

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'
 - o Name: QRadar 8, PII Objects - Alert preceded by Unauthorized Users
 - o Date occurred:
 - o Severity: high
- Create

The screenshot shows the 'Cases' page in the QRadar interface. The breadcrumb is 'Homepage / Cases'. The case title is 'QRadar 8, PII Objects - Alert preceded by Unauthorized Users'. Below the title is the 'Description' section with the text 'PII data access'. A horizontal tab bar includes 'Details' (selected), 'Tasks', 'Notes', 'Members', 'News Feed', 'Attachments', 'Stats', 'Timeline', 'Artifacts', and 'System & User Info'. The 'Basic Details' section lists the following information:

Field	Value
Name	QRadar 8, PII Objects - Alert preceded by Unauthorized Users
Description	PII data access
Incident Type	—
NIST Attack Vectors	—
Incident Disposition	Confirmed
Phase	SGPB_DiamondPhase-Adversary
Resolution	Resolved
Resolution Summary	Suspicious activity clarified
Owner	analyst
Created By	analyst

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

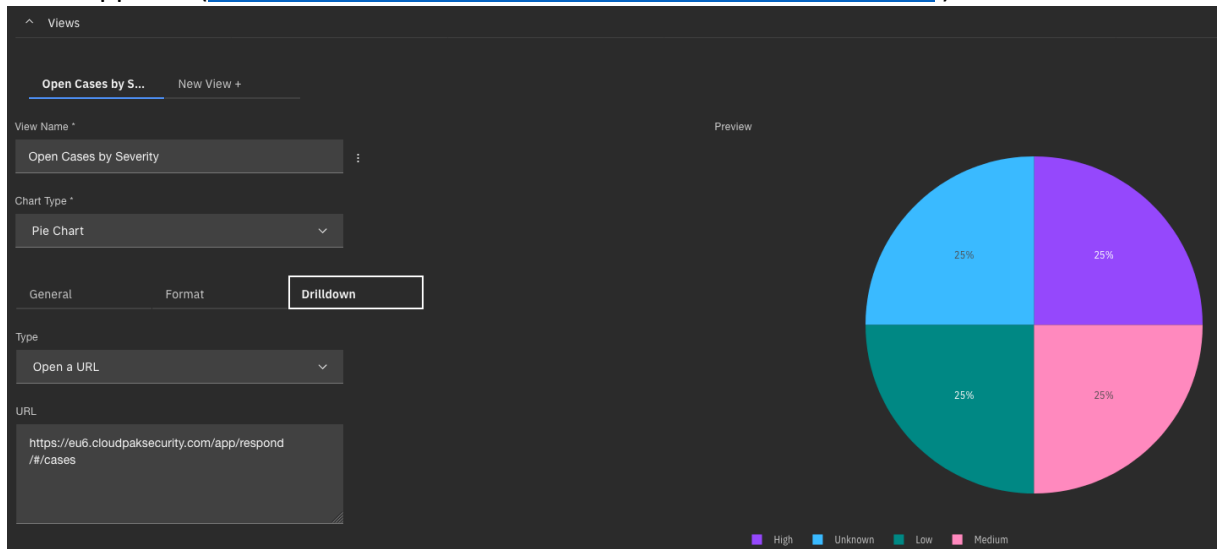
The screenshot shows a form for adding a case artifact. It has a label 'IP Address: Source' followed by the value '10.10.9.56' and the owner 'analyst'.

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

SGPB_DiamondPhase-Adversary	
Task Name	Associated Rules
SG_Investigate which person or application generated the action	(A) SGPB_Diamond
SG_Collect information who participated in activity	(A) SGPB_Diamond
SGPB_DiamondPhase-Infrastructure	
Task Name	Associated Rules
SG: Analyze critical data access	(A) SGPB_Diamond
SG_Investigate network activities	(A) SGPB_Diamond
SG_Analyze where the attack originated	(A) SGPB_Diamond
SGPB_DiamondPhase-Capability	
Task Name	Associated Rules
SG_Investigate the attack timeframe	(A) SGPB_Diamond
SG_Investigate techniques & kill chain steps	(A) SGPB_Diamond
SGPB_DiamondPhase-Victim	
Task Name	Associated Rules
SG_Investigate victim	(A) SGPB_Diamond
SG_Analyze the attack reason	(A) SGPB_Diamond

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

Customization Settings

Layouts Rules Scripts Workflows Functions Message Destinations Phases & Tasks Incident Types Breach Artifacts

Rules / SGPB_Diamond

Display Name * SGPB_Diamond

Object Type Incident

Conditions Add conditions in which to invoke the rule. [Clear All](#)

Description contains PII

Activities

Ordered Ordered Activities will be invoked in the order specified below. They include: Add Tasks, Run Script, and Set Field. Clear All

1 Add Tasks SG_Investigate which person or application generated the action x SG_Collect information who participated in activity x SG_Analyze critical data access x SG_Investigate network activities x SG_Analyze where the attack originated x SG_Investigate the attack timeframe x SG_Investigate techniques & kill chain steps x SG_Investigate victim x SG_Analyze the attack reason x

Workflows Workflow Activities are started after all Ordered Activities complete.

Select Workflows

Destinations Transaction Data is posted to Message Destinations after all Ordered Activities complete and all Workflows have been started.

Select Destinations

- 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”

CARDData-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.