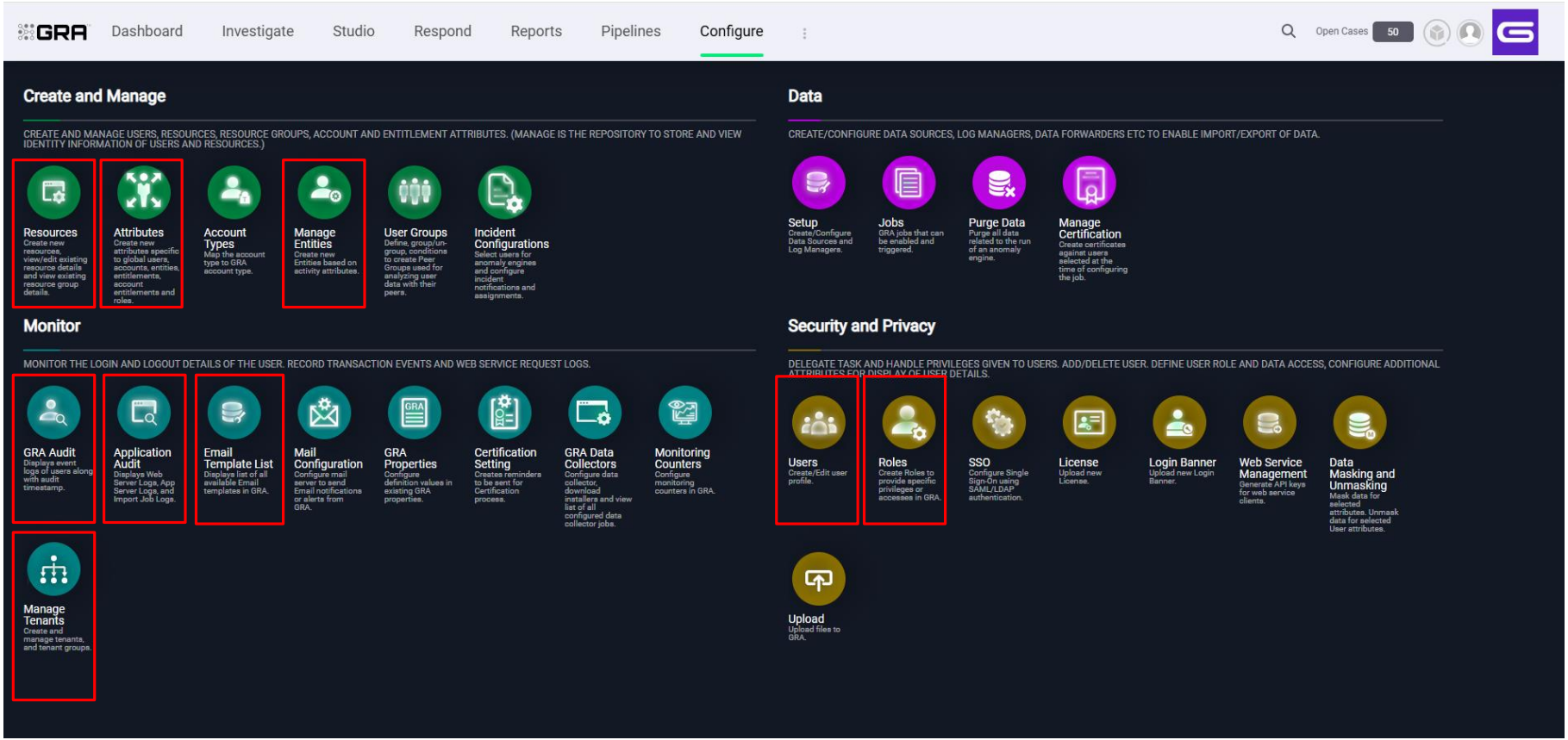
July 31, 2024

Workshop Walkthrough

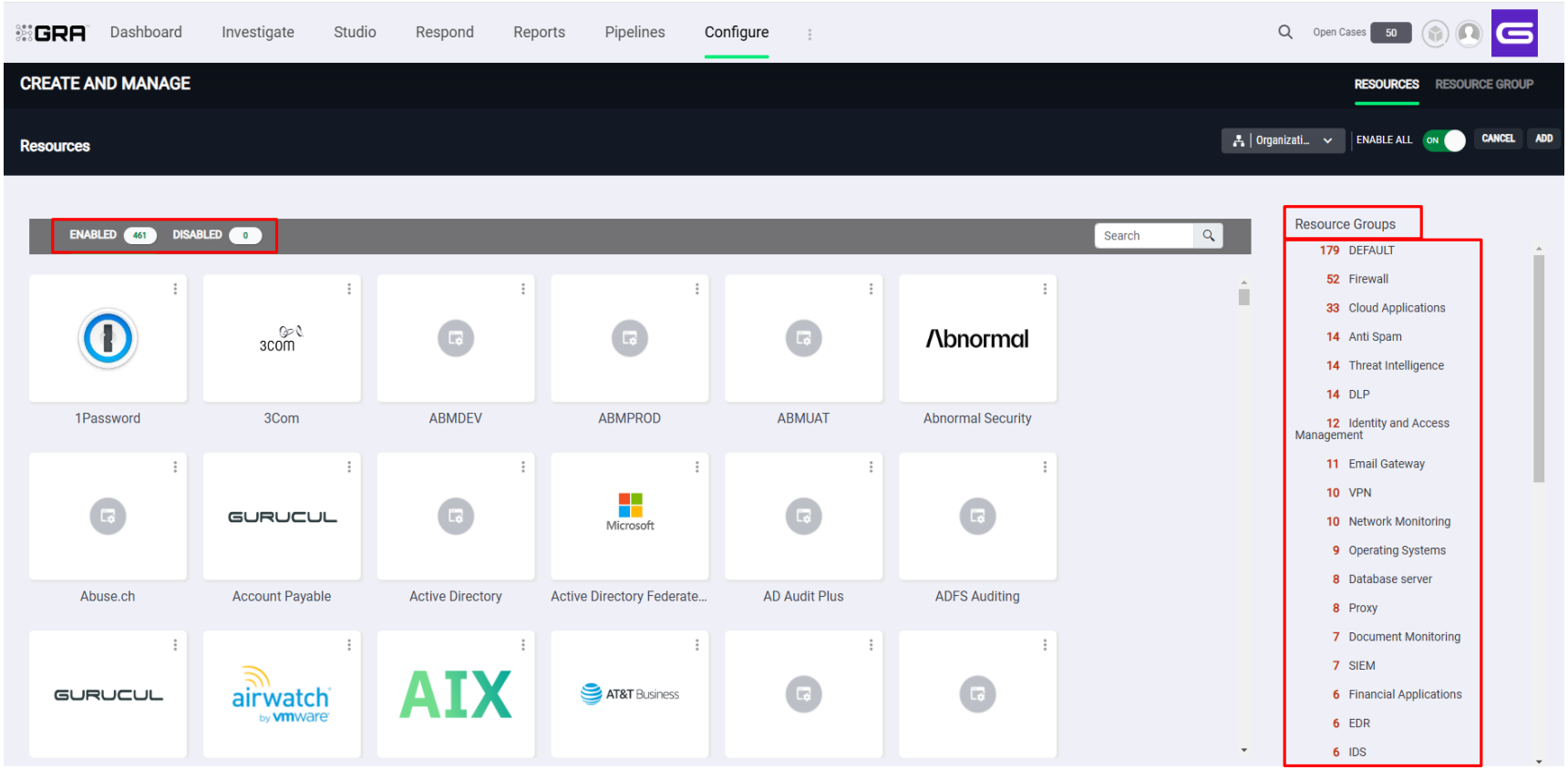
Gurucul

Table Of Content

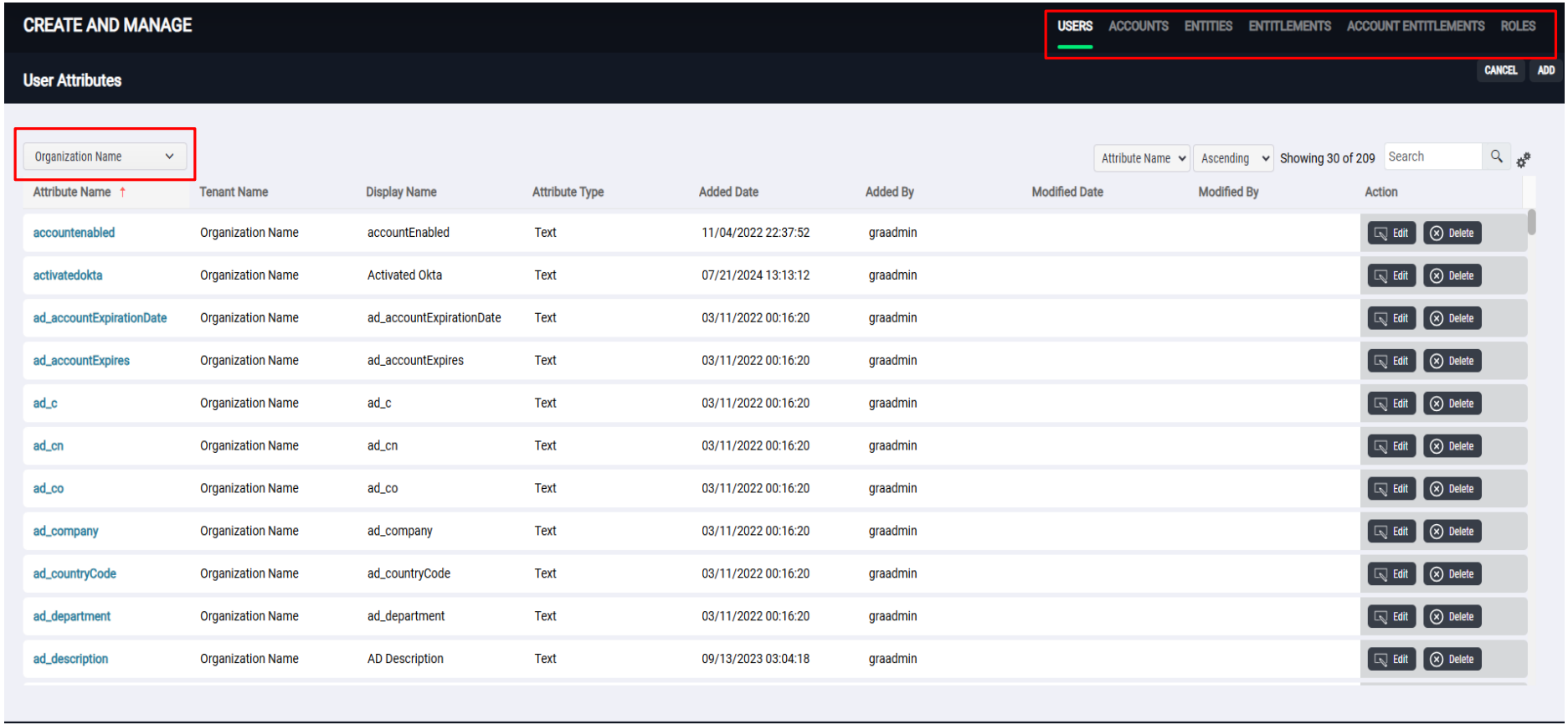
Configurations



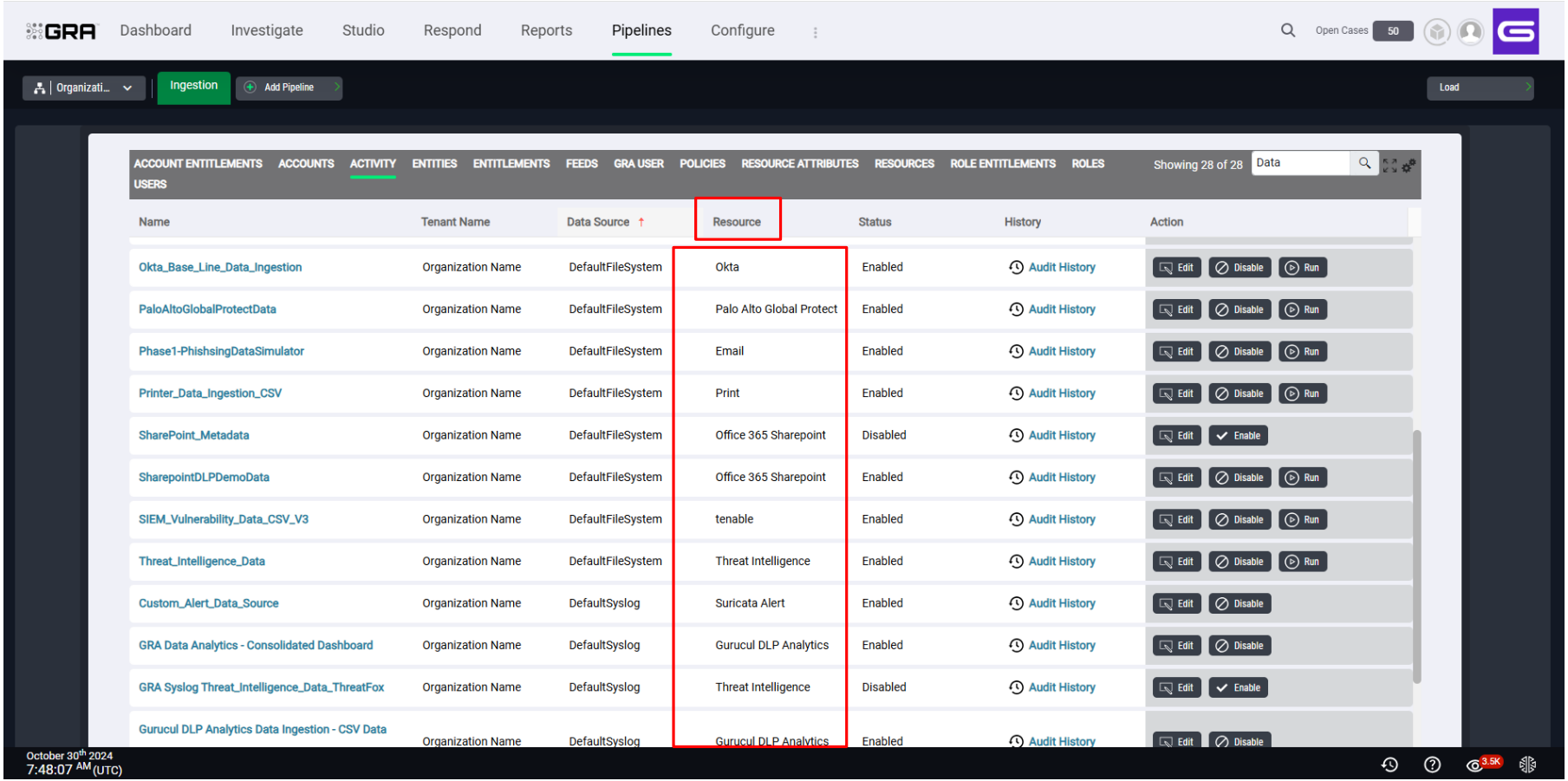
Resource Configuration Screen



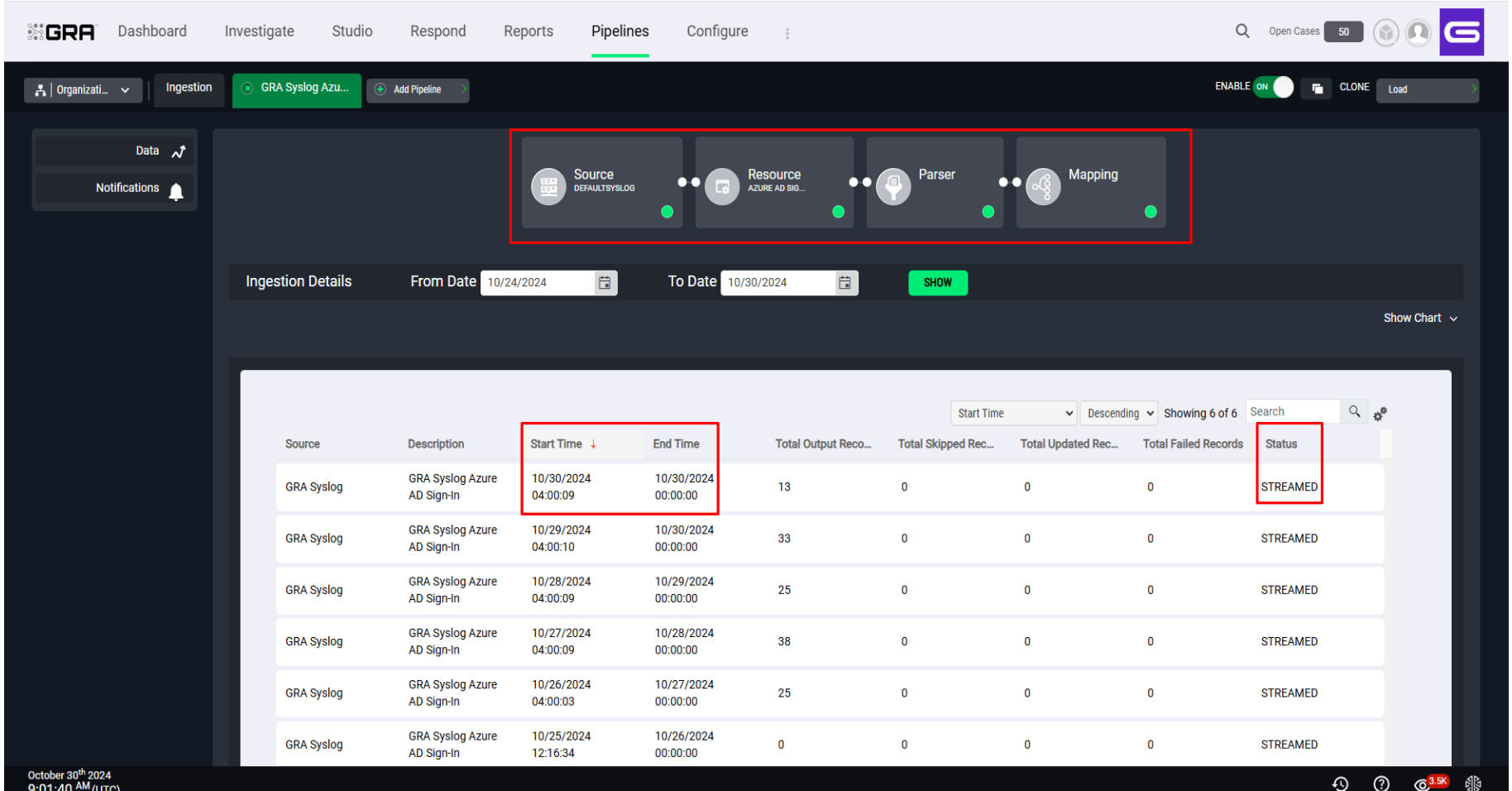
Attributes Configurations



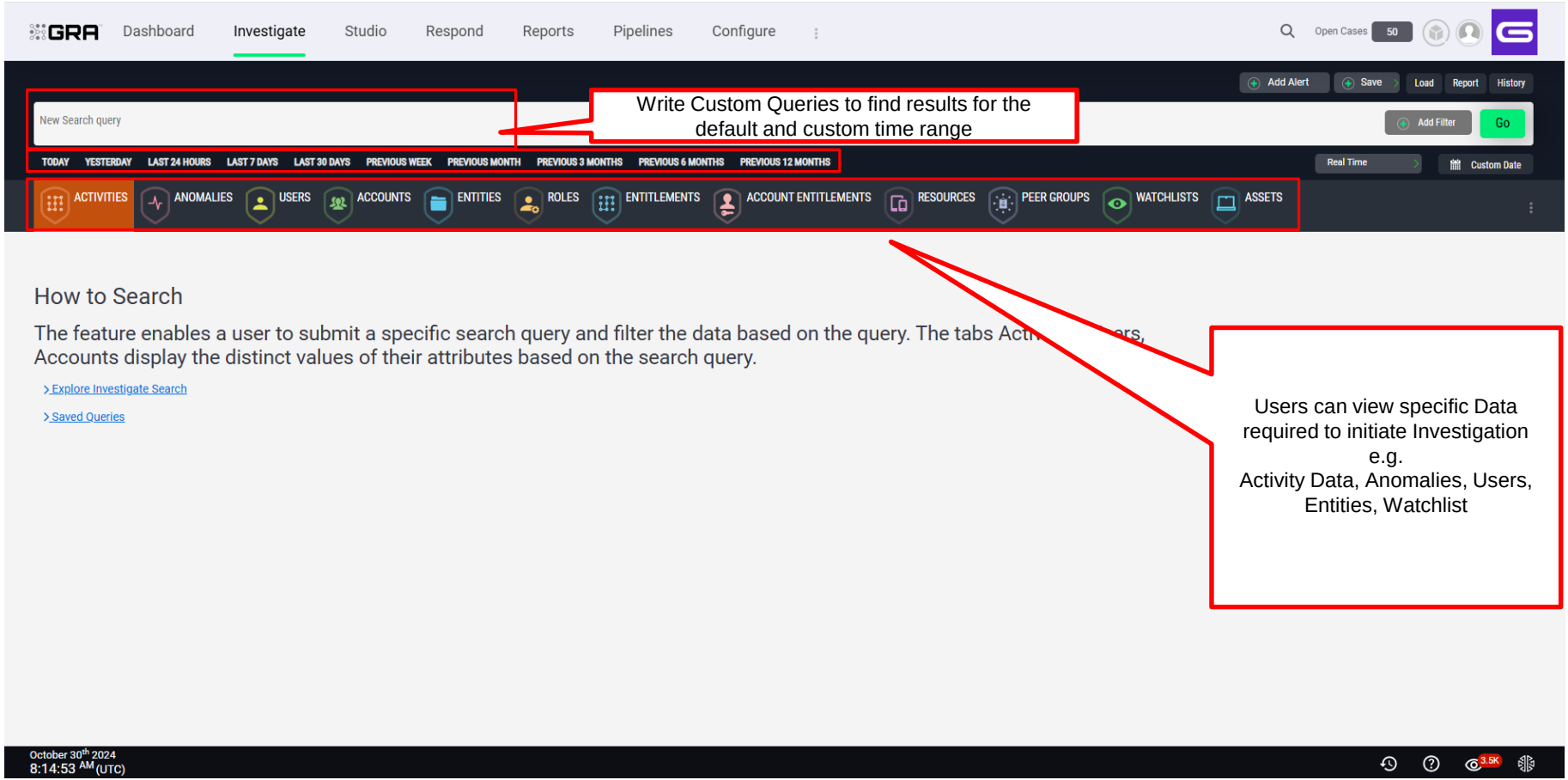
Pipelines Creation for respective data sources



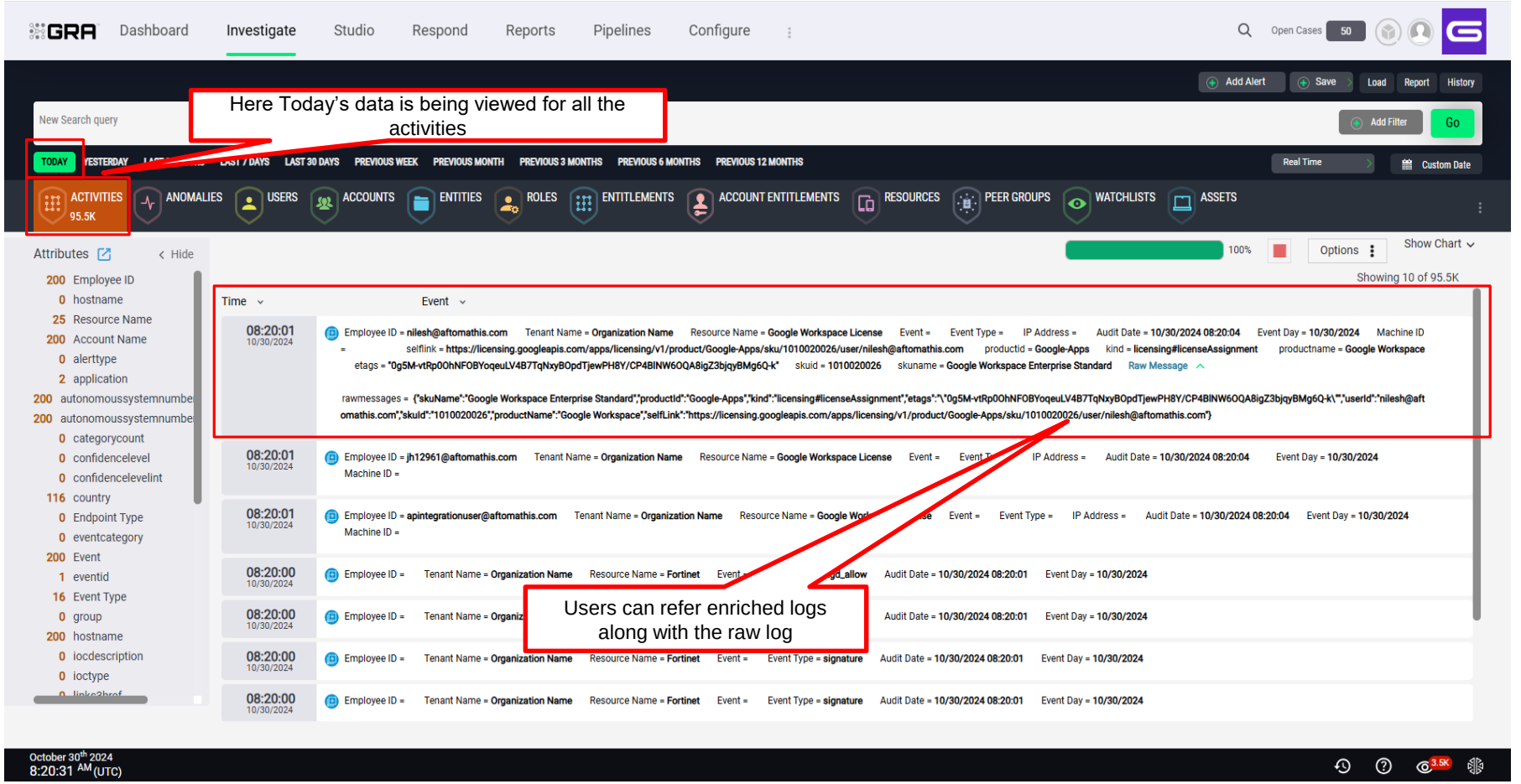
Data Ingestion Status for each pipeline



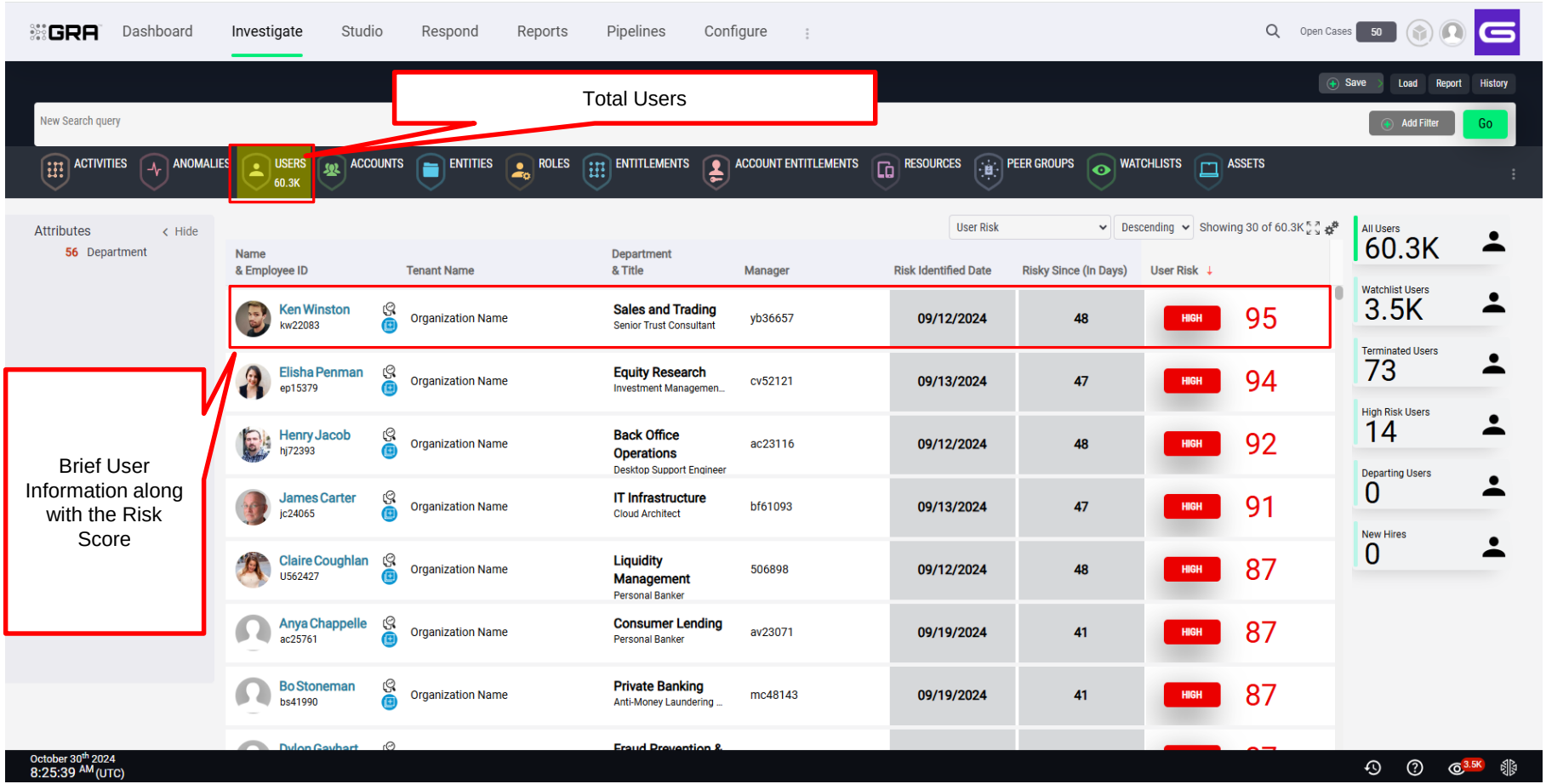
Investigate 01



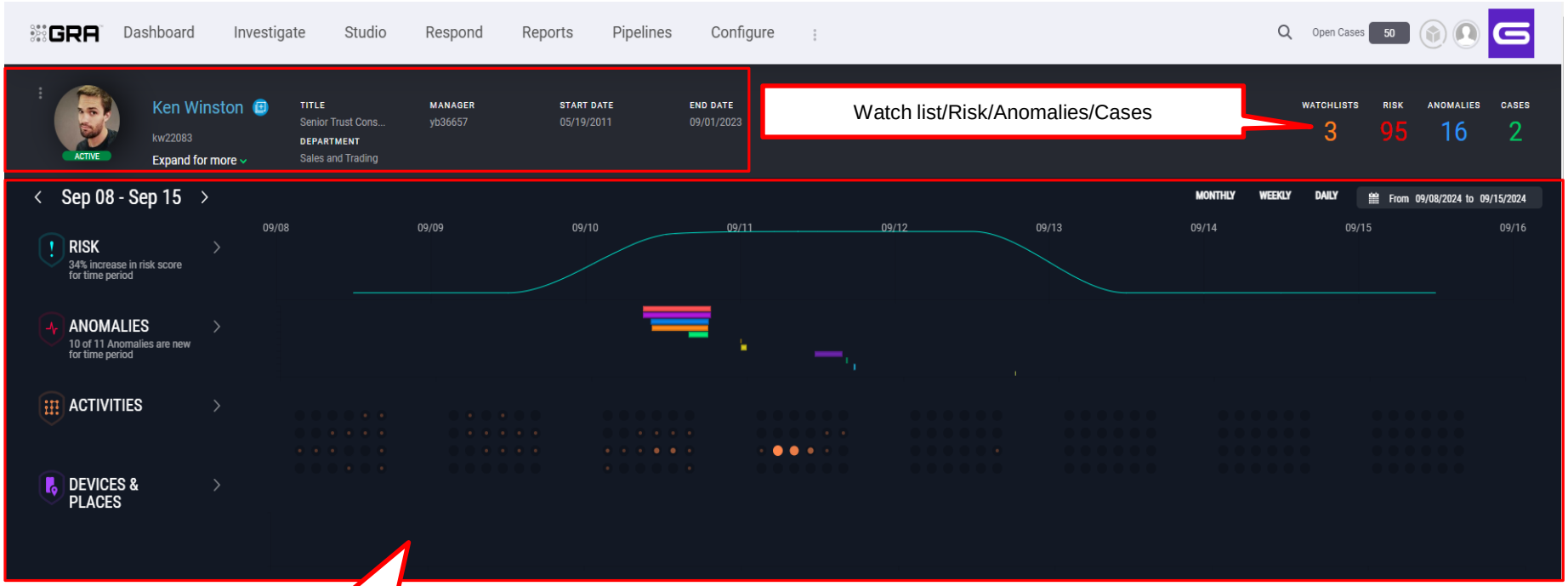
Investigate 02 (Activities)



Investigate 03 (Users)

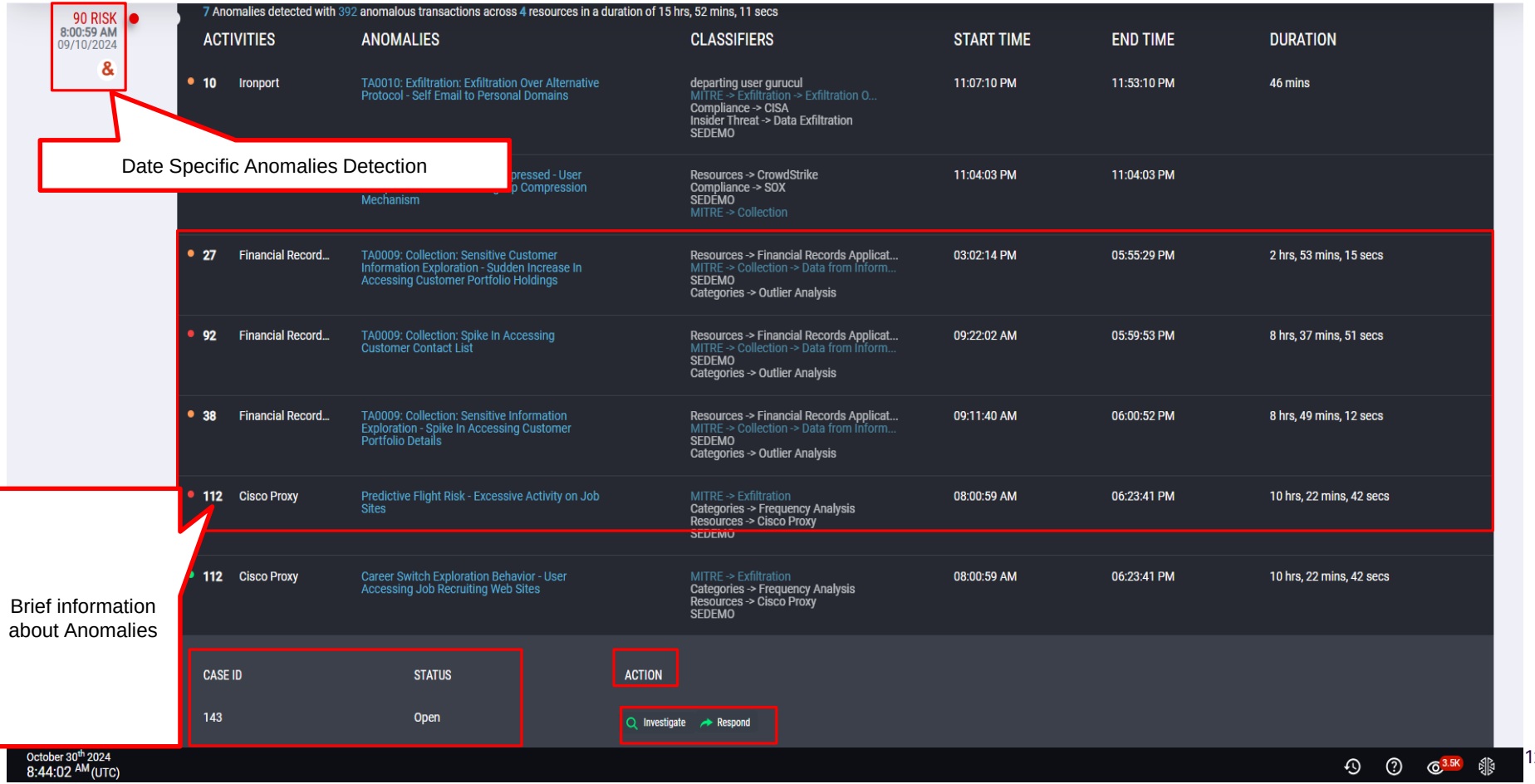


User Profile 01

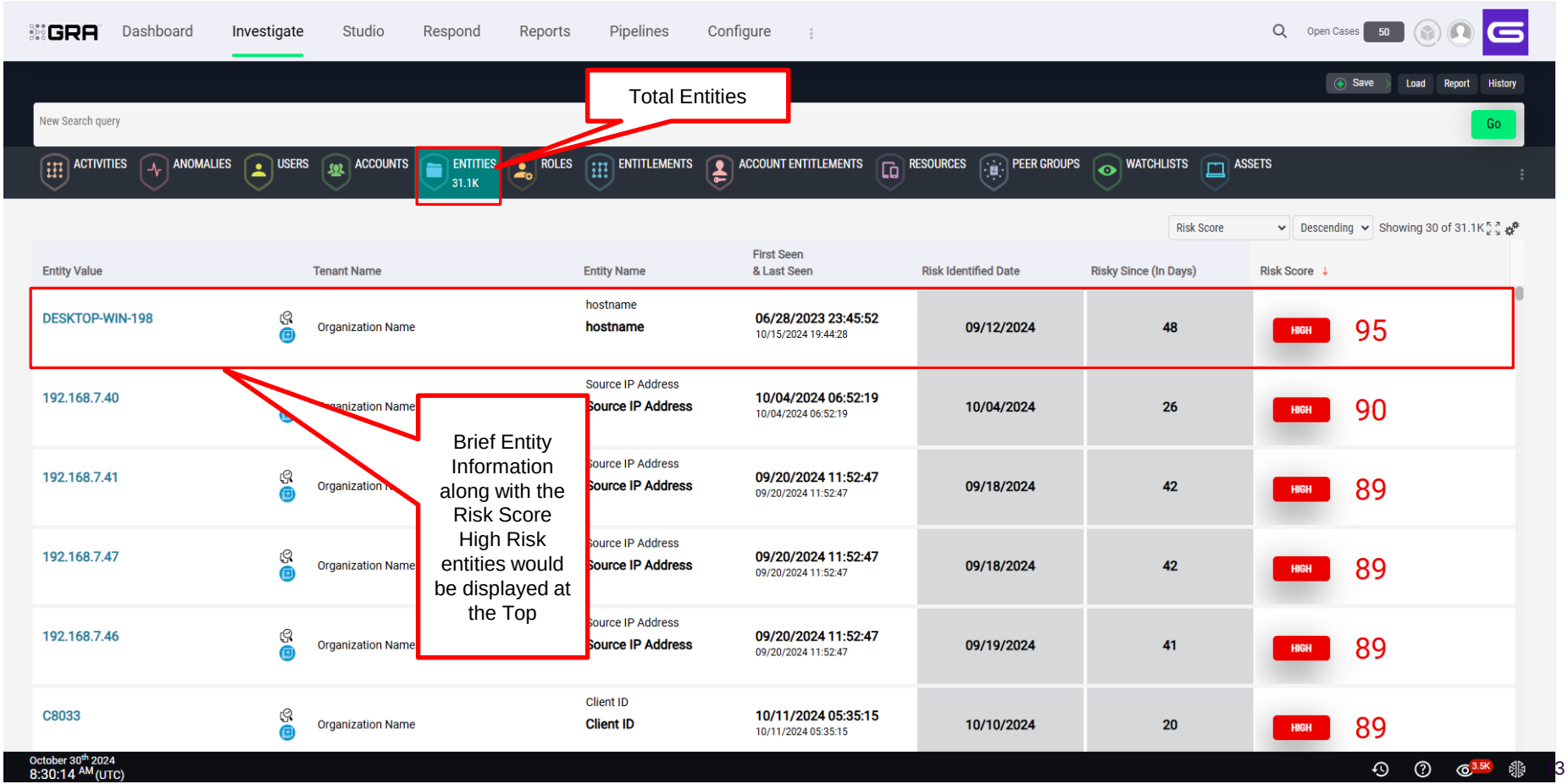


User Profile Overview

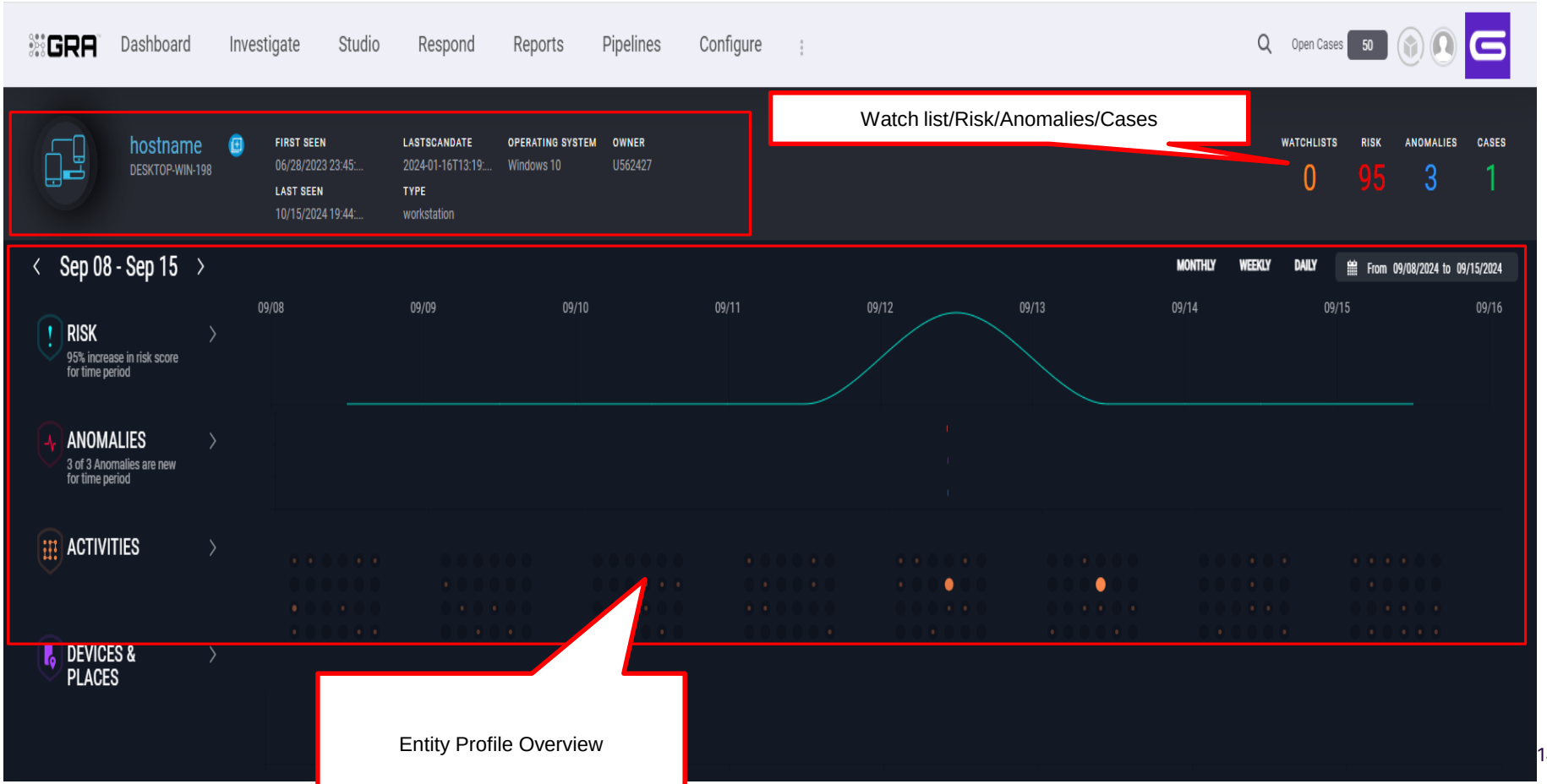
User Profile 02



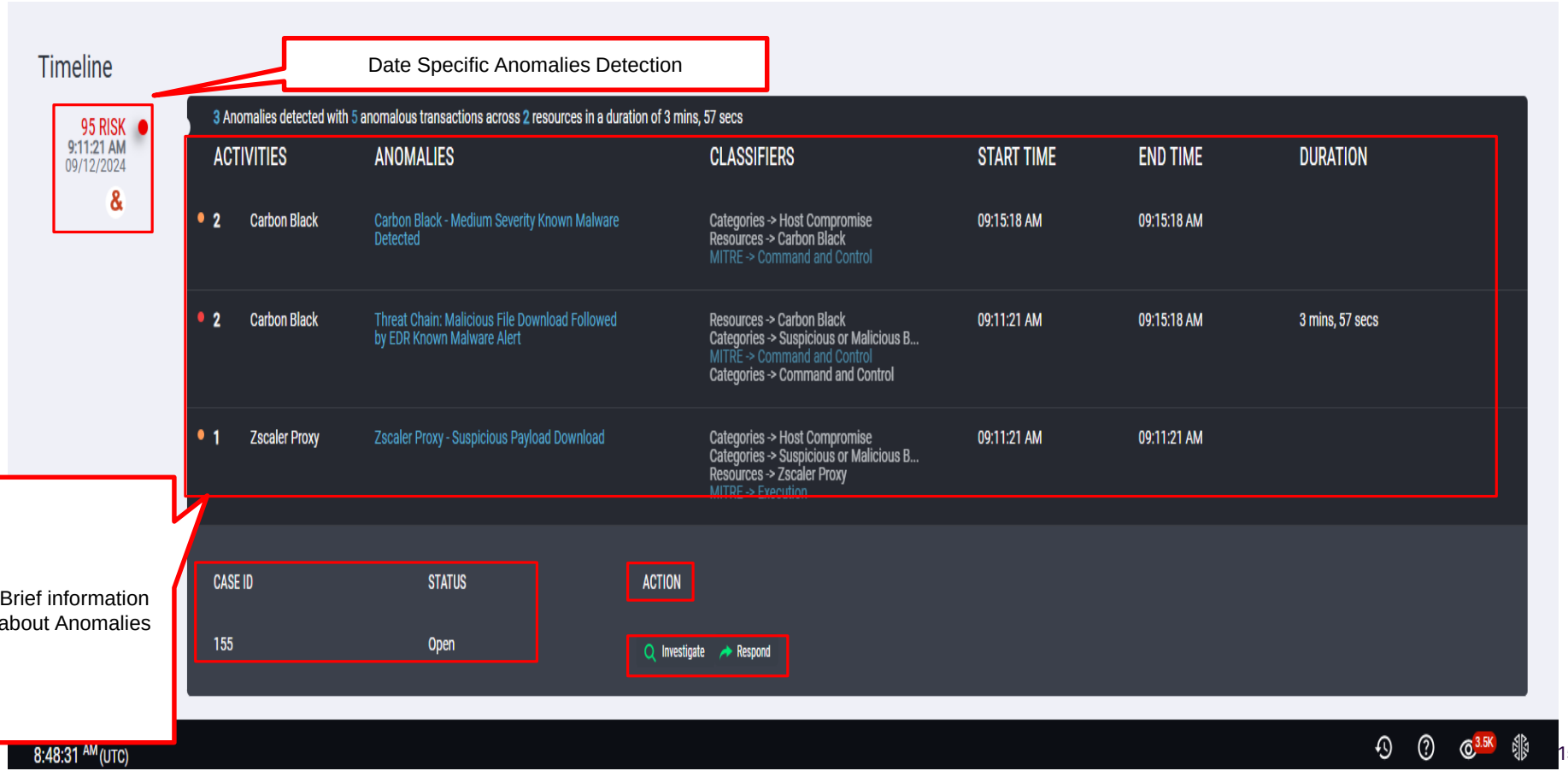
Investigate 04 (Entities)



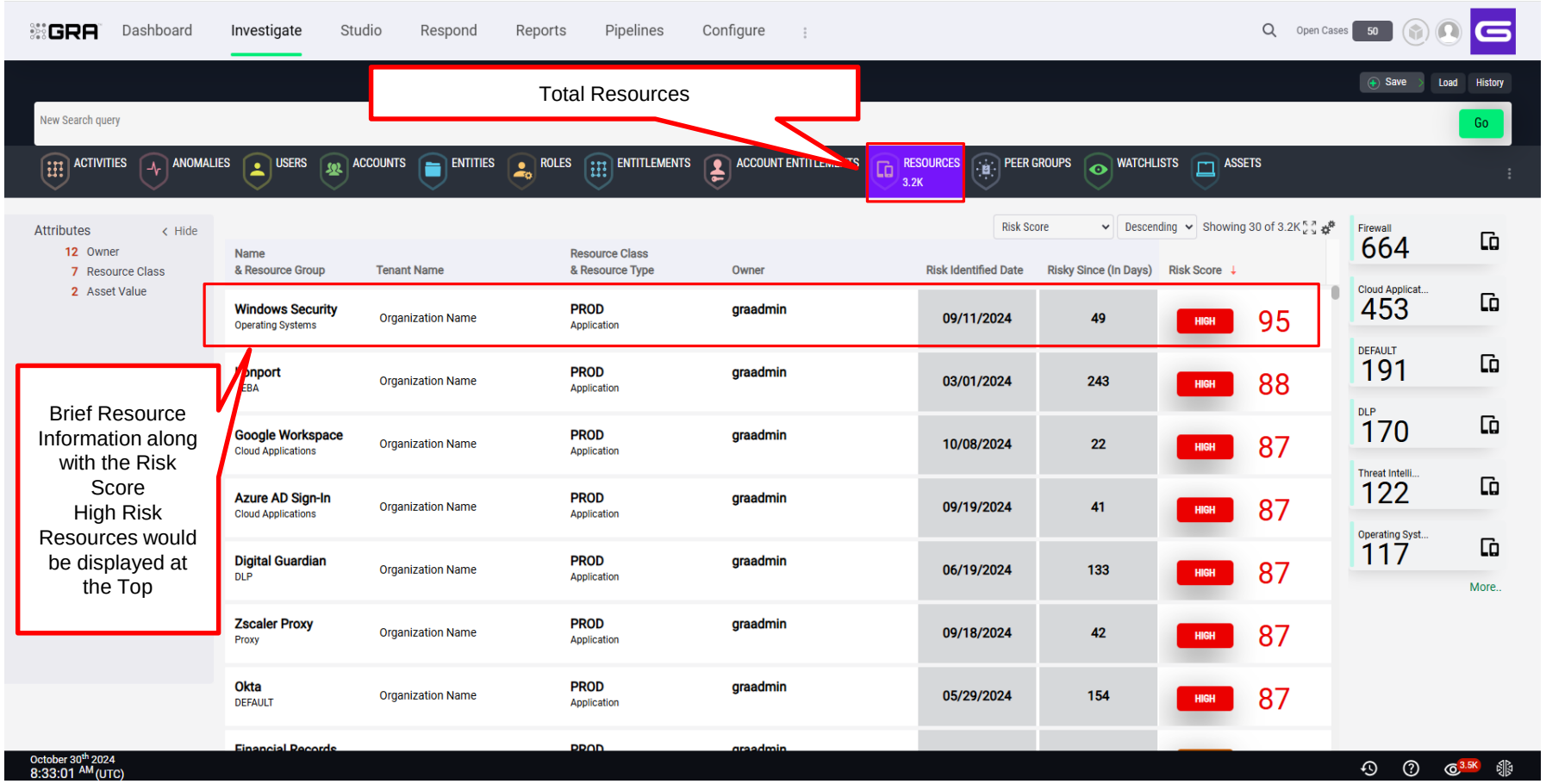
Entity Profile 01



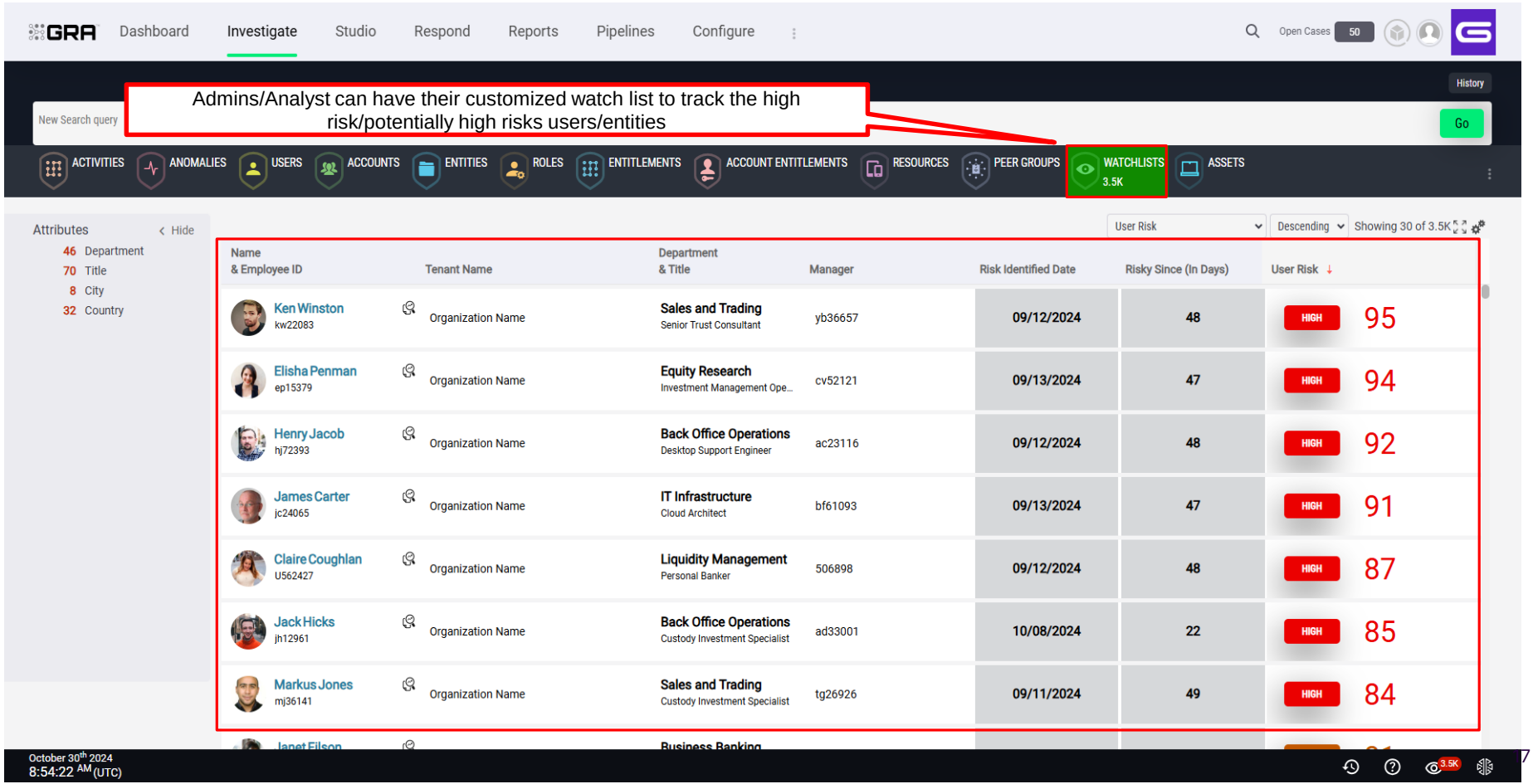
Entity Profile 02



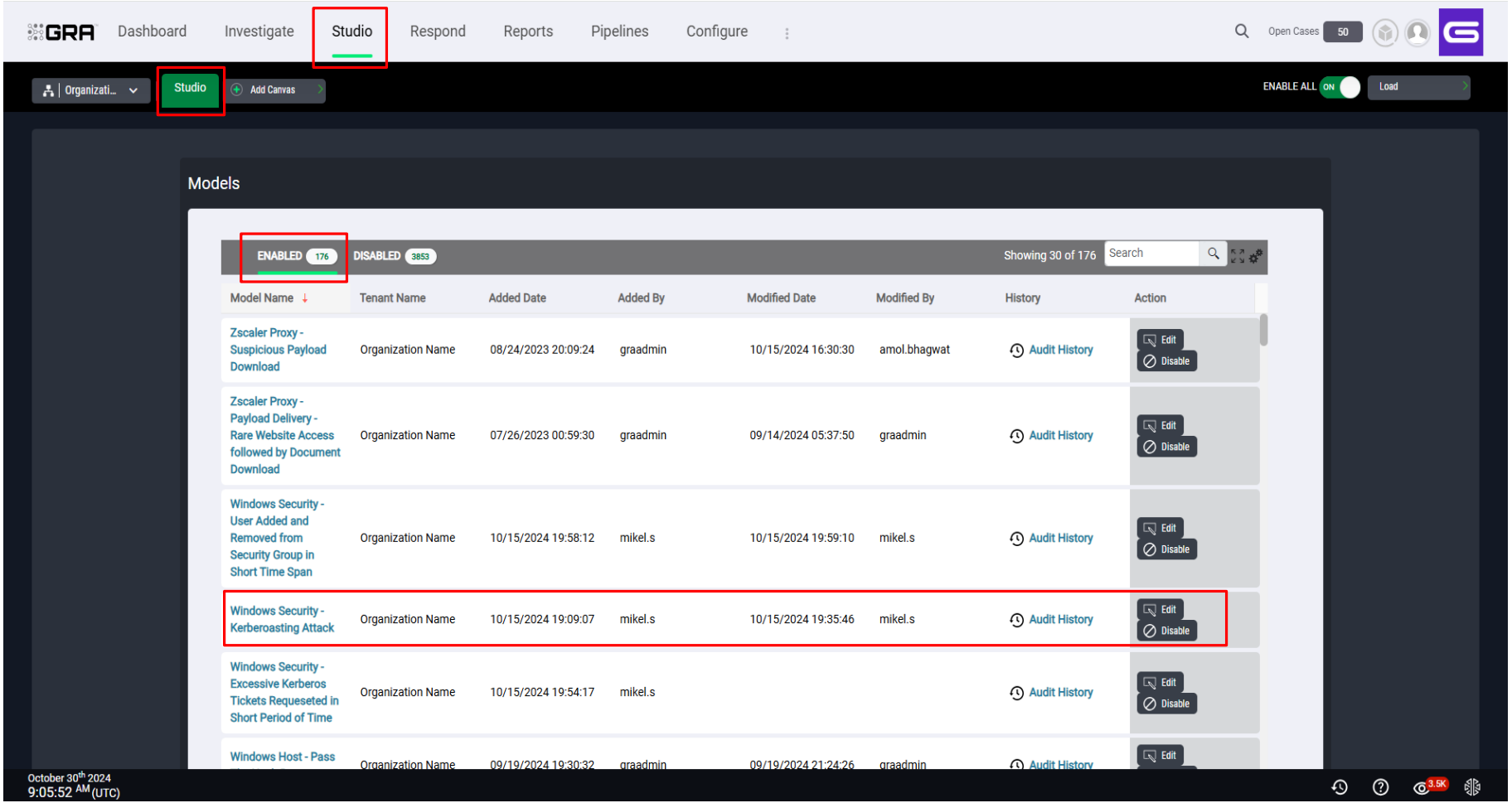
Investigate 05 (Resources)



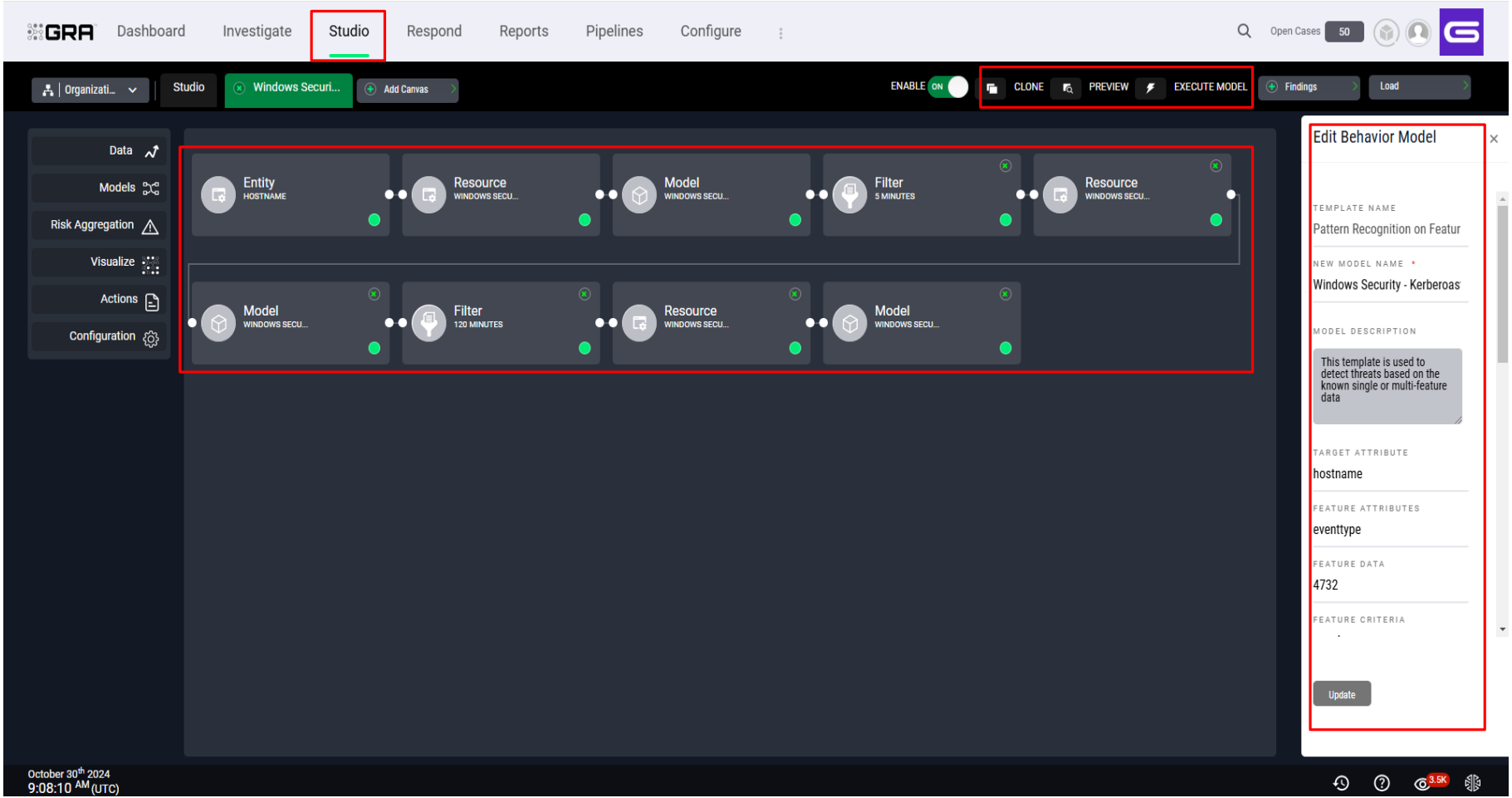
Investigate 06 (Watchlist)



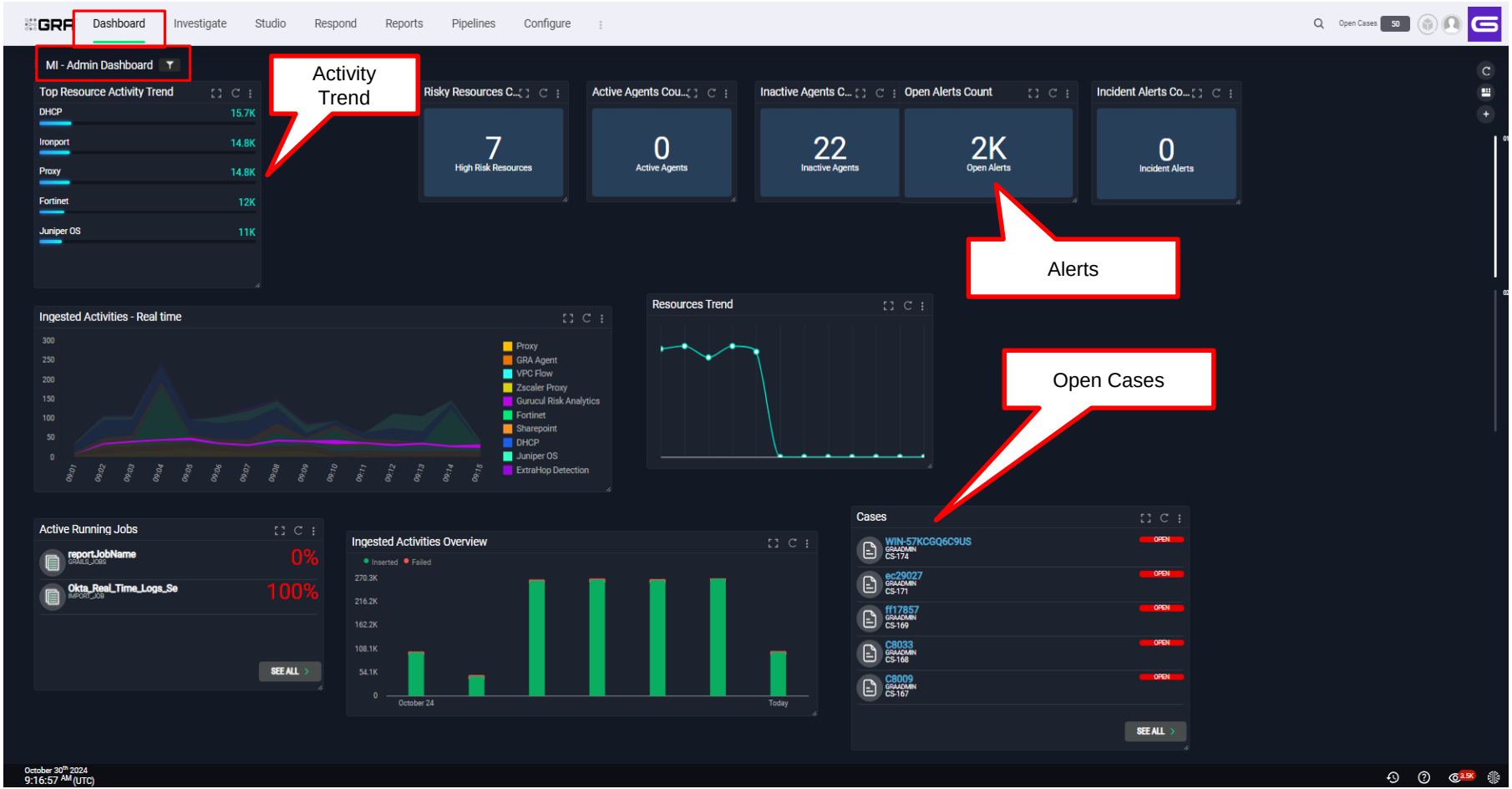
Models 01


GRA
Dashboard
Investigate
Studio
Respond
Reports
Pipelines
Configure
Open Cases
50
Organizati...
Studio
Add Canvas
ENABLE ALL
ON
Load
Models
ENABLED 176
DISABLED 3853
Showing 30 of 176
Search
Model Name
Tenant Name
Added Date
Added By
Modified Date
Modified By
History
Action
Zscaler Proxy - Suspicious Payload Download
Organization Name
08/24/2023 20:09:24
graadmin
10/15/2024 16:30:30
amol.bhagwat
Audit History
Edit
Disable
Zscaler Proxy - Payload Delivery - Rare Website Access followed by Document Download
Organization Name
07/26/2023 00:59:30
graadmin
09/14/2024 05:37:50
graadmin
Audit History
Edit
Disable
Windows Security - User Added and Removed from Security Group in Short Time Span
Organization Name
10/15/2024 19:58:12
mikel.s
10/15/2024 19:59:10
mikel.s
Audit History
Edit
Disable
Windows Security - Kerberoasting Attack
Organization Name
10/15/2024 19:09:07
mikel.s
10/15/2024 19:35:46
mikel.s
Audit History
Edit
Disable
Windows Security - Excessive Kerberos Tickets Requeseted in Short Period of Time
Organization Name
10/15/2024 19:54:17
mikel.s
Audit History
Edit
Disable
Windows Host - Pass
Organization Name
09/19/2024 19:30:32
graadmin
09/19/2024 21:24:26
graadmin
Audit History
Edit
October 30th 2024
9:05:52 AM (UTC)
3.5K

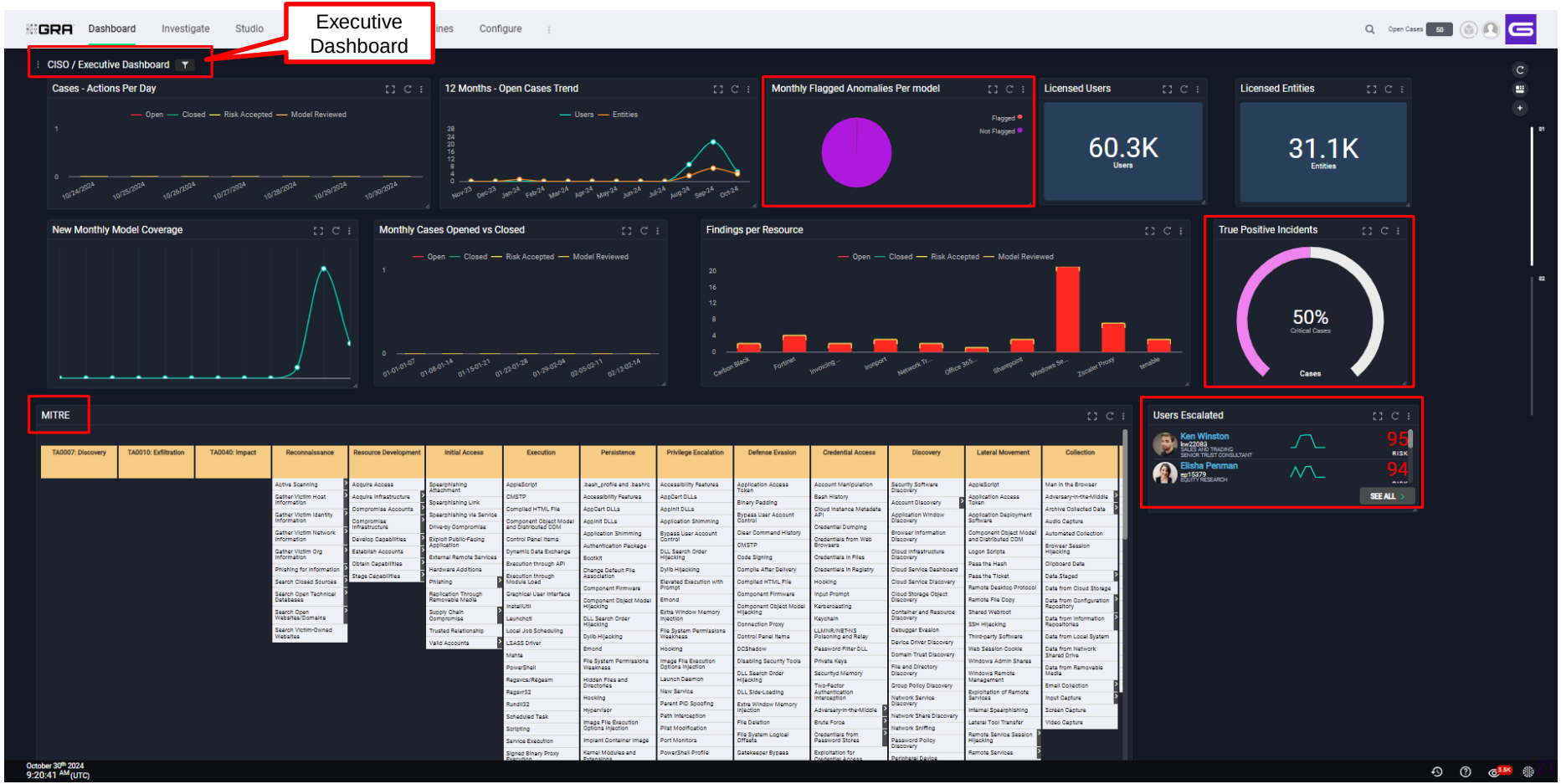
Models 02


GRA
Dashboard
Investigate
Studio
Respond
Reports
Pipelines
Configure
Open Cases
50
Organizati...
Studio
Windows Securi...
Add Canvas
ENABLE
ON
CLONE
PREVIEW
EXECUTE MODEL
Findings
Load
Data
Models
Risk Aggregation
Visualize
Actions
Configuration
Entity
HOSTNAME
Resource
WINDOWS SECU...
Model
WINDOWS SECU...
Filter
5 MINUTES
Resource
WINDOWS SECU...
Model
WINDOWS SECU...
Filter
120 MINUTES
Resource
WINDOWS SECU...
Model
WINDOWS SECU...
Edit Behavior Model
TEMPLATE NAME
Pattern Recognition on Featur
NEW MODEL NAME *
Windows Security - Kerberoas
MODEL DESCRIPTION
This template is used to detect threats based on the known single or multi-feature data
TARGET ATTRIBUTE
hostname
FEATURE ATTRIBUTES
eventtype
FEATURE DATA
4732
FEATURE CRITERIA
Update
October 30th 2024
9:08:10 AM (UTC)
3.5K

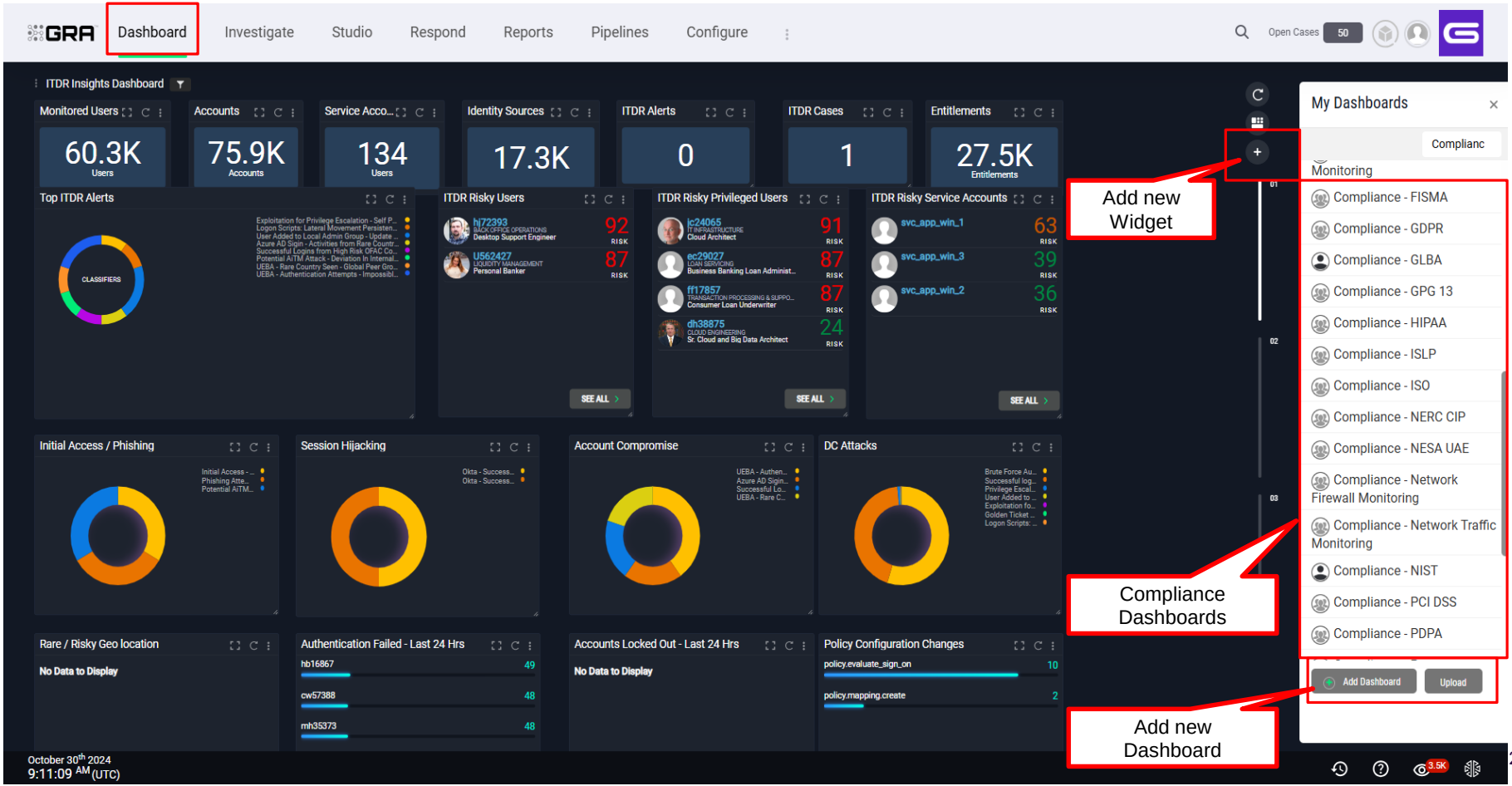
Custom Dashboards 01 (Admin)



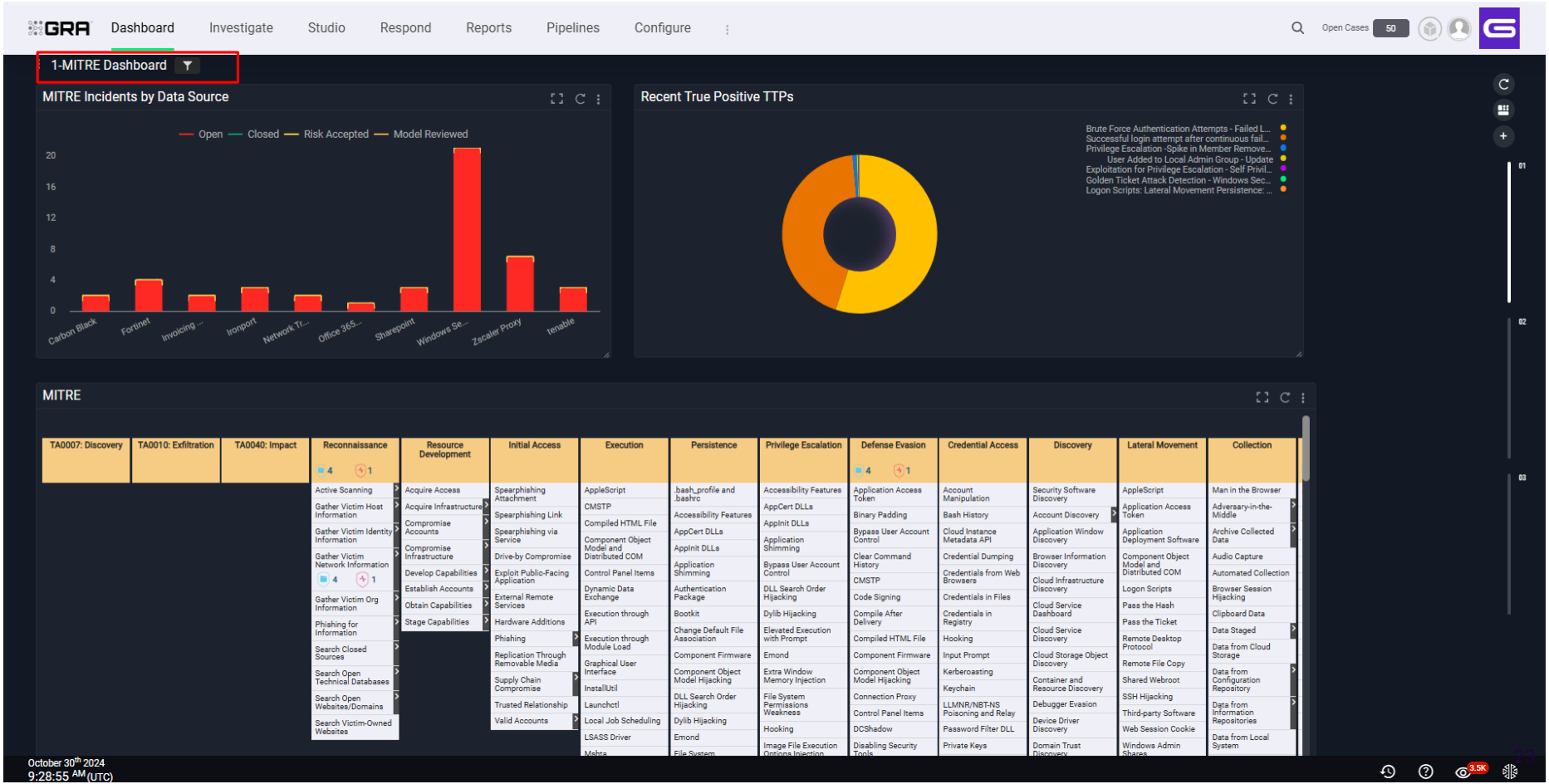
Custom Dashboards 02 (Executive)



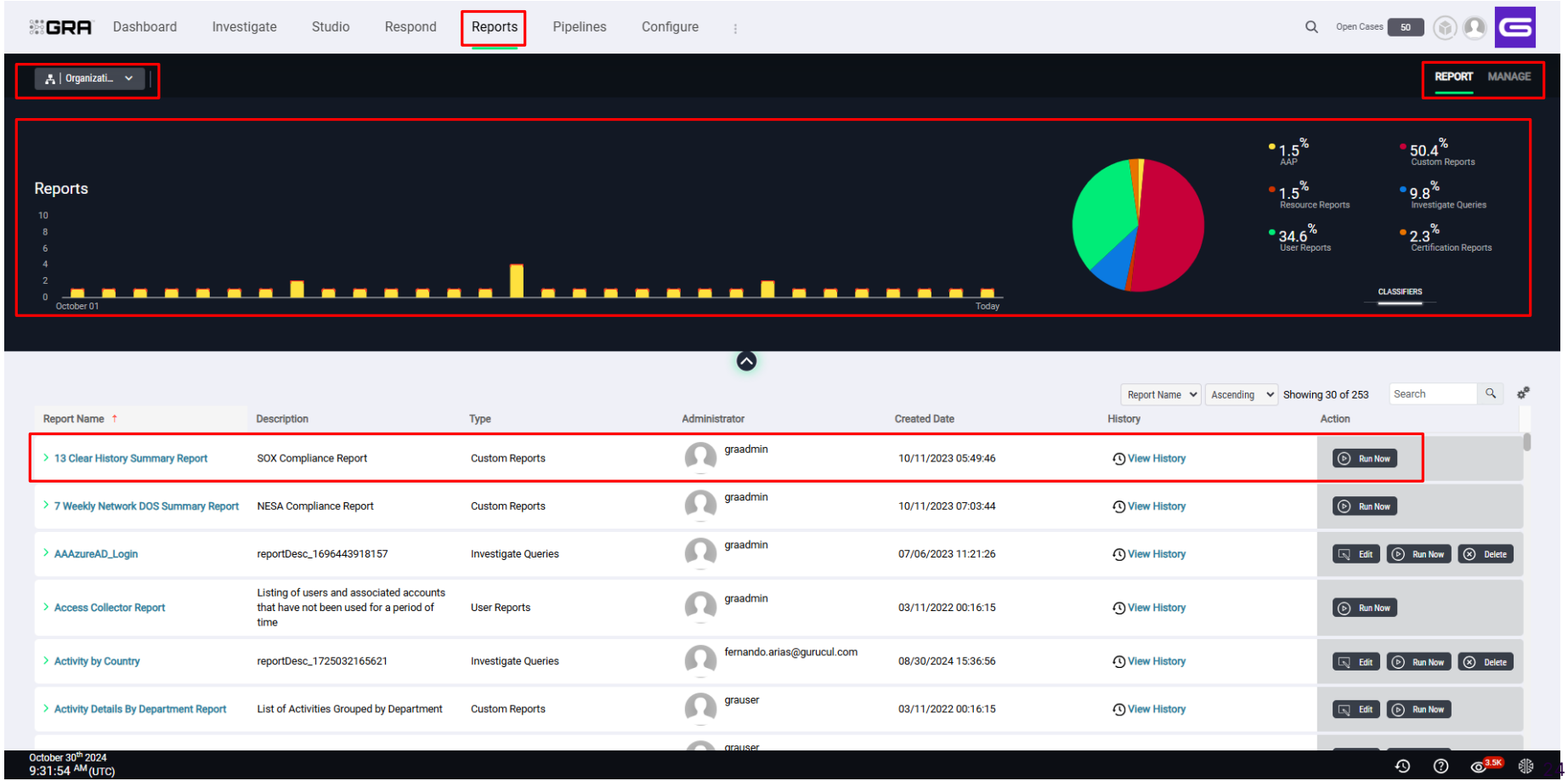
Custom Dashboards 03 (Compliance)



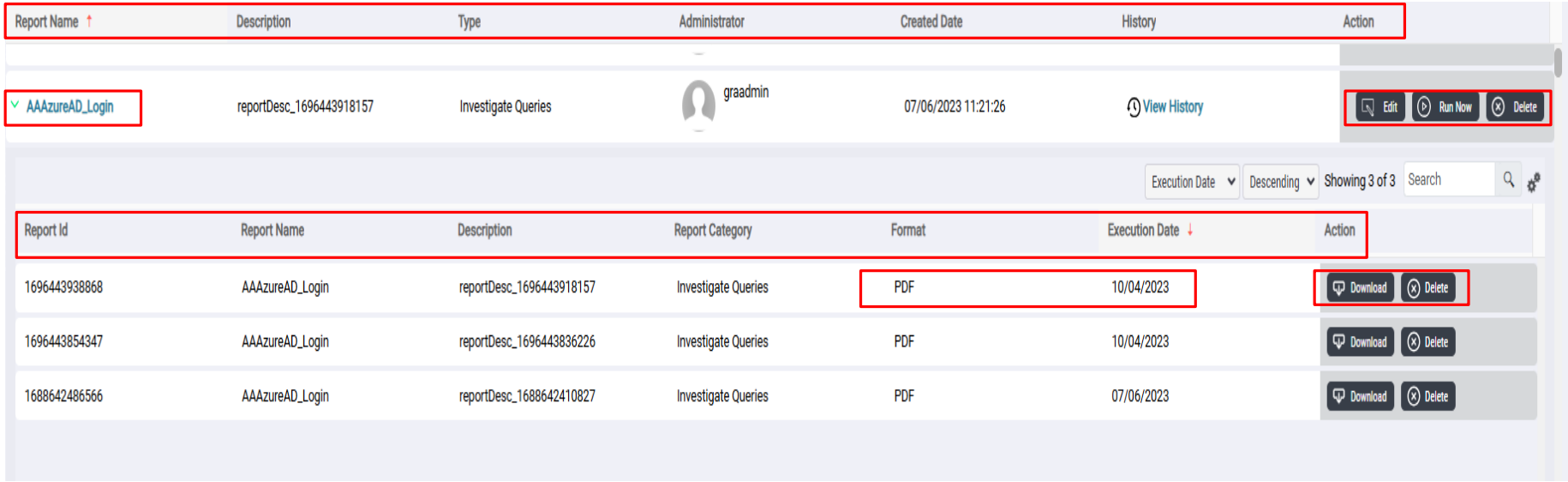
Custom Dashboards 04 (MITRE)



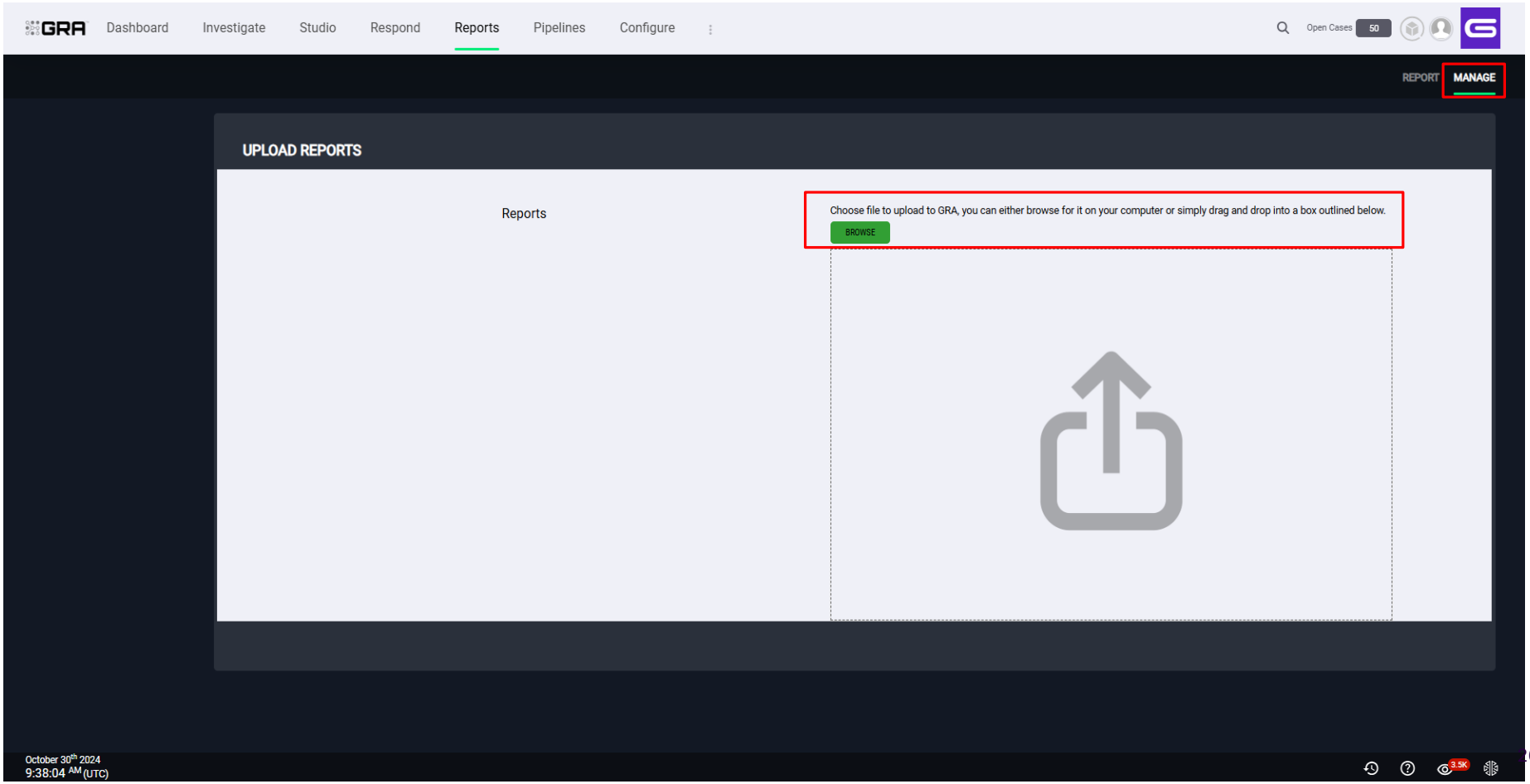
Reports 01


GRA
Dashboard
Investigate
Studio
Respond
Reports
Pipelines
Configure
Open Cases
50
Organizati...
REPORT
MANAGE
Reports
10
8
6
4
2
0
October 01
Today
1.5% AAP
50.4% Custom Reports
1.5% Resource Reports
9.8% Investigate Queries
34.6% User Reports
2.3% Certification Reports
CLASSIFIERS
Report Name
Ascending
Showing 30 of 253
Search
Report Name
Description
Type
Administrator
Created Date
History
Action
13 Clear History Summary Report
SOX Compliance Report
Custom Reports
graadmin
10/11/2023 05:49:46
View History
Run Now
7 Weekly Network DOS Summary Report
NESA Compliance Report
Custom Reports
graadmin
10/11/2023 07:03:44
View History
Run Now
AAAzureAD_Login
reportDesc_1696443918157
Investigate Queries
graadmin
07/06/2023 11:21:26
View History
Edit
Run Now
Delete
Access Collector Report
Listing of users and associated accounts that have not been used for a period of time
User Reports
graadmin
03/11/2022 00:16:15
View History
Run Now
Activity by Country
reportDesc_1725032165621
Investigate Queries
fernando.arias@gurucul.com
08/30/2024 15:36:56
View History
Edit
Run Now
Delete
Activity Details By Department Report
List of Activities Grouped by Department
Custom Reports
grauser
03/11/2022 00:16:15
View History
Edit
Run Now
grauser
October 30th 2024
9:31:54 AM (UTC)
3.5K

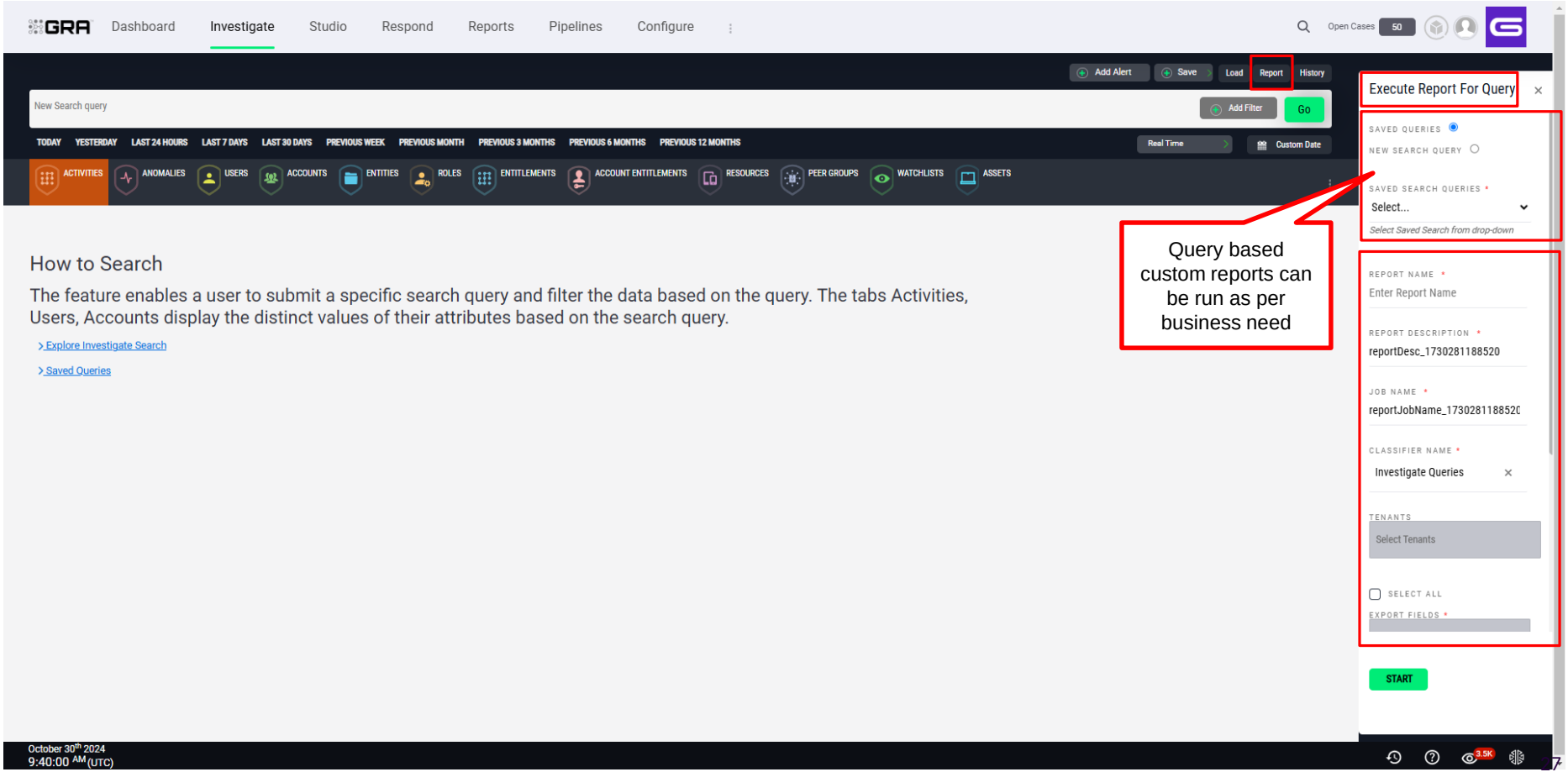
Reports 02


Report Name
Description
Type
Administrator
Created Date
History
Action
AAAzureAD_Login
reportDesc_1696443918157
Investigate Queries
graadmin
07/06/2023 11:21:26
View History
Edit
Run Now
Delete
Execution Date
Descending
Showing 3 of 3
Search
Report Id
Report Name
Description
Report Category
Format
Execution Date
Action
1696443938868
AAAzureAD_Login
reportDesc_1696443918157
Investigate Queries
PDF
10/04/2023
Download
Delete
1696443854347
AAAzureAD_Login
reportDesc_1696443836226
Investigate Queries
PDF
10/04/2023
Download
Delete
1688642486566
AAAzureAD_Login
reportDesc_1688642410827
Investigate Queries
PDF
07/06/2023
Download
Delete

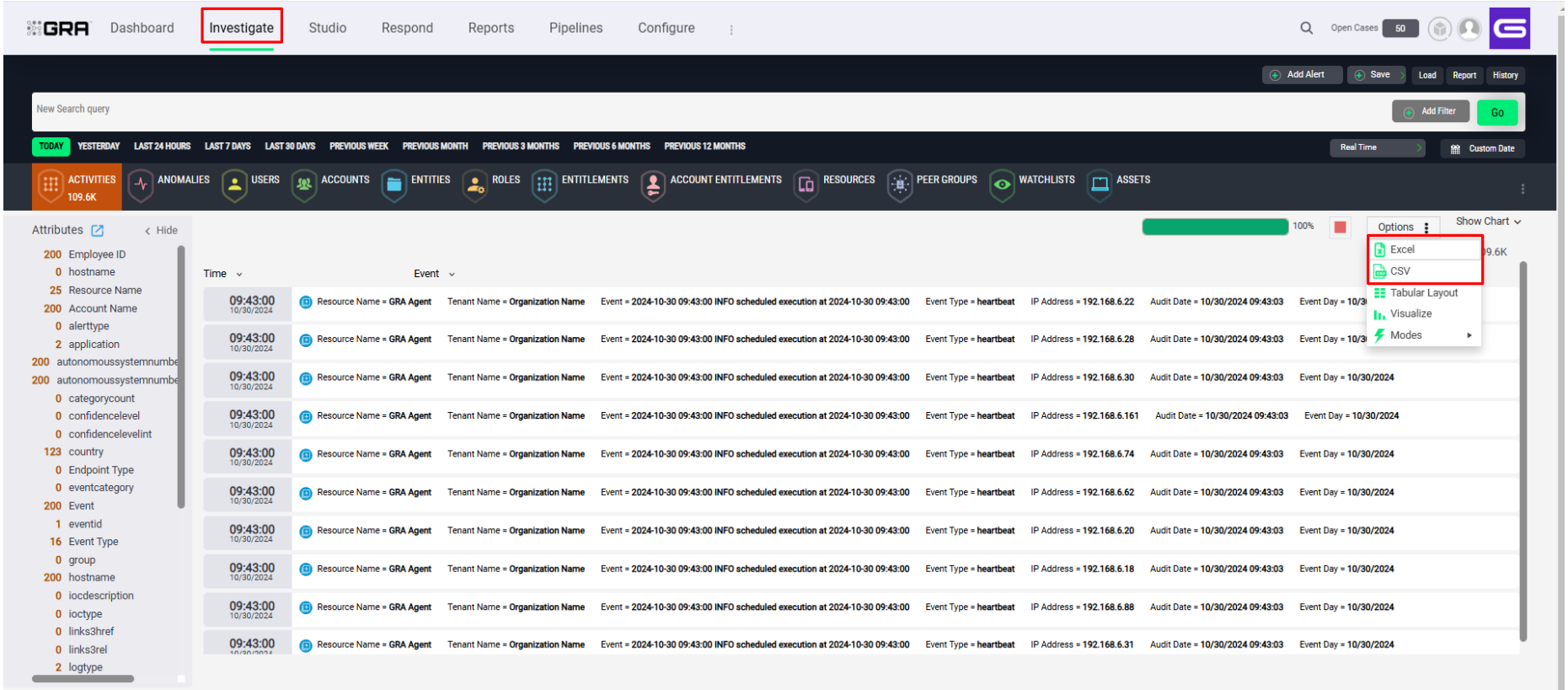
Reports 03


GRA
Dashboard
Investigate
Studio
Respond
Reports
Pipelines
Configure
Open Cases
50
REPORT
MANAGE
UPLOAD REPORTS
Reports
Choose file to upload to GRA, you can either browse for it on your computer or simply drag and drop into a box outlined below.
BROWSE
October 30th 2024
9:38:04 AM (UTC)
3.5K

Reports 04

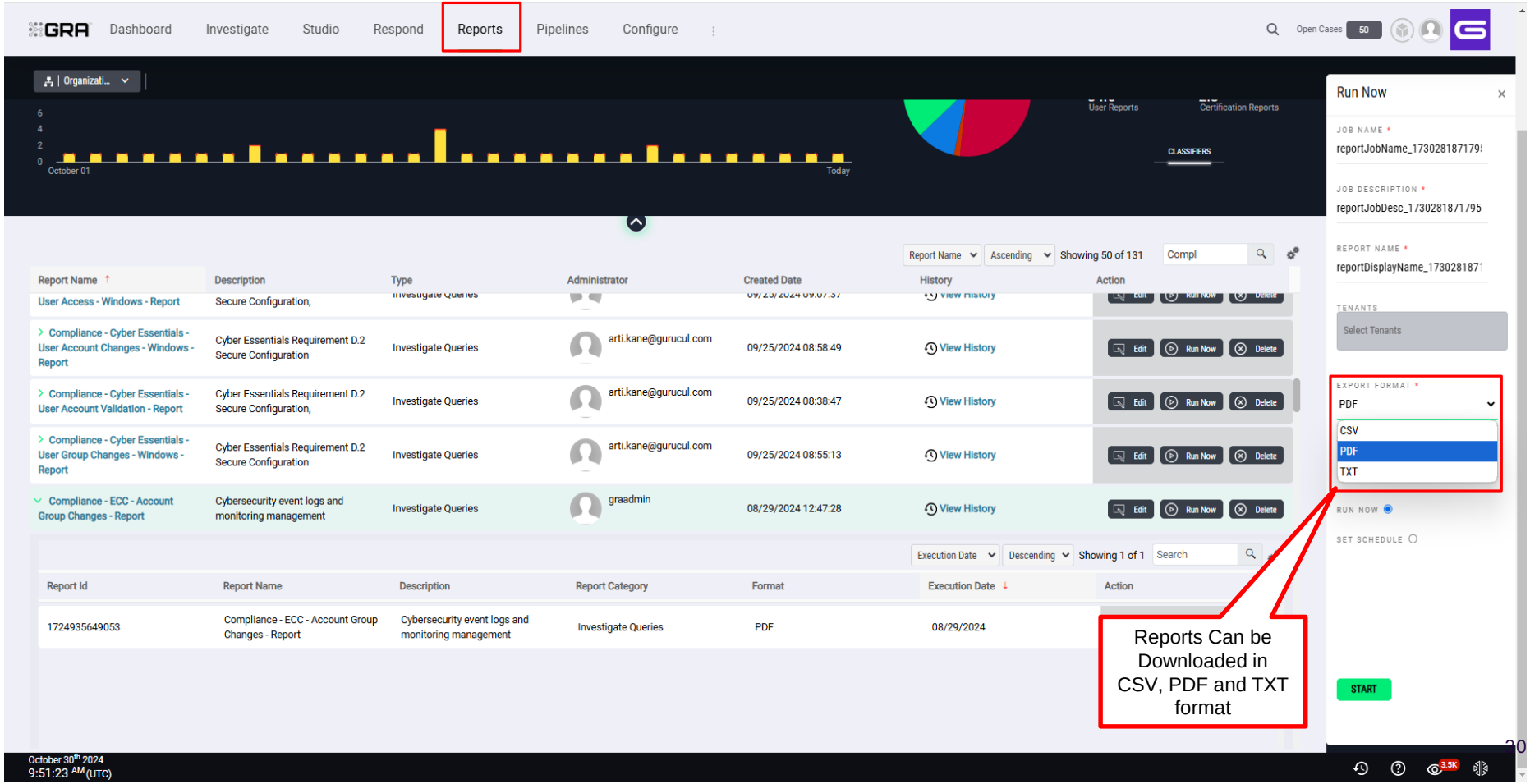

GRA
Dashboard
Investigate
Studio
Respond
Reports
Pipelines
Configure
Open Cases
50
Add Alert
Save
Load
Report
History
New Search query
Add Filter
Go
TODAY
YESTERDAY
LAST 24 HOURS
LAST 7 DAYS
LAST 30 DAYS
PREVIOUS WEEK
PREVIOUS MONTH
PREVIOUS 3 MONTHS
PREVIOUS 6 MONTHS
PREVIOUS 12 MONTHS
Real Time
Custom Date
ACTIVITIES
ANOMALIES
USERS
ACCOUNTS
ENTITIES
ROLES
ENTITLEMENTS
ACCOUNT ENTITLEMENTS
RESOURCES
PEER GROUPS
WATCHLISTS
ASSETS
How to Search
The feature enables a user to submit a specific search query and filter the data based on the query. The tabs Activities, Users, Accounts display the distinct values of their attributes based on the search query.
Explore Investigate Search
Saved Queries
Query based custom reports can be run as per business need
Execute Report For Query
SAVED QUERIES
NEW SEARCH QUERY
SAVED SEARCH QUERIES *
Select...
Select Saved Search from drop-down
REPORT NAME *
Enter Report Name
REPORT DESCRIPTION *
reportDesc_1730281188520
JOB NAME *
reportJobName_1730281188520
CLASSIFIER NAME *
Investigate Queries
TENANTS
Select Tenants
SELECT ALL
EXPORT FIELDS *
START
October 30th 2024
9:40:00 AM (UTC)
3.5K

Data Export 01 (Investigate)



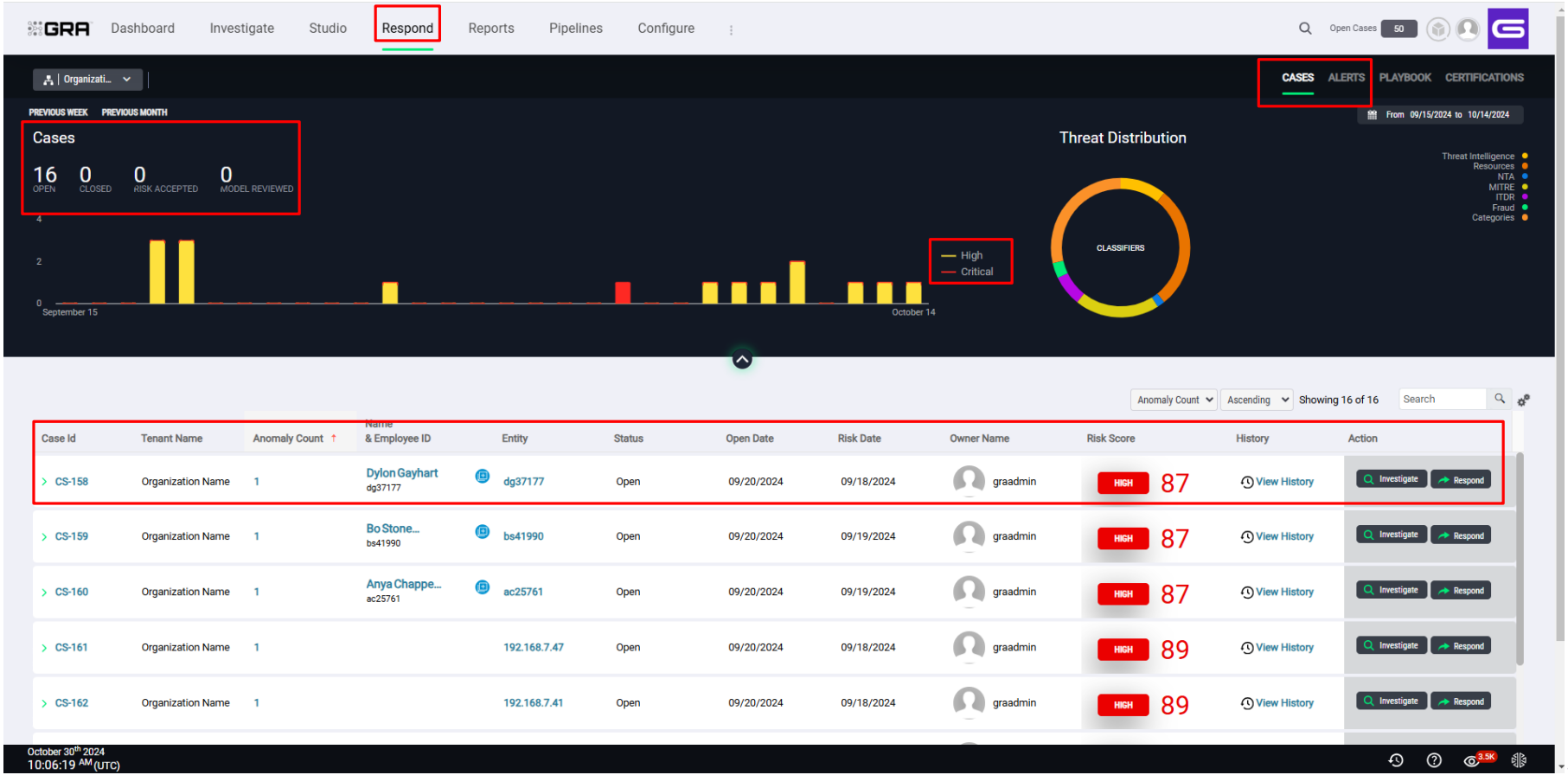
Data Export 02 (Dashboard)

Data Export 03 (Reports)

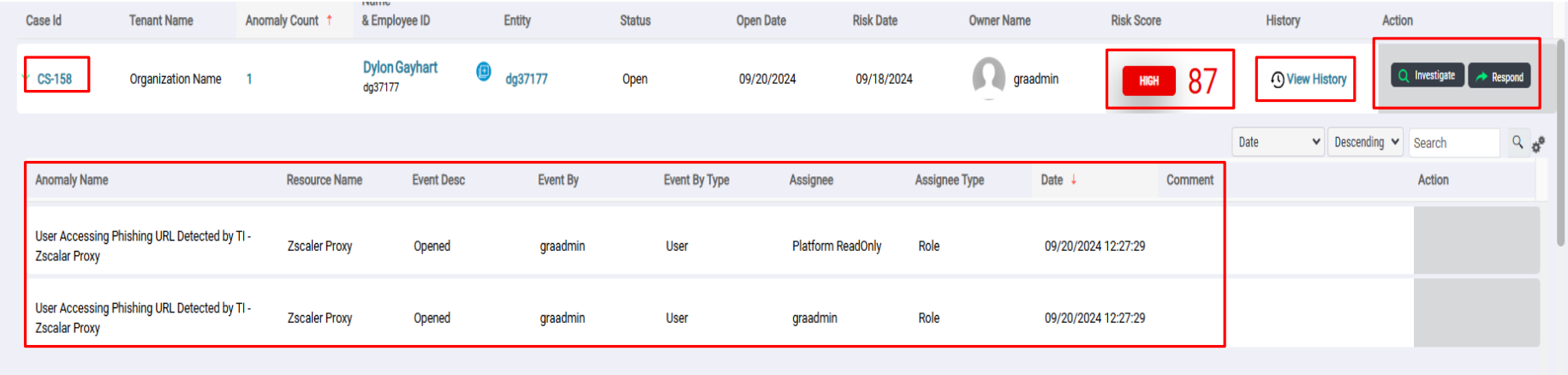


Export 04 (User/Entity Profile)

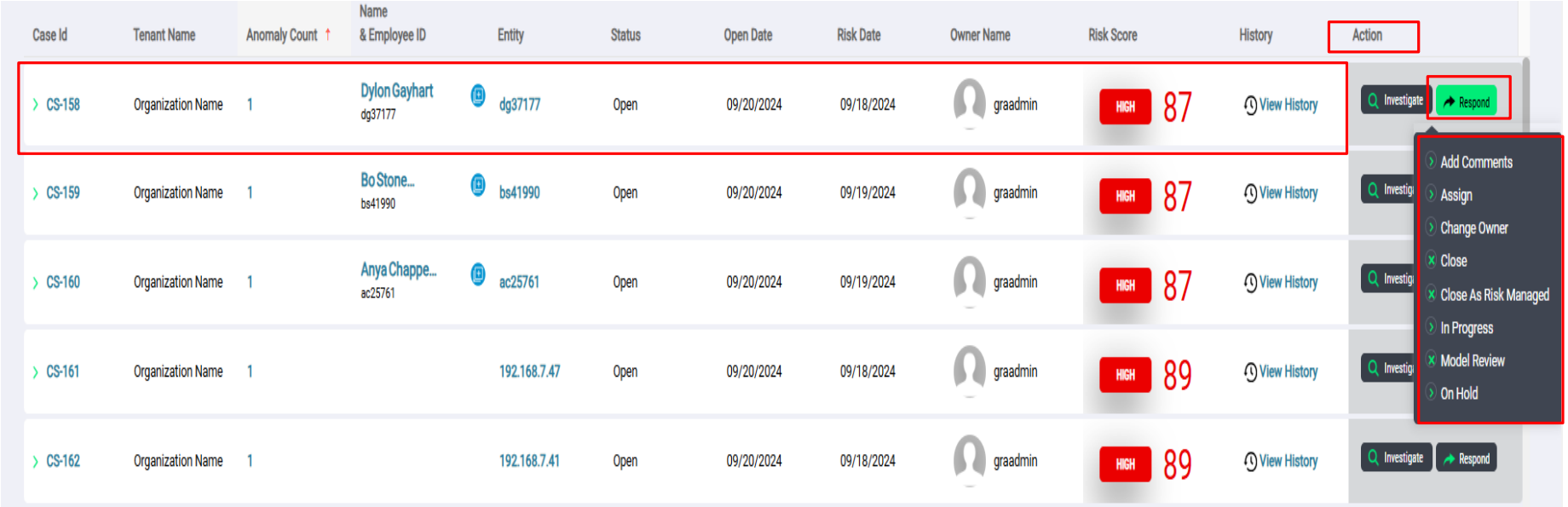
Case Management 01 (Case)



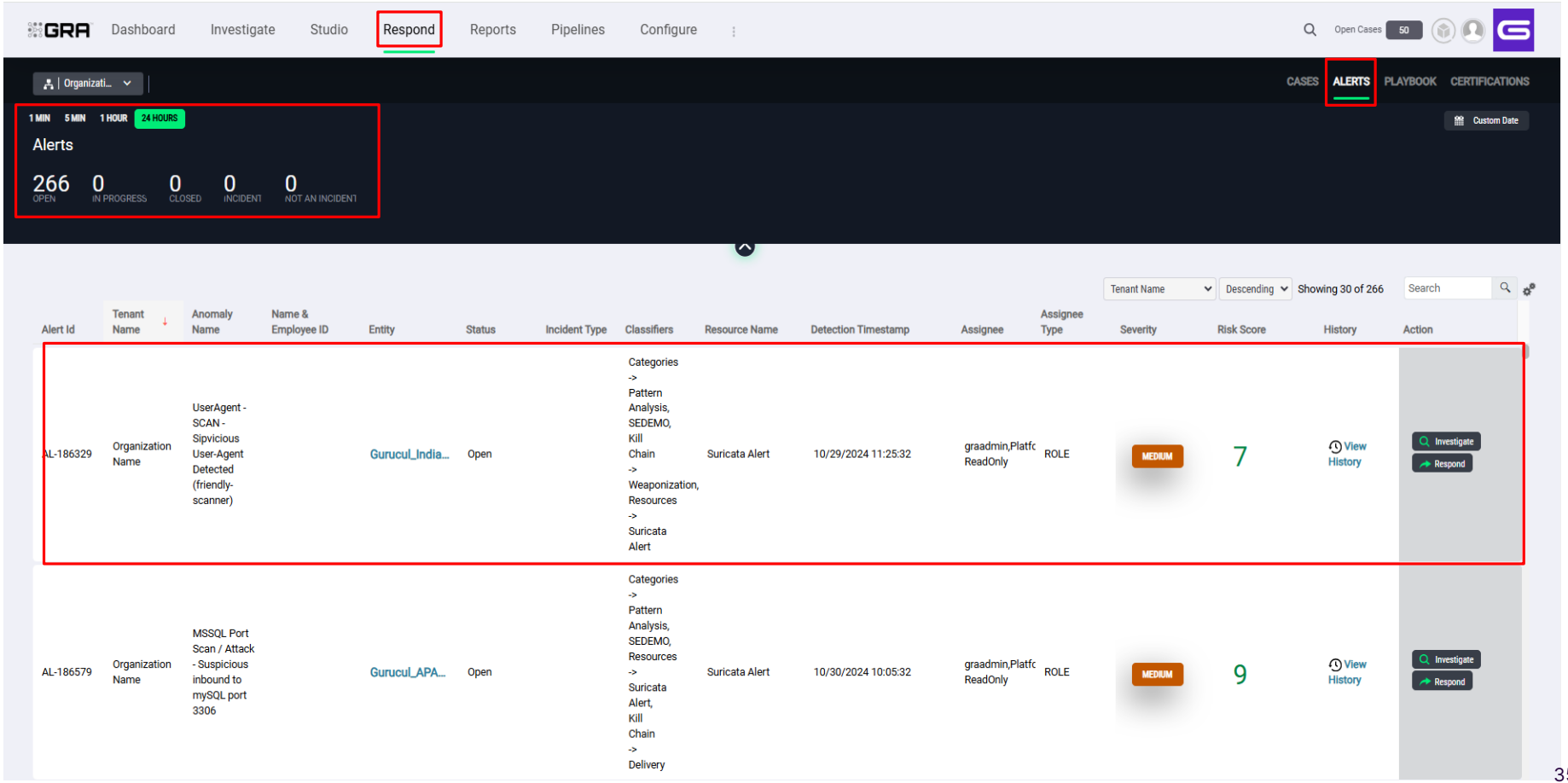
Case Management 02 (Case)



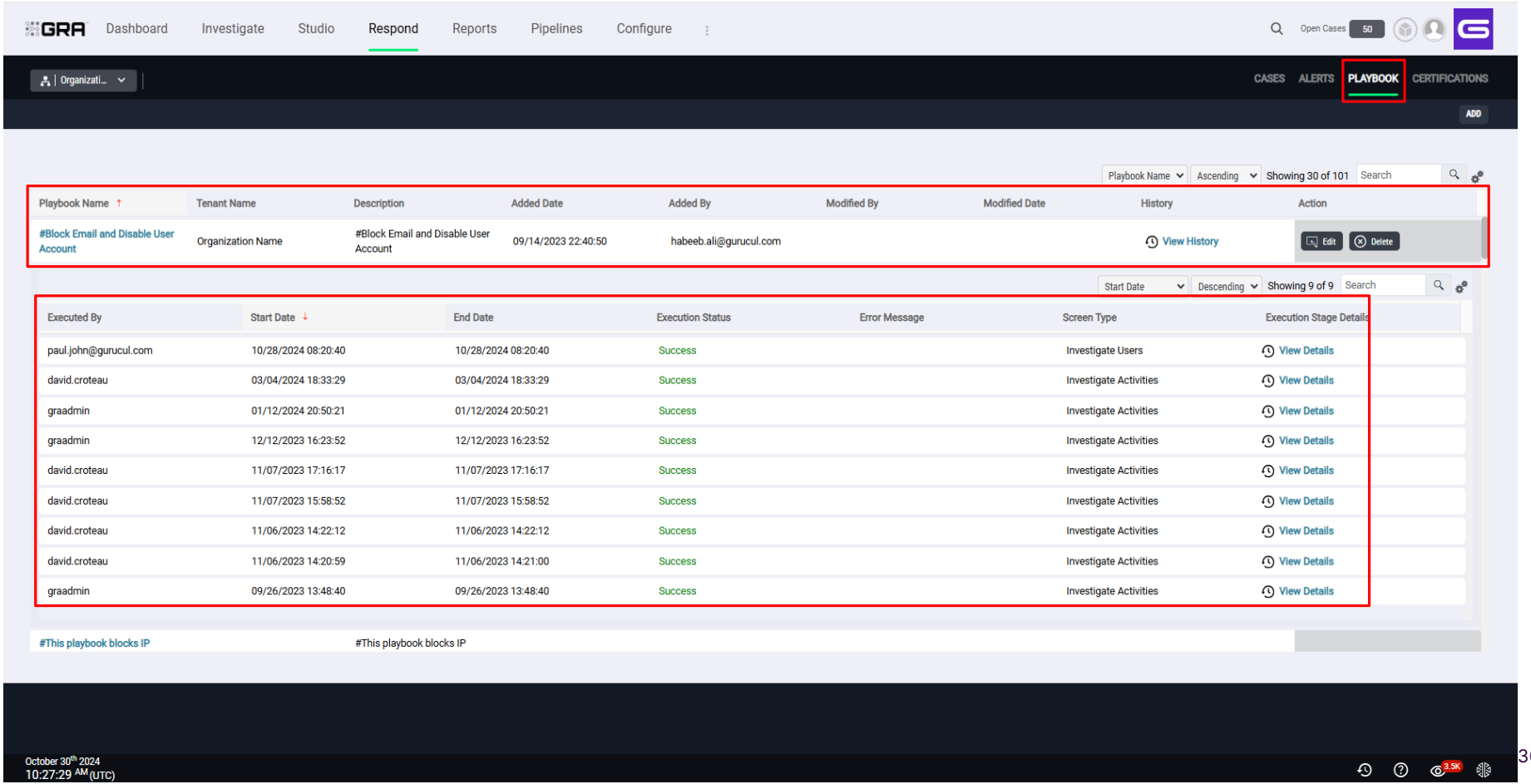
Case Management 03 (Actions)



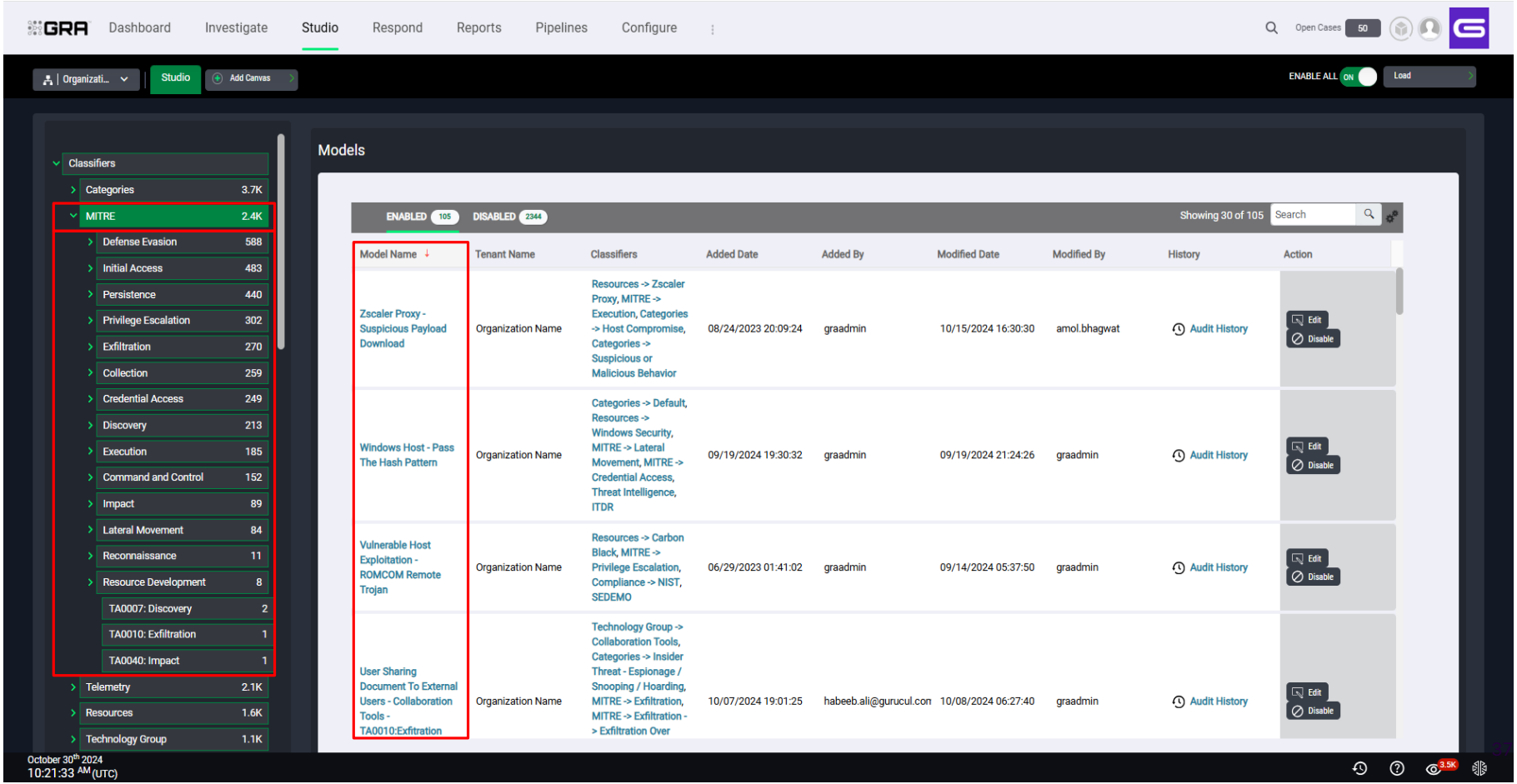
Alerts


GRA
Dashboard
Investigate
Studio
Respond
Reports
Pipelines
Configure
Open Cases 50
Organizati...
CASES
ALERTS
PLAYBOOK
CERTIFICATIONS
1 MIN
5 MIN
1 HOUR
24 HOURS
Custom Date
Alerts
266 OPEN
0 IN PROGRESS
0 CLOSED
0 INCIDENT
0 NOT AN INCIDENT
Tenant Name
Descending
Showing 30 of 266
Search
Alert Id
Tenant Name
Anomaly Name
Name & Employee ID
Entity
Status
Incident Type
Classifiers
Resource Name
Detection Timestamp
Assignee
Assignee Type
Severity
Risk Score
History
Action
AL-186329
Organization Name
UserAgent - SCAN - Sipvicious User-Agent Detected (friendly-scanner)
Gurucul_India...
Open
Categories -> Pattern Analysis, SEDEMO, Kill Chain -> Weaponization, Resources -> Suricata Alert
Suricata Alert
10/29/2024 11:25:32
graadmin,Platfc ReadOnly
ROLE
MEDIUM
7
View History
Investigate
Respond
AL-186579
Organization Name
MSSQL Port Scan / Attack - Suspicious inbound to mySQL port 3306
Gurucul_APA...
Open
Categories -> Pattern Analysis, SEDEMO, Resources -> Suricata Alert, Kill Chain -> Delivery
Suricata Alert
10/30/2024 10:05:32
graadmin,Platfc ReadOnly
ROLE
MEDIUM
9
View History
Investigate
Respond

Playbook Action



MITRE Mapping with Models



Thank you

Gurucul