Diamond Model demo

Setup steps:

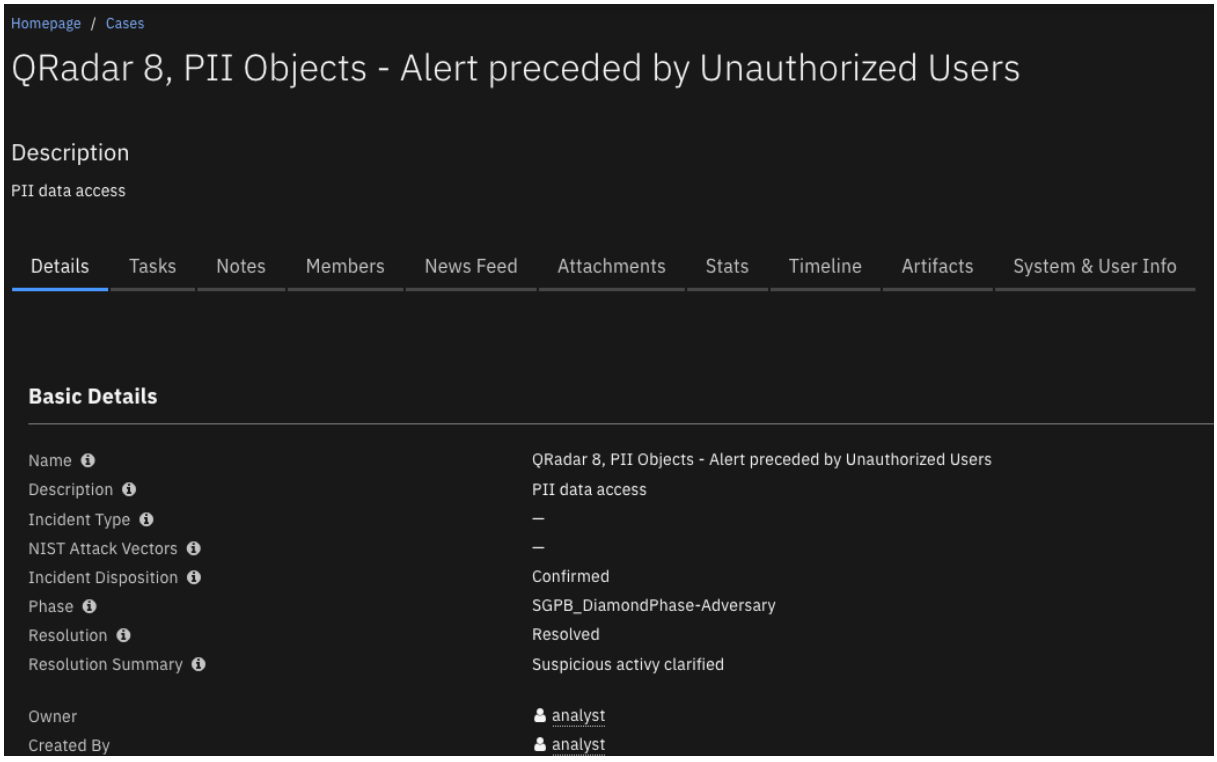
Add data sources with STIXX bundles:

- Guardium
  https://github.com/pbworker/CP4Sdemo/blob/master/Guardium02.json
- QRadar https://github.com/pbworker/CP4Sdemo/blob/master/qradar101.json

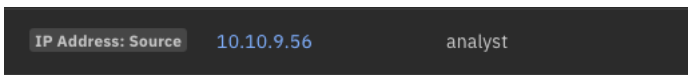
Ingest CAR data:
https://github.com/pbworker/CP4Sdemo/blob/master/CARData-LuisLaptop.json
Using a tool like 'Postman'

Add a new case (manually):

- Select 'Create' in 'Case Management' – 'Cases'
  - Name: QRadar 8, PII Objects - Alert preceded by Unauthorized Users
  - Date occurred:
  - Severity: high
- Create



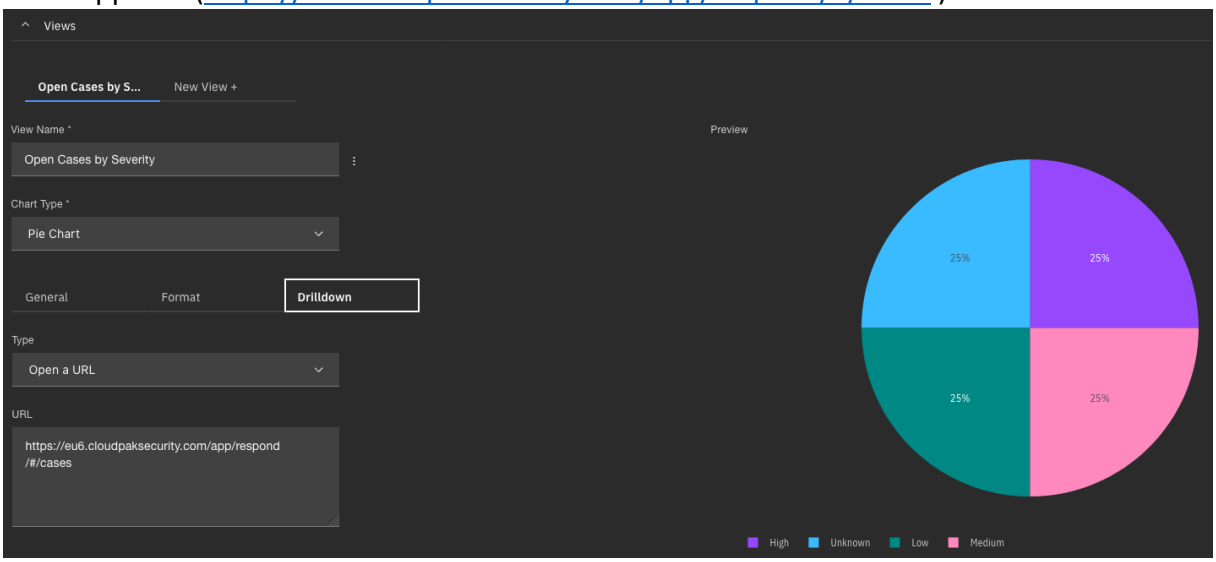
- Add case artifact:
  - Type: IP address
  - Select 'Source'
  - Value: 10.10.9.56



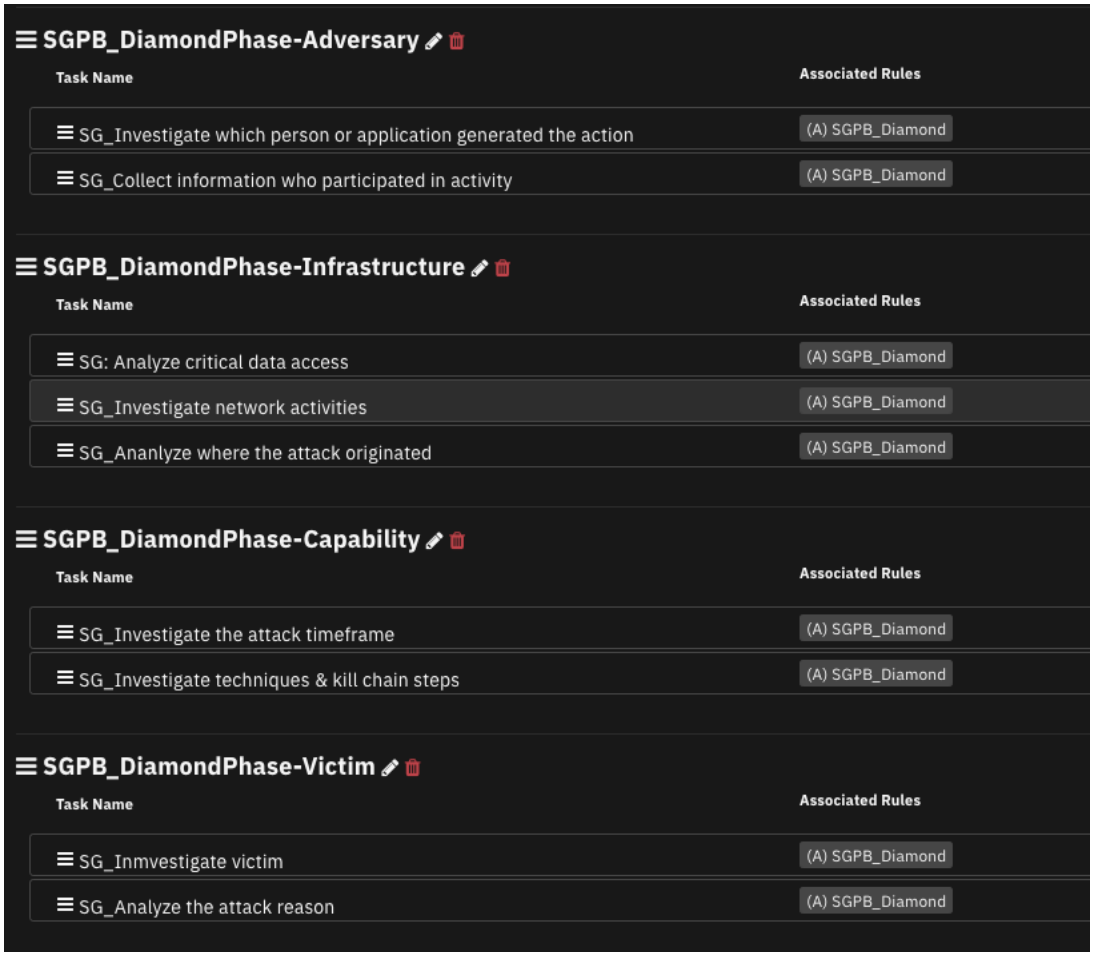
Demo Flow in Mural:
https://app.mural.co/t/cloudsec7477/m/cloudsec7477/1603178738521/97e04e84059d5c2c072f5d80be7732a20b84a341

Optional setup tasks:

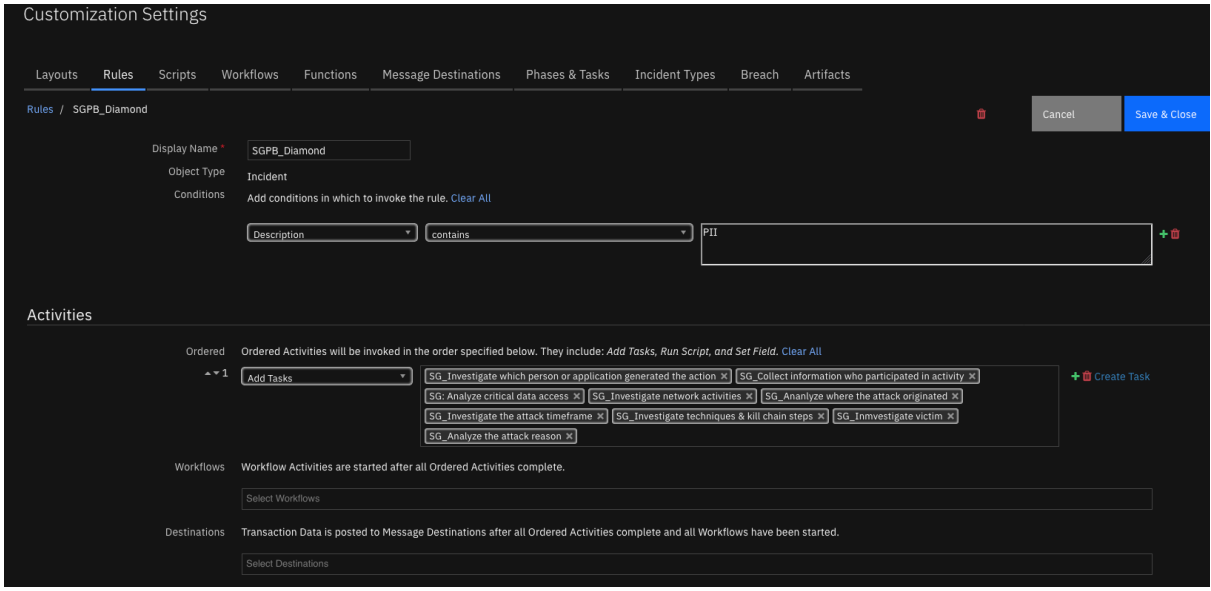
- Create custom dashboard with widget ‘open Cases by Severity’ & set Drilldown to cases app URL (https://xxx.cloudpaksecurity.com/app/respond/#/cases)



- SOAR:
  - Create SOAR phases & tasks to reflect the Diamond Model



- Define rule that fires on change in description in the task -> if description contains “PII”



- Use Skytap (Remote Lab Reservation) to include Guardium & QRadar in the demo

  - Skytap - Hands-on Environment: IBM Security Guardium V11 Data Protection with QRadar - Integrated Demo Environment
    https://ibm.ent.box.com/s/eeiy4gfhxgab3ughpy9jklrz71tukrju

STIXX bundle content

qradar101.json:

Contains 3 entries

1. Alert coming from Guardium (source guardium@g11)
2. User Luis with IP 10.10.9.56 & faked malware
3. User BADGUY using IP 10.10.9.56

Guardium02.json

Contains 2 entries

1. User Luis accessing database “SALESDB”
2. User BADGUY accessing database “SALESDB”

CARData-LuisLaptop.json

1. CAR database entries for user “Luis Mandela”, IP “10.10.9.56” & Luis Laptop with related vulnerabilities.
2. CAR database entries for user “Mike Person”, IP “192.168.0.10” & Mike Laptop with related vulnerabilities.