

4.1 Manage Incidents in Microsoft Sentinel

4.1.1 Open Incident Tab in Sentinel

The screenshot shows the Microsoft Sentinel interface under the 'Incidents & alerts' section. The left sidebar includes options like Home, Exposure management, Investigation & response (Incidents, Alerts), Hunting, Actions & submissions, Partner catalog, Threat intelligence, Assets, and Microsoft Sentinel. The main area is titled 'Incidents' and displays a table of 'Most recent incidents and alerts'. The table columns include Incident ID, Priority (sorted by priority), Tags, Severity (Medium, High, Medium, Medium, Medium, Not set, Medium), Investigation state (Persistence, Persistence, Command and control, Initial access, Initial access, Initial access), and Categories. There are buttons for Export, Copy list link, Refresh, and a search bar for 'Search for name or ID'.

4.1.2 Let's Resolve incident Sign-ins from IPs that attempt sign-ins to disabled accounts

The screenshot shows the 'Advanced hunting' dialog box. The left sidebar has sections for Home, Exposure management, Investigation & response (Rule description, Related events, Query results, View query), Threat intelligence, Assets, Microsoft Sentinel, Email & collaboration, Cloud infrastructure, Cases, SOC optimization, Reports, and Learning hub. The main area shows a Kusto query editor with the following code:

```
// The query now parameter represents the time (in UTC) at which the scheduled analytics rule ran to produce this alert
let query_time = now();
let timestamp = now();
$> SigninLogs_CL
| where timestamp > query_time
| where disabledAccountLoginAttempts > 0
| where disabledAccountsTargeted > 0
| project StartTime, EndTime, IPAddress, disabledAccountLoginAttempts, disabledAccountsTargeted, timestamp
```

Below the query are export and search buttons, and a table showing the results of the query.

4.1.3 After Investigation → Create New Automation Rule

The screenshot shows the Microsoft Sentinel interface. The left sidebar includes Home, Microsoft Sentinel, Threat management (Incidents, Workbooks, Hunting, Notebooks, Entry behavior, Threat intelligence, MITRE ATT&CK (Preview), SOC optimization, Content management, Content hub, Repositories, Community, Configuration, Workspace manager (Preview), Data connectors, Analytics). The main area shows the 'Incidents' tab with 5 Open Incidents, 4 New incidents, and 1 Active Incident. The table lists incidents by severity (Medium, Medium, Medium, High, Medium) and provider (Microsoft Defender, Microsoft Sentinel). The right side shows the 'Create new automation rule' dialog box. The 'Automation rule name' is 'Sign-ins from IPs that attempt sign-ins to disabled accounts'. The 'Trigger' is 'When incident is created'. The 'Conditions' section contains two conditions: 'Analytic rule name Contains Value: Sign-ins from IPs that attempt sign-ins to disabled accounts' and 'IoT device operating system Equals Value: 175.45.176.99'. The 'Actions' section includes 'Change status' (Closed) and 'Comment' (Closing the incident will archive the associated team). The 'Rule expiration' is set for 12/5/2023 at 3:18 PM.

4.1.4 Closed the Ticket

4.2 Solorigate Incident → After Investigation of Story and Impact

4.3 Go to hunting and search for solorigate → click on view result

→ Bookmarks the event to add into incident

Microsoft Azure | Upgrade

Home > Microsoft Sentinel | Hunting >

Logs ...
SentinelWorkSpace

New Query 1* +

User Query Time range : Set in query Show : 500000 results Add

Results Chart Add bookmark

TimeGenerated [UTC]	NamedPipe	ProcessDetail	Account	timestamp [UTC]	AccountCustomEntity	HostCustomEntity	Computer	Type	Account_s	AccountType_s	EventSourceName_s
12/4/2025, 5:10:48,240 PM			CONTOSO\ADMINPC\$	12/4/2025, 5:10:48,240 PM	AdminPc.Contoso.Azure	AdminPc.Contoso.Azure	SecurityEvent_CL	CONTOSO\ADMINPC\$	Machine	Machine	Microsoft-Windows-Security\$
12/4/2025, 5:10:48,240 PM			CONTOSO\VICTIMPC\$	12/4/2025, 5:10:48,240 PM	VictimPc.Contoso.Azure	VictimPc.Contoso.Azure	SecurityEvent_CL	CONTOSO\VICTIMPC\$	Machine	Machine	Microsoft-Windows-Security\$
12/4/2025, 5:10:48,240 PM			CONTOSO\CLIENTPC\$	12/4/2025, 5:10:48,240 PM	ClientPc.Contoso.Azure	ClientPc.Contoso.Azure	SecurityEvent_CL	CONTOSO\CLIENTPC\$	Machine	Machine	Microsoft-Windows-Security\$

15s 991ms | Display time (UTC+0:00) ▾

After adding we can see other entities has added

Microsoft Azure | Upgrade

Home > Microsoft Sentinel | Incidents >

Solorigate Network Beacon on multiple endpoints reported by multiple sources ...

Incident number 2

Refresh Log Task Activity log

This is the new, improved incident page - Now generally available. You can use the toozie to switch back.

Severity High Active rhythmshar... Owner

Overview Entities

Investigate in Microsoft Defender XDR

Workspace name sentinelworkspace

Description

Alert product names

- Microsoft Defender XDR
- Microsoft Sentinel

Evidence

- Events 5
- Alerts 8
- Bookmarks 3

Last update time 12/4/2025, 4:09:20 PM Creation time 12/4/2025, 12:21:37 PM

Entities (8)

- victimpc
- adminpc
- clientpc
- CLIENTPC\$
- VICTIMPC\$
- ADMINPC\$

Tactics and techniques

- Command And Control

Incident workbook Loading Investigation...

Entities

Search Type: All

- victimpc
- adminpc
- clientpc
- CLIENTPC\$
- VICTIMPC\$
- ADMINPC\$

Top insights

- Last 24 hours before the first alert
- Windows sign-in activity

Title	Signin Co...	User Cour...
Successful	0	0
Failed	0	0

Sign-ins over time

See all windows sign-ins >

Windows sign-in activity