COMPETENCY QUESTIONS SPARQL QUERIES - IR ACTIVITIES DATA SOURCE

#1 - Learning from day to day events & #3 - Automated reporting and analysis of IR process

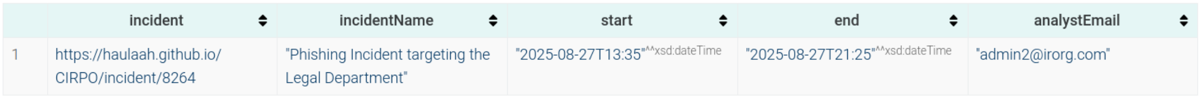
Category	Competency Question	Data Source
IR Metrics	1) What is the start time and end time for a specific/all incident handled by a specific analyst?	The Hive

SPARQL Query:

```
PREFIX ir: <https://haulaah.github.io/CIRPO#>
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX prov: <http://www.w3.org/ns/prov#>
SELECT ?incident ?incidentName ?start ?end ?analystEmail
WHERE {
 ?incident a ir:Incident ;
        ir:hasIncidentName ?incidentName ;
        ir:hasIncidentCreationDateTime ?start ;
        ir:hasEndDateTime ?end ;
        ir:hasConfirmationAnalyst/ir:hasAnalystEmail ?analystEmail .

  FILTER(?analystEmail = "admin2@irorg.com")
}
ORDER BY ?incidentName
```

GraphDB Output:



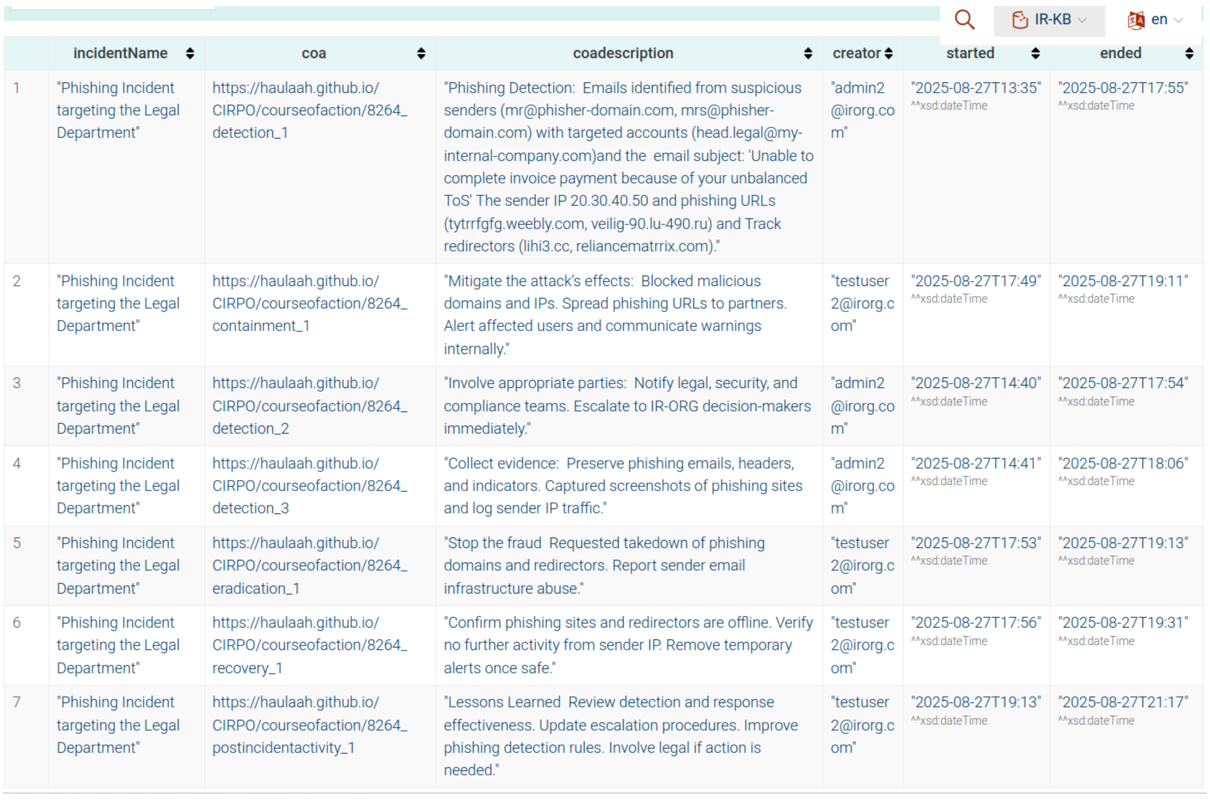
	incident	incidentName	start	end	analystEmail
1	https://haulaah.github.io/CIRPO/incident/8264	"Phishing Incident targeting the Legal Department"	"2025-08-27T13:35"^^xsd:dateTime	"2025-08-27T21:25"^^xsd:dateTime	"admin2@irorg.com"

Category	Competency Question	Data Source
IR Metrics	2) How long did it take from detection to containment, and from containment to recovery for a specific incident?	The Hive

SPARQL Query:

```
PREFIX ir: <https://haulaah.github.io/CIRPO#>
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX prov: <http://www.w3.org/ns/prov#>
SELECT ?incidentName ?coa ?coadescription ?creator ?started ?ended
WHERE {
 ?incident rdf:type ir:Incident ;
        ir:hasIncidentName "Phishing Incident targeting the Legal Department" ;
        ir:hasIncidentName ?incidentName ;
        ir:hasCoa ?coa .
 OPTIONAL { ?coa ir:hasCoaDescription ?coadescription }
 OPTIONAL { ?coa ir:hasCoaStartDateTime ?started }
 OPTIONAL { ?coa ir:hasCoaEndDateTime ?ended }
 OPTIONAL { ?coa ir:hasCoaCreationAnalyst/ir:hasAnalystEmail ?creator }
}
ORDER BY ?created
```

GraphDB Output:



	incidentName	coa	coadescription	creator	started	ended
1	"Phishing Incident targeting the Legal Department"	https://haulaah.github.io/CIRPO/courseofaction/8264_detection_1	"Phishing Detection: Emails identified from suspicious senders (mr@phisher-domain.com, mrs@phisher-domain.com) with targeted accounts (head.legal@my-internal-company.com)and the email subject: 'Unable to complete invoice payment because of your unbalanced ToS' The sender IP 20.30.40.50 and phishing URLs (tytrrfgfg.weebly.com, veilig-90.lu-490.ru) and Track redirectors (lihi3.cc, reliancematrrix.com)."	"admin2@irorg.com"	"2025-08-27T13:35"^^xsd:dateTime	"2025-08-27T17:55"^^xsd:dateTime
2	"Phishing Incident targeting the Legal Department"	https://haulaah.github.io/CIRPO/courseofaction/8264_containment_1	"Mitigate the attack's effects: Blocked malicious domains and IPs. Spread phishing URLs to partners. Alert affected users and communicate warnings internally."	"testuser2@irorg.com"	"2025-08-27T17:49"^^xsd:dateTime	"2025-08-27T19:11"^^xsd:dateTime
3	"Phishing Incident targeting the Legal Department"	https://haulaah.github.io/CIRPO/courseofaction/8264_detection_2	"Involve appropriate parties: Notify legal, security, and compliance teams. Escalate to IR-ORG decision-makers immediately."	"admin2@irorg.com"	"2025-08-27T14:40"^^xsd:dateTime	"2025-08-27T17:54"^^xsd:dateTime
4	"Phishing Incident targeting the Legal Department"	https://haulaah.github.io/CIRPO/courseofaction/8264_detection_3	"Collect evidence: Preserve phishing emails, headers, and indicators. Captured screenshots of phishing sites and log sender IP traffic."	"admin2@irorg.com"	"2025-08-27T14:41"^^xsd:dateTime	"2025-08-27T18:06"^^xsd:dateTime
5	"Phishing Incident targeting the Legal Department"	https://haulaah.github.io/CIRPO/courseofaction/8264_eradication_1	"Stop the fraud Requested takedown of phishing domains and redirectors. Report sender email infrastructure abuse."	"testuser2@irorg.com"	"2025-08-27T17:53"^^xsd:dateTime	"2025-08-27T19:13"^^xsd:dateTime
6	"Phishing Incident targeting the Legal Department"	https://haulaah.github.io/CIRPO/courseofaction/8264_recovery_1	"Confirm phishing sites and redirectors are offline. Verify no further activity from sender IP. Remove temporary alerts once safe."	"testuser2@irorg.com"	"2025-08-27T17:56"^^xsd:dateTime	"2025-08-27T19:31"^^xsd:dateTime
7	"Phishing Incident targeting the Legal Department"	https://haulaah.github.io/CIRPO/courseofaction/8264_postincidentactivity_1	"Lessons Learned Review detection and response effectiveness. Update escalation procedures. Improve phishing detection rules. Involve legal if action is needed."	"testuser2@irorg.com"	"2025-08-27T19:13"^^xsd:dateTime	"2025-08-27T21:17"^^xsd:dateTime

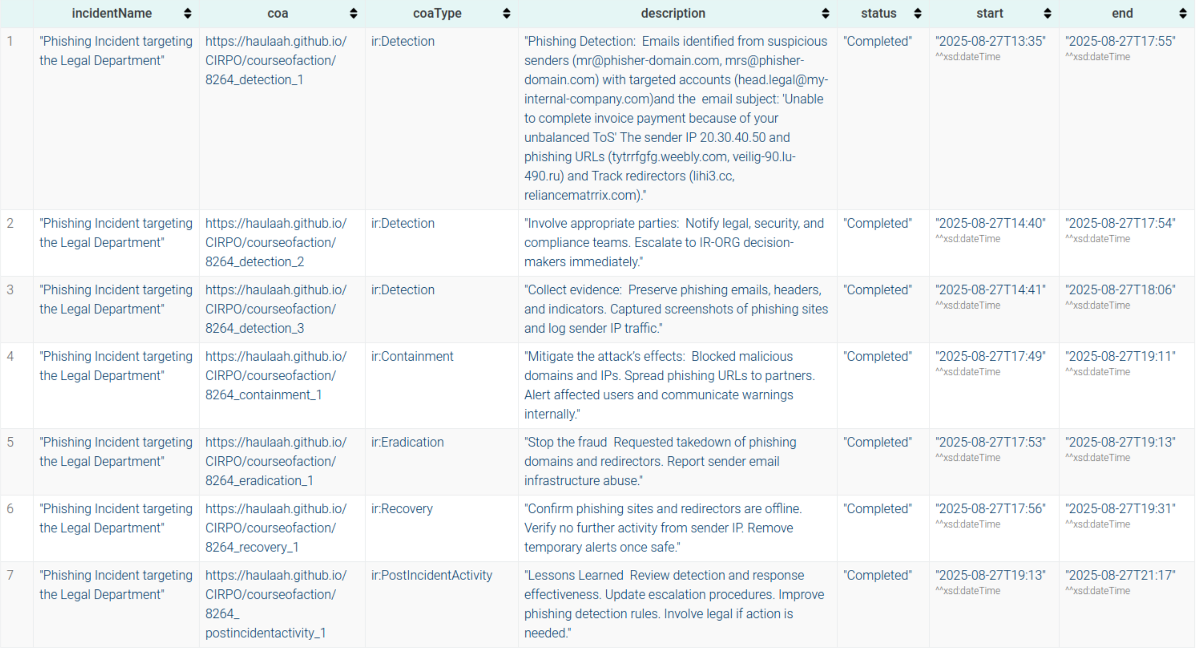
Category	Competency Question	Data Source
IR Metrics	3) What were the response actions taken for a specific incident?	The Hive

SPARQL Query:

```
PREFIX ir: <https://haulaah.github.io/CIRPO#>
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX prov: <http://www.w3.org/ns/prov#>

SELECT ?incidentName ?coa ?coaType ?description ?status ?start ?end
WHERE {
  ?incident a ir:Incident ;
          ir:hasIncidentName "Phishing Incident targeting the Legal Department" ;
          ir:hasIncidentName ?incidentName ;
          ir:hasCoa ?coa .
  ?coa a ?coaType ;
      ir:hasCoaDescription ?description ;
      ir:hasCoaStatus ?status ;
      ir:hasCoaStartDateTime ?start ;
      ir:hasCoaEndDateTime ?end .
  FILTER(?coaType IN (ir:Detection, ir:Containment, ir:Eradication, ir:Recovery, ir:PostIncidentActivity))
}
ORDER BY ?start
```

GraphDB Output:



	incidentName	coa	coaType	description	status	start	end
1	"Phishing Incident targeting the Legal Department"	https://haulaah.github.io/CIRPO/courseofaction/8264_detection_1	ir:Detection	"Phishing Detection: Emails identified from suspicious senders (mr@phisher-domain.com, mrs@phisher-domain.com) with targeted accounts (head.legal@my-internal-company.com)and the email subject: 'Unable to complete invoice payment because of your unbalanced ToS' The sender IP 20.30.40.50 and phishing URLs (tytrrfgfg.weebly.com, veilig-90.lu-490.ru) and Track redirectors (lihi3.cc, reliancematrrix.com)."	"Completed"	"2025-08-27T13:35" ^^xsd:dateTime	"2025-08-27T17:55" ^^xsd:dateTime
2	"Phishing Incident targeting the Legal Department"	https://haulaah.github.io/CIRPO/courseofaction/8264_detection_2	ir:Detection	"Involve appropriate parties: Notify legal, security, and compliance teams. Escalate to IR-ORG decision-makers immediately."	"Completed"	"2025-08-27T14:40" ^^xsd:dateTime	"2025-08-27T17:54" ^^xsd:dateTime
3	"Phishing Incident targeting the Legal Department"	https://haulaah.github.io/CIRPO/courseofaction/8264_detection_3	ir:Detection	"Collect evidence: Preserve phishing emails, headers, and indicators. Captured screenshots of phishing sites and log sender IP traffic."	"Completed"	"2025-08-27T14:41" ^^xsd:dateTime	"2025-08-27T18:06" ^^xsd:dateTime
4	"Phishing Incident targeting the Legal Department"	https://haulaah.github.io/CIRPO/courseofaction/8264_containment_1	ir:Containment	"Mitigate the attack's effects: Blocked malicious domains and IPs. Spread phishing URLs to partners. Alert affected users and communicate warnings internally."	"Completed"	"2025-08-27T17:49" ^^xsd:dateTime	"2025-08-27T19:11" ^^xsd:dateTime
5	"Phishing Incident targeting the Legal Department"	https://haulaah.github.io/CIRPO/courseofaction/8264_eradication_1	ir:Eradication	"Stop the fraud Requested takedown of phishing domains and redirectors. Report sender email infrastructure abuse."	"Completed"	"2025-08-27T17:53" ^^xsd:dateTime	"2025-08-27T19:13" ^^xsd:dateTime
6	"Phishing Incident targeting the Legal Department"	https://haulaah.github.io/CIRPO/courseofaction/8264_recovery_1	ir:Recovery	"Confirm phishing sites and redirectors are offline. Verify no further activity from sender IP. Remove temporary alerts once safe."	"Completed"	"2025-08-27T17:56" ^^xsd:dateTime	"2025-08-27T19:31" ^^xsd:dateTime
7	"Phishing Incident targeting the Legal Department"	https://haulaah.github.io/CIRPO/courseofaction/8264_postincidentactivity_1	ir:PostIncidentActivity	"Lessons Learned Review detection and response effectiveness. Update escalation procedures. Improve phishing detection rules. Involve legal if action is needed."	"Completed"	"2025-08-27T19:13" ^^xsd:dateTime	"2025-08-27T21:17" ^^xsd:dateTime

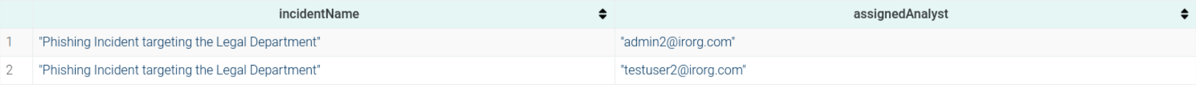
Category	Competency Question	Data Source
Responder Actions	4) Who were the analysts assigned to a specific incident?	The Hive, MISP, Cortex, RT

SPARQL Query:

```
PREFIX ir: <https://haulaah.github.io/CIRPO#>
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX prov: <http://www.w3.org/ns/prov#>

SELECT DISTINCT ?incidentName ?assignedAnalyst
WHERE {
  ?incident a ir:Incident ;
          ir:hasIncidentName "Phishing Incident targeting the Legal Department" ;
          ir:hasIncidentName ?incidentName ;
          ir:hasCoa ?coa .
  ?coa ir:hasCoaAssignedAnalyst/ir:hasAnalystEmail ?assignedAnalyst .
}
ORDER BY ?assignedAnalyst
```

GraphDB Output:



	incidentName	assignedAnalyst
1	"Phishing Incident targeting the Legal Department"	"admin2@irorg.com"
2	"Phishing Incident targeting the Legal Department"	"testuser2@irorg.com"

Category	Competency Question	Data Source
Responder Actions	5) What actions did each analyst perform on a specific incident, and when?	The Hive, MISP, Cortex

SPARQL Query:

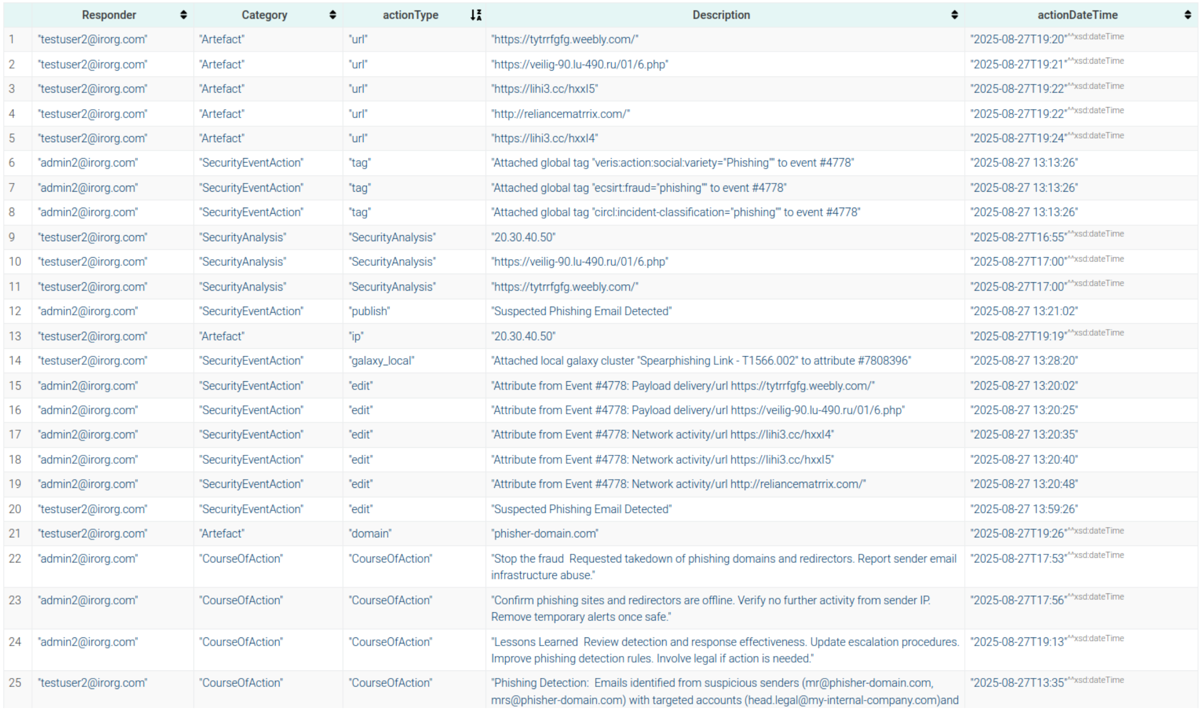
```
PREFIX ir: <https://haulaah.github.io/CIRPO#>
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX prov: <http://www.w3.org/ns/prov#>

SELECT DISTINCT ?Responder ?Category ?actionType ?Description ?actionDateTime
WHERE {
 ?incident a ir:Incident ;
      ir:hasIncidentName "Phishing Incident targeting the Legal Department" ;
      ?relation ?activity .
 {
  ?activity a ir:CourseOfAction ;
       ir:hasCoaDescription ?Description ;
       ir:hasCoaStartDateTime ?actionDateTime ;
       ir:hasCoaAssignedAnalyst ?analystNode .
  ?analystNode ir:hasAnalystEmail ?Responder .
  BIND("CourseOfAction" AS ?Category)
  BIND("CourseOfAction" AS ?actionType)
 }
 UNION
 {
  ?activity a ir:Artefact ;
       ir:hasArtefactType ?actionType ;
       ir:hasArtefactDataValue ?Description ;
       ir:hasArtefactCreationDateTime ?actionDateTime ;
       ir:hasArtefactCreator ?analystNode .
  ?analystNode ir:hasAnalystEmail ?Responder .
  BIND("Artefact" AS ?Category)
 }
 UNION
 {

  ?activity a ir:SecurityEventAction ;
       ir:hasSecurityEventActivity ?actionType ;
       ir:hasSecurityEventDescription ?Description ;
       ir:hasSecurityEventActivityDateTime ?actionDateTime ;
       prov:wasPerformedBy ?analystNode .
  ?analystNode ir:hasAnalystEmail ?Responder .
  BIND("SecurityEventAction" AS ?Category)
 }
 UNION
 {

  ?activity a ir:SecurityAnalysis ;
       ir:hasSecurityAnalysisData ?Description ;
       ir:hasSecurityAnalysisDateTime ?actionDateTime ;
       ir:hasSecurityAnalysisPerformer ?analystNode .
  ?analystNode ir:hasAnalystEmail ?Responder .
  BIND("SecurityAnalysis" AS ?Category)
  BIND("SecurityAnalysis" AS ?actionType)
 }
}
ORDER BY ?Responder ?actionDateTime
```

GraphDB Output:



	Responder	Category	actionType	Description	actionDateTime
1	"testuser2@irorg.com"	"Artefact"	"url"	"https://tytrrfgfg.weebly.com/"	"2025-08-27T19:20"^^xsd:dateTime
2	"testuser2@irorg.com"	"Artefact"	"url"	"https://veilig-90.lu-490.ru/01/6.php"	"2025-08-27T19:21"^^xsd:dateTime
3	"testuser2@irorg.com"	"Artefact"	"url"	"https://lihi3.cc/hxxl5"	"2025-08-27T19:22"^^xsd:dateTime
4	"testuser2@irorg.com"	"Artefact"	"url"	"http://reliancematrrix.com/"	"2025-08-27T19:22"^^xsd:dateTime
5	"testuser2@irorg.com"	"Artefact"	"url"	"https://lihi3.cc/hxxl4"	"2025-08-27T19:24"^^xsd:dateTime
6	"admin2@irorg.com"	"SecurityEventAction"	"tag"	"Attached global tag "veris:action:social:variety="Phishing"" to event #4778"	"2025-08-27 13:13:26"
7	"admin2@irorg.com"	"SecurityEventAction"	"tag"	"Attached global tag "ecsirt:fraud="phishing"" to event #4778"	"2025-08-27 13:13:26"
8	"admin2@irorg.com"	"SecurityEventAction"	"tag"	"Attached global tag "circl:incident-classification="phishing"" to event #4778"	"2025-08-27 13:13:26"
9	"testuser2@irorg.com"	"SecurityAnalysis"	"SecurityAnalysis"	"20.30.40.50"	"2025-08-27T16:55"^^xsd:dateTime
10	"testuser2@irorg.com"	"SecurityAnalysis"	"SecurityAnalysis"	"https://veilig-90.lu-490.ru/01/6.php"	"2025-08-27T17:00"^^xsd:dateTime
11	"testuser2@irorg.com"	"SecurityAnalysis"	"SecurityAnalysis"	"https://tytrrfgfg.weebly.com/"	"2025-08-27T17:00"^^xsd:dateTime
12	"admin2@irorg.com"	"SecurityEventAction"	"publish"	"Suspected Phishing Email Detected"	"2025-08-27 13:21:02"
13	"testuser2@irorg.com"	"Artefact"	"ip"	"20.30.40.50"	"2025-08-27T19:19"^^xsd:dateTime
14	"testuser2@irorg.com"	"SecurityEventAction"	"galaxy_local"	"Attached local galaxy cluster "Spearphishing Link - T1566.002" to attribute #7808396"	"2025-08-27 13:28:20"
15	"admin2@irorg.com"	"SecurityEventAction"	"edit"	"Attribute from Event #4778: Payload delivery/url https://tytrrfgfg.weebly.com/"	"2025-08-27 13:20:02"
16	"admin2@irorg.com"	"SecurityEventAction"	"edit"	"Attribute from Event #4778: Payload delivery/url https://veilig-90.lu-490.ru/01/6.php"	"2025-08-27 13:20:25"
17	"admin2@irorg.com"	"SecurityEventAction"	"edit"	"Attribute from Event #4778: Network activity/url https://lihi3.cc/hxxl4"	"2025-08-27 13:20:35"
18	"admin2@irorg.com"	"SecurityEventAction"	"edit"	"Attribute from Event #4778: Network activity/url https://lihi3.cc/hxxl5"	"2025-08-27 13:20:40"
19	"admin2@irorg.com"	"SecurityEventAction"	"edit"	"Attribute from Event #4778: Network activity/url http://reliancematrrix.com/"	"2025-08-27 13:20:48"
20	"testuser2@irorg.com"	"SecurityEventAction"	"edit"	"Suspected Phishing Email Detected"	"2025-08-27 13:59:26"
21	"testuser2@irorg.com"	"Artefact"	"domain"	"phisher-domain.com"	"2025-08-27T19:26"^^xsd:dateTime
22	"admin2@irorg.com"	"CourseOfAction"	"CourseOfAction"	"Stop the fraud Requested takedown of phishing domains and redirectors. Report sender email infrastructure abuse."	"2025-08-27T17:53"^^xsd:dateTime
23	"admin2@irorg.com"	"CourseOfAction"	"CourseOfAction"	"Confirm phishing sites and redirectors are offline. Verify no further activity from sender IP. Remove temporary alerts once safe."	"2025-08-27T17:56"^^xsd:dateTime
24	"admin2@irorg.com"	"CourseOfAction"	"CourseOfAction"	"Lessons Learned Review detection and response effectiveness. Update escalation procedures. Improve phishing detection rules. Involve legal if action is needed."	"2025-08-27T19:13"^^xsd:dateTime
25	"testuser2@irorg.com"	"CourseOfAction"	"CourseOfAction"	"Phishing Detection: Emails identified from suspicious senders (mr@phisher-domain.com, mrs@phisher-domain.com) with targeted accounts (head.legal@my-internal-company.com)and	"2025-08-27T13:35"^^xsd:dateTime

Category	Competency Question	Data Source
Incident Data	6) What artifacts were collected at each investigation stage for a specific incident and what analyst analysed it using what analyser?	MISP, Cortex, The Hive

SPARQL Query:

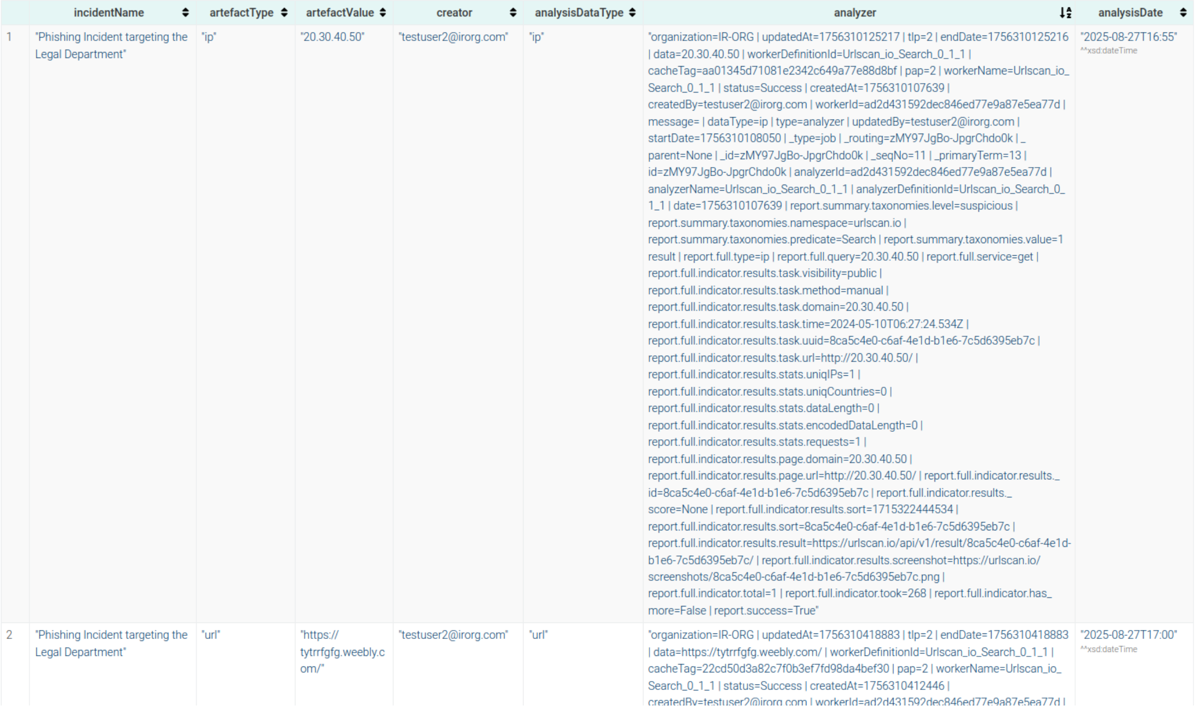
```
PREFIX ir: <https://haulaah.github.io/CIRPO#>
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX prov: <http://www.w3.org/ns/prov#>

SELECT DISTINCT ?incidentName ?artefactType ?artefactValue ?creator ?analysisDataType ?analyzer
?analysisDate
WHERE {
 ?incident a ir:Incident ;
      ir:hasIncidentName "Phishing Incident targeting the Legal Department" ;
      ir:hasIncidentName ?incidentName ;
      ir:hasArtefact ?artefact ;
      ir:hasSecurityAnalysis ?analysis .

 ?artefact ir:hasArtefactType ?artefactType ;
      ir:hasArtefactDataValue ?artefactValue ;
      ir:hasArtefactCreator/ir:hasAnalystEmail ?creator .

 ?analysis ir:hasSecurityAnalysisData ?artefactValue ;
      ir:hasSecurityAnalysisDataType ?analysisDataType ;
      ir:hasSecurityAnalysisReport ?analyzer ;
      ir:hasSecurityAnalysisDateTime ?analysisDate .
}
ORDER BY ?artefactType ?analysisDate
```

GraphDB Output:



	incidentName	artefactType	artefactValue	creator	analysisDataType	analyzer	analysisDate
1	"Phishing Incident targeting the Legal Department"	"ip"	"20.30.40.50"	"testuser2@irorg.com"	"ip"	"organization=IR-ORG | updatedAt=1756310125217 | tlp=2 | endDate=1756310125216 | data=20.30.40.50 | workerDefinitionId=Urlscan_io_Search_0_1_1 | cacheTag=aa01345d71081e2342c649a77e88d8bf | pap=2 | workerName=Urlscan_io_Search_0_1_1 | status=Success | createdAt=1756310107639 | createdBy=testuser2@irorg.com | workerId=ad2d431592dec846ed77e9a87e5ea77d | message= | dataType=ip | type=analyzer | updatedBy=testuser2@irorg.com | startDate=1756310108050 | _type=job | _routing=zMY97JgBo-JpgrChdo0k | _parent=None | _id=zMY97JgBo-JpgrChdo0k | _seqNo=11 | _primaryTerm=13 | id=zMY97JgBo-JpgrChdo0k | analyzerId=ad2d431592dec846ed77e9a87e5ea77d | analyzerName=Urlscan_io_Search_0_1_1 | analyzerDefinitionId=Urlscan_io_Search_0_1_1 | date=1756310107639 | report.summary.taxonomies.level=suspicious | report.summary.taxonomies.namespace=urlscan.io | report.summary.taxonomies.predicate=Search | report.summary.taxonomies.value=1 result | report.full.type=ip | report.full.query=20.30.40.50 | report.full.service=get | report.full.indicator.results.task.visibility=public | report.full.indicator.results.task.method=manual | report.full.indicator.results.task.domain=20.30.40.50 | report.full.indicator.results.task.time=2024-05-10T06:27:24.534Z | report.full.indicator.results.task.uuid=8ca5c4e0-c6af-4e1d-b1e6-7c5d6395eb7c | report.full.indicator.results.task.url=http://20.30.40.50/ | report.full.indicator.results.stats.uniqIPs=1 | report.full.indicator.results.stats.uniqCountries=0 | report.full.indicator.results.stats.dataLength=0 | report.full.indicator.results.stats.encodedDataLength=0 | report.full.indicator.results.stats.requests=1 | report.full.indicator.results.page.domain=20.30.40.50 | report.full.indicator.results.page.url=http://20.30.40.50/ | report.full.indicator.results._id=8ca5c4e0-c6af-4e1d-b1e6-7c5d6395eb7c | report.full.indicator.results._score=None | report.full.indicator.results.sort=1715322444534 | report.full.indicator.results.sort=8ca5c4e0-c6af-4e1d-b1e6-7c5d6395eb7c | report.full.indicator.results.result=https://urlscan.io/api/v1/result/8ca5c4e0-c6af-4e1d-b1e6-7c5d6395eb7c/ | report.full.indicator.results.screenshot=https://urlscan.io/screenshots/8ca5c4e0-c6af-4e1d-b1e6-7c5d6395eb7c.png | report.full.indicator.total=1 | report.full.indicator.took=268 | report.full.indicator.has_more=False | report.success=True"	"2025-08-27T16:55" ^^xsd:dateTime
2	"Phishing Incident targeting the Legal Department"	"url"	"https://tytrrfgfg.weebly.com/"	"testuser2@irorg.com"	"url"	"organization=IR-ORG | updatedAt=1756310418883 | tlp=2 | endDate=1756310418883 | data=https://tytrrfgfg.weebly.com/ | workerDefinitionId=Urlscan_io_Search_0_1_1 | cacheTag=22cd50d3a82c7f0b3ef7fd98da4bef30 | pap=2 | workerName=Urlscan_io_Search_0_1_1 | status=Success | createdAt=1756310412446 | createdBy=testuser2@irorg.com | workerId=ad2d431592dec846ed77e9a87e5ea77d |	"2025-08-27T17:00" ^^xsd:dateTime

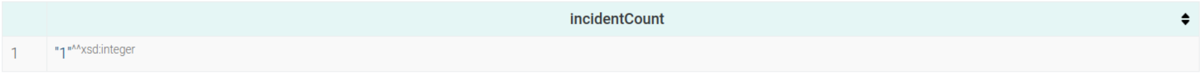
Category	Competency Question	Data Source
Incident Data	7) How many incidents were handled during a specific period?	The Hive

SPARQL Query:

```
PREFIX : <https://haulaah.github.io/CIRPO#>
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX prov: <http://www.w3.org/ns/prov#>
SELECT (COUNT(?incident) AS ?incidentCount)
WHERE {
 ?incident a :Incident ;
      :hasIncidentCreationDateTime ?creationTime .

 FILTER(
  STR(?creationTime) >= "2025-08-01T00:00" &&
  STR(?creationTime) <= "2025-08-31T23:59"
 )
}
```

GraphDB Output:



	incidentCount
1	"1"^^xsd:integer

Category	Competency Question	Data Source
Incident Data	8) What related past incidents share IOCs with a current open incident?	MISP, Cortex, The Hive

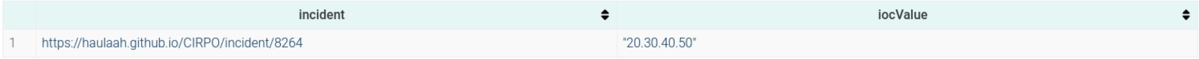
SPARQL Query:

```
PREFIX ir: <https://haulaah.github.io/CIRPO#>
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>

SELECT DISTINCT ?incident ?iocValue
WHERE {
 ?incident a ir:Incident ;
          ir:hasArtefact ?artefact .
 ?artefact ir:hasArtefactDataValue ?iocValue .

 FILTER(?iocValue = "20.30.40.50")
}
ORDER BY ?incident
```

GraphDB Output:



	incident	iocValue
1	https://haulaah.github.io/CIRPO/incident/8264	"20.30.40.50"

#4 - Playbook generation

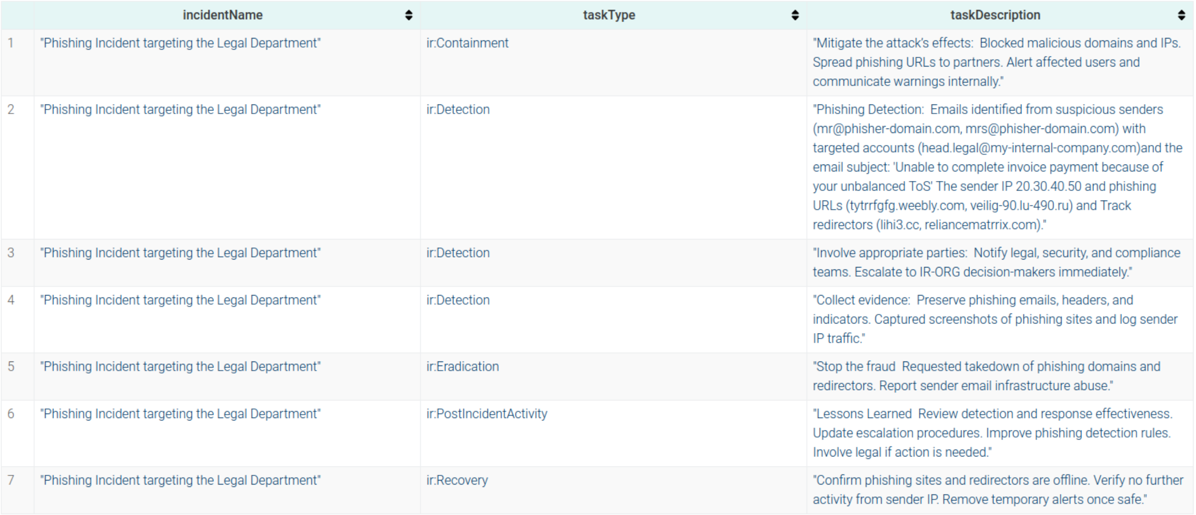
Playbooks Generation	9) What are the different case tasks related to a specific incident type?	The Hive

SPARQL Query:

```
PREFIX ir: <https://haulaah.github.io/CIRPO#>
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX prov: <http://www.w3.org/ns/prov#>

SELECT DISTINCT ?incidentName ?taskType ?taskDescription
WHERE {
 ?incident a ir:Incident ;
          ir:hasIncidentName "Phishing Incident targeting the Legal Department" ;
          ir:hasIncidentName ?incidentName ;
          ir:hasCoa ?coa .
 ?coa a ?taskType ;
      ir:hasCoaDescription ?taskDescription .
 FILTER(?taskType IN (ir:Detection, ir:Containment, ir:Eradication, ir:Recovery, ir:PostIncidentActivity))
}
ORDER BY ?taskType
```

GraphDB Output:



	incidentName	taskType	taskDescription
1	"Phishing Incident targeting the Legal Department"	ir:Containment	"Mitigate the attack's effects: Blocked malicious domains and IPs. Spread phishing URLs to partners. Alert affected users and communicate warnings internally."
2	"Phishing Incident targeting the Legal Department"	ir:Detection	"Phishing Detection: Emails identified from suspicious senders (mr@phisher-domain.com, mrs@phisher-domain.com) with targeted accounts (head.legal@my-internal-company.com)and the email subject: 'Unable to complete invoice payment because of your unbalanced ToS' The sender IP 20.30.40.50 and phishing URLs (tytrrfgfg.weebly.com, veilig-90.lu-490.ru) and Track redirectors (lihi3.cc, reliancematrrix.com)."
3	"Phishing Incident targeting the Legal Department"	ir:Detection	"Involve appropriate parties: Notify legal, security, and compliance teams. Escalate to IR-ORG decision-makers immediately."
4	"Phishing Incident targeting the Legal Department"	ir:Detection	"Collect evidence: Preserve phishing emails, headers, and indicators. Captured screenshots of phishing sites and log sender IP traffic."
5	"Phishing Incident targeting the Legal Department"	ir:Eradication	"Stop the fraud Requested takedown of phishing domains and redirectors. Report sender email infrastructure abuse."
6	"Phishing Incident targeting the Legal Department"	ir:PostIncidentActivity	"Lessons Learned Review detection and response effectiveness. Update escalation procedures. Improve phishing detection rules. Involve legal if action is needed."
7	"Phishing Incident targeting the Legal Department"	ir:Recovery	"Confirm phishing sites and redirectors are offline. Verify no further activity from sender IP. Remove temporary alerts once safe."