2025 9:44:...	Oct 22, 2025 9:44:52 PM	0	nicdemo1	5	5
Oct 22, 2025 9:44:...	Oct 22, 2025 9:44:52 PM	0	nicedemo2	5	5
Oct 22, 2025 9:44:...	Oct 22, 2025 9:44:53 PM	0	nicdemo4	5	5



Advanced hunting

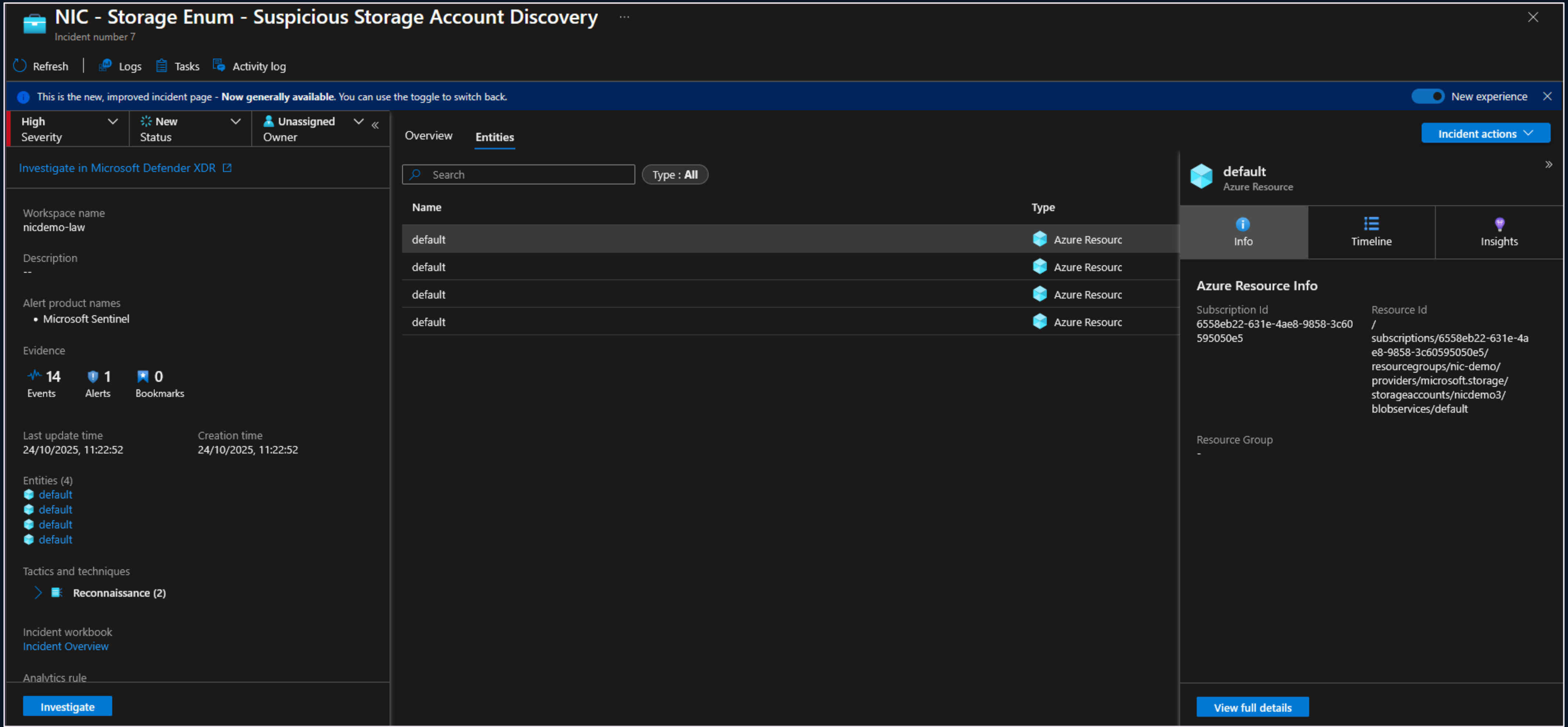
```
let maxTimeBetweenRequests = 30s;
let maxWindowTime = 12h;
let timeRange = 30d;
let authTypes = dynamic(["Anonymous"]);
StorageBlobLogs
| where TimeGenerated > ago(timeRange)
// Collect anonymous requests to storage
| where AuthenticationType has_any(authTypes)
| where Uri !endswith "favicon.ico"
| where OperationName == "ListBlobs"
// Process the filepath out of the request URI
| extend FilePath = array_slice(split(split(Uri, "?")[0], "/"), 3, -1)
| extend FullPath = strcat("/", strcat_array(FilePath, "/"))
| project
  TimeGenerated,
  AccountName,
  FullPath,
  UserAgentHeader,
```

☐	SessionStarted	AccountName	Paths	Statuses	DistinctPathCount	AllRequestsCount	CallerUACount	SessionEnded
☐	Oct 22, 2025 8:55:...	nicdemo4	["/2015/","/2014/","/001...	["409"]	5	5	1	Oct 22, 2025 8:55:24 PM
☐	Oct 22, 2025 8:55:...	nicedemo2	["/001/","/002/","/2014/"...	["409"]	5	5	1	Oct 22, 2025 8:55:24 PM
☐	Oct 22, 2025 8:55:...	nicdemo1	["/001/","/003/","/2015/"...	["409"]	5	5	1	Oct 22, 2025 8:55:24 PM
☑	Oct 22, 2025 8:55:...	nicdemo3	["/001/","/002/","/003/",...	["404","200"]	274	276	2	Oct 22, 2025 8:56:02 PM
☐	Oct 22, 2025 9:44:...	nicdemo3	["/2014/","/002/","/003/"...	["404","200"]	274	275	1	Oct 22, 2025 9:44:51 PM
☐	Oct 22, 2025 9:44:...	nicdemo1	["/003/","/2014/","/002/"...	["409"]	5	5	1	Oct 22, 2025 9:44:52 PM



Parrot OS 6.4 MATE Security Edition [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places System
Wed Oct 22, 19:52
Parrot Terminal
File Edit View Search Terminal Help
Menu
[Parrot Terminal]
Parrot Terminal
[Mozilla Firefox]
CTRL (HØYRE

```
┌─[root@parrot]─[/home/user/cloud_enum]
└──╼ #
```



NIC - Storage Enum - Suspicious Storage Account Discovery

Incident number 7

This is the new, improved incident page - **Now generally available.** You can use the toggle to switch back. New experience

High
Severity

New
Status

Unassigned
Owner

Investigate in Microsoft Defender XDR

Workspace name
nicdemo-law

Description
--

Alert product names
- Microsoft Sentinel

Evidence

14	1	0
Events	Alerts	Bookmarks

Last update time
24/10/2025, 11:22:52

Creation time
24/10/2025, 11:22:52

Entities (4)
default
default
default
default

Tactics and techniques
Reconnaissance (2)

Incident workbook
Incident Overview

Analytics rule

Name	Type
default	Azure Resourc
default	Azure Resourc
default	Azure Resourc
default	Azure Resourc

default
Azure Resource

Azure Resource Info

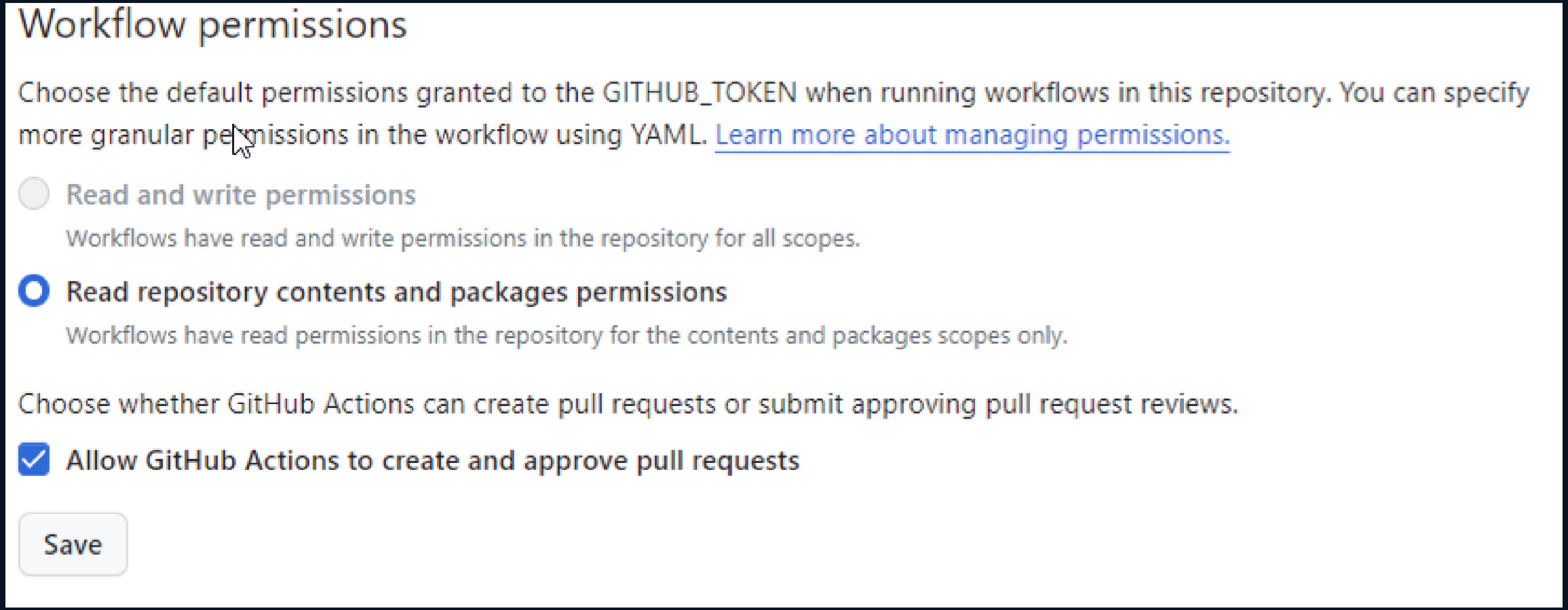
Subscription Id
6558eb22-631e-4ae8-9858-3c60595050e5

Resource Id
/subscriptions/6558eb22-631e-4ae8-9858-3c60595050e5/resourcegroups/nic-demo/providers/microsoft.storage/storageaccounts/nicdemo3/blobservices/default

Resource Group
-

CI/CD GitHub Action

If you building more advanced flows that require GH Action to create PR



Workflow permissions

Choose the default permissions granted to the GITHUB_TOKEN when running workflows in this repository. You can specify more granular permissions in the workflow using YAML. Learn more about managing permissions.

○ Read and write permissions

Workflows have read and write permissions in the repository for all scopes.

● Read repository contents and packages permissions

Workflows have read permissions in the repository for the contents and packages scopes only.

Choose whether GitHub Actions can create pull requests or submit approving pull request reviews.

☑ Allow GitHub Actions to create and approve pull requests

NIC REBEL EDITION

Sentinel CI/CD Sync

- Still in preview (my prediction is that it will never leave preview)
- Change to OICD login auth
- Support Bicep and ARM
- build your own like demonstrated