Phase 6 – Incident 2-Sign-ins to disabled accounts

Intro (What & Why)

In this investigation, we analyze a suspicious authentication pattern where:

- Multiple failed login attempts were made against a **disabled account**
- The same IP successfully authenticated to a different active account
- Alerts were grouped under one incident
- Activity sustained for ~50 minutes

This indicates possible brute force / password spray behavior with potential account compromise.

Steps

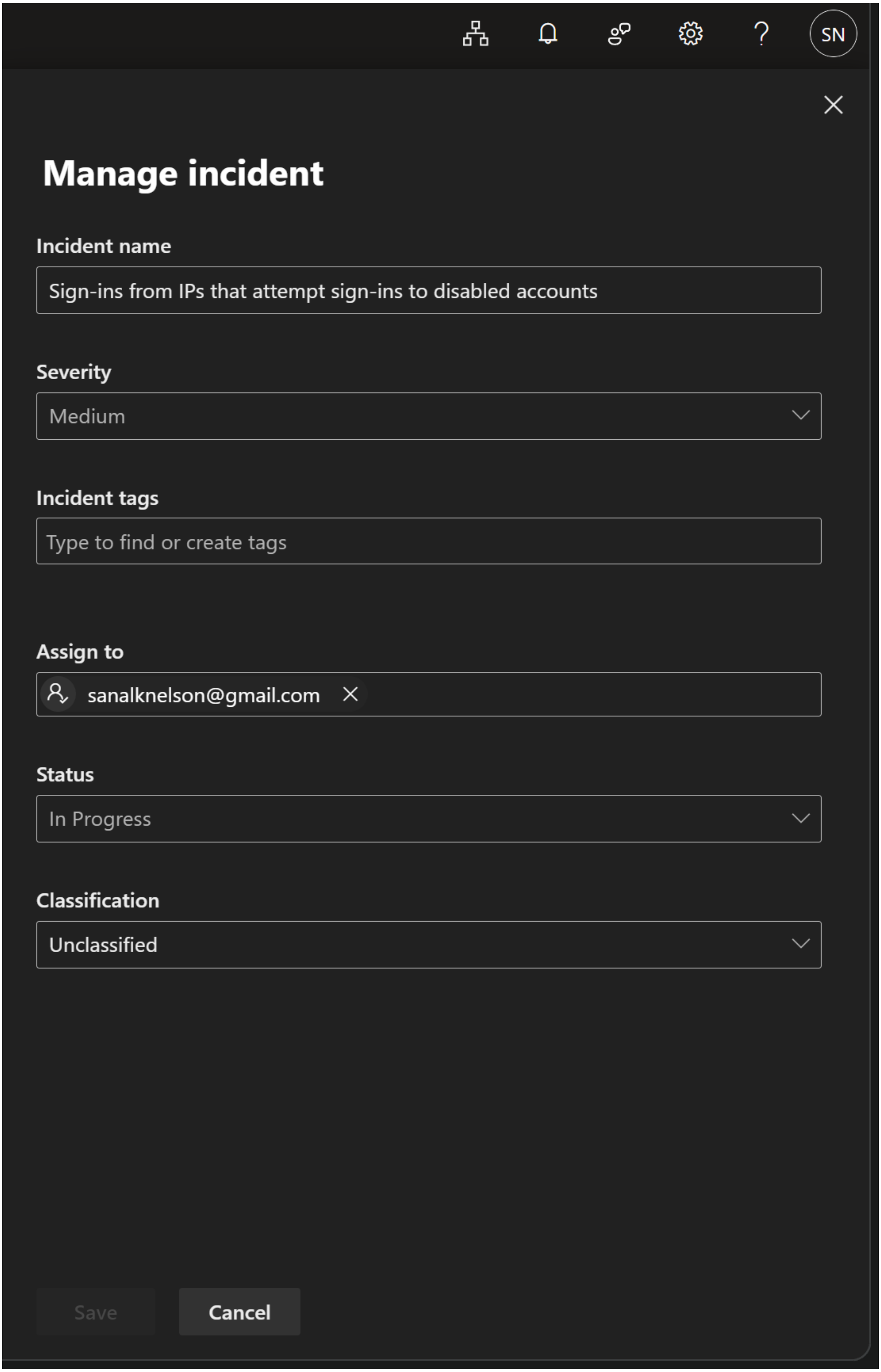
1. Take Ownership of the Incident

We should:

- Assign the incident to ourselves
- Change status to **In Progress**
- Confirm classification is not set yet

GUI Flow

Browser → https://security.microsoft.com → Microsoft Sentinel → Incidents → Select **Sign-ins from IPs that attempt sign-ins to disabled accounts** → Assign to yourself → Status → In Progress



Manage incident

Incident name

Sign-ins from IPs that attempt sign-ins to disabled accounts

Severity

Medium

Incident tags

Type to find or create tags

Assign to

sanalknelson@gmail.com

Status

In Progress

Classification

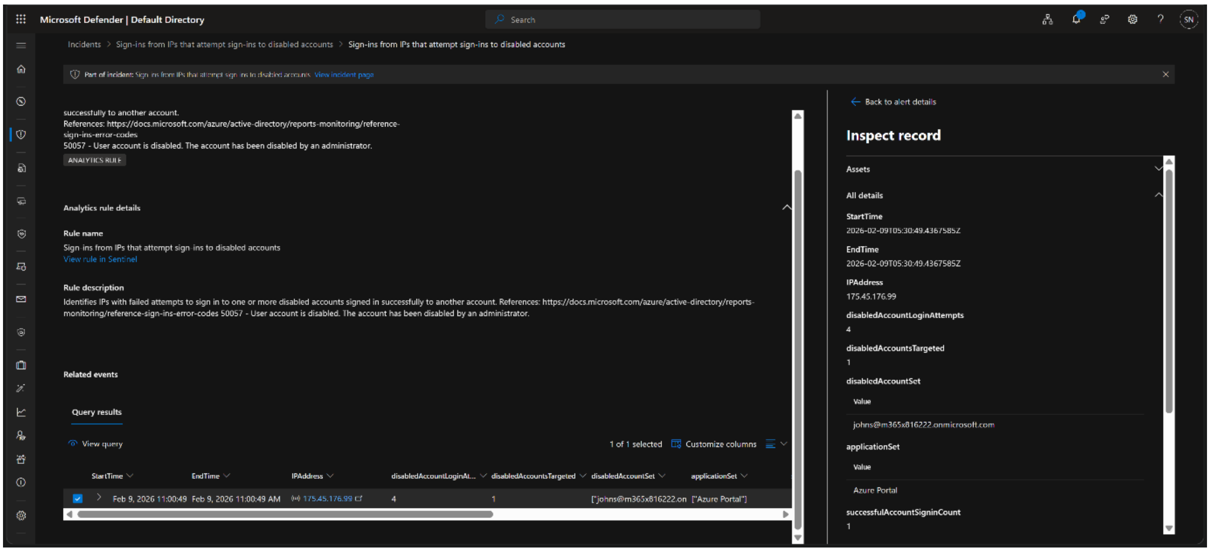
Unclassified

2. Analyse Incident Graph

Inside the incident:

- Open **Incident graph**
- Identify common entity: **IP 175.45.176.99**
- Observe relationship between:
  - Disabled account (johns@)
  - Active account (adelev@)
  - Same source IP

This confirms entity-level correlation.



Incidents > Sign-ins from IPs that attempt sign-ins to disabled accounts > Sign-ins from IPs that attempt sign-ins to disabled accounts

Part of incident: Sign-ins from IPs that attempt sign-ins to disabled accounts View incident page

successfully to another account.
References: https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-sign-ins-error-codes
50057 - User account is disabled. The account has been disabled by an administrator.

ANALYTICS RULE

Analytics rule details

Rule name
Sign-ins from IPs that attempt sign-ins to disabled accounts
View rule in Sentinel

Rule description
Identifies IPs with failed attempts to sign in to one or more disabled accounts signed in successfully to another account. References: https://docs.microsoft.com/azure/active-directory/reports-monitoring/reference-sign-ins-error-codes 50057 - User account is disabled. The account has been disabled by an administrator.

Related events

Query results

View query — 1 of 1 selected — Customize columns

	StartTime	EndTime	IPAddress	disabledAccountLoginAt...	disabledAccountsTargeted	disabledAccountSet	applicationSet
☑	Feb 9, 2026 11:00:49	Feb 9, 2026 11:00:49 AM	175.45.176.99	4	1	["johns@m365x816222.on	["Azure Portal"]

← Back to alert details

Inspect record

Assets

All details

StartTime
2026-02-09T05:30:49.4367585Z

EndTime
2026-02-09T05:30:49.4367585Z

IPAddress
175.45.176.99

disabledAccountLoginAttempts
4

disabledAccountsTargeted
1

disabledAccountSet
Value
johns@m365x816222.onmicrosoft.com

applicationSet
Value
Azure Portal

successfulAccountSigninCount
1

3. Review Alert Pattern & Timeline

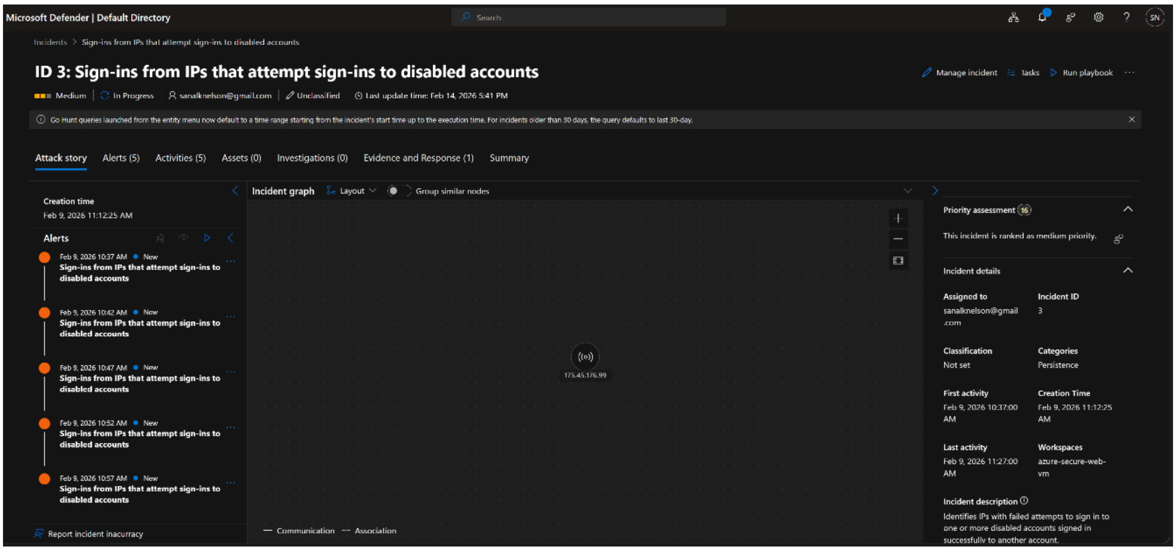
We observe:

- 5 alerts generated
- Each covering 30-minute window
- Overlapping ~5-minute execution intervals

- 4 attempts per window
- Sustained attack for ~50 minutes
- No escalation in attempt frequency

This suggests:

- Scheduled analytic rule execution
- Consistent brute force behaviour
- Organized attack pattern



ID 3: Sign-ins from IPs that attempt sign-ins to disabled accounts

Medium | In Progress | sanalknelson@gmail.com | Unclassified | Last update time: Feb 14, 2026 5:41 PM

Go Hunt queries launched from the entity menu now default to a time range starting from the incident's start time up to the execution time. For incidents older than 30 days, the query defaults to last 30-day.

Creation time
Feb 9, 2026 11:12:25 AM

Alerts

- Feb 9, 2026 10:37 AM • New
  Sign-ins from IPs that attempt sign-ins to disabled accounts
- Feb 9, 2026 10:42 AM • New
  Sign-ins from IPs that attempt sign-ins to disabled accounts
- Feb 9, 2026 10:47 AM • New
  Sign-ins from IPs that attempt sign-ins to disabled accounts
- Feb 9, 2026 10:52 AM • New
  Sign-ins from IPs that attempt sign-ins to disabled accounts
- Feb 9, 2026 10:57 AM • New
  Sign-ins from IPs that attempt sign-ins to disabled accounts

Priority assessment 16

This incident is ranked as medium priority.

Incident details

Assigned to sanalknelson@gmail.com	**Incident ID** 3
Classification Not set	**Categories** Persistence
First activity Feb 9, 2026 10:37:00 AM	**Creation Time** Feb 9, 2026 11:12:25 AM
Last activity Feb 9, 2026 11:27:00 AM	**Workspaces** azure-secure-web-vm

Incident description

Identifies IPs with failed attempts to sign in to one or more disabled accounts signed in successfully to another account.

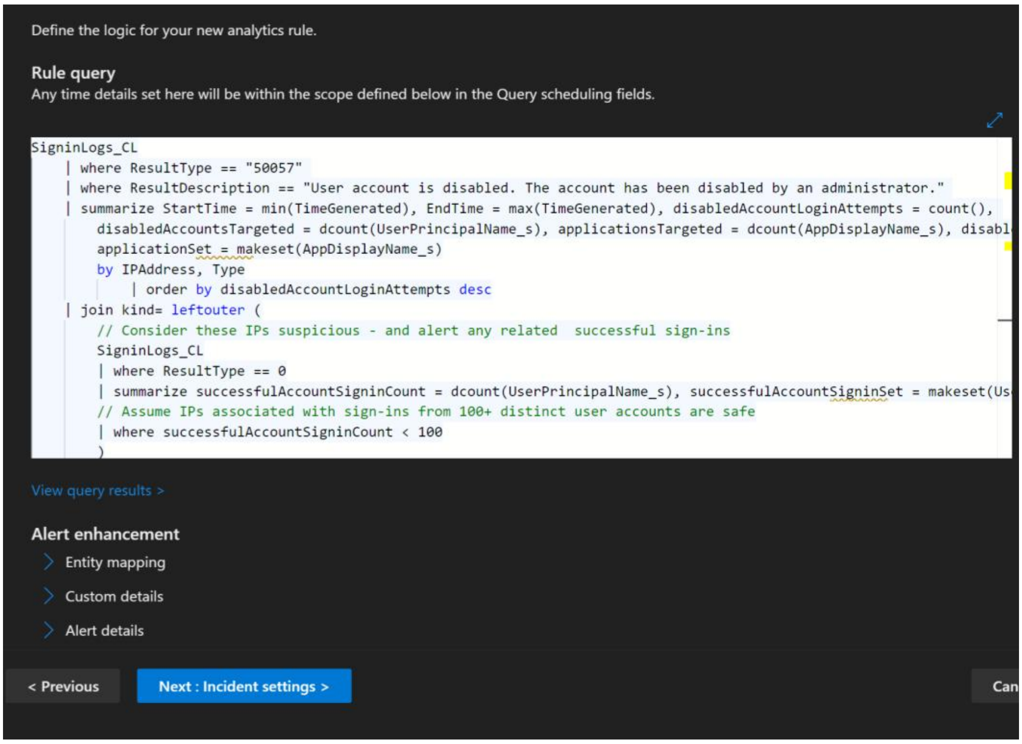
4. Investigate Alert Details

Select one alert and review:

- Analytics rule name
- Rule description
- Error code 50057 (User account disabled)
- Disabled account targeted: johns@m365x816222.onmicrosoft.com
- Successful login account: adelev@m365x816222.onmicrosoft.com
- Application used: Azure Portal

GUI Flow

Incident → Alerts → Select alert → View alert details → Analytics rule details



Define the logic for your new analytics rule.

Rule query

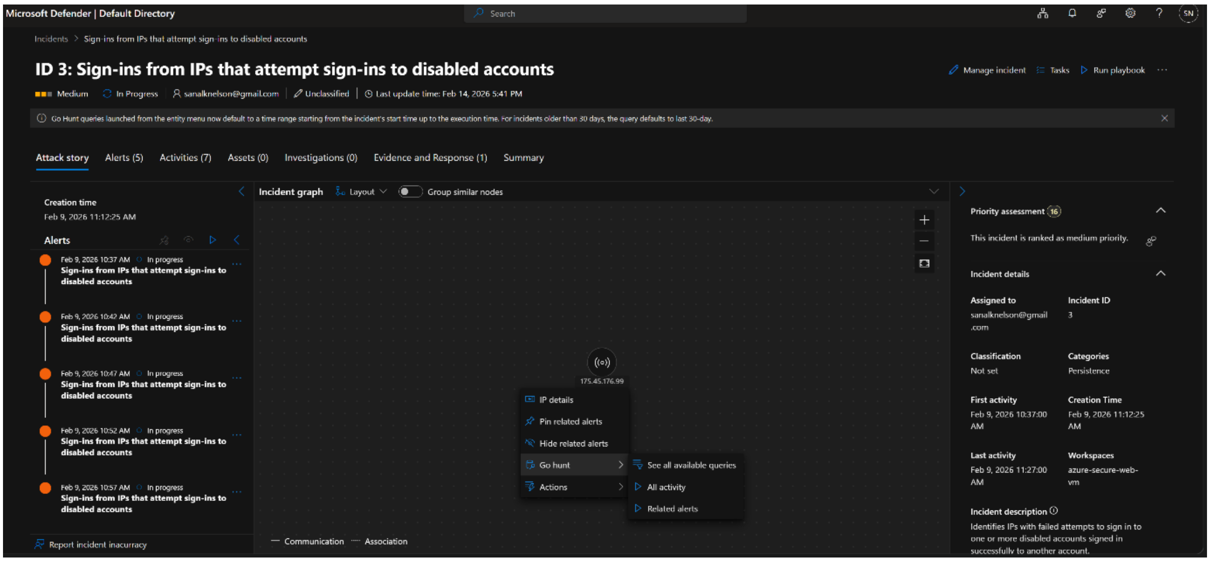
Any time details set here will be within the scope defined below in the Query scheduling fields.

```
SigninLogs_CL
    | where ResultType == "50057"
    | where ResultDescription == "User account is disabled. The account has been disabled by an administrator."
    | summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), disabledAccountLoginAttempts = count(),
      disabledAccountsTargeted = dcount(UserPrincipalName_s), applicationsTargeted = dcount(AppDisplayName_s), disabl
      applicationSet = makeset(AppDisplayName_s)
      by IPAddress, Type
          | order by disabledAccountLoginAttempts desc
    | join kind= leftouter (
      // Consider these IPs suspicious - and alert any related  successful sign-ins
      SigninLogs_CL
      | where ResultType == 0
      | summarize successfulAccountSigninCount = dcount(UserPrincipalName_s), successfulAccountSigninSet = makeset(Us
      // Assume IPs associated with sign-ins from 100+ distinct user accounts are safe
      | where successfulAccountSigninCount < 100
      )
```

5. Entity Investigation – IP 175.45.176.99

Right-click IP in incident graph:

- Select **IP details**
- Review entity reputation (Suspicious)
- Check detection count
- Observe all alerts tied to this IP



Microsoft Defender | Default Directory

Search

Incidents > Sign-ins from IPs that attempt sign-ins to disabled accounts

ID 3: Sign-ins from IPs that attempt sign-ins to disabled accounts

Medium | In Progress | sanalknelson@gmail.com | Unclassified | Last update time: Feb 14, 2026 5:41 PM

Manage incident | Tasks | Run playbook | ···

Go Hunt queries launched from the entity menu now default to a time range starting from the incident's start time up to the execution time. For incidents older than 30 days, the query defaults to last 30-day.

Attack story | Alerts (5) | Activities (7) | Assets (0) | Investigations (0) | Evidence and Response (1) | Summary

Creation time
Feb 9, 2026 11:12:25 AM

Alerts

- Feb 9, 2026 10:37 AM · In progress — **Sign-ins from IPs that attempt sign-ins to disabled accounts**
- Feb 9, 2026 10:42 AM · In progress — **Sign-ins from IPs that attempt sign-ins to disabled accounts**
- Feb 9, 2026 10:47 AM · In progress — **Sign-ins from IPs that attempt sign-ins to disabled accounts**
- Feb 9, 2026 10:52 AM · In progress — **Sign-ins from IPs that attempt sign-ins to disabled accounts**
- Feb 9, 2026 10:57 AM · In progress — **Sign-ins from IPs that attempt sign-ins to disabled accounts**

Report incident inacurracy

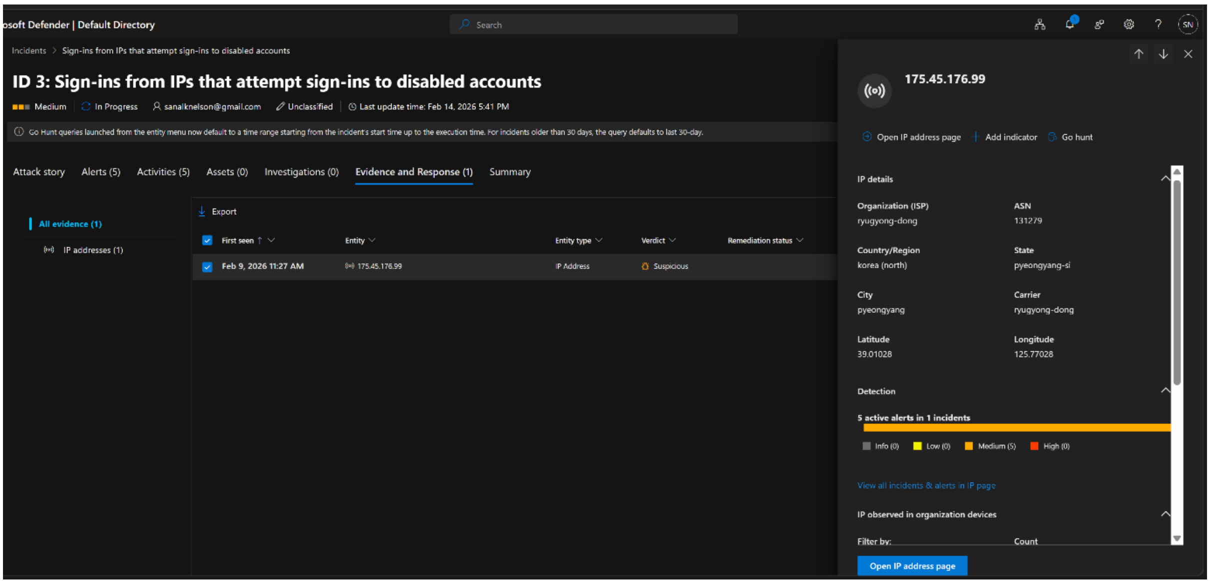
Priority assessment 16

This incident is ranked as medium priority.

Incident details

Assigned to sanalknelson@gmail.com	Incident ID 3
Classification Not set	Categories Persistence
First activity Feb 9, 2026 10:37:00 AM	Creation Time Feb 9, 2026 11:12:25 AM
Last activity Feb 9, 2026 11:27:00 AM	Workspaces azure-secure-web-vm

Incident description
Identifies IPs with failed attempts to sign in to one or more disabled accounts signed in successfullv to another account.



osoft Defender | Default Directory

Search

Incidents > Sign-ins from IPs that attempt sign-ins to disabled accounts

ID 3: Sign-ins from IPs that attempt sign-ins to disabled accounts

Medium | In Progress | sanalknelson@gmail.com | Unclassified | Last update time: Feb 14, 2026 5:41 PM

Go Hunt queries launched from the entity menu now default to a time range starting from the incident's start time up to the execution time. For incidents older than 30 days, the query defaults to last 30-day.

Attack story | Alerts (5) | Activities (5) | Assets (0) | Investigations (0) | Evidence and Response (1) | Summary

All evidence (1)
IP addresses (1)

Export

☑ First seen	Entity	Entity type	Verdict	Remediation status
☑ Feb 9, 2026 11:27 AM	175.45.176.99	IP Address	Suspicious	

175.45.176.99

Open IP address page | Add indicator | Go hunt

IP details

Organization (ISP) ryugyong-dong	ASN 131279
Country/Region korea (north)	State pyeongyang-si
City pyeongyang	Carrier ryugyong-dong
Latitude 39.01028	Longitude 125.77028

Detection

5 active alerts in 1 incidents

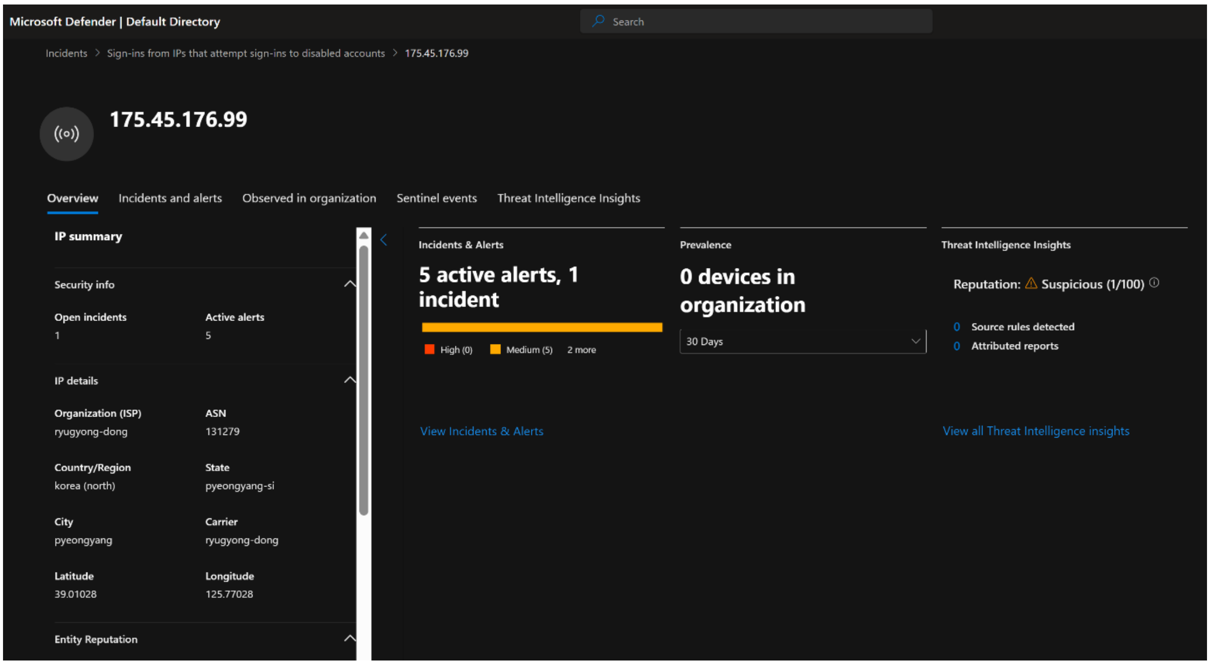
■ Info (0) ■ Low (0) ■ Medium (5) ■ High (0)

View all incidents & alerts in IP page

IP observed in organization devices

Filter by: Count

Open IP address page



Microsoft Defender | Default Directory

Search

Incidents > Sign-ins from IPs that attempt sign-ins to disabled accounts > 175.45.176.99

175.45.176.99

Overview | Incidents and alerts | Observed in organization | Sentinel events | Threat Intelligence Insights

IP summary

Security info

Open incidents 1	Active alerts 5

IP details

Organization (ISP) ryugyong-dong	ASN 131279
Country/Region korea (north)	State pyeongyang-si
City pyeongyang	Carrier ryugyong-dong
Latitude 39.01028	Longitude 125.77028

Entity Reputation

Incidents & Alerts

5 active alerts, 1 incident

■ High (0) ■ Medium (5) 2 more

View Incidents & Alerts

Prevalence

0 devices in organization

30 Days

Threat Intelligence Insights

Reputation: ⚠ Suspicious (1/100)

0 Source rules detected
0 Attributed reports

View all Threat Intelligence insights

6. Threat Assessment

Attack Classification

Brute Force / Password Spray

MITRE ATT&CK:

T1110 – Brute Force
Tactic: Credential Access / Persistence

Threat Indicators

- Disabled account targeted repeatedly
- Same IP successful on active account
- Azure Portal interactive login
- Single IP source (not distributed)
- Sustained 50-minute campaign

Correlation Findings

- Common entity: IP 175.45.176.99
- Appears in all 5 alerts
- Marked suspicious
- Same analytic rule correlation
- Grouped automatically by Sentinel

Risk Elevation

Originally Medium → Elevated to High due to:

✓ Successful login to adelev@
✓ Access to Azure Portal
✓ Continued activity without interruption

7. Final Diagnosis

Sustained brute force attack against disabled account with successful authentication to secondary account.

Attack Objectives

Primary: Credential testing against johns@
Secondary: Account access using adelev@

Evidence of Success

✓ Successful Azure Portal login
✓ Repeated attack attempts
✓ No detection interruption
✓ Same IP across all alerts

8. Recommended Immediate Actions

URGENT – Account Security

- Reset password for adelev@
- Force sign-out sessions using EntraID
- Verify MFA enforcement
- Review Conditional Access policies
- Check Azure AD sign-in logs

Network Controls

- Block IP 175.45.176.99
- Add to Conditional Access block list
- Review geo-location
- Monitor for repeat behaviour

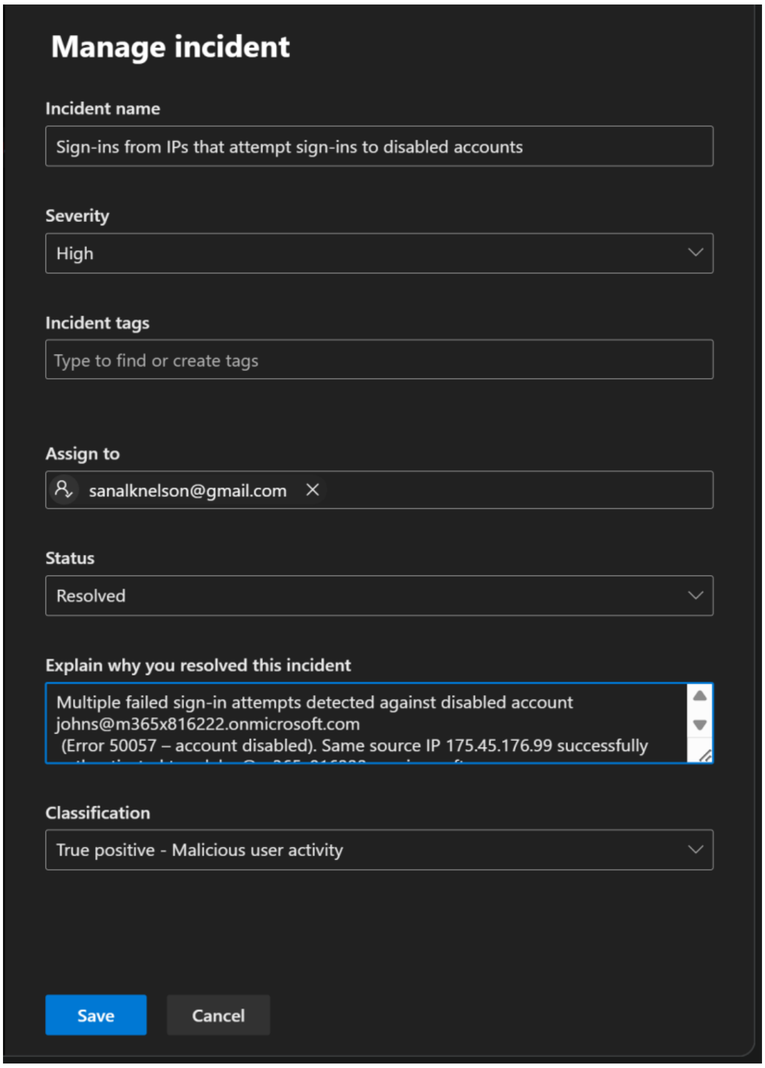
Incident Response

- Escalate to Tier 2/3
- Investigate 30-day sign-in history
- Review Azure Activity logs
- Check for additional targeted accounts

9. Final Analyst Action

After documentation, We should:

- Set Status → Resolved
- Classification → True positive – Malicious user activity
- Add detailed investigation comment



Manage incident

Incident name
Sign-ins from IPs that attempt sign-ins to disabled accounts

Severity
High

Incident tags
Type to find or create tags

Assign to
sanalknelson@gmail.com

Status
Resolved

Explain why you resolved this incident
Multiple failed sign-in attempts detected against disabled account
johns@m365x816222.onmicrosoft.com
(Error 50057 – account disabled). Same source IP 175.45.176.99 successfully

Classification
True positive - Malicious user activity

Investigation comment to add:

Multiple failed sign-in attempts detected against disabled account johns@m365x816222.onmicrosoft.com (Error 50057 – account disabled). Same source IP 175.45.176.99 successfully authenticated to adelev@m365x816222.onmicrosoft.com via Azure Portal. Activity sustained for ~50 minutes across 5 correlated alerts. Pattern consistent with brute force/password spray attack (MITRE T1110). Account adelev@ requires credential reset and MFA verification. IP recommended for blocklisting.

Outcome

By the end of this investigation, we have:

- Identified brute force attack pattern
- Confirmed successful authentication to active account
- Correlated all alerts to single IP
- Validated analytic rule trigger
- Performed entity-based investigation
- Elevated severity appropriately
- Documented remediation actions
- Completed proper SOC closure

This demonstrates:

- Credential attack detection capability
- Cross-entity correlation analysis
- Incident graph usage
- Alert-to-entity pivoting
- Proper escalation reasoning
- Mature SOC investigation workflow