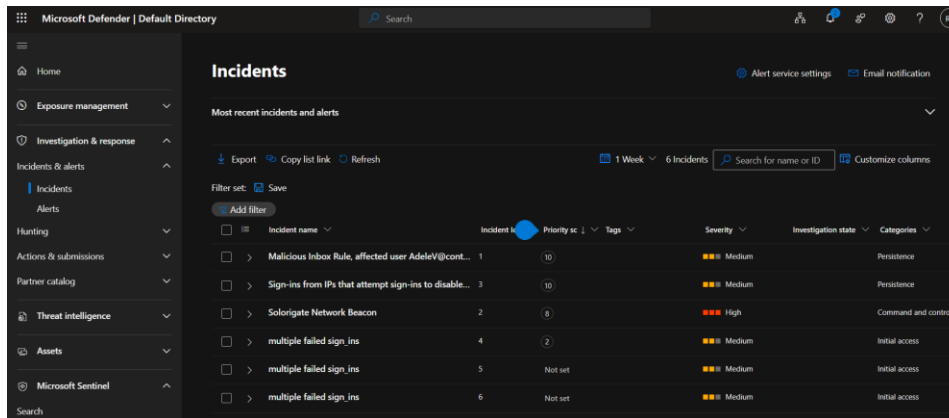
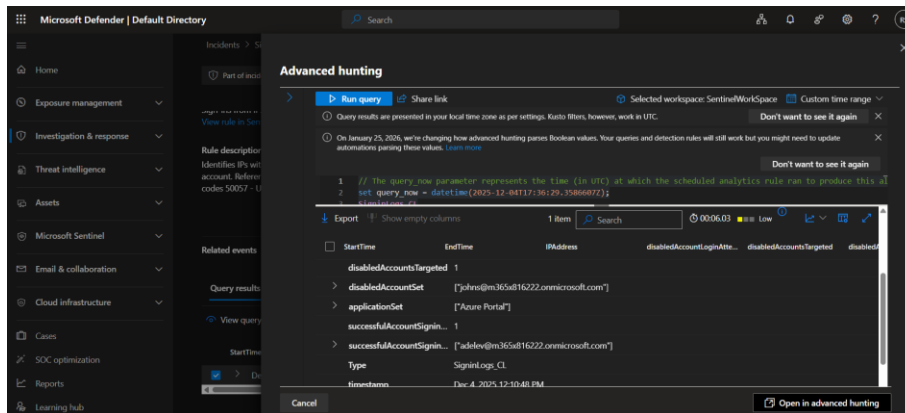


4.1 Manage Incidents in Microsoft Sentinel

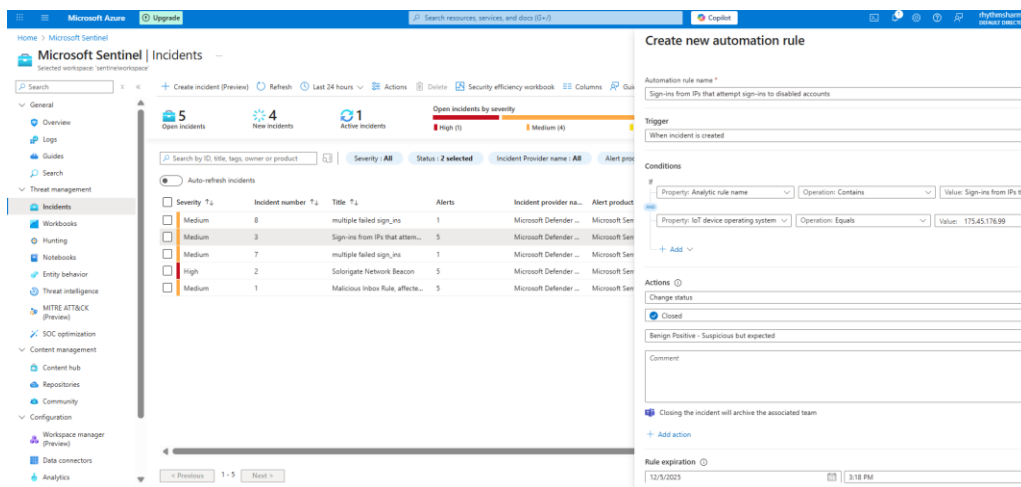
4.1.1 Open Incident Tab in Sentinel



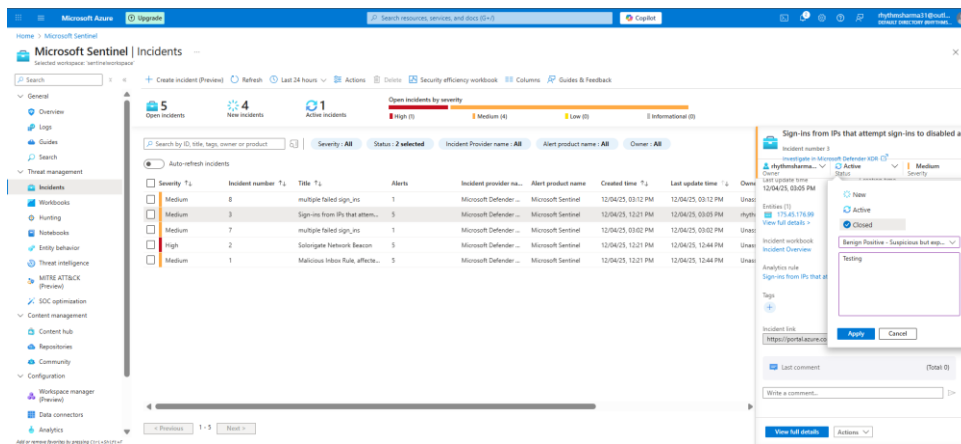
4.1.2 Let's Resolve incident Sign-ins from IPs that attempt sign-ins to disabled accounts



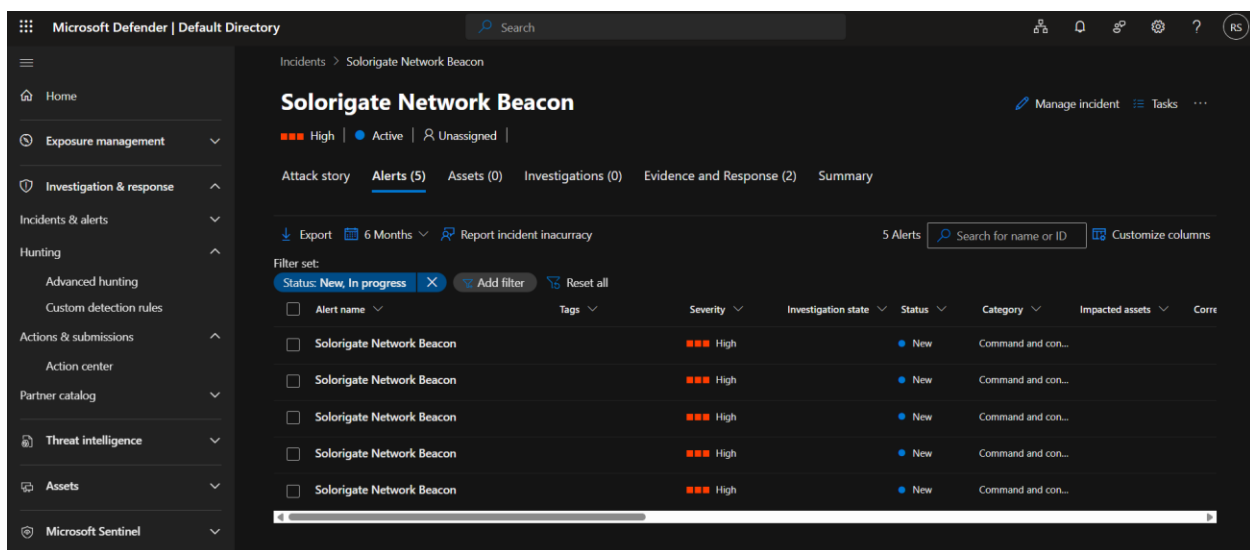
4.1.3 After Investigation → Create New Automation Rule



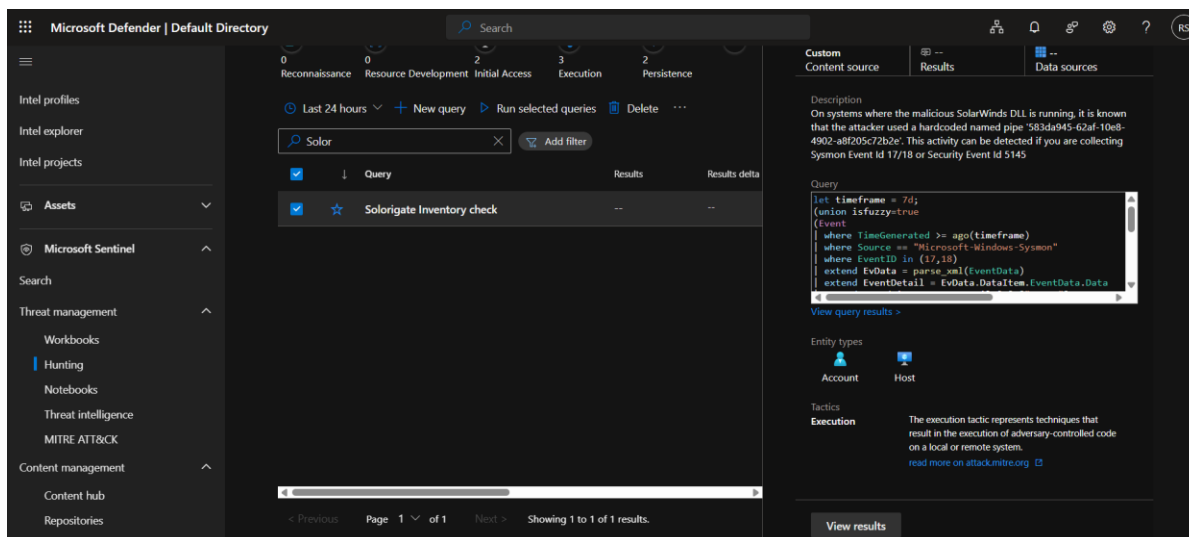
4.1.4 Closed the Ticket



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

The screenshot shows the Microsoft Sentinel Logs interface. A query has been executed, displaying 500,000 results. The table below lists the results:

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	Microsoft-Windows-Security-Auditing	
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	Microsoft-Windows-Security-Auditing	
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	Microsoft-Windows-Security-Auditing	

After adding we can see other entites has added

The screenshot shows the Microsoft Sentinel Incident page for an incident titled "Solorigate Network Beacon on multiple endpoints reported by multiple sources". The incident is in the "Active" state. The "Entities" tab is selected, showing a list of entities:

- victimpc**: Os Family: Unknown, Dns Domain: Contoso.Azure, Host Name: victimpc
- adminpc**: Os Family: Unknown, Dns Domain: Contoso.Azure, Host Name: adminpc
- clientpc**: Os Family: Unknown, Dns Domain: Contoso.Azure, Host Name: clientpc
- CLIENTPC\$**: Nt Domain: CONTOSO, Account Name: CLIENTPC\$, Is Domain Joined: true
- VICTIMPC\$**: Nt Domain: CONTOSO, Account Name: VICTIMPC\$, Is Domain Joined: true
- ADMINPC\$**

The "Incident timeline" section shows a message: "Something went wrong. Please refresh and try again." The "Similar incidents" section shows: "No similar incidents to display." The "Top insights" section shows a "Windows sign-in activity" insight for the time range 12/3/2025, 12:21:37 PM - 12/4/2025, 4:05:54 PM.