From anonymous user to Global Admin in 45min

... , or not!

MC2MC

CONNECT


CONNECT. COLLABORATE. CREATE
MC2MC
CONNECT


2Pint


PATCH
MY PC


robopack


wortell


INGRAM
MICRO


The Collective


bechtle


lebon.IT


ConXioN
The new style of IT


VirtualMetric


veeam


evri

ROGIER DIJKMAN

- name: Rogier Dijkman
- located_in: The Netherlands
- current_job: Cloud Security Architect
- company: Rubicon Cloud Advisors
- Microsoft MVP (Security / Identity)

FABIAN BADER

- Lives in Hamburg, Germany
- Cyber Security Architect @ glueckkanja AG
- Microsoft MVP (Security / Azure)
- Organizer of "Purple Elbe Security User Group"

Agenda

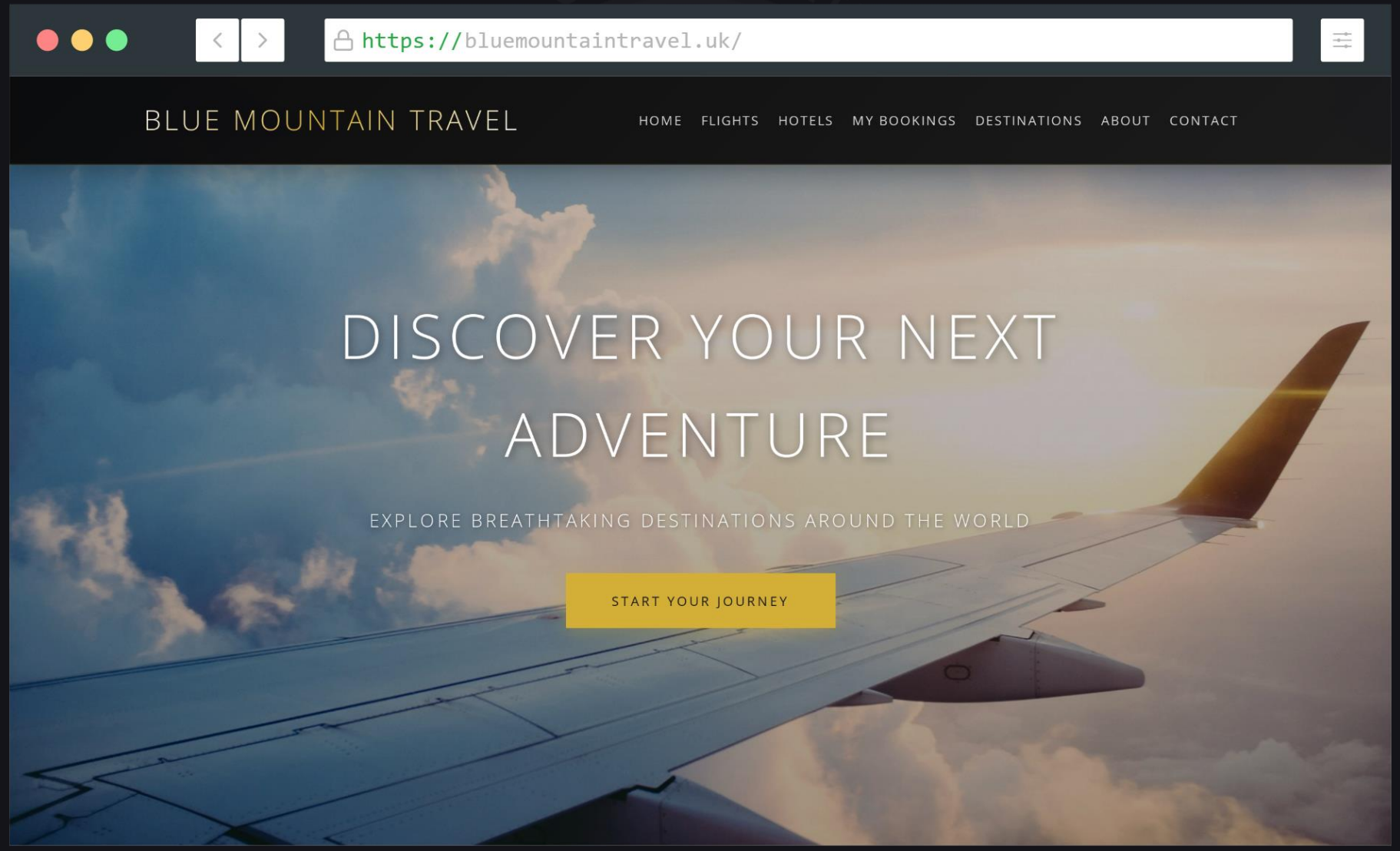
- Meet "Blue Mountain Travel Ltd."
- Live Hacking and Defending
- The end!?

Blue Mountain Travel

- UK-based travel agency undergoing digital transformation.

- Recently migrated their HR onboarding portal to Azure, using:
  - Azure App Service for the HR portal
  - Azure Files for onboarding document storage
  - Azure SQL for HR database
  - User Assigned Managed Identity (UAMI) for CI/CD automation
  - GitHub Actions for deployment pipelines

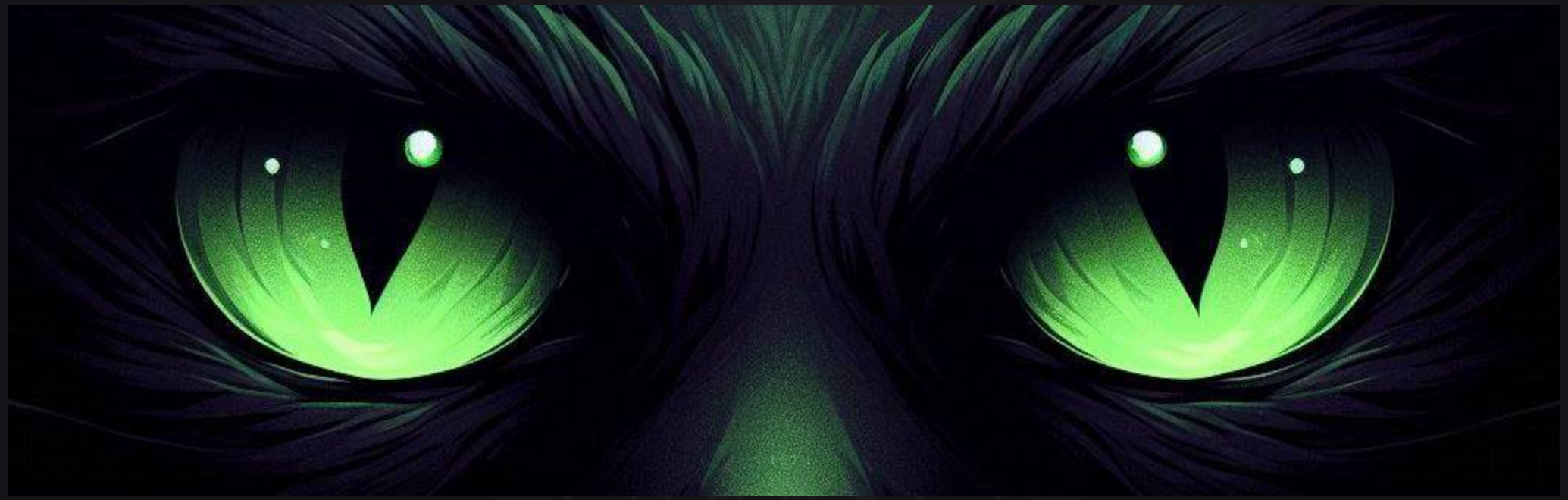
Blue Mountain Travel



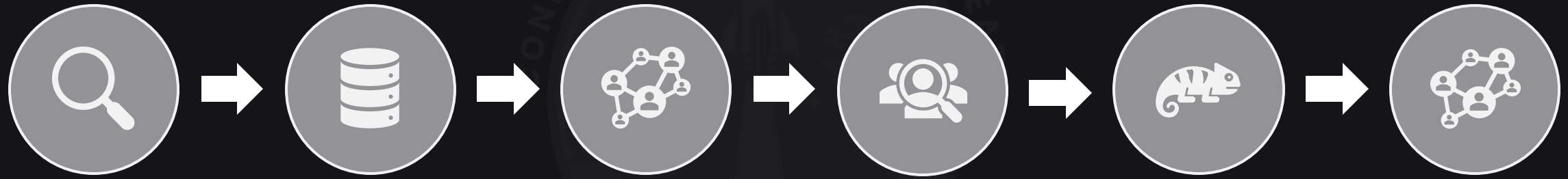
Protection

- Microsoft Defender XDR + Defender for Cloud
- Microsoft Sentinel
- Additional log sources:
  - Azure Activity
  - Entra ID Sign-in logs
  - Storage Activity Logs
  - User and behaviour analytics

B7 4 C K C @ T



The attack chain



TA0043
Reconnaissance

TA0009
Collection

TA0001
Initial Access

TA0007
Discovery

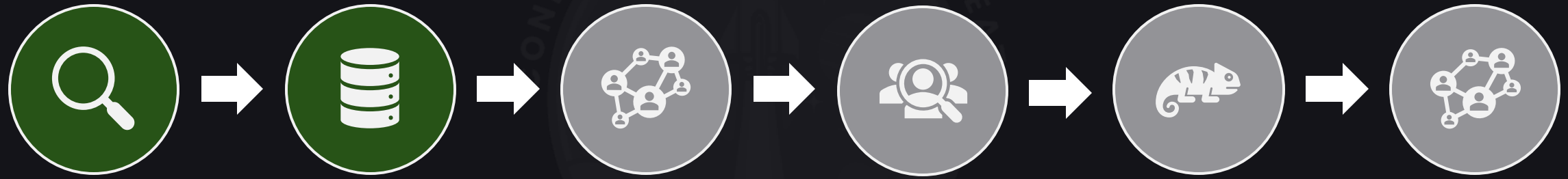
TA0003
Persistence

TA0004
Privilege Escalation

TA0003
Game Over

Phase #1 + #2

The attack chain



TA0043
Reconnaissance

TA0009
Collection

TA0001
Initial Access

TA0007
Discovery

TA0003
Persistence

TA0004
Privilege Escalation

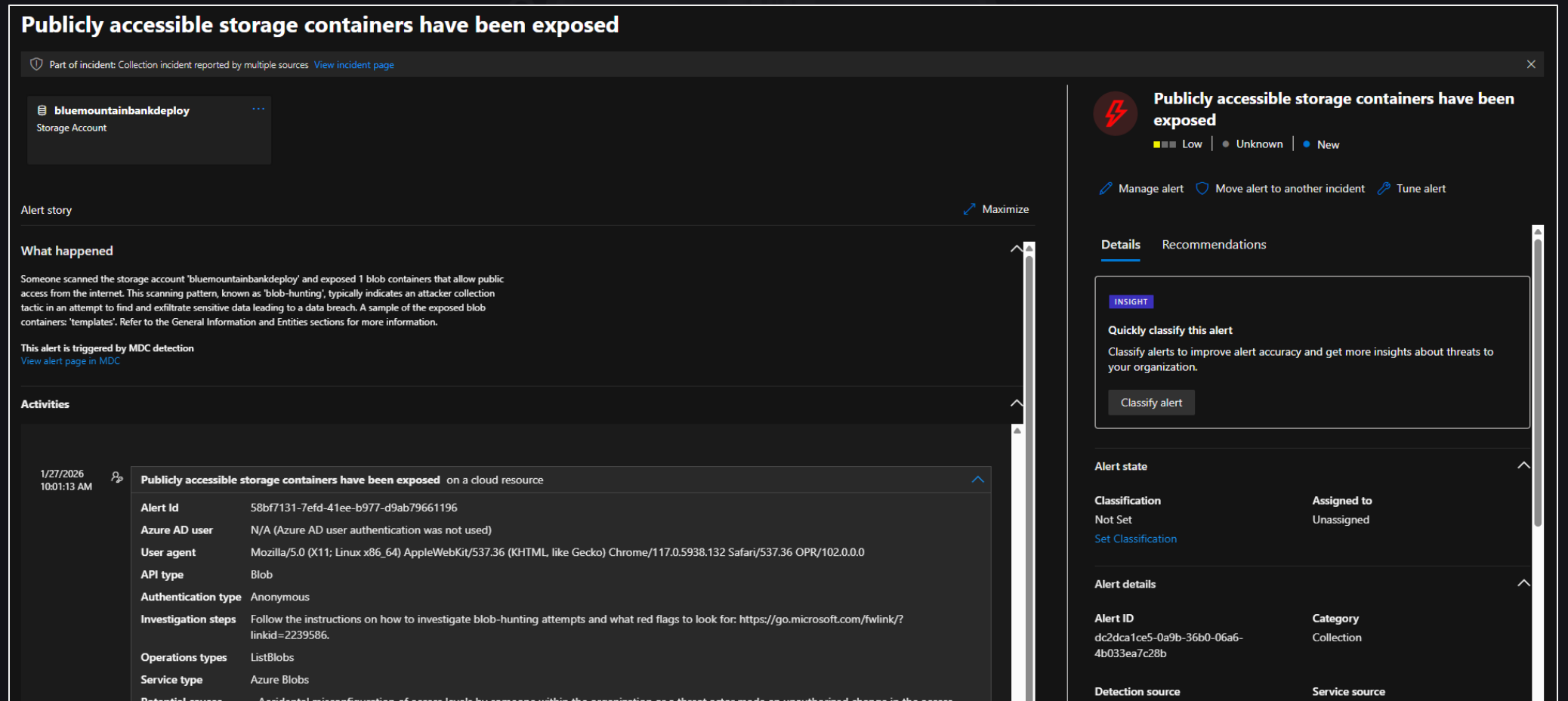
T1589
T1590
T1598.003

T1552
T1552.007

TA0003
Game Over

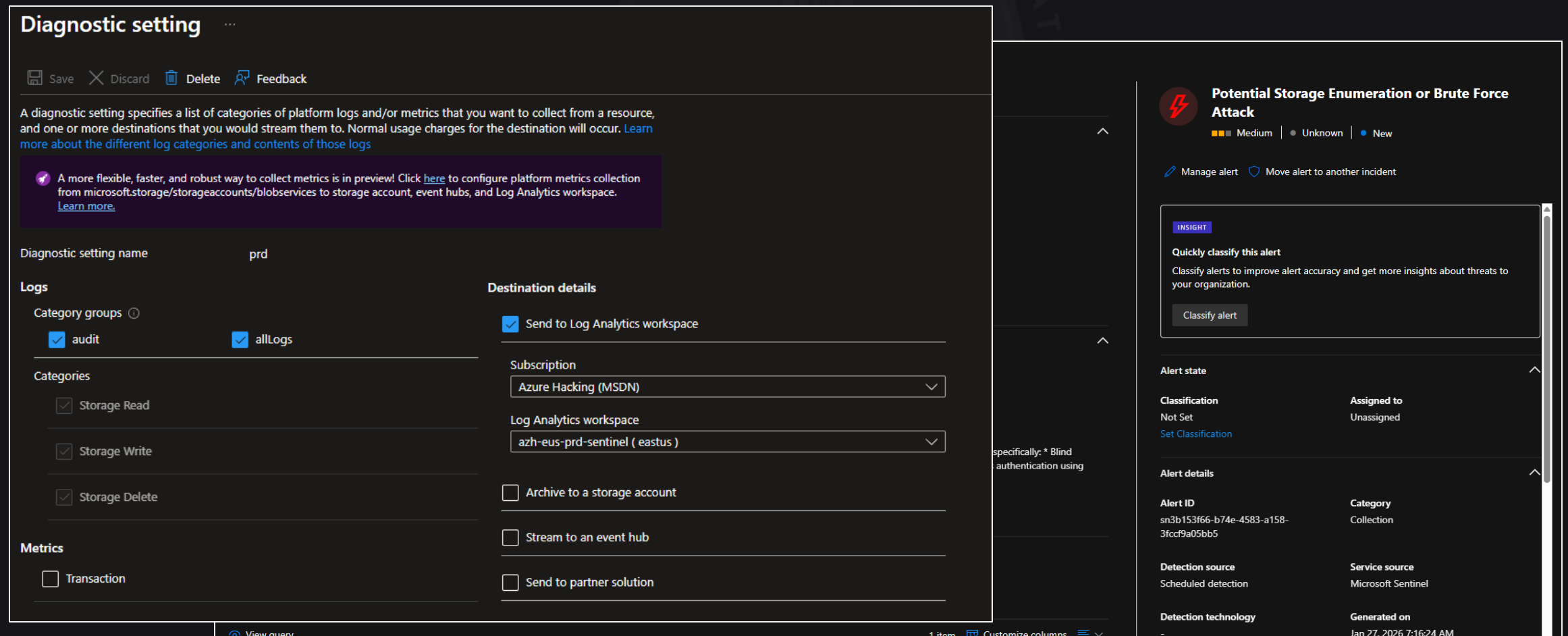
Detection

- Defender for Cloud - $10/Storage account/month



Detection

- Custom Detections requires Storage Diagnostic Logs



Detection

Anonymous Retrieval of Azure Blob Versions

Part of incident: Multi-stage incident involving Initial access & Collection involving multiple users reported by multiple sources View incident page

What happened

This rule detects a sequence of suspicious activities where an unauthenticated (anonymous) source enumerates the version history of a storage blob and subsequently downloads a blob from the same path within a 10-minute window.

While public access to storage containers may be intentional, attackers frequently target these containers to look for _soft-deleted_ data or previous versions of files. They do this to uncover sensitive information (such as hardcoded credentials, API keys, or PII) that may have been present in an older version of a file but removed in the current _live_ version.

ANALYTICS RULE

Anonymous Retrieval of Azure Blob Versions

Low | Unknown | New

Manage alert | Move alert to another incident

Classification
Not Set
Set Classification

Assigned to
Unassigned

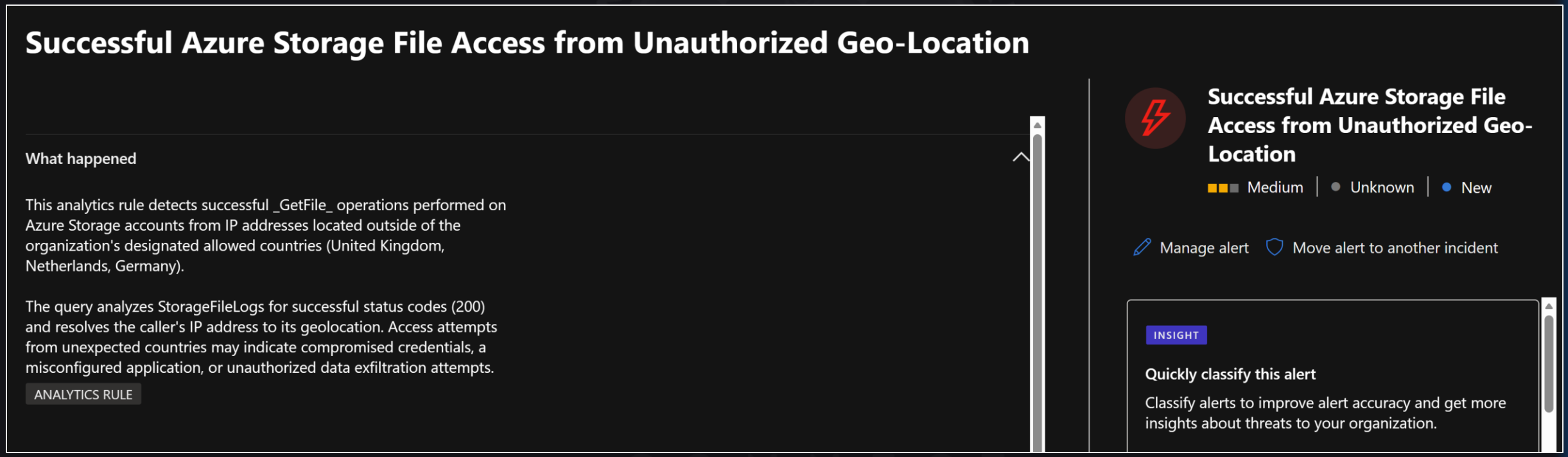
Alert details

Alert ID
sncf215ade-35ba-4114-a958-a1759c5699dd

Category
Collection

Detection

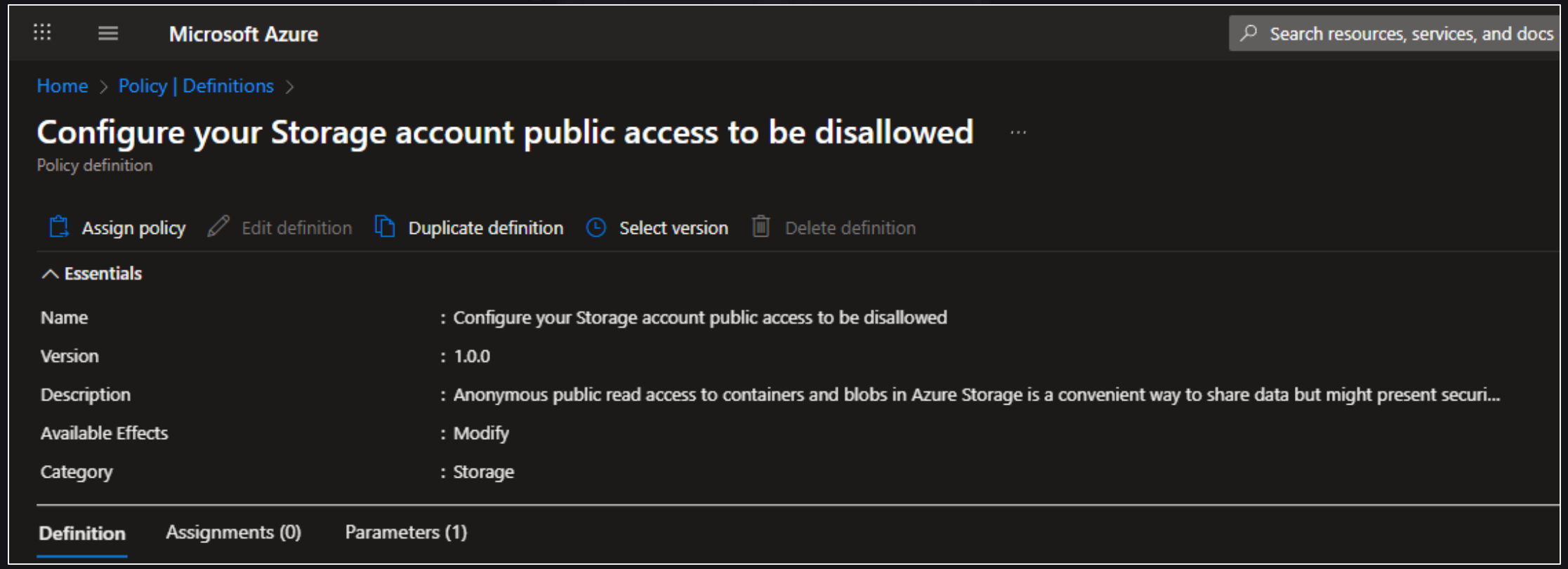
Successful Azure Storage File Access from Unauthorized Geo-Location



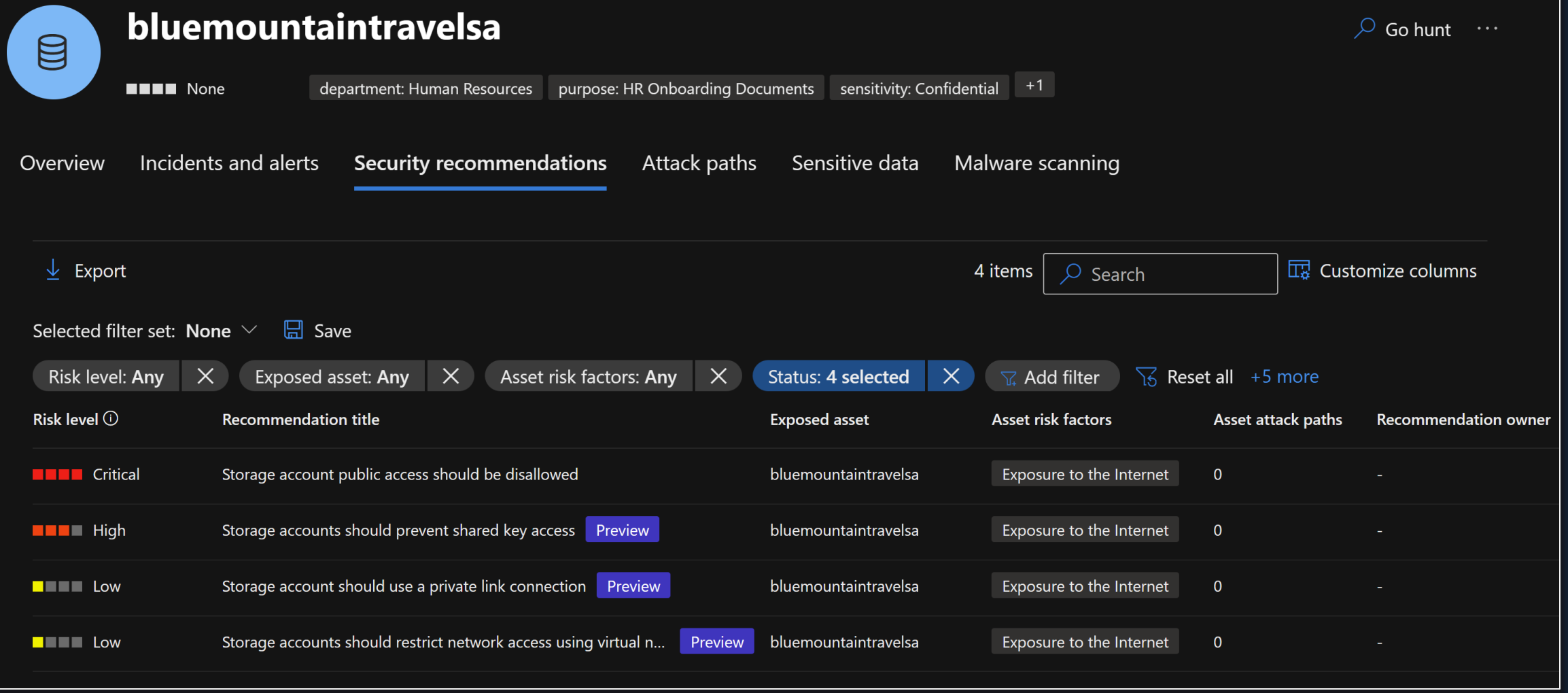
Demo

Prevention

- Use Azure Policies to prevent public exposure of storage accounts



Security recommendations



bluemountaintravelsa

Go hunt ···

None | department: Human Resources | purpose: HR Onboarding Documents | sensitivity: Confidential | +1

Overview | Incidents and alerts | **Security recommendations** | Attack paths | Sensitive data | Malware scanning

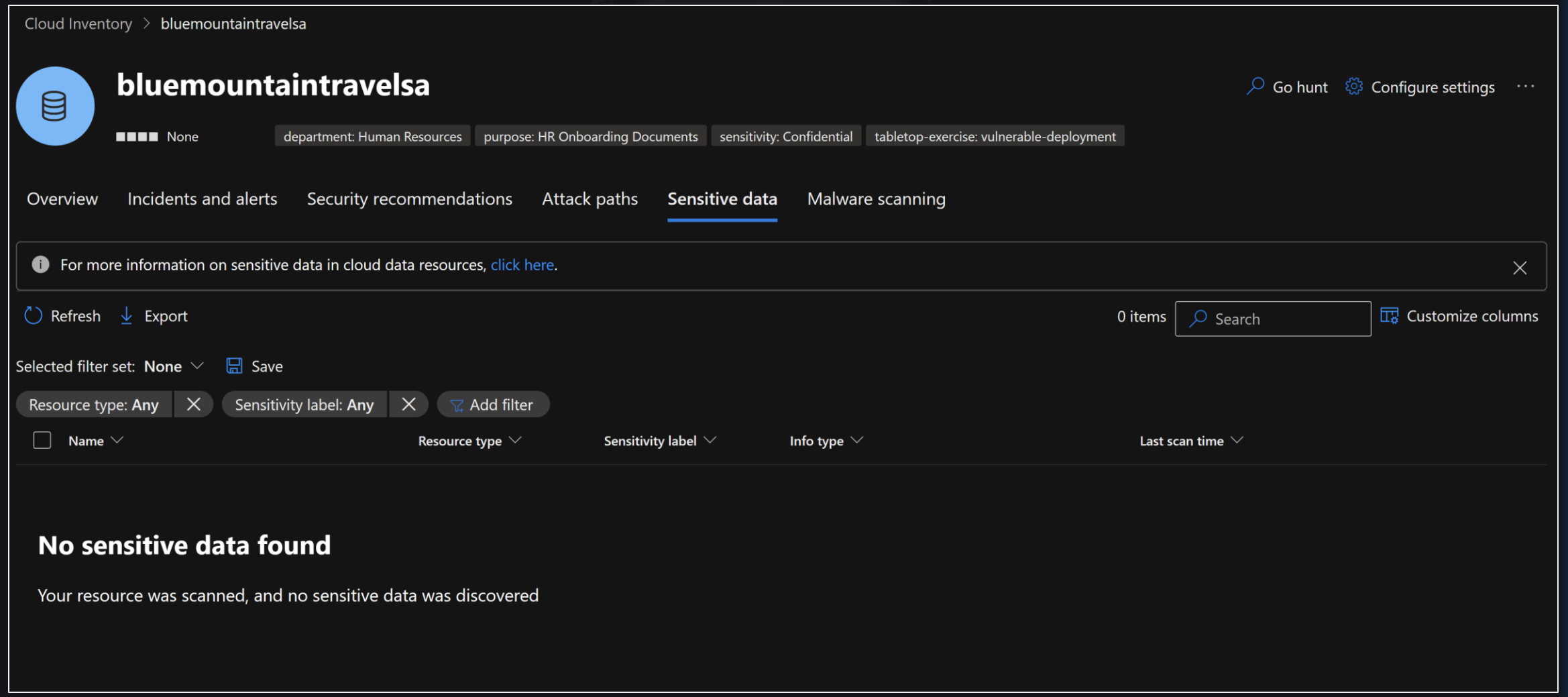
Export | 4 items | Search | Customize columns

Selected filter set: **None** | Save

Risk level: **Any** | Exposed asset: **Any** | Asset risk factors: **Any** | Status: **4 selected** | Add filter | Reset all | +5 more

Risk level	Recommendation title	Exposed asset	Asset risk factors	Asset attack paths	Recommendation owner
Critical	Storage account public access should be disallowed	bluemountaintravelsa	Exposure to the Internet	0	-
High	Storage accounts should prevent shared key access Preview	bluemountaintravelsa	Exposure to the Internet	0	-
Low	Storage account should use a private link connection Preview	bluemountaintravelsa	Exposure to the Internet	0	-
Low	Storage accounts should restrict network access using virtual n... Preview	bluemountaintravelsa	Exposure to the Internet	0	-

Secret scanning (not so much)



ID 68: Collection incident

Manage incident | Tasks | ...

Medium | Active | Unassigned | Unclassified | Last update time: Feb 5, 2026 10:01 AM

Attack story | Alerts (3) | Activities (7) | Assets (1) | Investigations (0) | Evidence and Response (2) | Summary

Detection & Categories

Active alerts
3/3

Categories
1

First activity
Feb 5, 2026 9:45:13 AM

Last activity
Feb 5, 2026 9:53:45 AM

Creation time
Feb 5, 2026 9:56:32 AM

Alerts

Feb 5, 2026 9:45 AM • New
Potential Storage Enumeration or Brute Force Attack
default

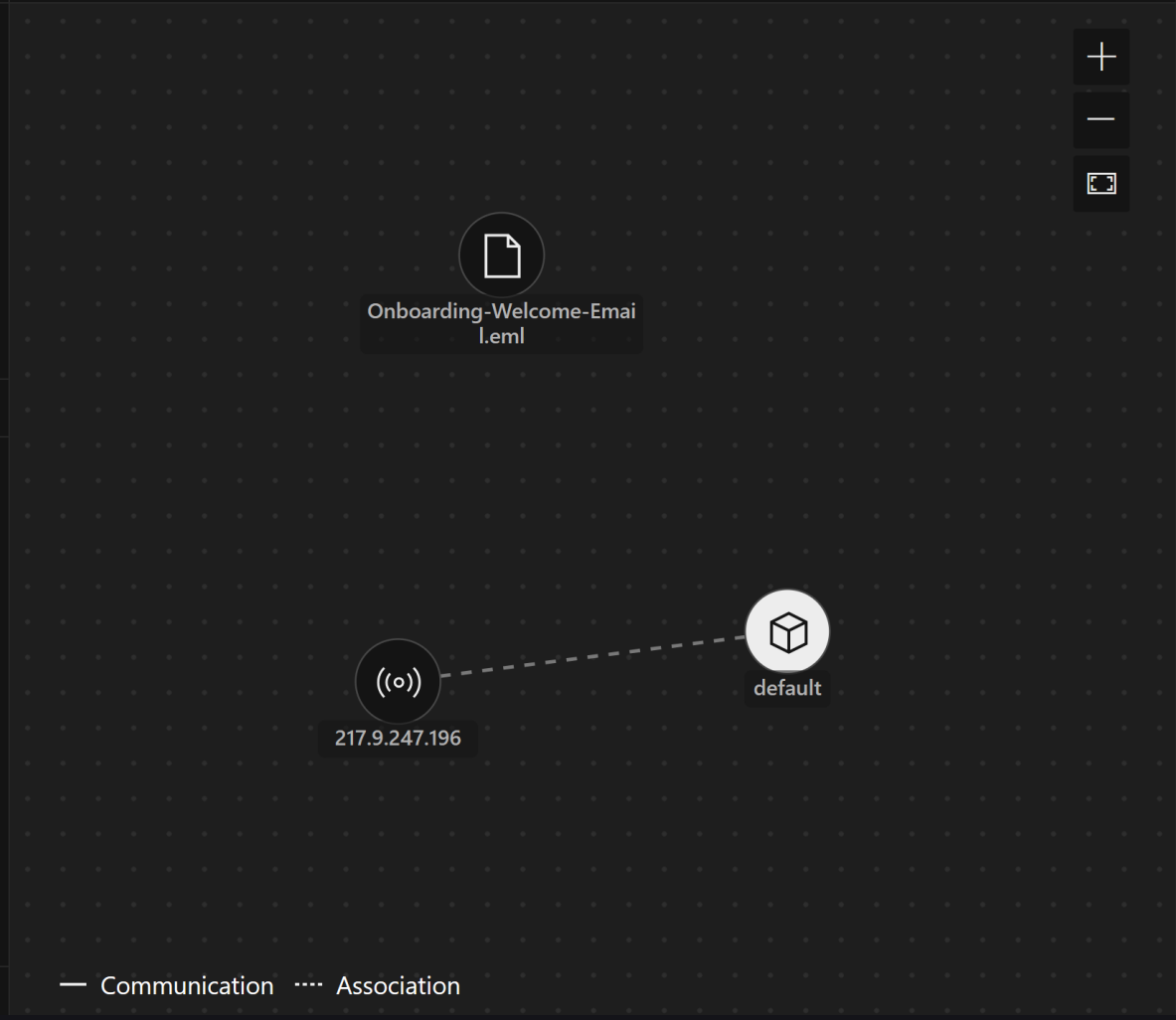
Feb 5, 2026 9:49 AM • New
Anonymous Retrieval of Azure Blob Versions

Feb 5, 2026 9:53 AM • New
Successful Azure Storage File Access from Unauthorized Geo-Location

Report incident inaccurracy

Incident graph

Layout | Group similar nodes



Priority assessment

Not set

This incident does not yet have a priority assigned.

Incident details

Assigned to
Unassigned

Incident ID
68

Classification
Not set

Categories
Collection

First activity
Feb 5, 2026 9:45:13 AM

Creation Time
Feb 5, 2026 9:56:32 AM

Last activity
Feb 5, 2026 9:53:45 AM

Workspaces
azh-eus-prd-sentinel

Incident description

Detected a pattern of failed access attempts against Azure Blob Storage where the failure rate exceeded 90% for a single source IP.

Choose your path

App Secret

User Password

Choose your path

App Secret

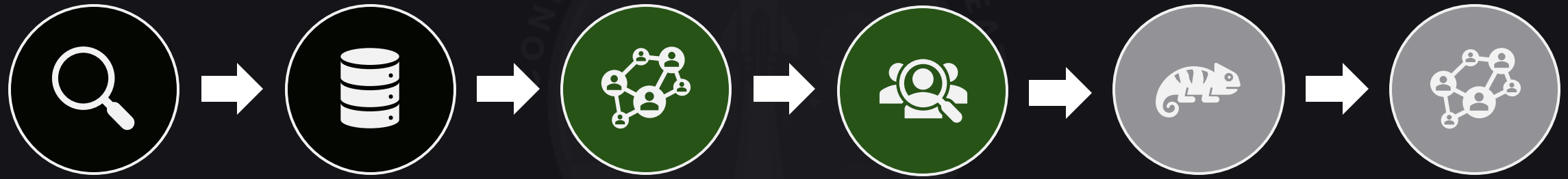
User Password

Choose your path

App Secret

Phase #3 + #4

The attack chain



TA0043
Reconnaissance

TA0009
Collection

TA0001
Initial Access

TA0007
Discovery

TA0003
Persistence

TA0004
Privilege Escalation

T1078.004
T1526

T1098.001
T1548.001
T1550.001

TA0003
Game Over

AppRoleAssignment.ReadWrite.All

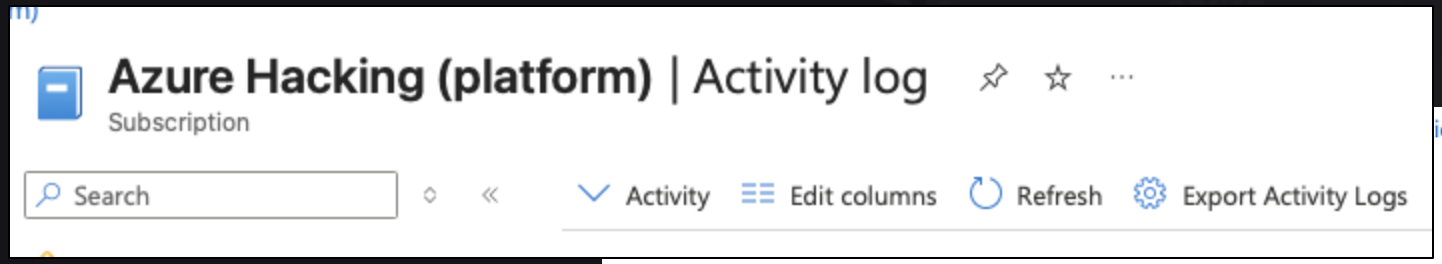
Permission	Justification Given	Actual Need	Real Risk
User.ReadWrite.All	"Create new employee accounts"	Legitimate	Medium
Group.ReadWrite.All	"Add employees to department groups"	Legitimate	Medium
Application.Read.All	"Read app info to validate assignments"	Sounds safe	Low
AppRoleAssignment.ReadWrite.All	"Assign new employees to Salesforce, ServiceNow, etc."	Sounds legitimate	**CRITICAL**

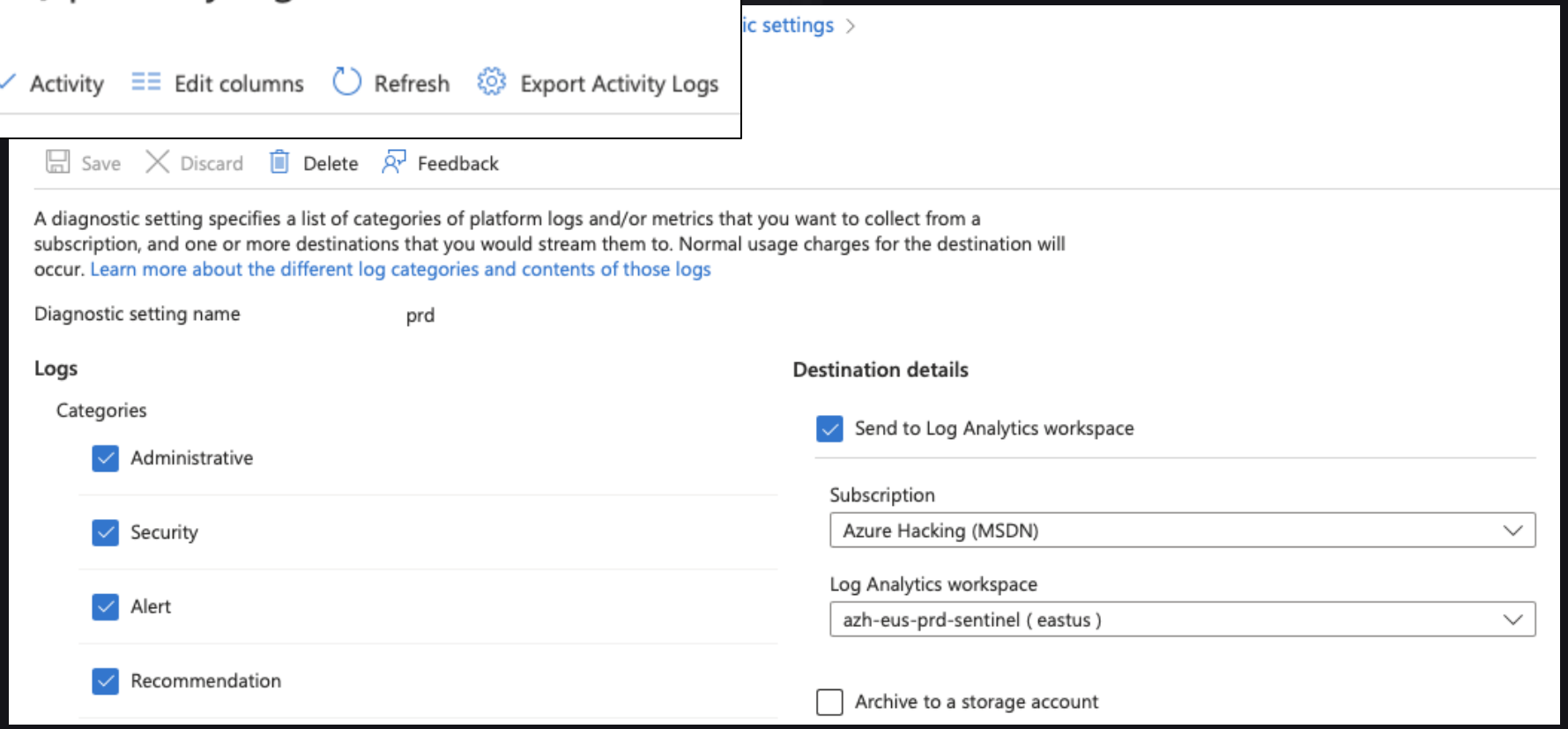
Detection

- Identity Protection for Workload Identities
- Custom detections
  - Based on location changes
  - Monitor for behavior changes
  - Monitor Microsoft Graph activity for discovery pattern
  - Alert when unknown Federated Identity Providers are used

Detection

- Custom Detection requires Subscription Diagnostic Logs (free)





Detection


Service Principal Sign-in from New Country
Part of incident: Multi-stage incident involving Initial access & Collection involving multiple users reported by multiple sources View incident page
What happened
This rule detects successful sign-ins (ResultType == 0) by a Service Principal from a country that has not been observed in the preceding 14 days. It establishes a baseline of _known_ locations for each AppId over a two-week period and alerts when a login occurs from a location outside of this baseline. This behavior may indicate that a Service Principal's credentials have been compromised and are being used from an anomalous location.
ANALYTICS RULE
Analytics rule details
Rule name
Service Principal Sign-in from New Country
Medium
Unknown
New
Manage alert
Move alert to another incident
INSIGHT
Quickly classify this alert
Classify alerts to improve alert accuracy and get more insights about threats to your organization.
Classify alert

Detection

Unauthorized Federated Credential Added to Managed Identity

rogier.dijkman

What happened

Detected the addition of an unauthorized Federated Identity Credential to a User Assigned Managed Identity.

The activity involved configuring a Managed Identity to trust a specific external repository or organization that was not on the approved allow-list.

This configuration established a potential backdoor, allowing:
* Persistence: External workflows (e.g., GitHub Actions) from the unauthorized organization (AttackerOrg) were authorized to exchange their OIDC tokens for valid Azure Access Tokens.
* Privilege Escalation: An external actor effectively gained the permissions associated with the internal Managed Identity without requiring a password or secret.
* Defense Evasion: The actor utilized legitimate cloud federation protocols to bypass traditional credential monitoring.

ANALYTICS RULE

Unauthorized Federated Credential Added to Managed Identity

Medium | Unknown | New

Manage alert | Move alert to another incident

INSIGHT

Quickly classify this alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

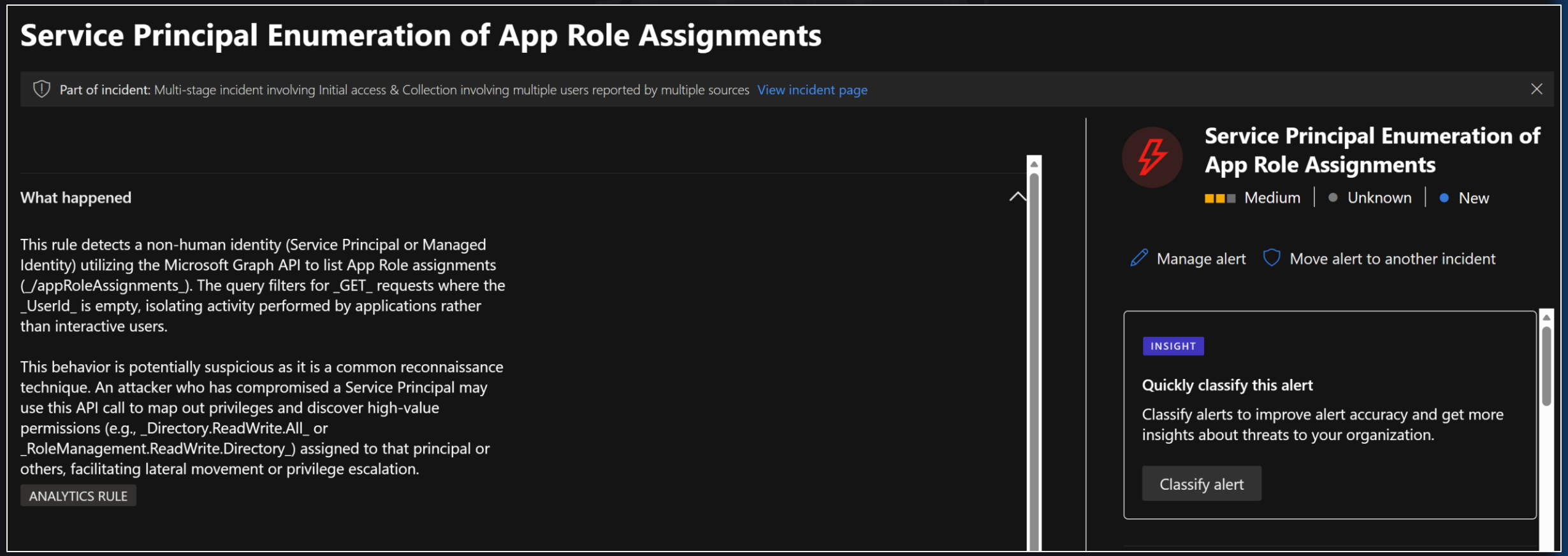
Classify alert

Alert state

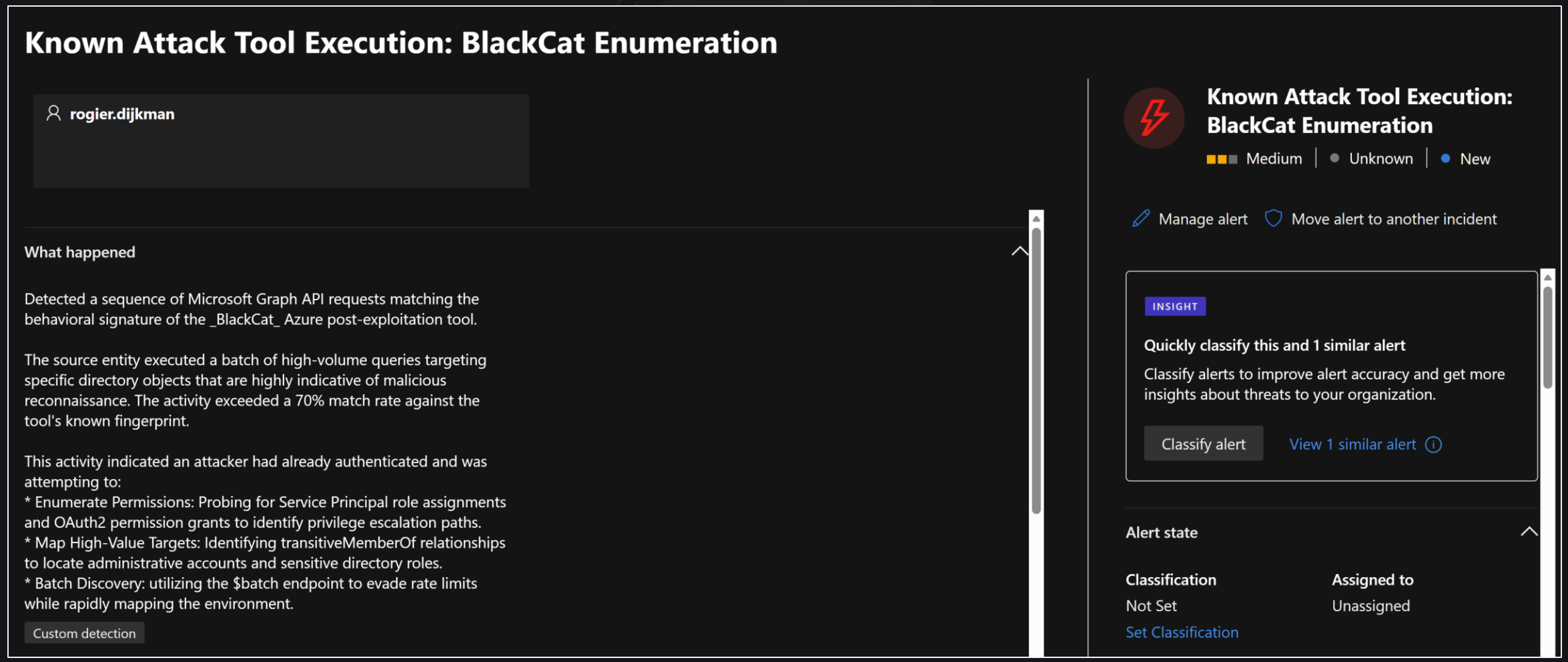
Classification	Assigned to
Not Set	Unassigned

Set Classification

Detection

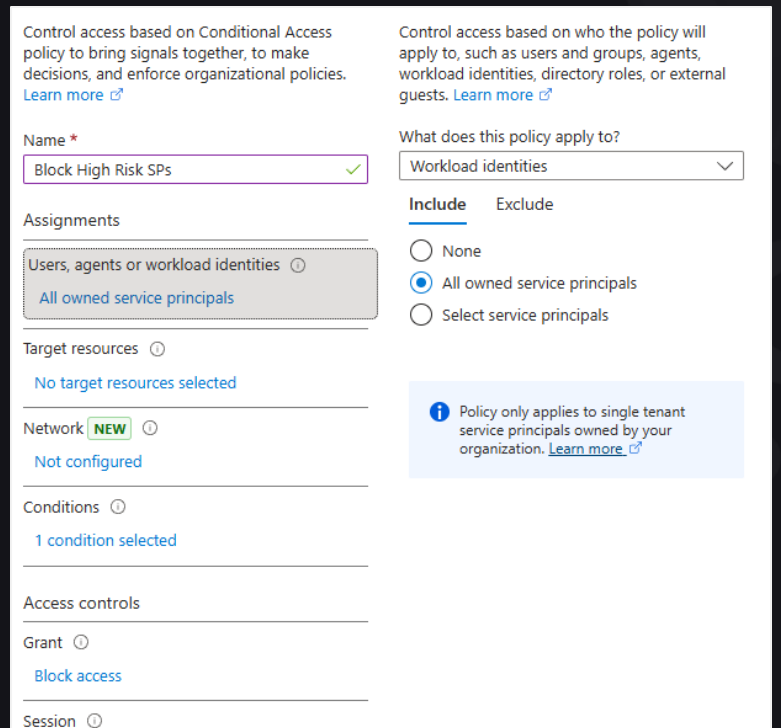

Service Principal Enumeration of App Role Assignments
Part of incident: Multi-stage incident involving Initial access & Collection involving multiple users reported by multiple sources View incident page
What happened
This rule detects a non-human identity (Service Principal or Managed Identity) utilizing the Microsoft Graph API to list App Role assignments (_/appRoleAssignments_). The query filters for _GET_ requests where the _UserId_ is empty, isolating activity performed by applications rather than interactive users.
This behavior is potentially suspicious as it is a common reconnaissance technique. An attacker who has compromised a Service Principal may use this API call to map out privileges and discover high-value permissions (e.g., _Directory.ReadWrite.All_ or _RoleManagement.ReadWrite.Directory_) assigned to that principal or others, facilitating lateral movement or privilege escalation.
ANALYTICS RULE
Service Principal Enumeration of App Role Assignments
Medium
Unknown
New
Manage alert
Move alert to another incident
INSIGHT
Quickly classify this alert
Classify alerts to improve alert accuracy and get more insights about threats to your organization.
Classify alert

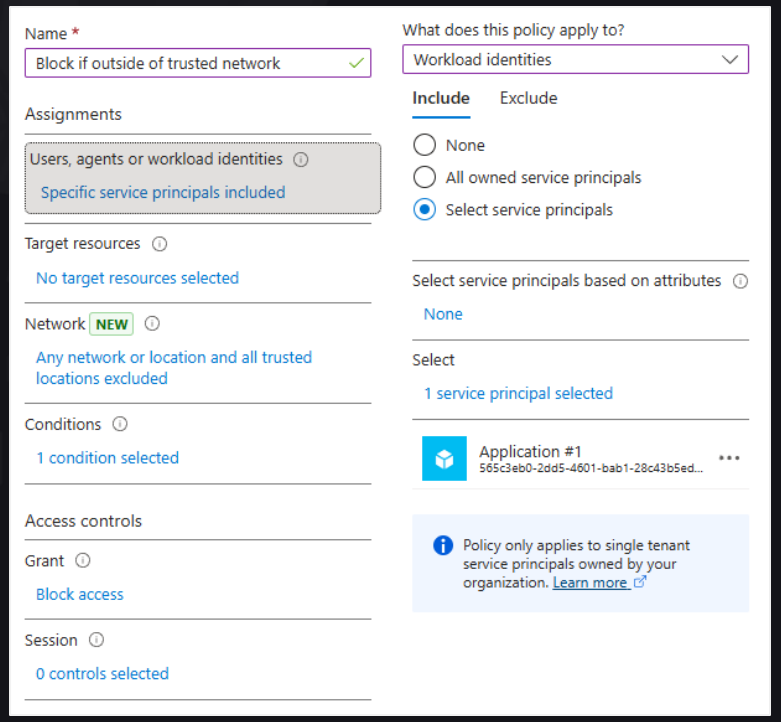
Detection


Known Attack Tool Execution: BlackCat Enumeration
rogier.dijkman
What happened
Detected a sequence of Microsoft Graph API requests matching the behavioral signature of the _BlackCat_ Azure post-exploitation tool.
The source entity executed a batch of high-volume queries targeting specific directory objects that are highly indicative of malicious reconnaissance. The activity exceeded a 70% match rate against the tool's known fingerprint.
This activity indicated an attacker had already authenticated and was attempting to:
* Enumerate Permissions: Probing for Service Principal role assignments and OAuth2 permission grants to identify privilege escalation paths.
* Map High-Value Targets: Identifying transitiveMemberOf relationships to locate administrative accounts and sensitive directory roles.
* Batch Discovery: utilizing the $batch endpoint to evade rate limits while rapidly mapping the environment.
Custom detection
Known Attack Tool Execution: BlackCat Enumeration
Medium
Unknown
New
Manage alert
Move alert to another incident
INSIGHT
Quickly classify this and 1 similar alert
Classify alerts to improve alert accuracy and get more insights about threats to your organization.
Classify alert
View 1 similar alert
Alert state
Classification
Not Set
Set Classification
Assigned to
Unassigned

Prevention

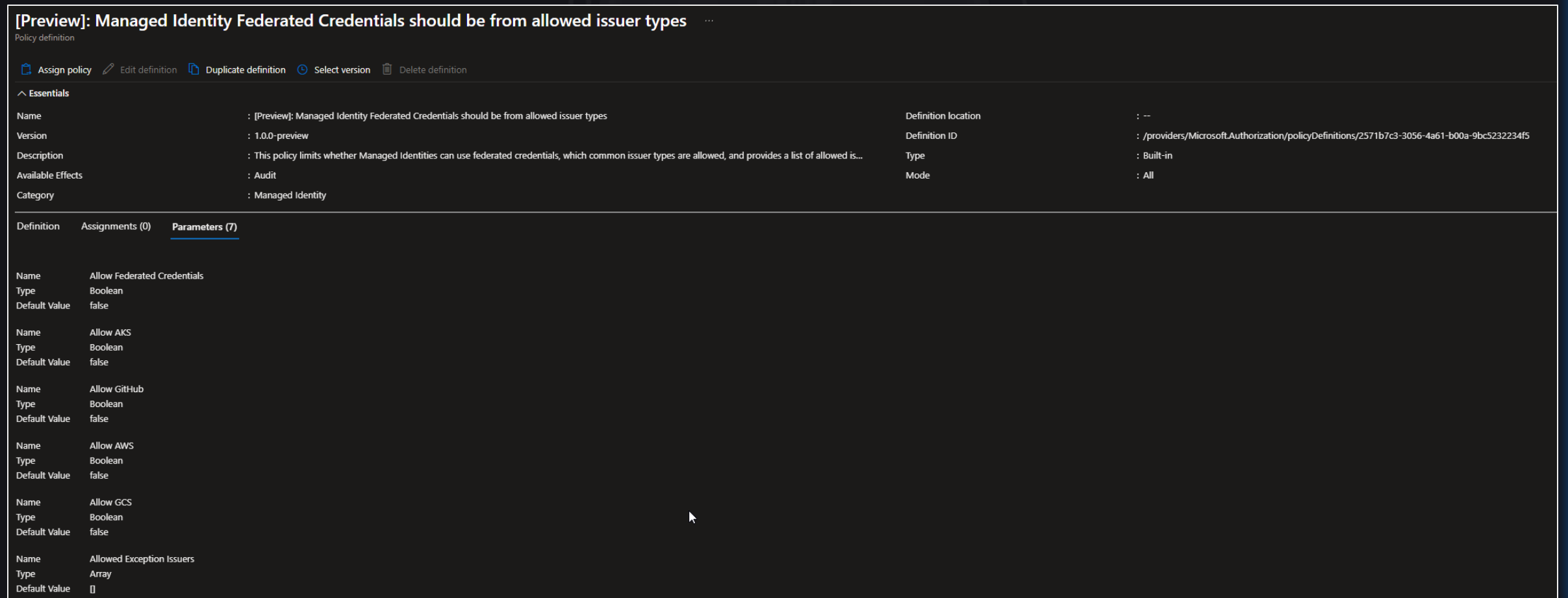
- Use Conditional Access for workload identities
- Limit to known IP ranges if possible
- Do not use secrets but certificates or federated identities





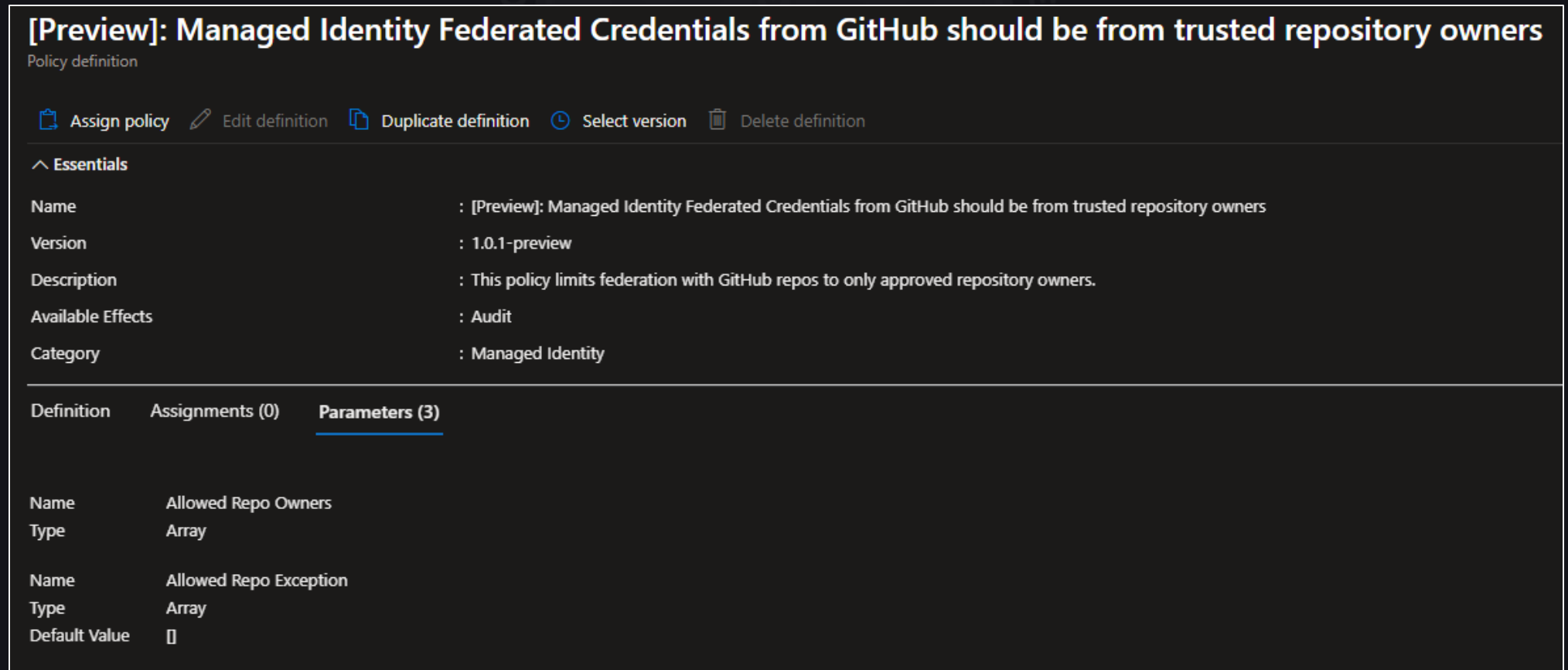
Prevention

- Azure Policy: Limit Federated Credentials to allowed issuers



Prevention

- Azure Policy: Limit Federated Credentials to trusted repository owners



Prevention

Password addition restriction

Refresh | Got feedback?

Status: Off

Policy name

Policy description

Restrict password lifetime

Refresh | Got feedback?

Status

Policy name

Policy description

Block custom passwords

Refresh | Got feedback?

Status: Off

Policy name: Block custom passwords

Policy description: Policy blocking the addition of custom passwords, meaning new passwords that are added must be system-generated

Block password addition

Restrict max password lifetim

Block custom passwords

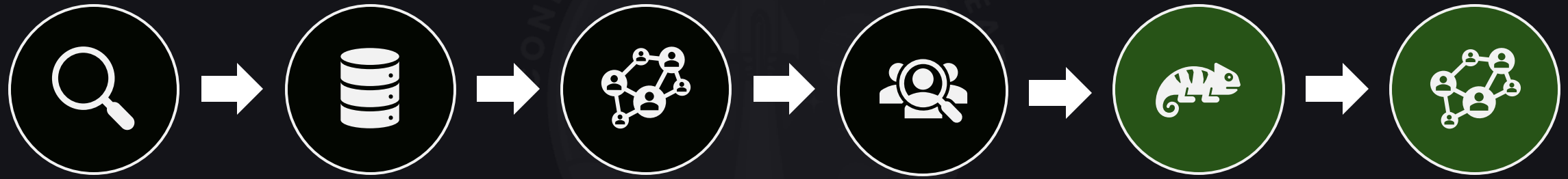
Certificate restrictions

Restrict max certificate lifetime

Identifier URI restrictions

Phase #5

The attack chain



TA0043
Reconnaissance

TA0009
Collection

TA0001
Initial Access

TA0007
Discovery

TA0003
Persistence

TA0004
Privilege Escalation

TA0003
Game Over

Detection

- Custom detections
  - Assignment of high privileged roles to non-human identities
  - Assignment of high privileged roles outside of PIM
  - Assignment of high privileged roles to non control plane admin
- Microsoft email

Detect

- Custom de
  - Assignm
  - Assignm
  - Assignm
- Microsoft e

ies

dmin

Microsoft Security

Azure Active Directory is now Microsoft Entra ID. Learn More.

The Global Administrator role for the Azure Hacking (ID: 3da86d62-c862-48da-973f-487ab98166a8) directory was assigned outside of PIM

Always use Microsoft Entra ID (ME-ID) Privileged Identity Management (PIM) to manage your privileged directory roles.

Assignment details:

Settings	Value
User:	Azure-Backup-Automation-Service
Role:	Global Administrator
Assigner:	[redacted]
Detected on:	January 27, 2026 21:54 UTC

View assignment >

Learn more about Microsoft Entra Privileged Identity Management >

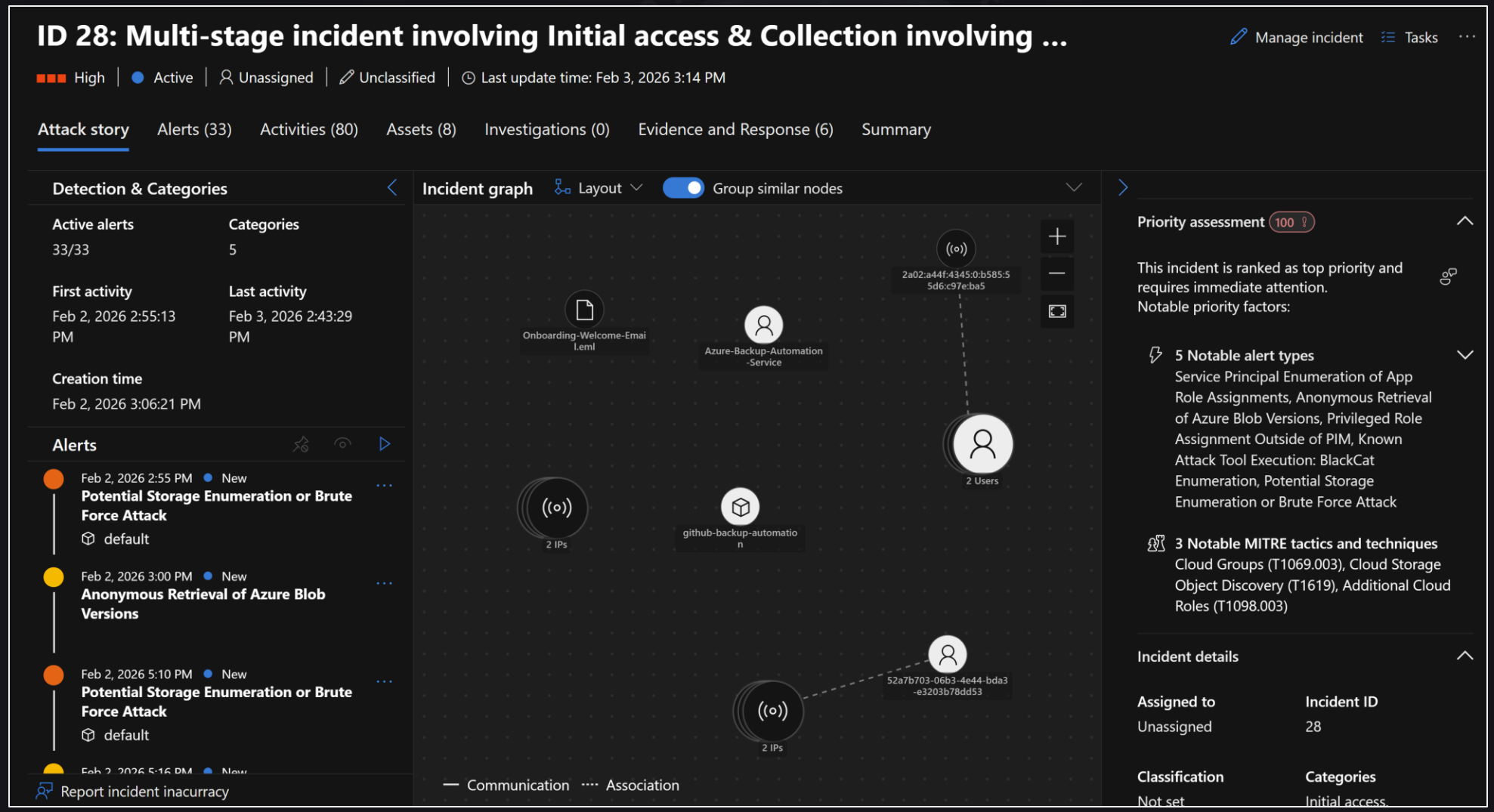
Detection


Service Principal Added to Global Administrator Role
User
What happened
This rule detects when a Service Principal is granted the Global Administrator role in Entra ID (formerly Azure AD). Assigning highly privileged roles to non-human accounts (Service Principals) increases the attack surface and is often an indicator of persistence mechanisms or privilege escalation by an attacker.
Note: The query filters for a specific Role Object ID (39a06fbe...). Ensure this ID matches the Global Administrator Role Object ID in your specific tenant, or replace it with the standard Global Admin Role Template ID (62e90394-69f5-4237-9190-012177145e10) for broader applicability.
ANALYTICS RULE
Service Principal Added to Global Administrator Role
High
Unknown
New
Manage alert
Move alert to another incident
INSIGHT
Quickly classify this alert
Classify alerts to improve alert accuracy and get more insights about threats to your organization.
Classify alert
Alert state

Detection


Privileged Role Assignment Outside of PIM
2 Users
What happened
Detected that a user account was assigned to an Azure AD directory role without using Privileged Identity Management (PIM).
This activity indicated that standard security governance controls—such as Just-In-Time (JIT) access, approval workflows, and time-bound duration—were bypassed.
This action created _standing access_ (permanent privileges) for the target account, which is a significant security risk indicating:
* Persistence: An attacker solidifying their foothold by hard-coding an account into a high-privileged role to survive future token resets or PIM policy changes.
* Policy Violation/Evasion: An administrator intentionally circumventing audit trails and justification requirements associated with PIM.
ANALYTICS RULE
Privileged Role Assignment Outside of PIM
High
Unknown
New
Manage alert
Move alert to another incident
INSIGHT
Quickly classify this alert
Classify alerts to improve alert accuracy and get more insights about threats to your organization.
Classify alert
Alert state
Classification
Assigned to

Unified XDR = Unified Incident



More protection: maester

- https://maester.dev/
- Fully automated and free best practice analysis
- 100s of tests from the community for the everybody

Thank you

Please give feedback