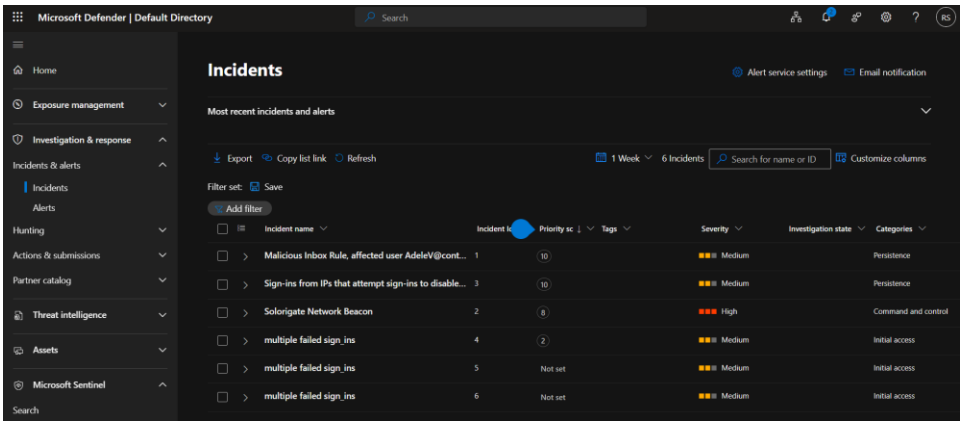
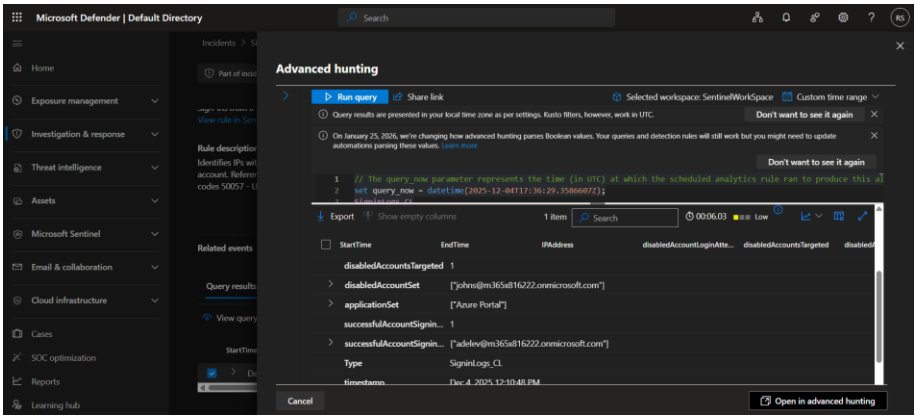
4.1 Manage Incidents in Microsoft Sentinel

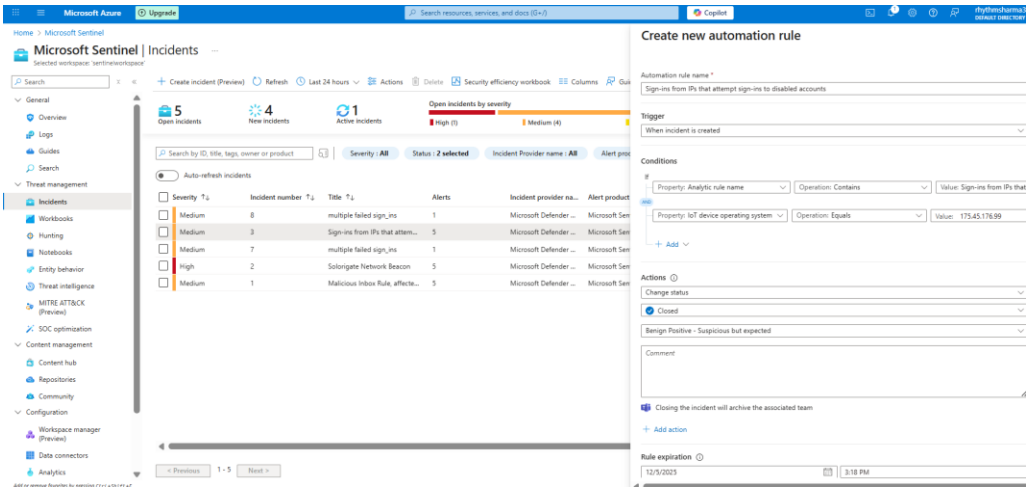
4.1.1 Open Incident Tab in Sentinel



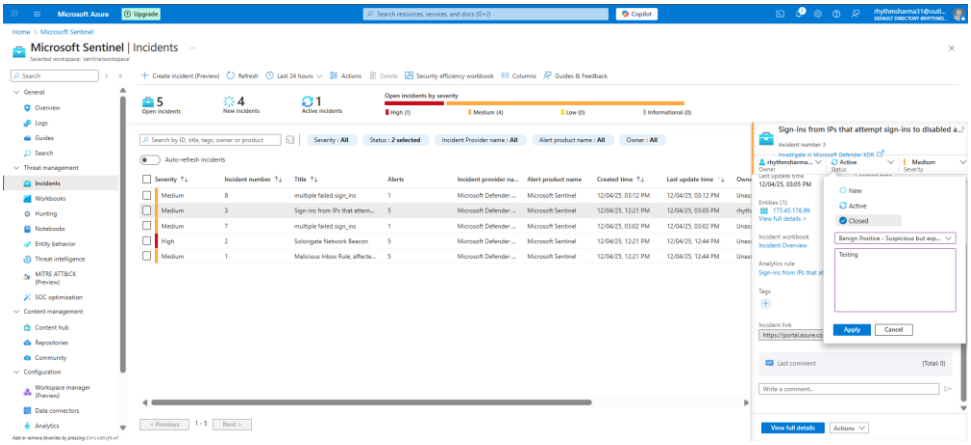
4.1.2 Let’s Resolve incident Sign-ins from IPs that attempt sign-ins to disabled accounts



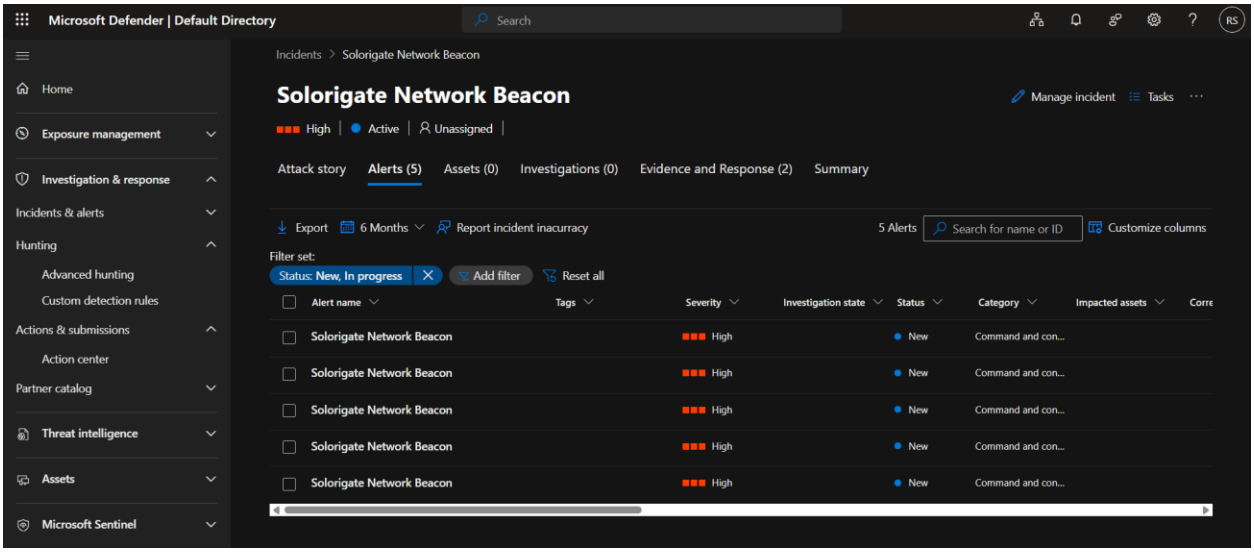
4.1.3 After Investigation → Create New Automation Rule



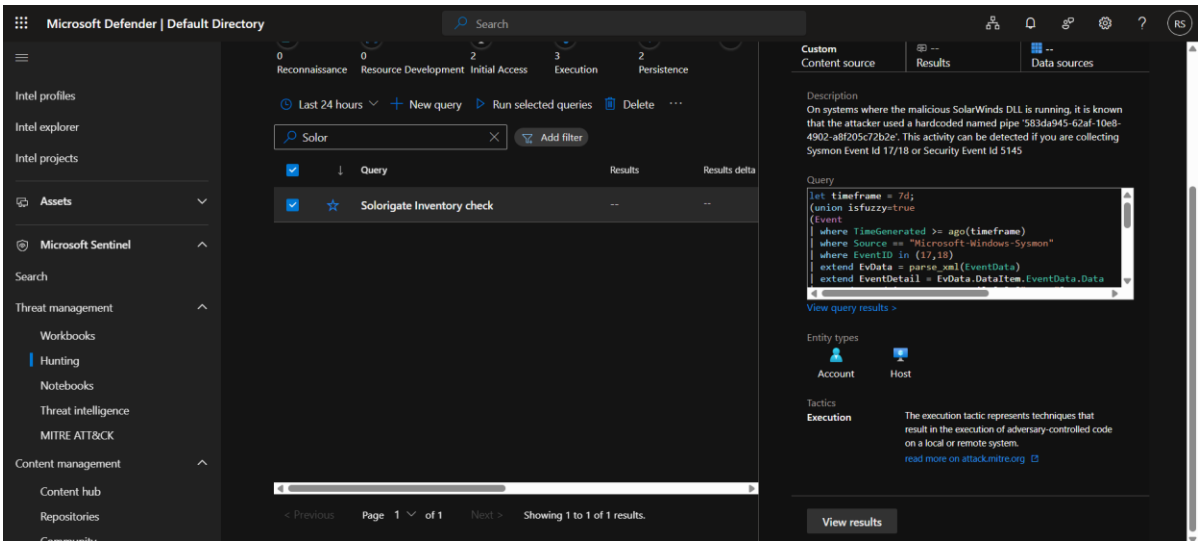
4.1.4 Closed the Ticket



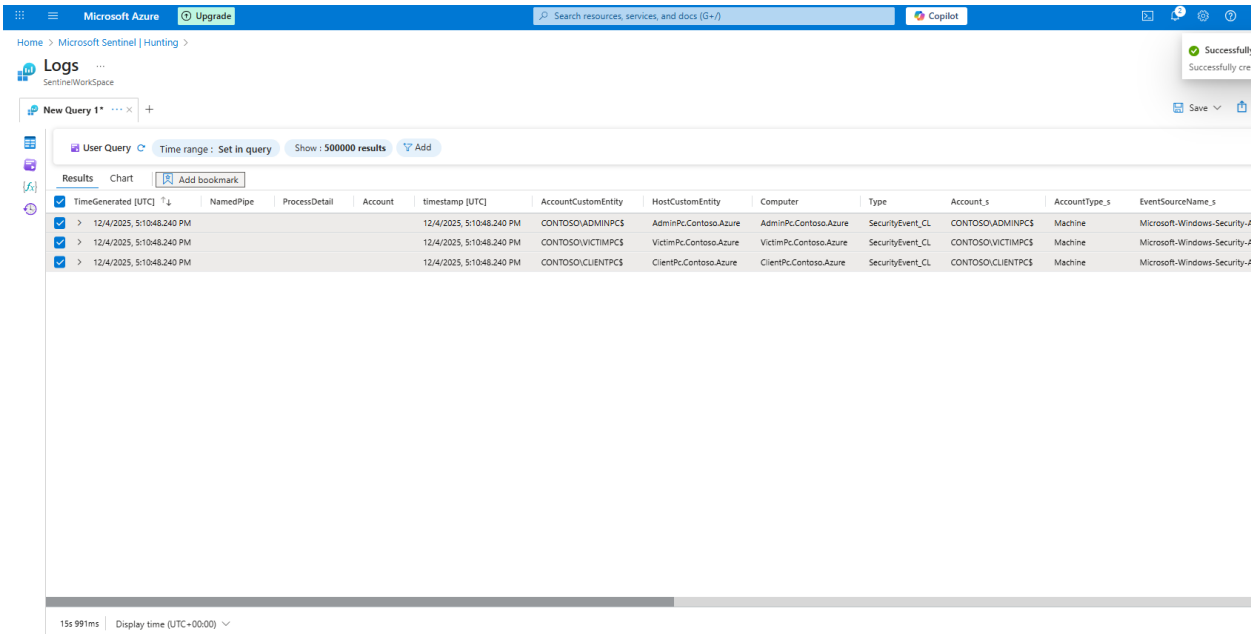
4.2 Solorigate Incident → After Investigation of Story and Impact



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



➔ Bookmarks the event to add into incident



After adding we can see other entites has added