Demonstration Lab Guide

CP4S 300 Use Case Demonstration Data Exfiltration

Author – Sonja Gresser
Demo Platform Version – 1.6
Contact Sonja.Gresser@de.ibm.com with feedback

Table of Contents

Table of Contents

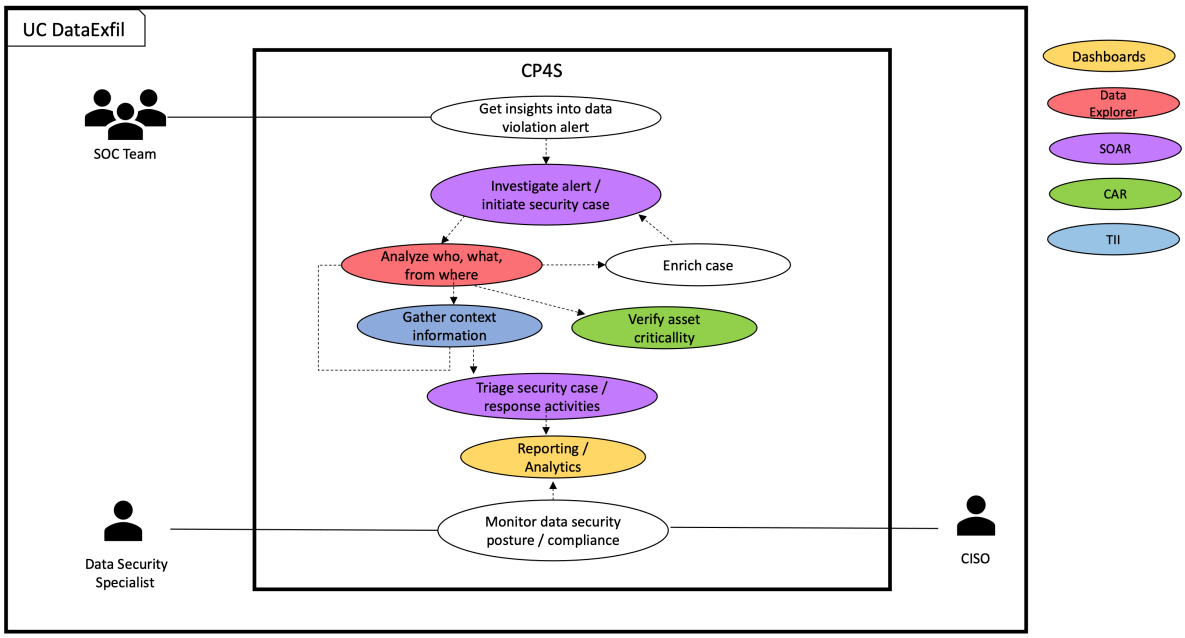
1 Demo Use Case overview

Objective: Detect and contain data leakage quickly

Challenge: Find out the real cause and, if appropriate, trace it back to internal misuse

Stakeholder: SOC analysts, CISO, Data Security Specialist

Logic:



Outcome: Incident of data misuse clarified in detail. Actual cause uncovered, attackers involved identified, required response actions initiated to contain incident and protect data from further leakage.

2 Assumptions, Requirements & Setup

2.1 Assumptions

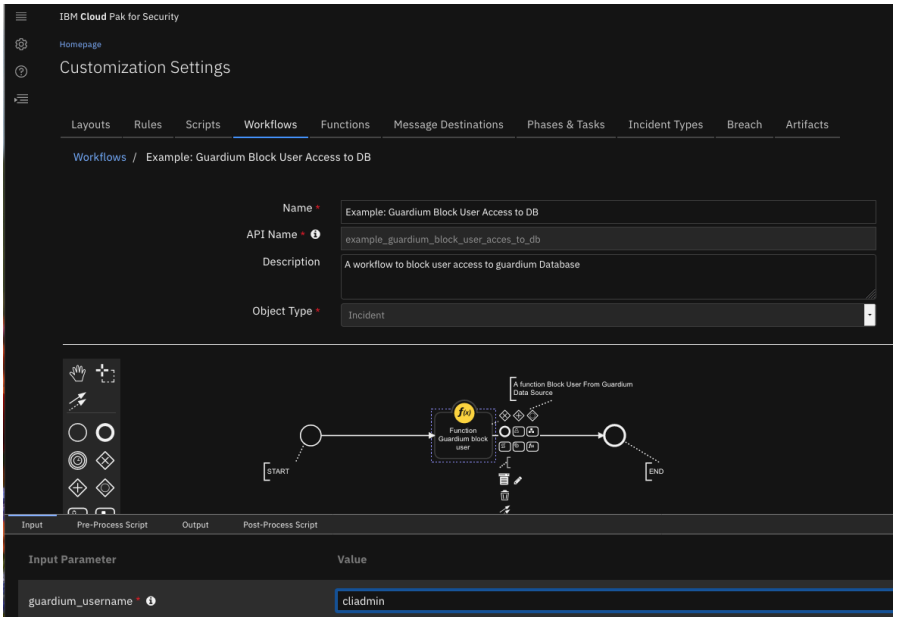
- Cloud Pak for Security (CP4S) version 1.6x on IBM ROKS instance is up and running
- QRadar Dashboard Populator System Connected in proxy mode, along with AppHost with Ansible app installed (Contact your Geo Leader or Sterling Jones if your ROKS cluster does not meet these requirements)
- The following threat intelligence sources are enabled
    - X-Force Advanced
    - CISCO Threat Grid enabled as 3rd party threat feed (if not skip some explanation in *Gather context information* section of demo flow).

2.2 Use case requirements

- Setup the required data sources with names of your choice using the STIX bundles below. Copy the links directly to Data Source Configuration.
    - qradar102.json
      https://cloud-pak-demo-files.mybluemix.net/21_demos/CP4S_300_Demo_DataExfil/qradar102.json
    - guardium102.json
      https://cloud-pak-demo-files.mybluemix.net/21_demos/CP4S_300_Demo_DataExfil/guardium102.json
    - carbonblack102.json
      https://cloud-pak-demo-files.mybluemix.net/21_demos/CP4S_300_Demo_DataExfil/carbonblack102.json
- Upload the following SOAR Apps (configuration is not really required for demo; tasks can be triggered without real integration behind it):
    - Ansible for Resilient (fn_ansible)
    - Guardium Integration Application for IBM Resilient (fn_guardium_integration)
    - Microsoft Exchange Online Integration for Resilient (fn_exchange_online)
    - ServiceNow Functions for IBM Resilient
- Add CAR (Connect Asset and Risk) data. CAR data is added through API using the provided json file below:
    - Create API key in CP4S
    - Download Postman (Postman link)
    - In Postman, navigate to the Authorization Tab. Select Basic Auth from Type dropdown then add in your API Key in username and your secret API key into password
    - Go to POST - https://yourCP4Sinstancename/api/car/v2/databases
    - Note it may take a bit to generate the CAR database, you can check this status by performing GET - https://yourCP4Sinstancename/api/car/v2/databases
    - Next, navigate to the Body tab.
    - Select raw and JSON
    - Copy/paste the sample CAR data into the body from the link below
      https://cloud-pak-demo-files.mybluemix.net/21_demos/CP4S_300_Demo_DataExfil/CARData_UC_DataExFil.json
    - Go to POST - https://yourCP4Sinstancename/api/car/v2/imports

2.3 Setup Tasks

1. Manually create an incident. Only the following settings are required:
   - Name: “QRadar 354, Outbound Transfer of Sensitive Data (PII) containing Web.HTTPWeb“
   - Severity: High
   - Was personal information or personal data involved? Yes
   - Is harm/risk/misuse foreseeable? Yes
   - Was the data encrypted? No
   - Regulators page: choose settings of your country or any choice
   - Artifacts (added after incident was created):
     - IP Address: Source – 192.168.1.114
     - IP Address: Destination – 124.240.198.66
2. In the SOAR workflow “Example: Guardium Block User Access to DB” set the guardium_username to e.g. “cliadmin” (if left blank, an error occurs when starting the workflow)
   This is done in CP4S under “Application settings” -> Orchestration & Automations” -> “SOAR playbooks” -> Workflows tab -> search for Guardium -> select “Example: Guardium Block User Access to DB” workflow -> (DO NOT change Display Name) click on the function displayed in the lower canvas -> select the little pencil (this opens up the Input Parameter section below) -> enter “cliadmin” in the value fields -> Save & Close



Optional steps:

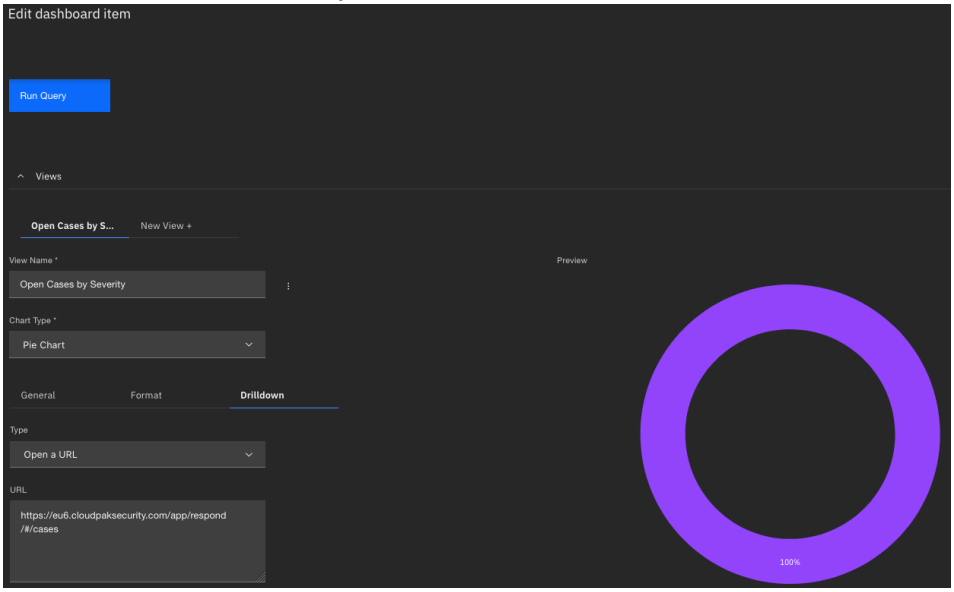
3. Change the default SOAR rule names so that they do not start with "example": “
   - „Example: Exchange Online Send Message“ -> “Exchange Online Send Message”
   - “Example: Ansible - Run a Playbook from an Artifact” -> ” Ansible - Run a Playbook from an Artifact”

   This is done in CP4S under “Application settings” -> Orchestration & Automations” -> “SOAR playbooks” -> Rules tab -> search for Exchange -> select “Example: Exchange Online Send Message” rule -> only change Display Name -> Save & Close
4. Setup a custom dashboard on the homepage (e.g. named “SOC analyst custom dashboard”) and select various widgets of interests for a SOC analyst.

Create a new as copy from existing widget “Open Cases by Severity” -> leave all settings as they are -> under “Views” change the settings in the “Drilldown” tab to:

- Type: Open a url
- URL: https://yourCP4Sinstancename/app/respond/#/cases

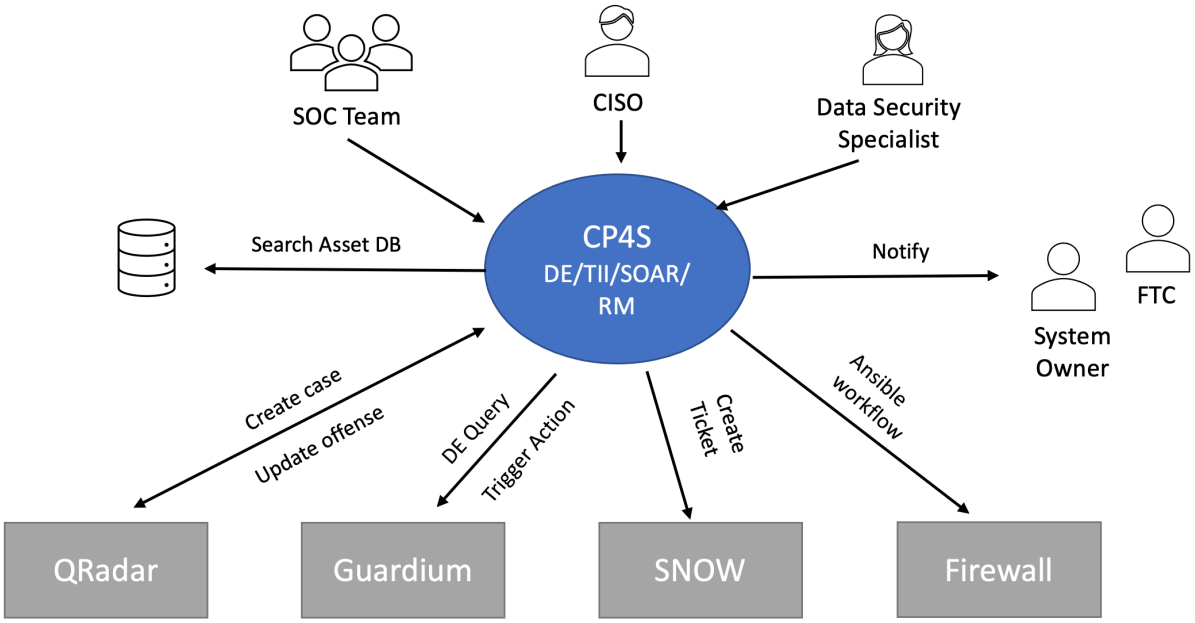
This allows to launch directly to the cases overview list from the dashboard.



3 Demo Use Case detailed Outline

UC Context:

- Data breach is detected by data security solution e.g. Guardium Data Protection
- Policy alert is triggered (in Guardium) and automatically forwarded to QRadar
- QRadar offense is automatically created based on the forwarded alert
- In parallel, a QRadar event is triggered based on an outbound data flow containing a suspicious content alert / SuspectContent_SensitiveData_Detected
- QRadar offense is enriched with event & flow data "Outbound transfer of sensitive data (PII)"
- Case is automatically created in CP4S SOAR from QRadar offense
- Dynamic SOAR playbook is triggered and appropriate data breach tasks are automatically added as PII data is affected
- *Get insights into data violation alert:*
    - SOC analyst checks newly created cases with high severity from CP4S dashboard
- *Investigate alert / initiate security case:*
    - Analyst verifies the case in CP4S SOAR and makes changes as appropriate
    - SOAR playbook tasks are dynamically updated after the incident type in case is changed to phishing
- *Analyze who, what, from where; Enrich case:*
    - Data investigation is performed by analysts using CP4S Data Explorer to identify actual root cause, user and attackers involved
    - The analyst enriches the case with the insights/artifacts gained from the analyses with CP4S Data Explorer
- *Gather context information:*
    - Threat data can be additionally collected to enrich the case using the X-Force threat data in CP4S TII or data from third-party feeds
- *Verify asset criticality:*
    - Using the information in the CP4S CAR database, the analyst verifies the asset context and criticality
- *Triage security case / response activities:*
    - Automatic or manual task are triggered through SOAR to:
        - notify owners of systems used for phishing attack
        - report suspicious activity to the FTC
        - create a ticket in Service Now (SNOW)
        - block access to database for suspicious internal user
        - update the firewall to block IP – using an Ansible workflow



UC Personas:

Jeff
SOC Security Analyst

Handles incoming security incidents in the Security Operations Center.

Incidents are worked on according to defined guidelines.

He has to deal with a large number of incidents and make decisions on a daily basis

Peter
CISO

Defines security strategy, policies and measures

Is responsible for maintaining compliance

Must report risks, security status and findings to management

Jean
Data Security Specialist

Requires insight into the data security posture

Ensures risks to sensitive data and anomalies are quickly identified and acted upon

Must implement and review compliance measures

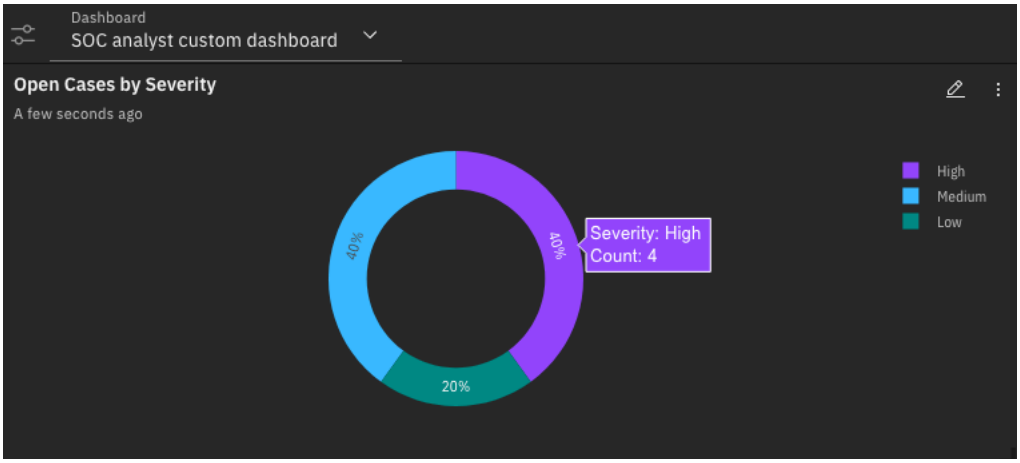
4 Demo Flow

Get insights into data violation alert

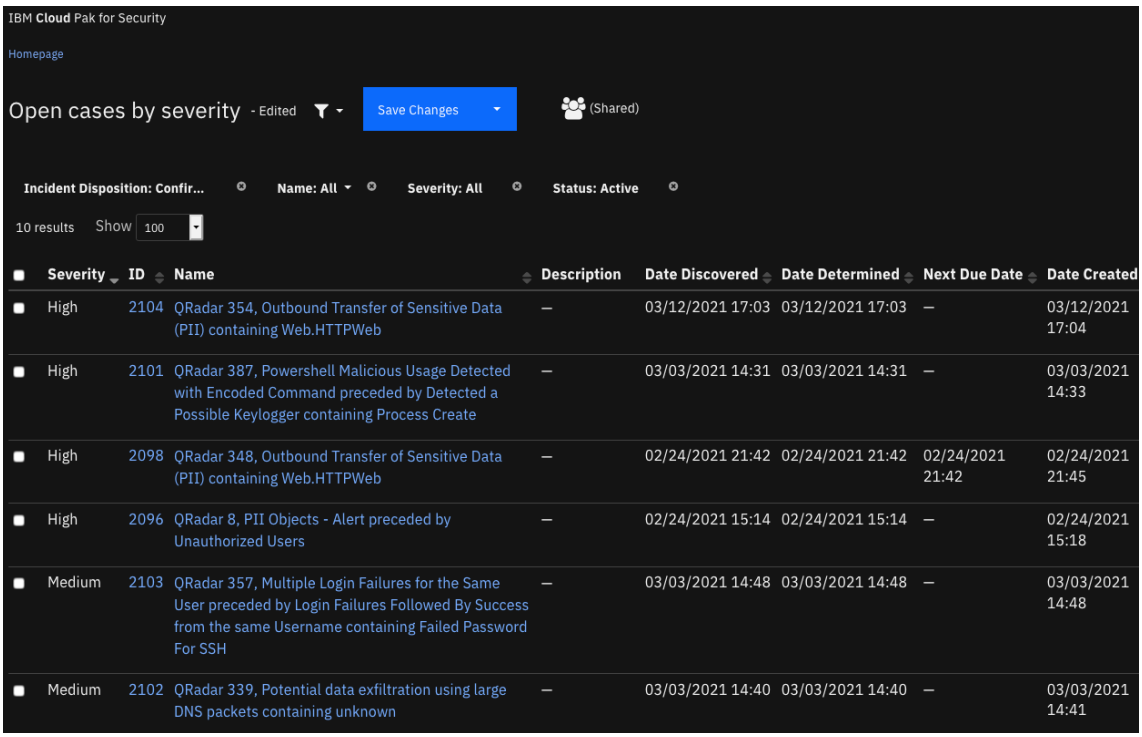
A Security Operations Center (SOC) centrally monitors the entire IT environment of an organization. Accordingly, a SOC should have an overall view of security status and incidents and be able to respond quickly and efficiently when an incident occurs, as well as act proactively and take appropriate action.

Security analysts in a SOC continuously evaluate data, processes and alerts from many different security solutions to detect attacks or threats in a timely manner. Decisions on the necessary countermeasures must be reviewed and initiated.
In order to provide a high level of security in the company (ideally in a 24/7 operation), a large number of highly qualified employees is required or a high level of automation.

Jeff is a Security Analyst on the SOC team whose daily tasks include checking to see if there are any new open events and, in particular, investigating the high severity cases.
To fulfill this task, he uses the analyst dashboard in the central security platform IBM Cloud Pak for Security, which has been adapted to his focus topics.
Using the "Open cases by severity" tile, he can see at a glance which unprocessed events with a high severity are pending, for example.



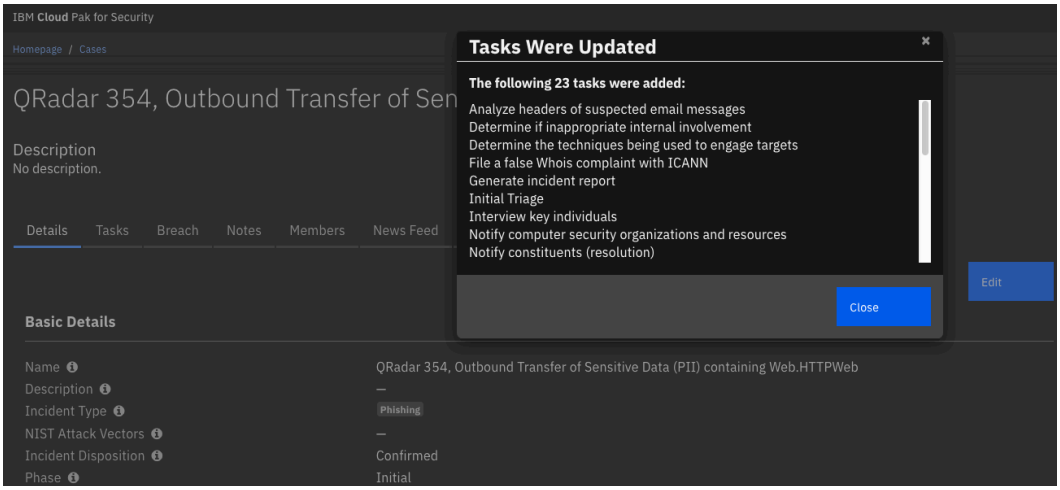
From his dashboard, the analyst Jeff can launch directly into the case summary overview by clicking on the "open cases by severity".



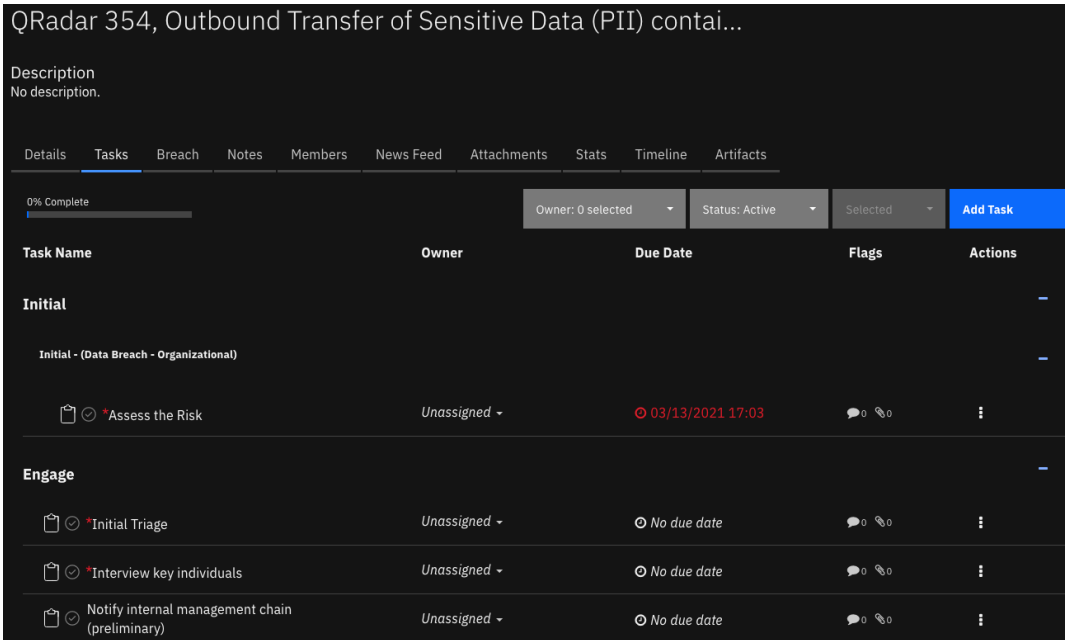
Here he can see at a glance the high severity cases and drill down into the case details.
One of the last high severity cases was opened due to an outbound transfer of sensitive data (PII) detected by QRadar, as indicated in the case name (case name: QRadar 354, Outbound Transfer of Sensitive Data (PII) containing Web.HTTPWeb) .

4.1 Investigate alert / initiate security case

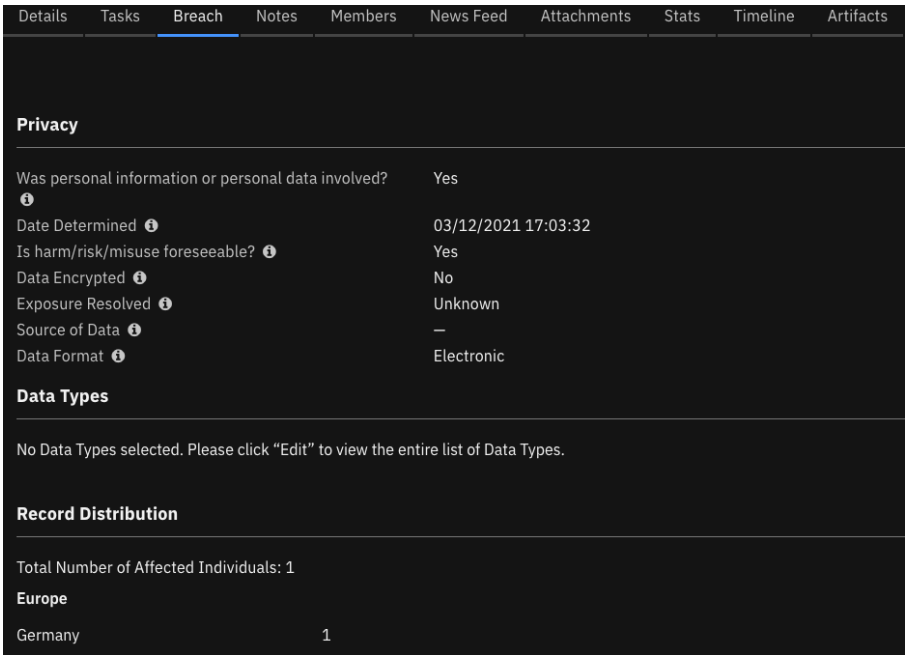
When opening this case, Jeff reviews the details provided, which show the possible incident type, creation date, and other information. Jeff changes the Incident Type to “Phishing” as his initial findings indicate that this may be this type of attack.
Depending on the type of incident, an appropriate playbook is automatically assigned that contains clearly defined tasks to guide the analyst in working through the case.



The playbook's steps, seen under the “Task” tab, function like a checklist along the lines of, "If this incident occurs, check the following."

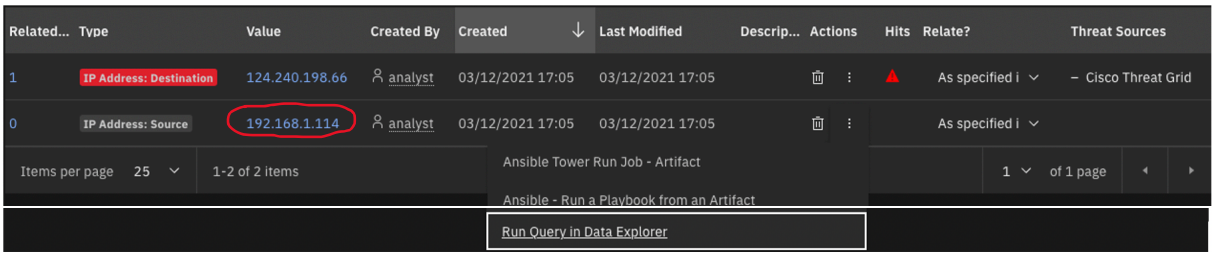


If regulatory requirements need to be considered, as in this case of the potential loss of sensitive data, they are summarized in the Breach tab and are also reflected in the Playbook tasks. This can be assigned automatically based on the attack information sent by QRadar, or manually by the analyst who knows that personal data was involved in the attack and sets the privacy information accordingly.
Additional tasks are dynamically added to the playbook to ensure that relevant steps are taken to meet regulatory requirements.

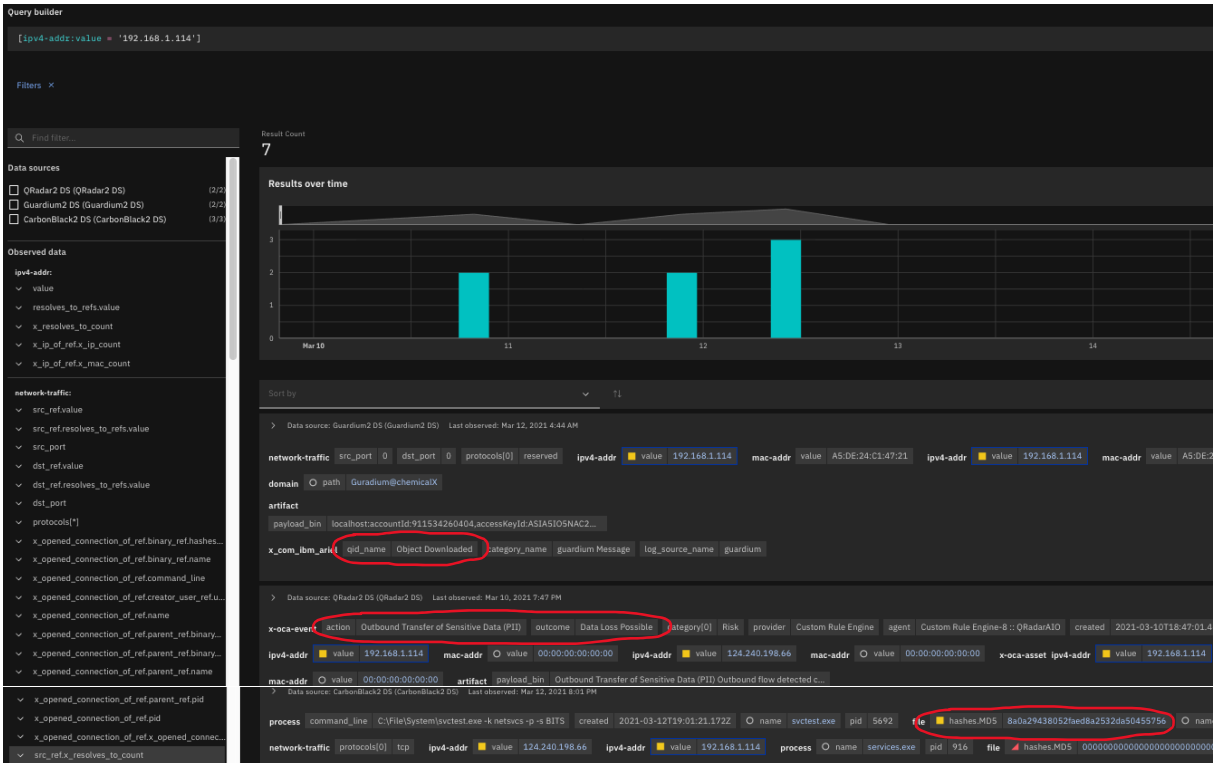


4.2 Analyze who, what, from where

The initial triage requires Analyst Jeff to determine if the incident is an actual event or a false alarm. To analyze the incident in more detail, Jeff reviews the artifacts provided with the case. The Artifacts tab contains the source and destination IP information.
From here, the analyst can directly perform a deeper analysis by invoking a data query with Data Explorer (DE).



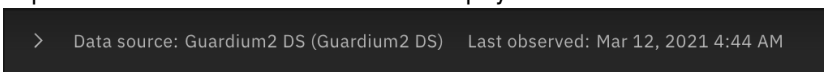
Using the data query, Jeff can gain immediate visibility into all connected security tools and possible further insights without having to collect and store the data first.
The query for the source IP address from the case is based on a search in the open standard STIX and returns results from QRadar, Guardium and Carbon Black.



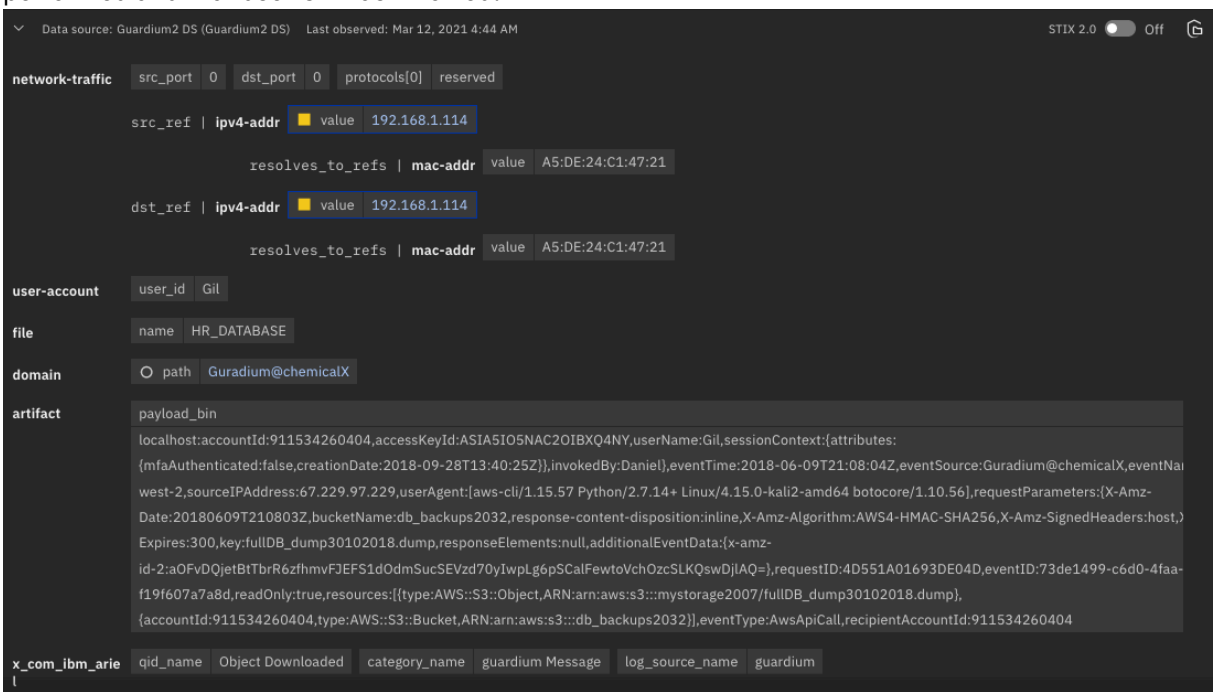
Based on the returned results of the query, the analyst Jeff can use filters to analyze when the events occurred, which processes were executed, which users are involved, and which data was accessed (file name).
It might makes sense to define a specific time to limit the search, e.g. search between March 9th – 14th :
[ipv4-addr:value = '192.168.1.114'] START t'2021-03-09T00:00:00.000Z' STOP t'2021-03-14T00:00:00.000Z'

Using the analytics capabilities, Jeff can find out details, for example which file have been involved (property file:name).

Filtering by the file name found reduces the results list to entries with the file name. Here Jeff sees that data has been found for example in Guardium and that payload data was included in the search results. Jeff expands the Stix results to see the full payload information.

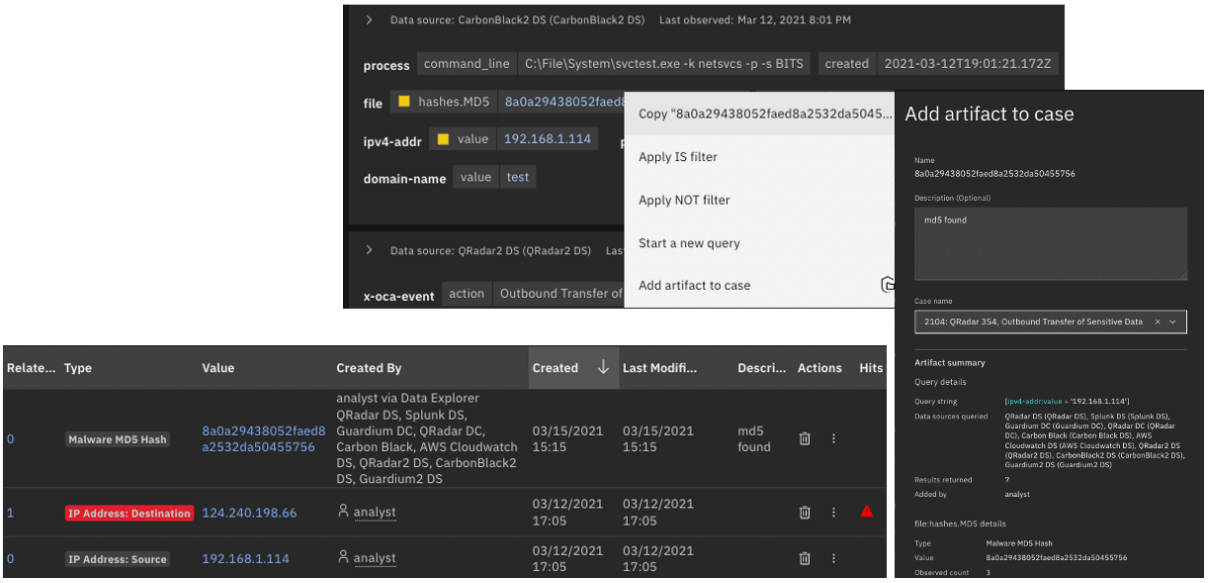


Based on the included payload he quickly recognizes that a full data dump of the HR_DATABASE file was performed and that user Gil was involved.



4.3 Enrich case

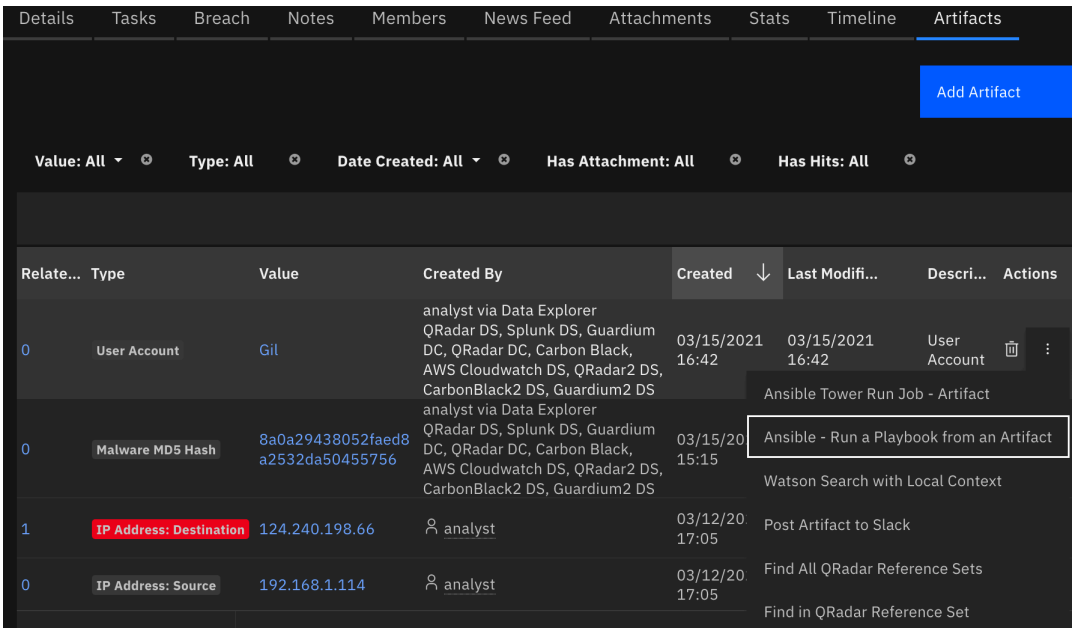
Jeff can easily add new information to the incident directly from the query, sharing the findings with other SOC members involved in the incident. For example, he right-clicks next to the MD5 hash from the Carbon Black results and selects “Add Artifact to Case”.
After selecting the existing case created based on the QRadar attack, the md5 is added to the list of artifacts.



Jeff also adds the user account information to the case.

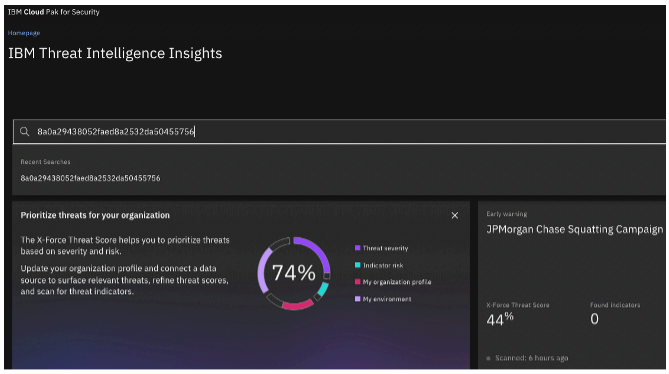
4.4 Gather context information

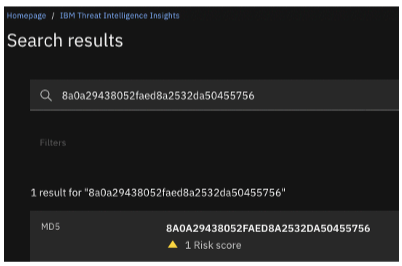
The analyst has the ability to perform additional in-depth analysis as well as enrich the incident with further contextual information.
In addition to the analyses in the Data Explorer, the analyst has access to a variety of integrated workflows and tasks in Case Management. For example, through the integration of Ansible workflows and many other applications.

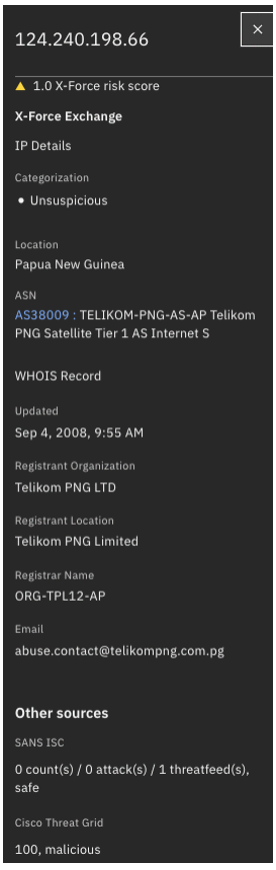


Using the built-in threat capabilities in CP4S, Analyst Jeff can also gain additional context from the threat data provided by X-Force and third-party threat feeds.

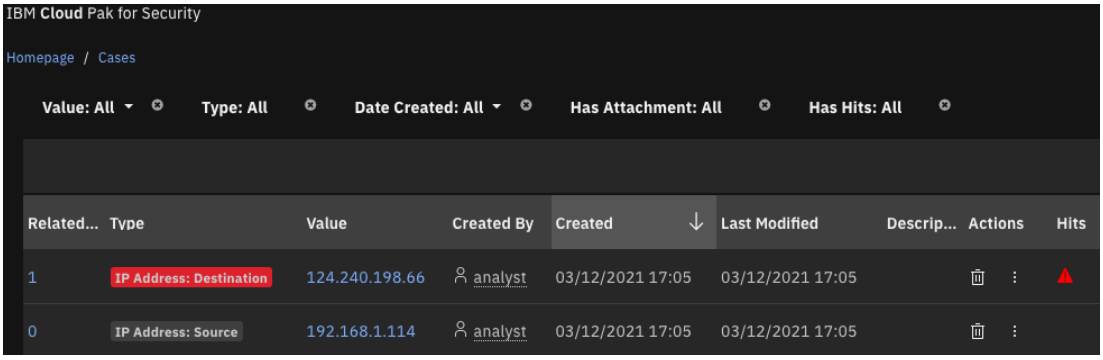
To do so he can either leverage the TII application from the homepage and search for the destination IP address, md5 value or url found in the query entries. Or directly select entries from the query result list and verify what data is available for example for an IP address from threat feeds.



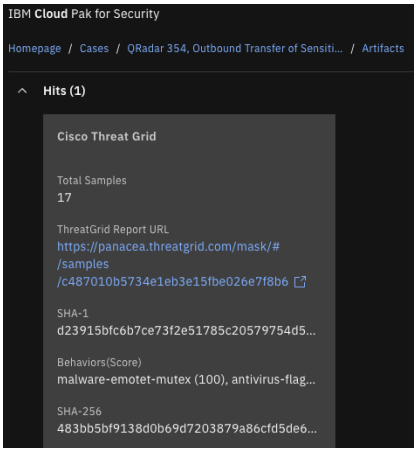




The artifacts in the case are also automatically matched against the threat feeds and classified as hits if information in the threat feeds can be matched.



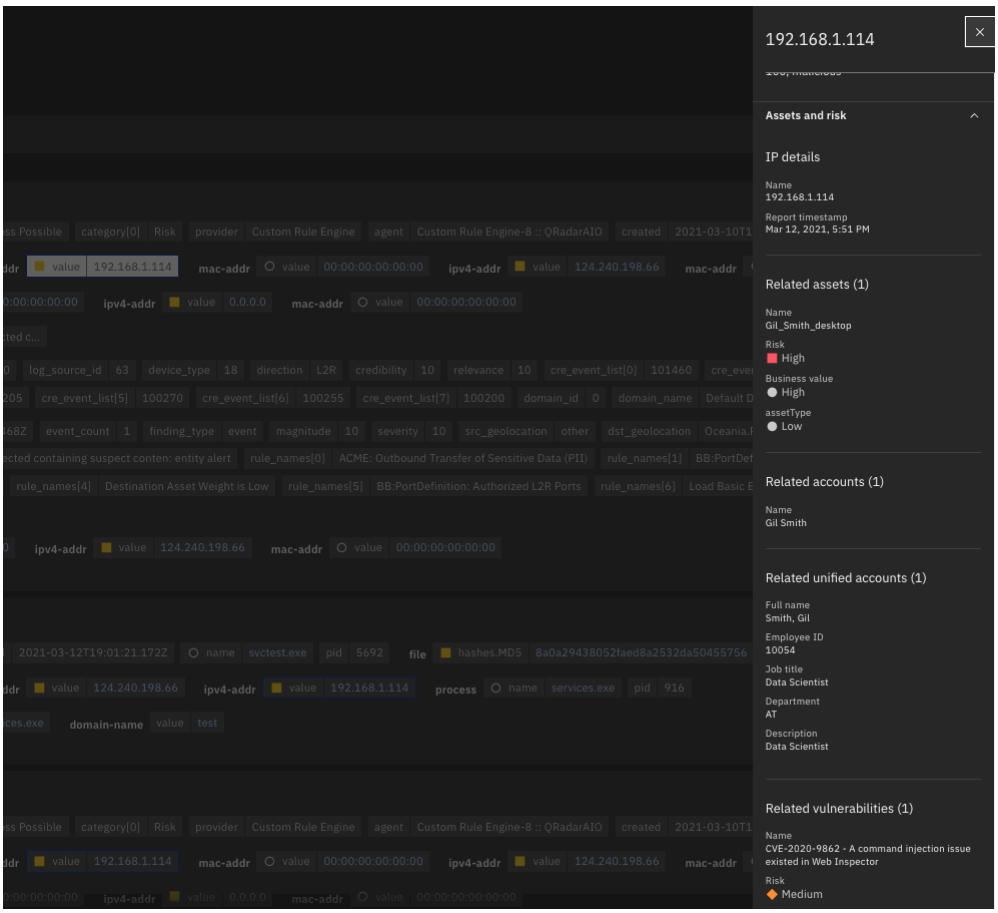
If Jeff selects the target IP address shown in red, he can get more details about the artifacts and the hits. For example, in this example he sees that this IP address is known to be malicious according to CISCO Threat Grid.



4.5 Verify asset criticality

To properly assess the incident and the associated risk to the organization, Jeff, the analyst, needs to understand the importance of the assets involved, as well as possible vulnerabilities associated with them. For this purpose, Jeff can access the built-in asset and risk database (CAR database) in Cloud Pak for Security. Here he gets the information about what type of asset it is, who the user is and what value it has to the organization, and what vulnerabilities, if any, are known.

Jeff retrieves the available information about the source IP address and sees that the source IP belongs to Gil Smith's desktop. She is a Data Scientist and her desktop shows high business risk, as well as known vulnerabilities for that asset. Based on this information, Jeff estimates the overall risk of this incident to be correspondingly higher.

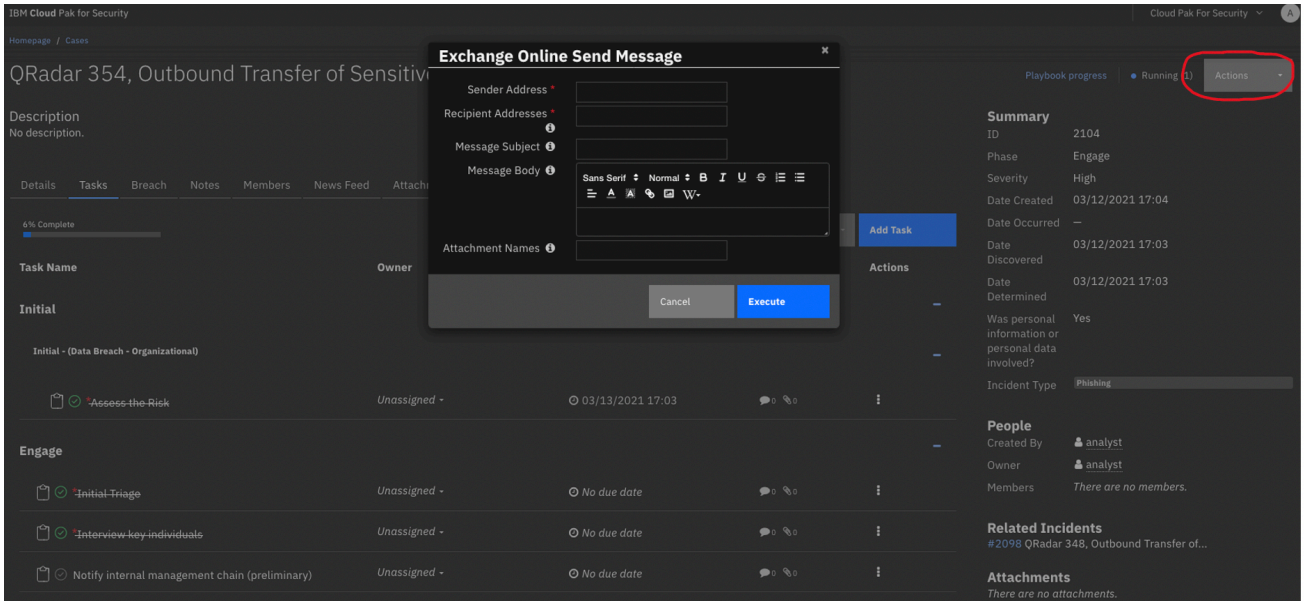


4.6 Triage security case / response activities

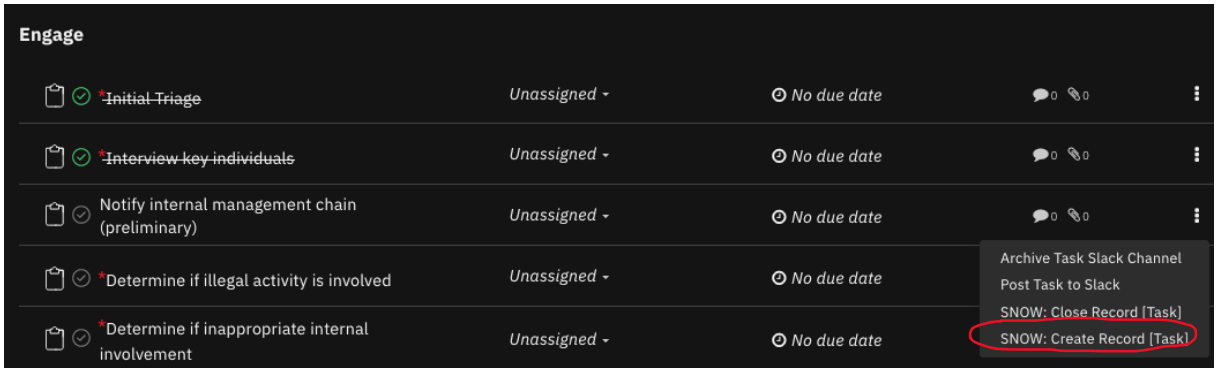
Based on the triage that Jeff and other analysts on the SOC team have performed to this point and the completion of the initial tasks according to the playbook, the incident has been identified as an actual event and critical to the organization.

The necessary steps, such as reporting the suspicious activity to the appropriate authorities (FTC) and notify owners of systems used in phishing attack, as well as the data owner, are being taken. Either manually, semi-automatically or automatically via tasks in Case Management.

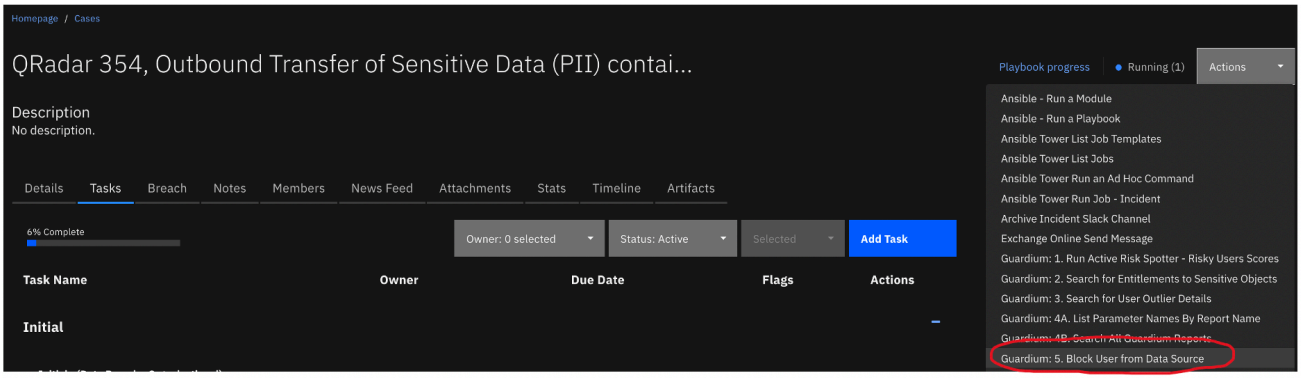
- To notify the owners of systems used for phishing attacks or to report the suspicious activity involving PII data to the FTC as required by law, the analyst Jeff can send an email directly from the case action drop down menu.



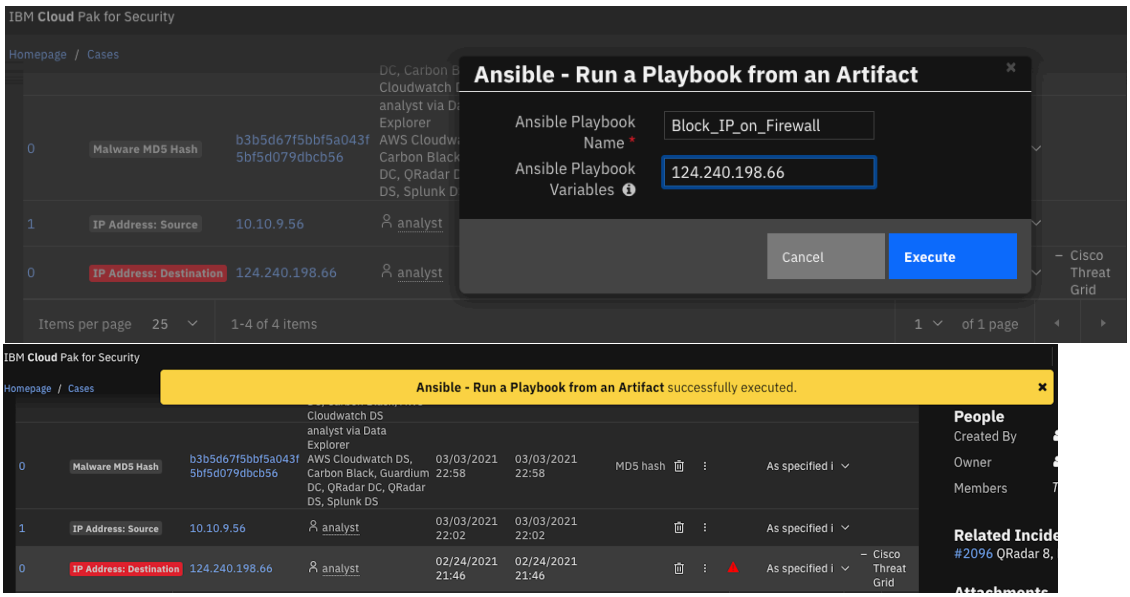
- Optionally, the analyst can create a ticket in the connected Service Now (SNOW) system directly from a playbook task.



- One of the mitigation steps Jeff will trigger in order to avoid more data exfiltration is to block the user access to the database. Leveraging the Guardium integration application in SOAR he can directly block the user in Guardium from the case action drop down menu.



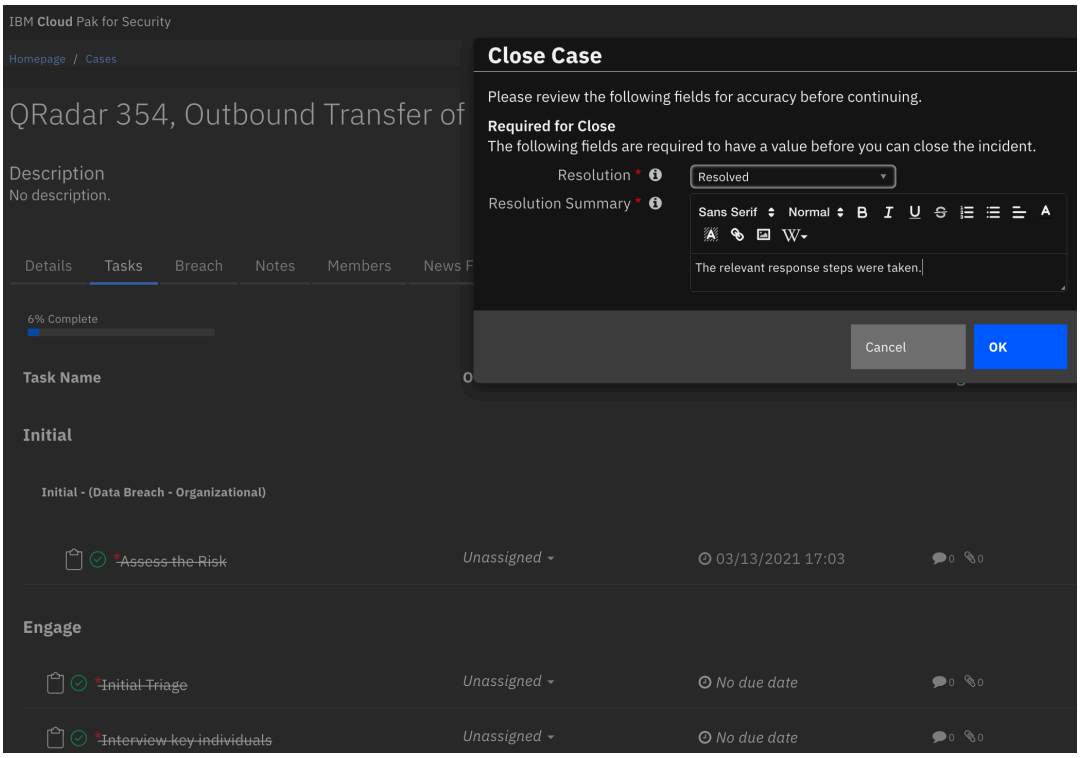
- An Ansible workflow can be used to change the firewall rule to block the external IP address in question. To do this, Jeff selects "Ansible - Run a Playbook from an Artifact" and chooses the "Block_IP_on_Firewall" workflow with the target external IP address to be blocked.



With this, the analyst Jeff has implemented the necessary actions according to the playbook to contain the threat and address the regulatory requirements.

Further investigation by the SOC team, which included an interview with the user involved and analysis of his activities, revealed that the user Gil had been the victim of a phishing attack and that the attacker had thus obtained the credentials.
Appropriate measures are being taken with regard to the user access credentials.

After implementing all relevant response actions and mitigating the risk of attack, Analyst Jeff closes the incident with an appropriate note. From the Case Actions drop-down menu, he selects "Close Case," selects the "Resolution," and enters the appropriate comments.



4.7 Reporting / Analytics

The CISO in the company must have an overall view of the security situation and ensure adherence to legal compliance requirements. To accomplish this task, he must determine if his organization is affected by security breaches or vulnerabilities.

Also the Data Security Specialist responsible for the critical data assets must monitor data security posture and is responsible for compliance.

Using the dashboard feature in CP4S, the CISO and the Data Security Specialist can view and track open cases. The dashboard shows how many open cases there are, what their risk value is, what the current status is, and who is working on the cases.

Using the user behavior dashboard analysis in Cloud Pak for Security, the CISO can gain insight into privileged users in the enterprise and quickly identify potential risks related to their activities here.