Automating Response to Phishing with Cortex XSOAR

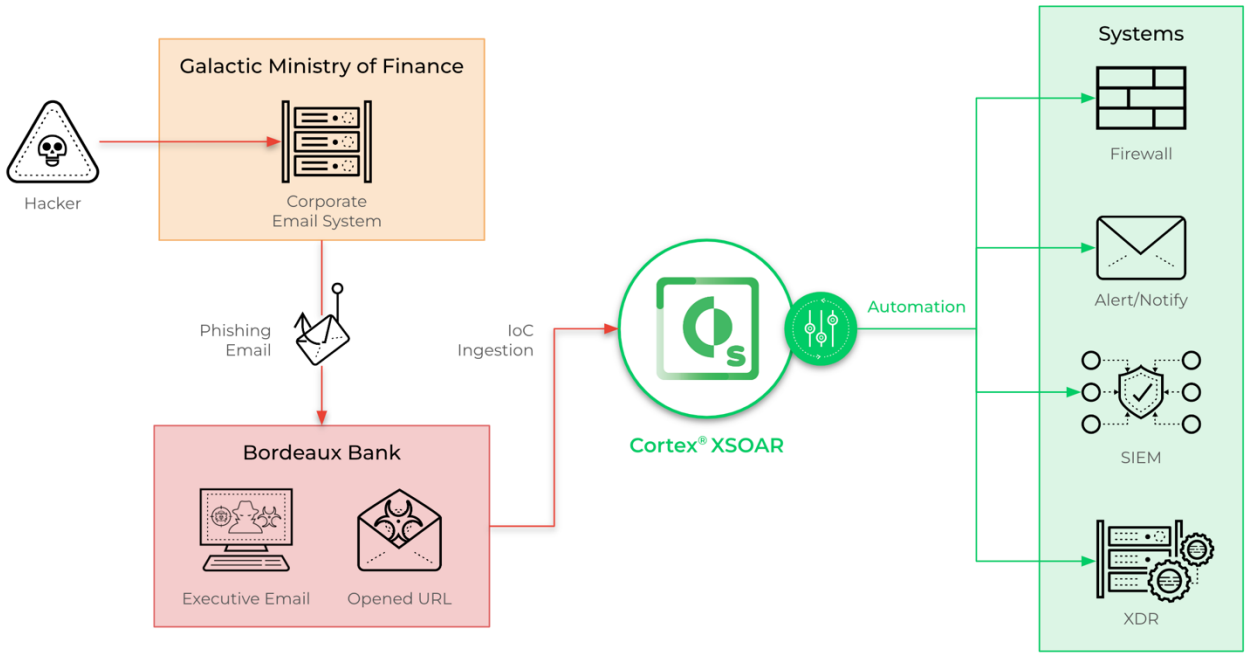
Lab Overview

This lab was designed to help me understand how to use Cortex XSOAR (XSOAR) to automate incident response to phishing attacks. The scenario involves a spear-phishing campaign targeting a fictional bank, the Galactic Ministry of Finance, followed by phishing emails sent to executives at Bordeaux Bank. The lab was hosted in partnership with Google Cloud and provided access to a Cortex XSOAR threat intelligence management instance.

Learning Objectives

By the end of this lab, I learned how to:

- Investigate incidents using Cortex XSOAR
- Understand Cortex XSOAR War Rooms
- Create an incident response plan using Cortex XSOAR



Setup and Requirements

Prerequisites

- Access to a standard internet browser (Chrome recommended)
- Use of an Incognito or private browser window to avoid conflicts with personal accounts
- Ensured I had uninterrupted time to complete the lab

Starting the Lab

1. **Access the Lab Environment**:
    - Clicked the "Start Lab" button
    - Selected a payment method if required
    - Opened the Google Cloud console (right-clicked and selected “Open Link in Incognito Window” when using Chrome)
2. **Sign In to the Google Cloud Console**:
    - Used the temporary credentials from the Lab Details pane
    - Clicked “Use Another Account” if prompted
    - Pasted the provided username and password
    - Accepted the terms and conditions
    - Skipped adding recovery options or two-factor authentication
    - Did not sign up for any free trials
3. **Access Cortex XSOAR**:
    - Used the provided URL and credentials to access the XSOAR console
    - Waited several minutes for the console to become fully accessible

Task 1: Introduction to XSOAR & Phishing

Understanding Phishing

- **Definition**: I learned that phishing is a type of social engineering attack primarily executed through email. Attackers craft fraudulent messages that mimic legitimate communication to deceive recipients.
- **Current Limitations**: I discovered that responding to phishing emails manually is time-consuming and error-prone, often requiring multiple tools and steps.
- **XSOAR's Solution**: I learned that Cortex XSOAR addresses these challenges through automation and orchestration, improving speed, accuracy, and consistency in phishing response workflows.

Task 2: Investigating Incidents

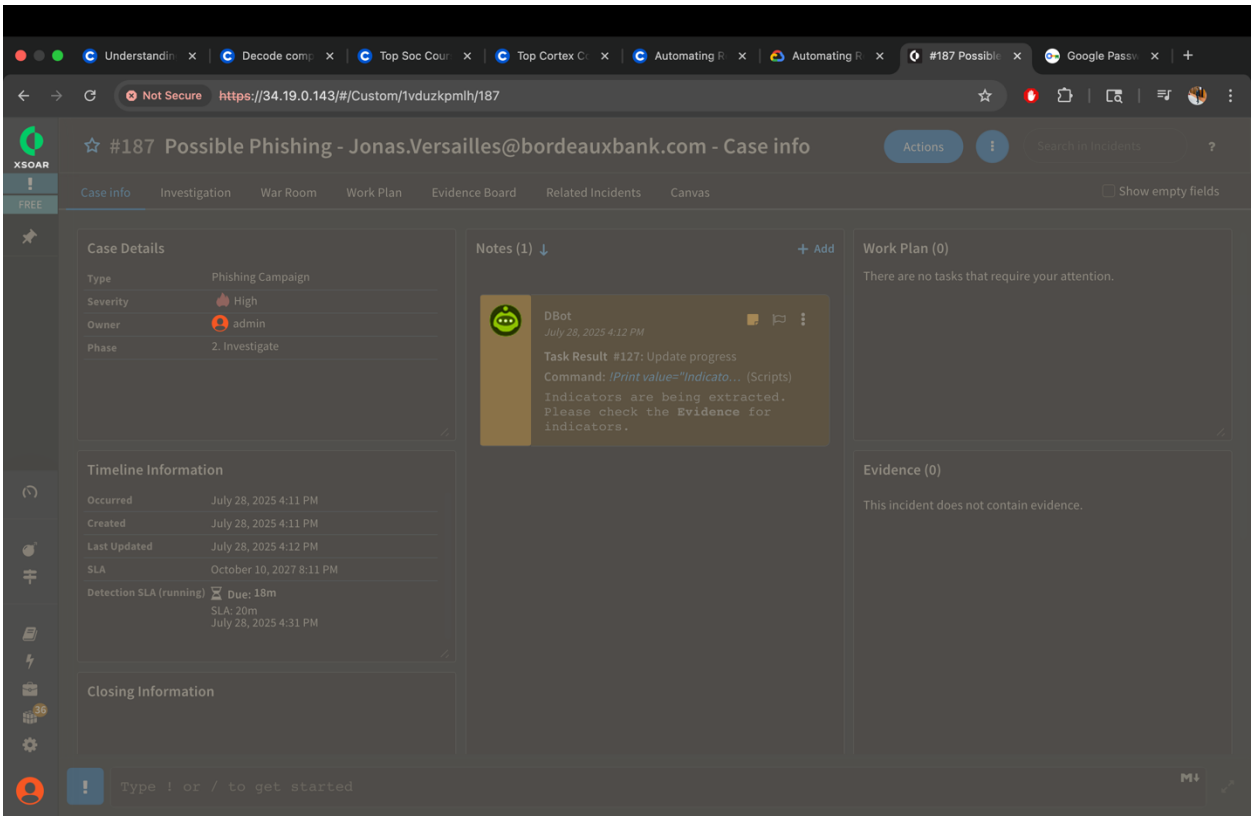
Step 1: Generate a Phishing Incident

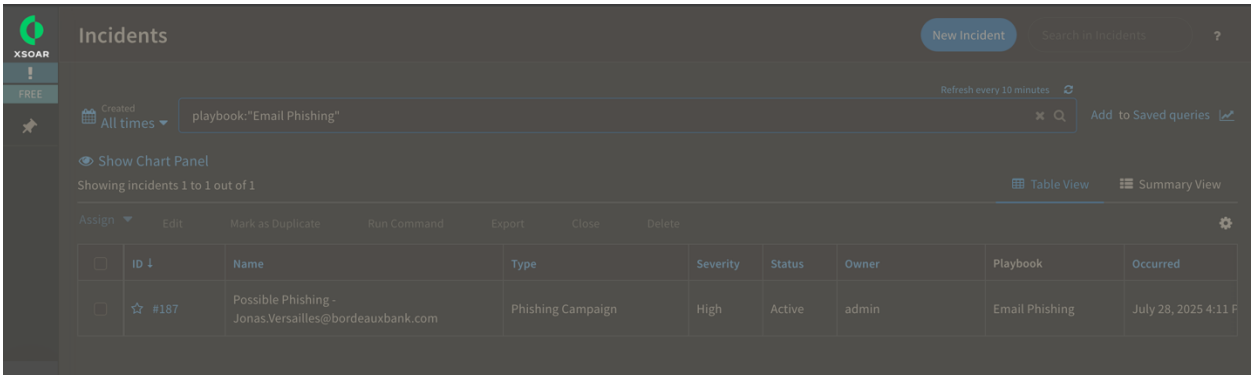
1. **Access Cortex XSOAR**:
    - Logged in using the provided URL and credentials
    - Navigated to the **Incidents** section
    - Set the *Created* range to “All times”
    - Clicked **New Incident**
    - Set the *workshop scenario* to **Phishing Campaign** and *Type* to **Scenario**

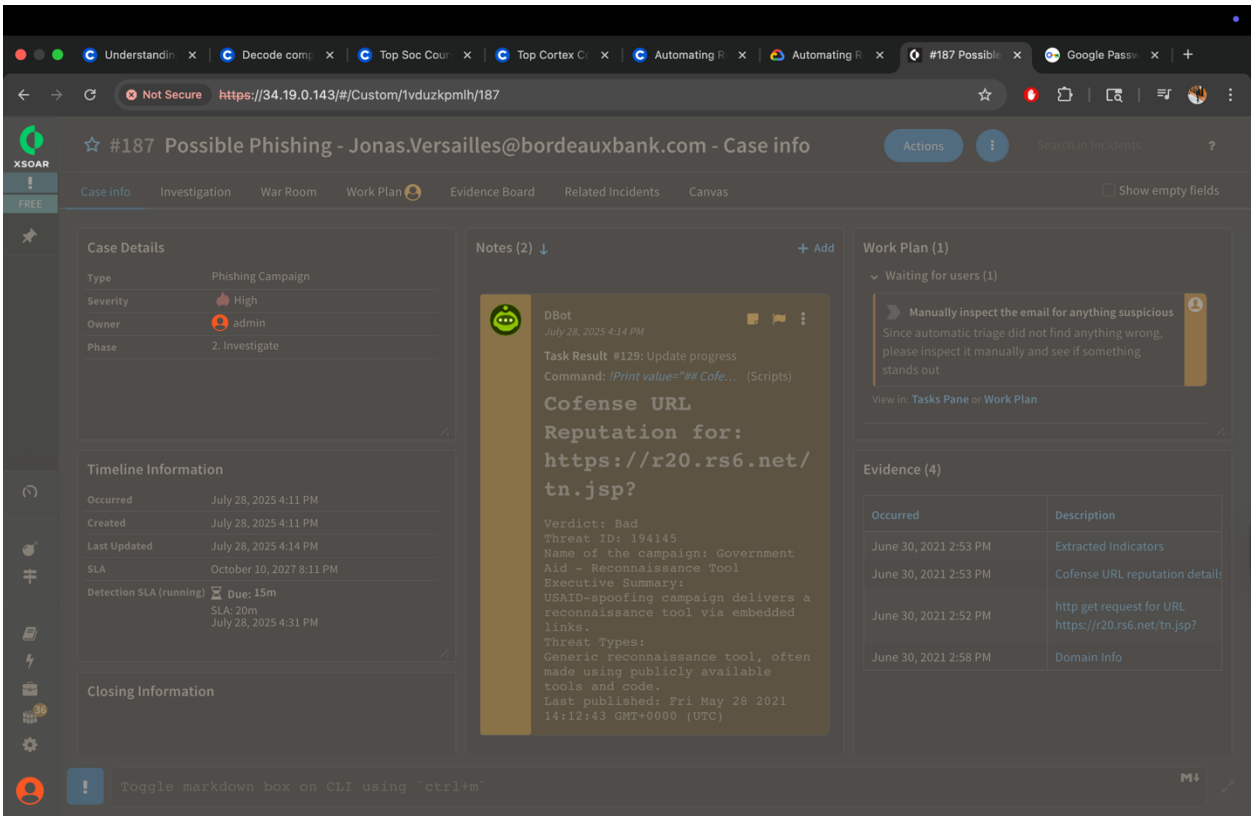
- Clicked **Create New Incident**

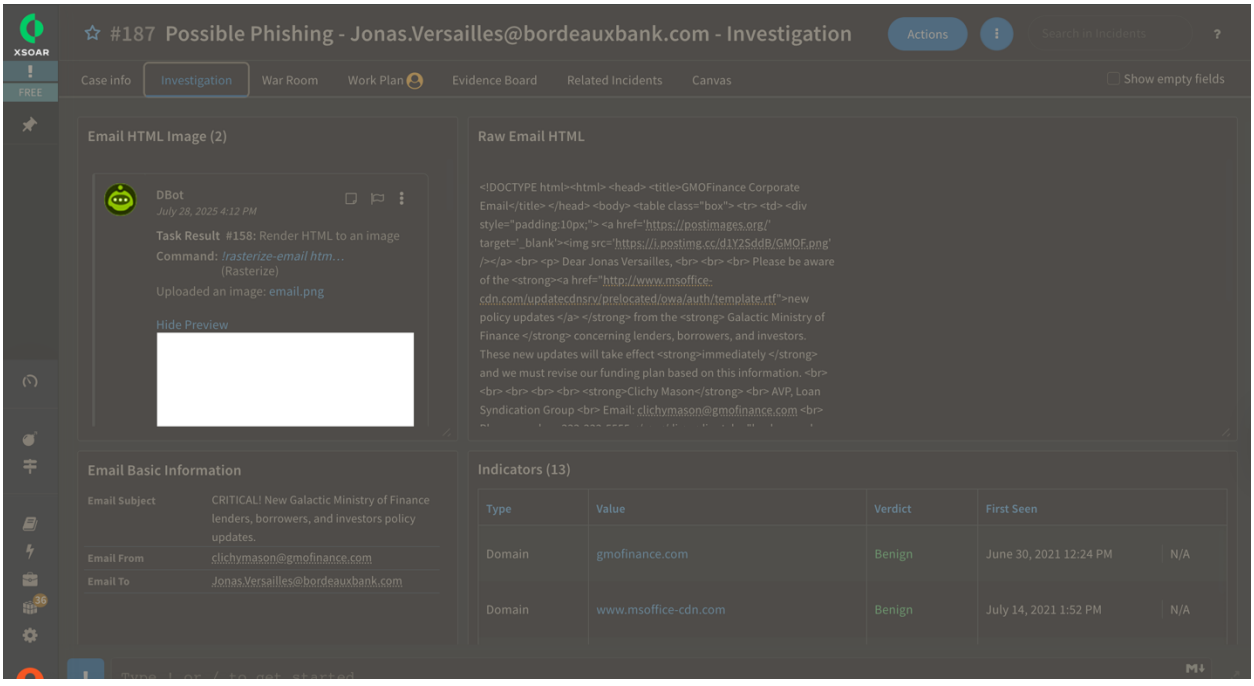
Step 2: Investigate the Phishing Incident

1. **Filter Incidents**:
   - Used the search filter: `playbook:"Email Phishing"`
   - Selected the most recent incident to review details
   - Reviewed the incident's status, case info, timeline, notes, and evidence
   - Clicked the **Investigation** tab to analyze email content, indicators, and incident files






Not Secure https://34.19.0.143/#/Custom/1vduzkpmlh/187
#187 Possible Phishing - Jonas.Versailles@bordeauxbank.com - Case info
Actions
Case info
Investigation
War Room
Work Plan
Evidence Board
Related Incidents
Canvas
Show empty fields
Case Details
Type Phishing Campaign
Severity High
Owner admin
Phase 2. Investigate
Notes (2)
+ Add
DBot
July 28, 2025 4:14 PM
Task Result #129: Update progress
Command: !Print value="## Cofe... (Scripts)
Cofense URL Reputation for: https://r20.rs6.net/tn.jsp?
Verdict: Bad
Threat ID: 194145
Name of the campaign: Government Aid - Reconnaissance Tool
Executive Summary:
USAID-spoofing campaign delivers a reconnaissance tool via embedded links.
Threat Types:
Generic reconnaissance tool, often made using publicly available tools and code.
Last published: Fri May 28 2021 14:12:43 GMT+0000 (UTC)
Work Plan (1)
Waiting for users (1)
Manually inspect the email for anything suspicious
Since automatic triage did not find anything wrong, please inspect it manually and see if something stands out
View in: Tasks Pane or Work Plan
Timeline Information
Occurred July 28, 2025 4:11 PM
Created July 28, 2025 4:11 PM
Last Updated July 28, 2025 4:14 PM
SLA October 10, 2027 8:11 PM
Detection SLA (running) Due: 15m
SLA: 20m
July 28, 2025 4:31 PM
Evidence (4)
Occurred
Description
June 30, 2021 2:53 PM Extracted Indicators
June 30, 2021 2:53 PM Cofense URL reputation details
June 30, 2021 2:52 PM http get request for URL https://r20.rs6.net/tn.jsp?
June 30, 2021 2:58 PM Domain Info
Closing Information
Toggle markdown box on CLI using `ctrl+m`


#187 Possible Phishing - Jonas.Versailles@bordeauxbank.com - Investigation
Actions
Case info
Investigation
War Room
Work Plan
Evidence Board
Related Incidents
Canvas
Show empty fields
Email HTML Image (2)
DBot
July 28, 2025 4:12 PM
Task Result #158: Render HTML to an image
Command: !rasterize-email htm...
(Rasterize)
Uploaded an image: email.png
Hide Preview
Raw Email HTML
<!DOCTYPE html><html> <head> <title>GMOFinance Corporate Email</title> </head> <body> <table class="box"> <tr> <td>
 <p> Dear Jonas Versailles,

 Please be aware of the new policy updates from the Galactic Ministry of Finance concerning lenders, borrowers, and investors. These new updates will take effect immediately and we must revise our funding plan based on this information.

 Clichy Mason
 AVP, Loan Syndication Group
 Email: clichymason@gmofinance.com
Email Basic Information
Email Subject CRITICAL! New Galactic Ministry of Finance lenders, borrowers, and investors policy updates.
Email From clichymason@gmofinance.com
Email To Jonas.Versailles@bordeauxbank.com
Indicators (13)
Type
Value
Verdict
First Seen
Domain gmofinance.com Benign June 30, 2021 12:24 PM N/A
Domain www.msoffice-cdn.com Benign July 14, 2021 1:52 PM N/A

Indicators (13) Indicators

Type	Value	Verdict	First Seen	
Domain	gmofinance.com	Benign	June 30, 2021 12:24 PM	N/A
Domain	www.msoffice-cdn.com	Benign	July 14, 2021 1:52 PM	N/A
Domain	postimages.org	Benign	June 30, 2021 12:36 PM	N/A
IPv6	2002:a05:620a:108f:0:0:0:0	Unknown	June 23, 2021 1:50 PM	N/A

Indicators (13) Indicators

Type	Value	Verdict	First Seen	
URL	http://www.msoffice-cdn.com/updatecdnsrv/prelocated/owa/auth/template.rtf	Suspicious	July 14, 2021 1:52 PM	N/A
URL	https://postimages.org/	Unknown	January 11, 2023 9:08 AM	N/A
Email	Jonas.Versailles@bordeauxbank.com	Unknown	June 30, 2021 12:24 PM	N/A
Domain	i.postimg.cc	Benign	June 30, 2021 12:36 PM	N/A

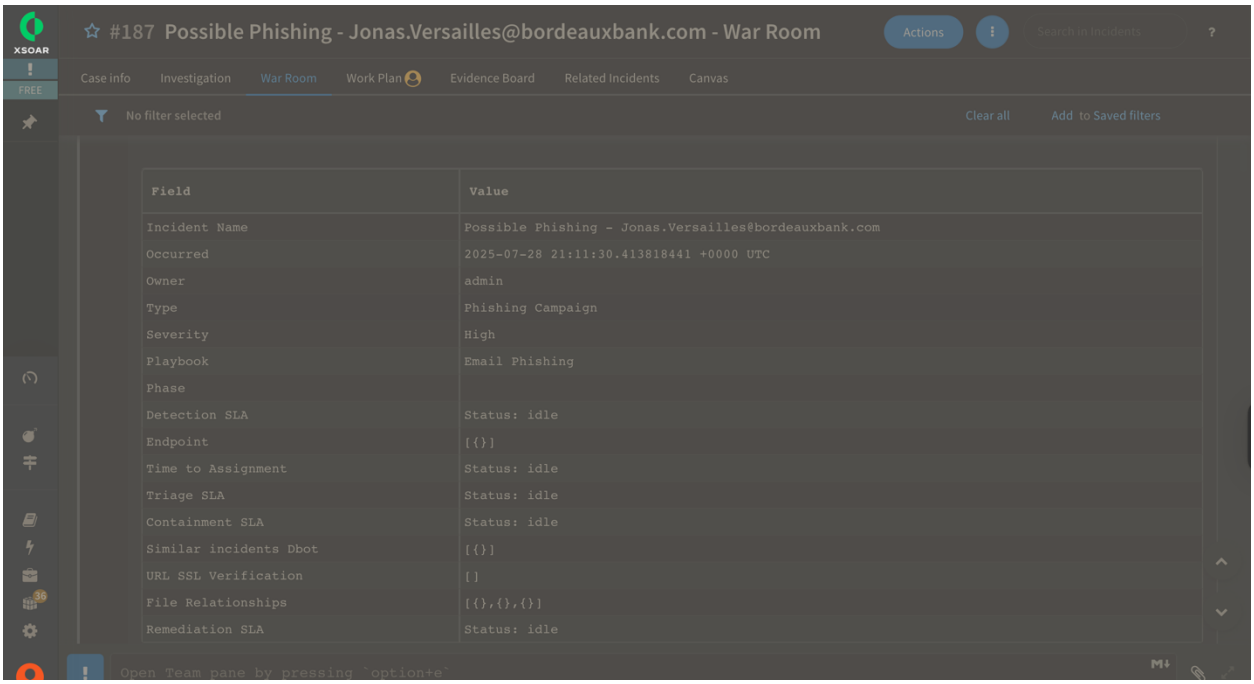
Task 3: War Room & Work Plan

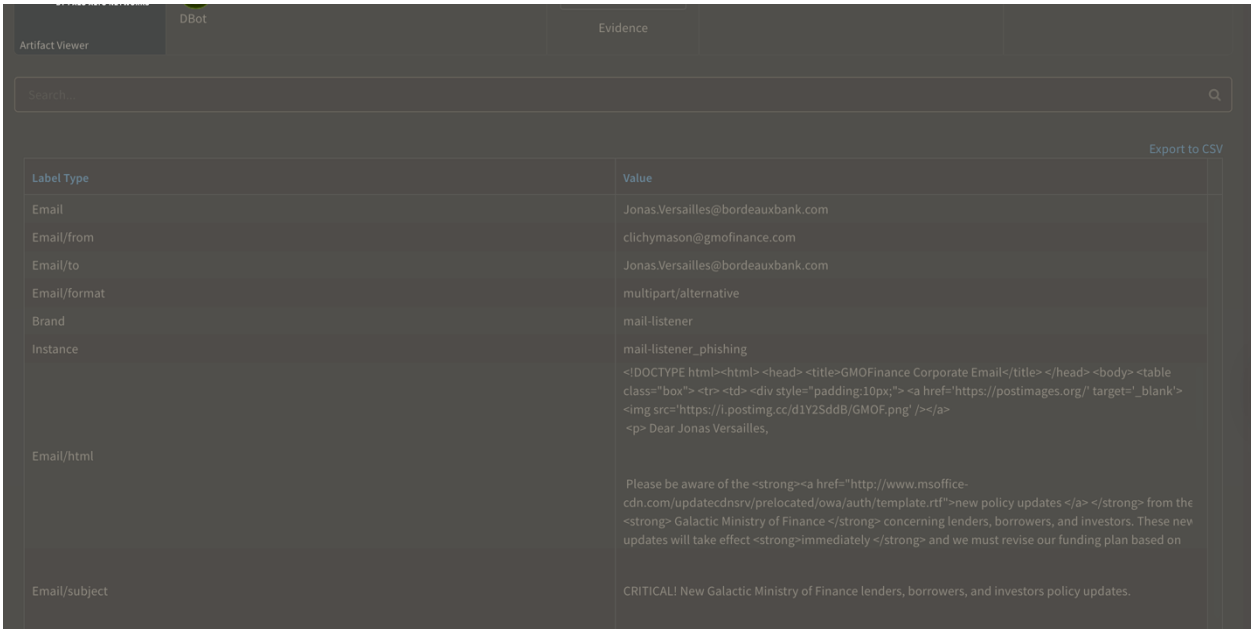
Step 1: War Room

1. **Navigate to the War Room**:
    - Clicked the **War Room** tab
    - Scrolled through event logs tied to the incident
    - Clicked **Complete in Task Pane → Open in Work Plan**

Step 2: Work Plan

1. **Review and Complete Work Plan Tasks**:
    - Reviewed actions taken in response to the incident
    - Marked key tasks as completed:
        - Assign and involve appropriate personnel
        - Assess severity
        - Are the hostnames in the URLs being misrepresented?
    - Explored additional tasks to dig deeper into the incident response process

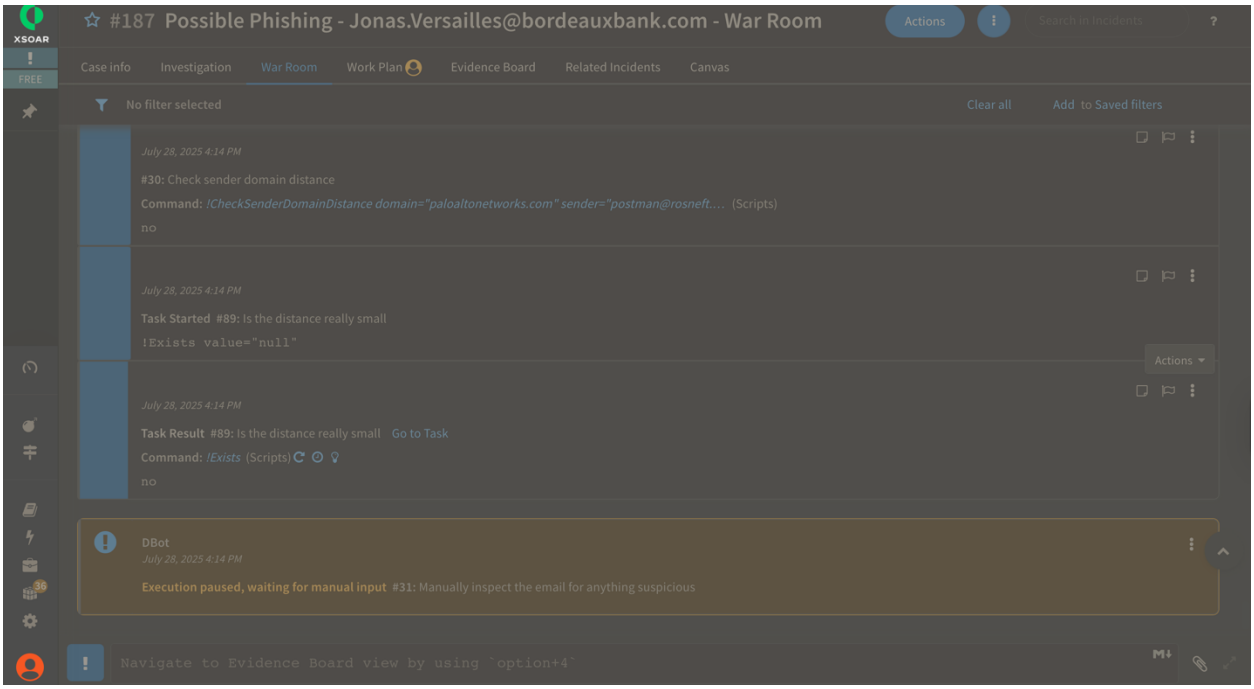

XSOAR
#187 Possible Phishing - Jonas.Versailles@bordeauxbank.com - War Room
Actions
Search in Incidents
FREE
Case info
Investigation
War Room
Work Plan
Evidence Board
Related Incidents
Canvas
No filter selected
Clear all
Add to Saved filters
Field
Value
Incident Name
Possible Phishing - Jonas.Versailles@bordeauxbank.com
Occurred
2025-07-28 21:11:30.413818441 +0000 UTC
Owner
admin
Type
Phishing Campaign
Severity
High
Playbook
Email Phishing
Phase
Detection SLA
Status: idle
Endpoint
[{}]
Time to Assignment
Status: idle
Triage SLA
Status: idle
Containment SLA
Status: idle
Similar incidents Dbot
[{}]
URL SSL Verification
[]
File Relationships
[{},{},{}]
Remediation SLA
Status: idle
Open Team pane by pressing `option+e`
M↓

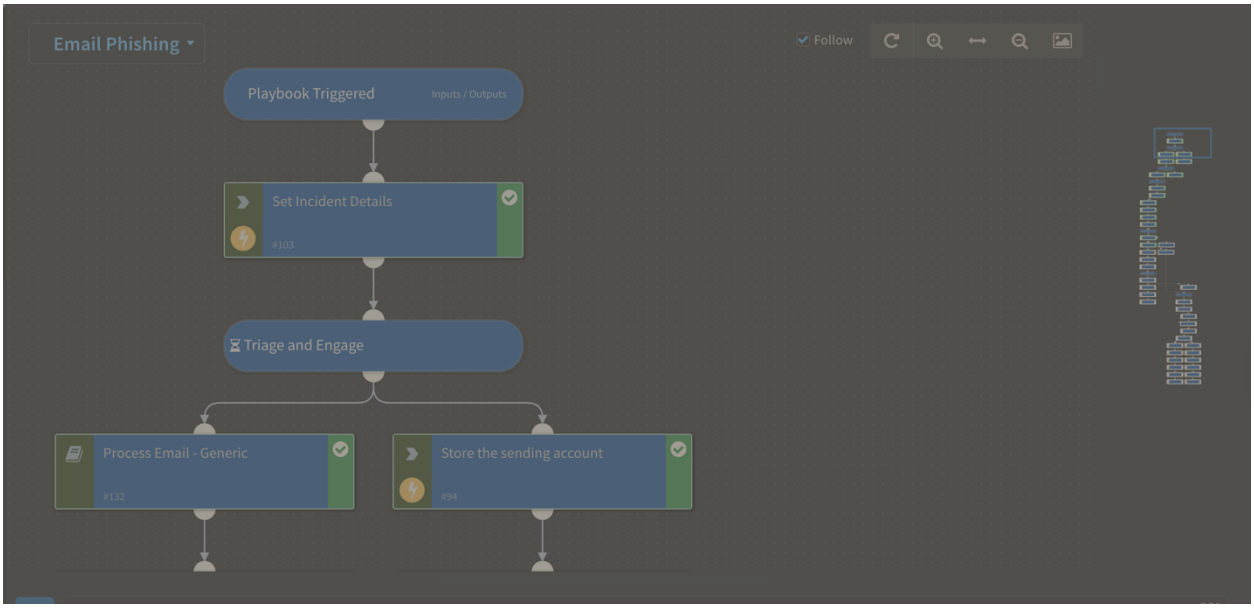

Artifact Viewer
DBot
Evidence
Search...
Export to CSV
Label Type
Value
Email
Jonas.Versailles@bordeauxbank.com
Email/from
clichymason@gmofinance.com
Email/to
Jonas.Versailles@bordeauxbank.com
Email/format
multipart/alternative
Brand
mail-listener
Instance
mail-listener_phishing
Email/html
<!DOCTYPE html><html> <head> <title>GMOFinance Corporate Email</title> </head> <body> <table class="box"> <tr> <td>
<p> Dear Jonas Versailles,
Please be aware of the new policy updates from the Galactic Ministry of Finance concerning lenders, borrowers, and investors. These new updates will take effect immediately and we must revise our funding plan based on
Email/subject
CRITICAL! New Galactic Ministry of Finance lenders, borrowers, and investors policy updates.

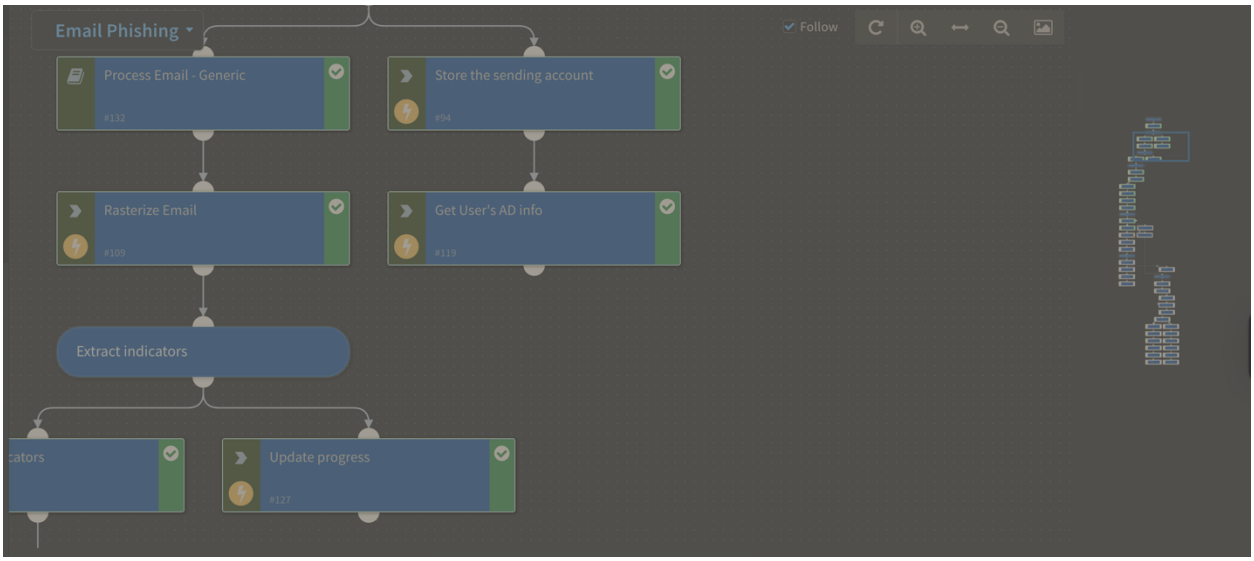
Search...

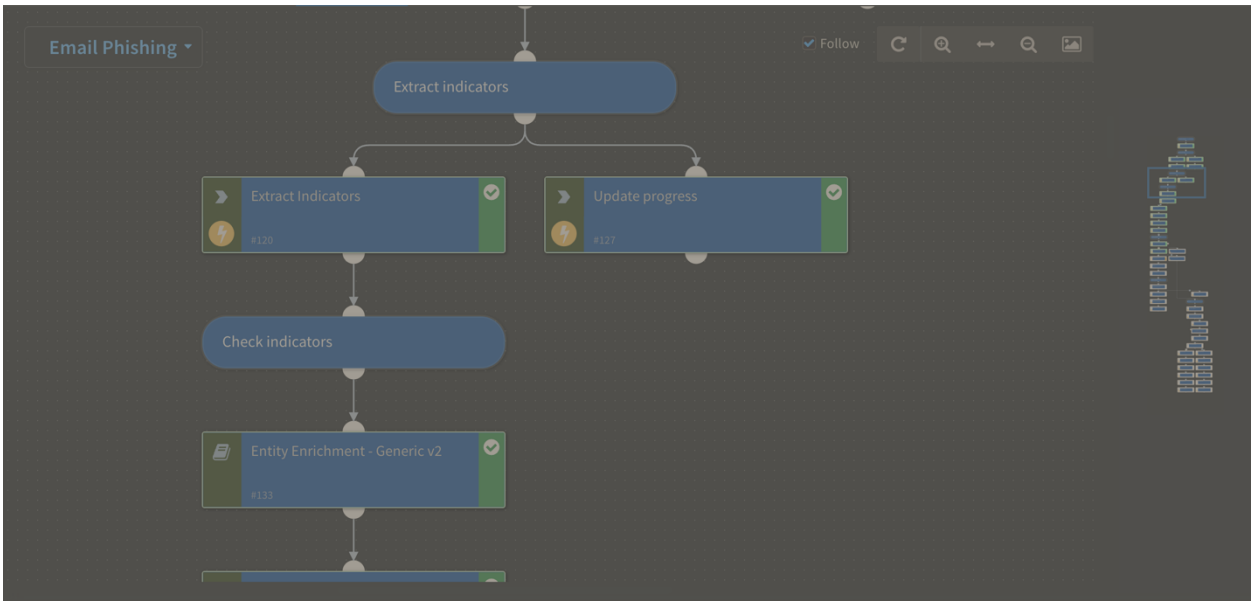
Export to CSV

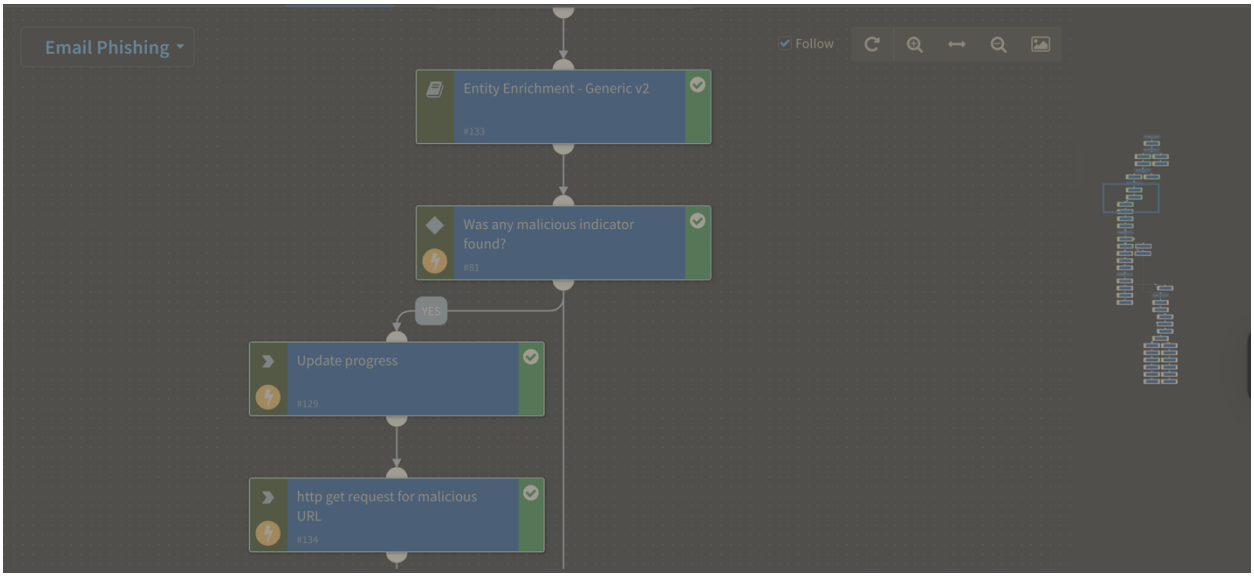
Label Type	Value
Email/headers	Delivered-To: Jonas.Versailles@bordeauxbank.com Received: by 2002:a05:620a:108f:0:0:0:0 with SMTP id g15csp10667557qkk;
Email/headers/Delivered-To	Jonas.Versailles@bordeauxbank.com
Email/headers/X-Received	by 2002:ac5:c30b:: with SMTP id j11mr2201922vkk.46.1551307053353; Mon, 06 Sep 2020 06:00:35Z
Email/headers/To	Jonas.Versailles@bordeauxbank.com
Email/headers/Subject	CRITICAL! New Galactic Ministry of Finance lenders, borrowers, and investors policy updates.
Email/headers/Content-type	multipart/alternative;
Email/headers/From	Galactic Ministry of Finance clichymason@gmofinance.com
Email/headers/Date	Mon, 06 Sep 2020 06:00:35Z
severity	high
brand	mail-listener
instance	mail-listener_phishing
Email/headers/Delivered-To	Jonas.Versailles@bordeauxbank.com
Email/headers/X-Received	by 2002:ac5:c30b:: with SMTP id j11mr2201922vkk.46.1551307053353; Mon, 06 Sep 2020 06:00:35Z
Email/headers/To	Jonas.Versailles@bordeauxbank.com
Email/headers/Subject	CRITICAL! New Galactic Ministry of Finance lenders, borrowers, and investors policy updates.
Email/headers/Content-type	multipart/alternative;
Email/headers/From	Galactic Ministry of Finance clichymason@gmofinance.com
Email/headers/Date	Mon, 06 Sep 2020 06:00:35Z
severity	high
brand	mail-listener
instance	mail-listener_phishing
randomUser	{"user_id": "1002", "deptartment": "Corporate Banking and Capital Markets", "manager": "Corporate Banking and Capital Markets, EVP", "title": "Corporate Banking and Capital Markets, Executive Vice President", "based_in": "Boston,MA", "computer_name": "Versailles-DT98660", "email_address": "Jonas.Versailles@bordeauxbank.com", "external_ip": "100.231.114.51", "first_name": "Jonas", "internal_ip": "172.16.94.221", "last_name": "Versailles", "mac_address": "00:00:02:04:F5:C2", "username": "jonas_versailles"}

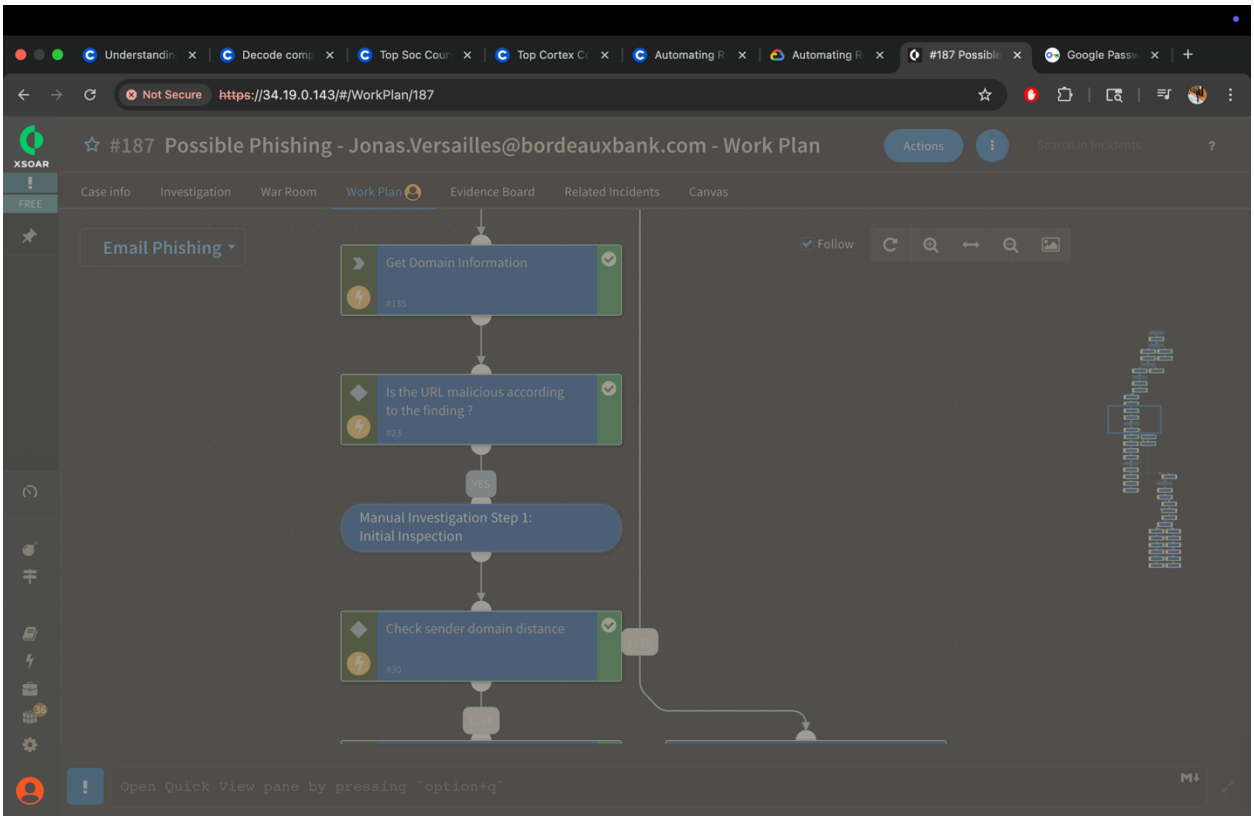

XSOAR
FREE
#187 Possible Phishing - Jonas.Versailles@bordeauxbank.com - War Room
Actions
Search in Incidents
Case info
Investigation
War Room
Work Plan
Evidence Board
Related Incidents
Canvas
No filter selected
Clear all
Add to Saved filters
July 28, 2025 4:14 PM
#30: Check sender domain distance
Command: !CheckSenderDomainDistance domain="paloaltonetworks.com" sender="postman@rosneft.... (Scripts)
no
July 28, 2025 4:14 PM
Task Started #89: Is the distance really small
!Exists value="null"
Actions
July 28, 2025 4:14 PM
Task Result #89: Is the distance really small Go to Task
Command: !Exists (Scripts)
no
DBot
July 28, 2025 4:14 PM
Execution paused, waiting for manual input #31: Manually inspect the email for anything suspicious
Navigate to Evidence Board view by using `option+4`

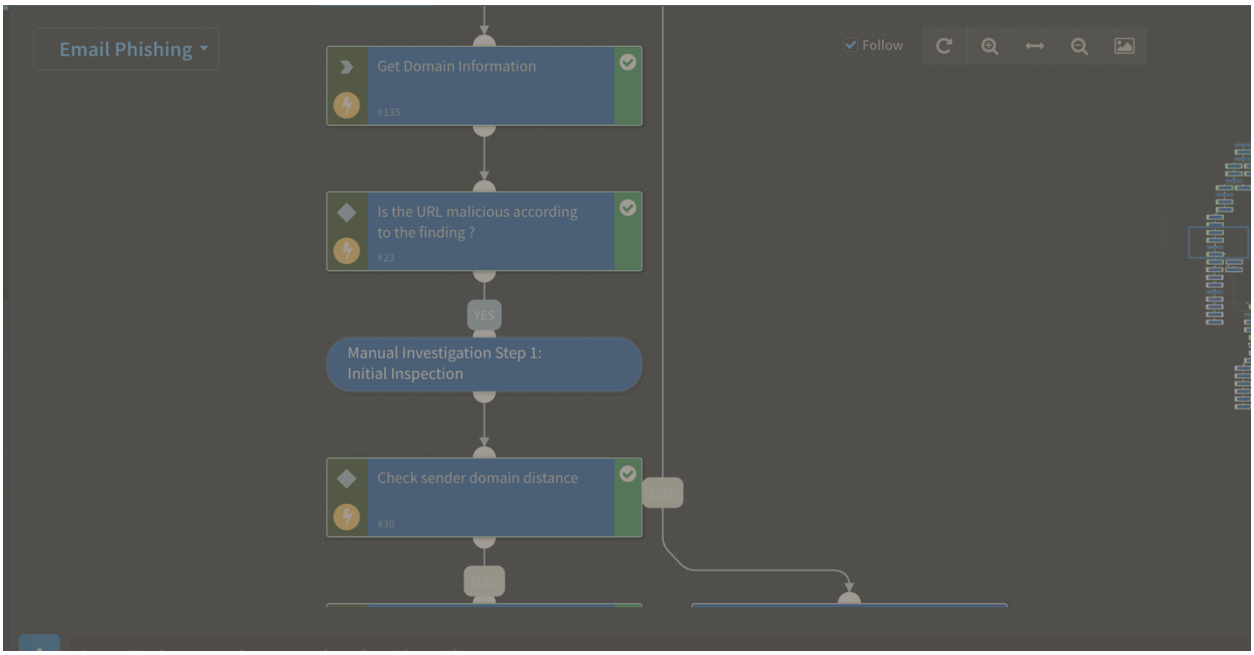

Email Phishing
Follow
Playbook Triggered
Inputs / Outputs
Set Incident Details
#103
Triage and Engage
Process Email - Generic
#132
Store the sending account
#94


Email Phishing
Follow
Process Email - Generic
#132
Store the sending account
#94
Rasterize Email
#109
Get User's AD info
#119
Extract indicators
Update progress
#127


Email Phishing
Follow
Extract indicators
Extract Indicators
#120
Update progress
#127
Check indicators
Entity Enrichment - Generic v2
#133


Email Phishing
Follow
Entity Enrichment - Generic v2
#133
Was any malicious indicator found?
#81
YES
Update progress
#129
http get request for malicious URL
#134

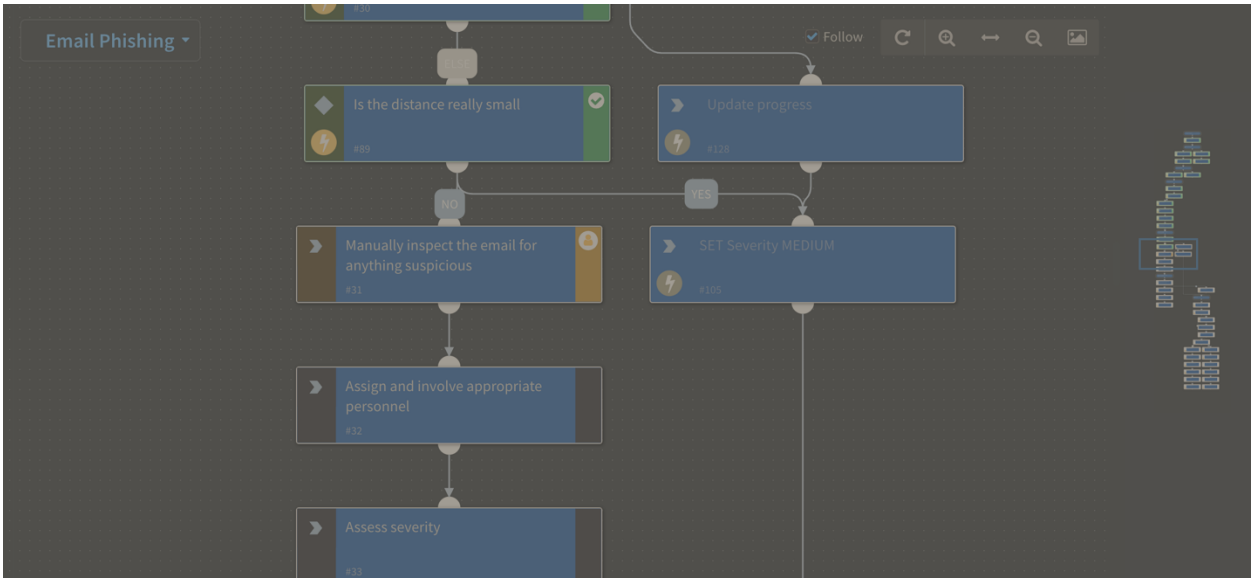

Not Secure
https://34.19.0.143/#/WorkPlan/187
#187 Possible Phishing - Jonas.Versailles@bordeauxbank.com - Work Plan
Actions
Case info
Investigation
War Room
Work Plan
Evidence Board
Related Incidents
Canvas
Email Phishing
Follow
Get Domain Information
#135
Is the URL malicious according to the finding ?
#23
YES
Manual Investigation Step 1: Initial Inspection
Check sender domain distance
#30
ELSE
Open Quick View pane by pressing `option+q`

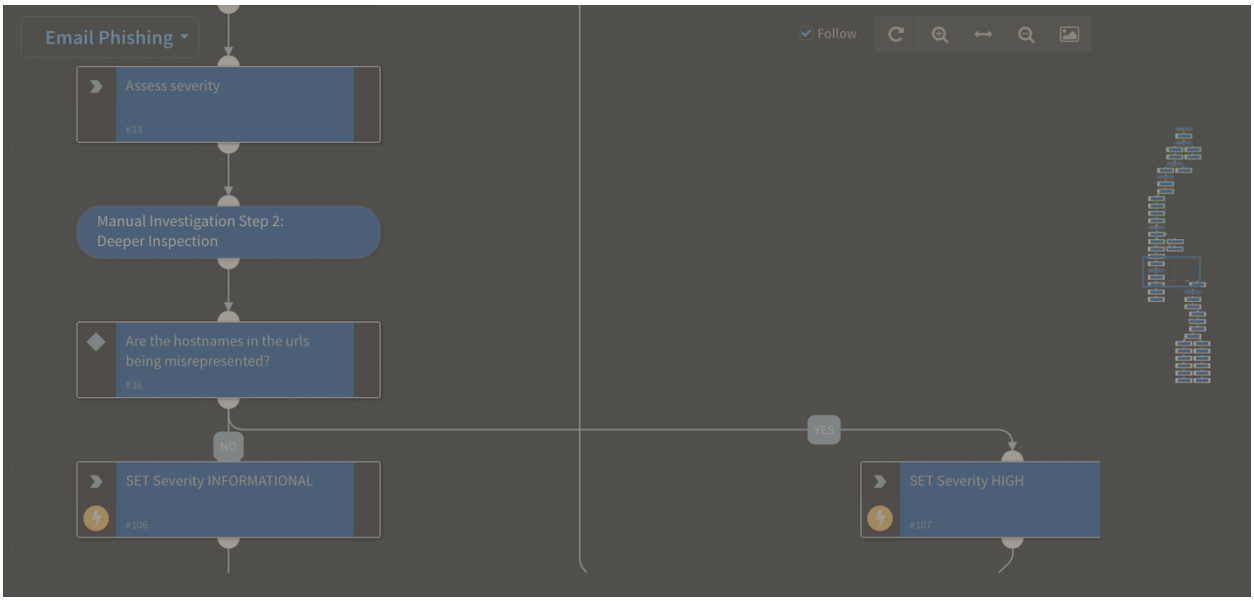

Email Phishing
Follow
Get Domain Information
#135
Is the URL malicious according to the finding ?
#23
YES
Manual Investigation Step 1: Initial Inspection
Check sender domain distance
#30
ELSE

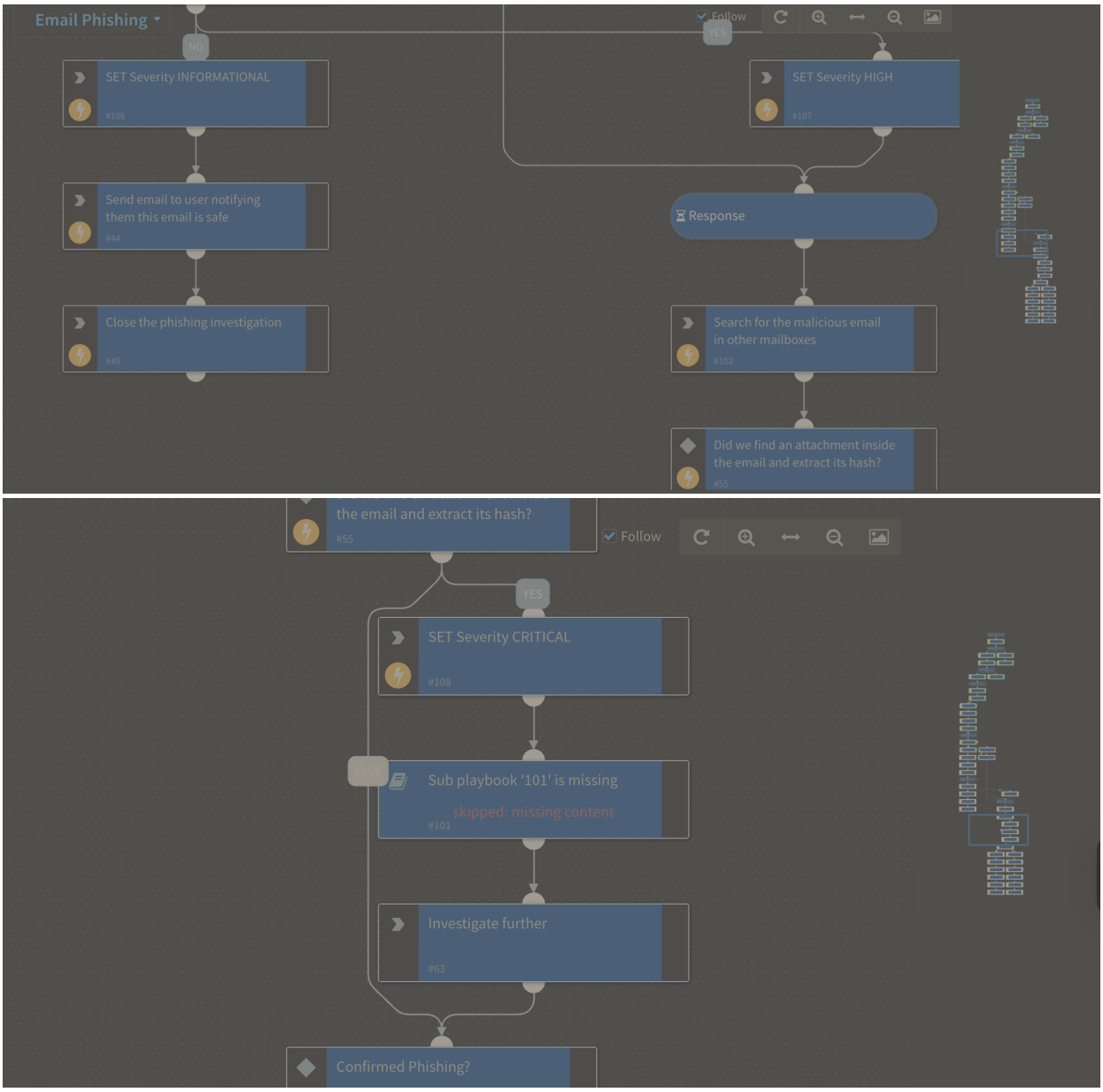
Indicators (13)

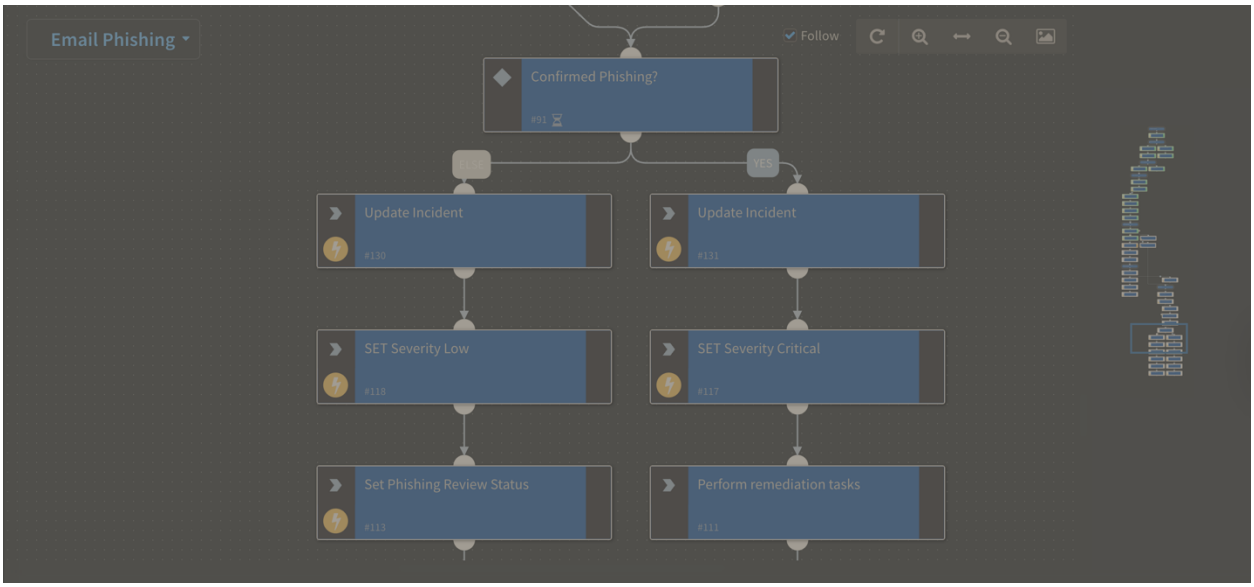
Indicators

Type	Value	Verdict	First Seen	
IP	172.16.94.221	Benign	June 23, 2021 1:52 PM	N/A
Domain	bordeauxbank.com	Benign	June 30, 2021 12:24 PM	N/A
URL	https://i.postimg.cc/d1Y2SddB/GMOF.png	Unknown	January 11, 2023 9:08 AM	N/A
IP	100.231.114.51	Benign	June 23, 2021 1:52 PM	N/A

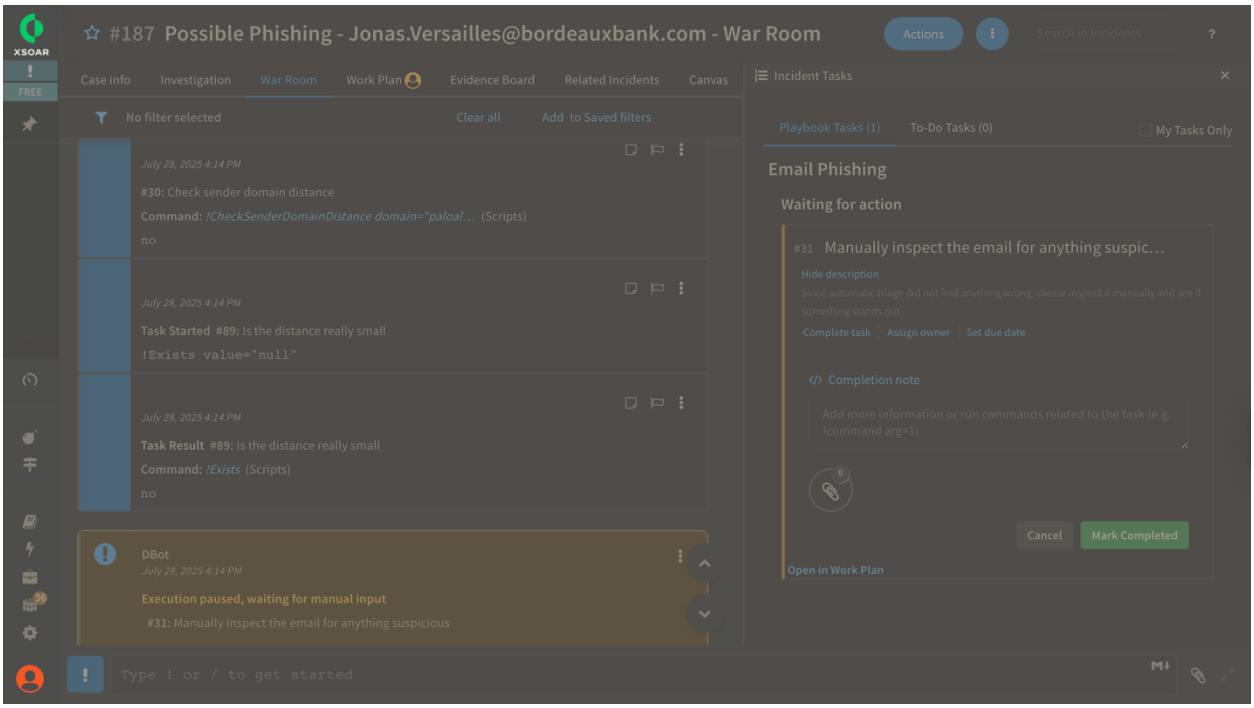


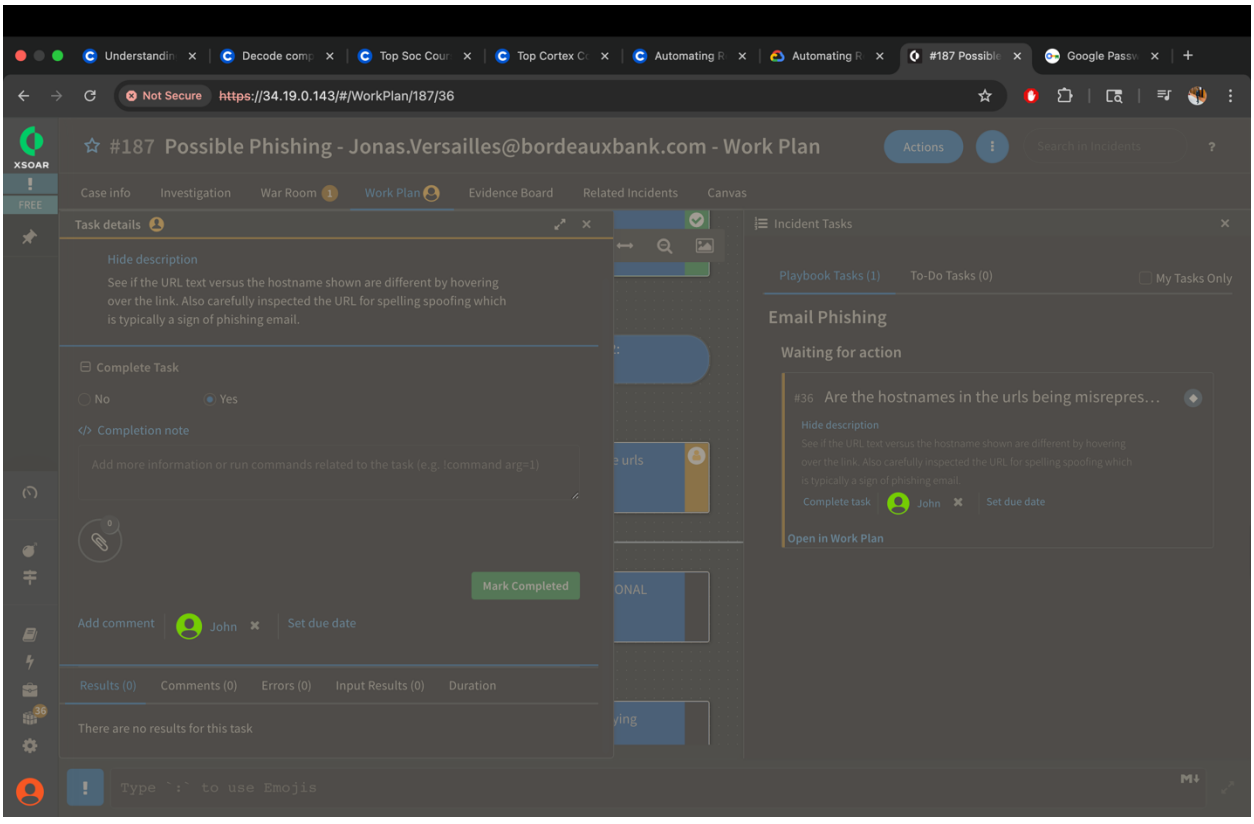


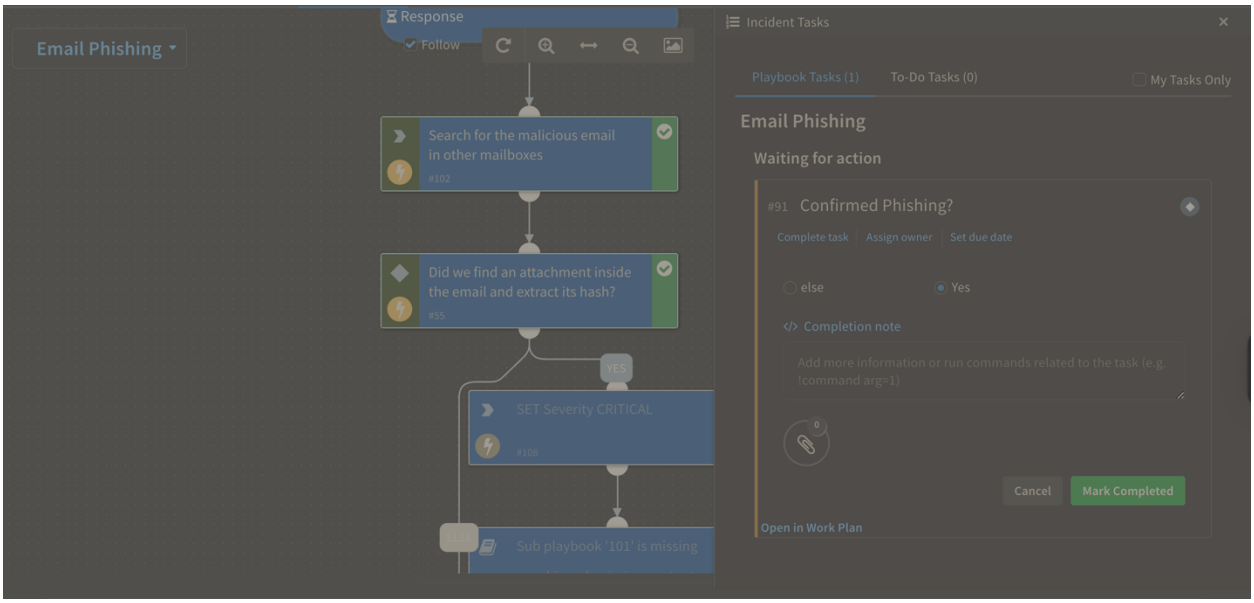

Email Phishing
Follow
NO
YES
SET Severity INFORMATIONAL
#106
SET Severity HIGH
#107
Send email to user notifying them this email is safe
#44
Response
Close the phishing investigation
#45
Search for the malicious email in other mailboxes
#102
Did we find an attachment inside the email and extract its hash?
#55
the email and extract its hash?
#55
Follow
YES
SET Severity CRITICAL
#108
ELSE
Sub playbook '101' is missing
skipped: missing content
#101
Investigate further
#63
Confirmed Phishing?


Email Phishing
Follow
Confirmed Phishing?
#91
NO
YES
Update Incident
#130
Update Incident
#131
SET Severity Low
#118
SET Severity Critical
#117
Set Phishing Review Status
#113
Perform remediation tasks
#111

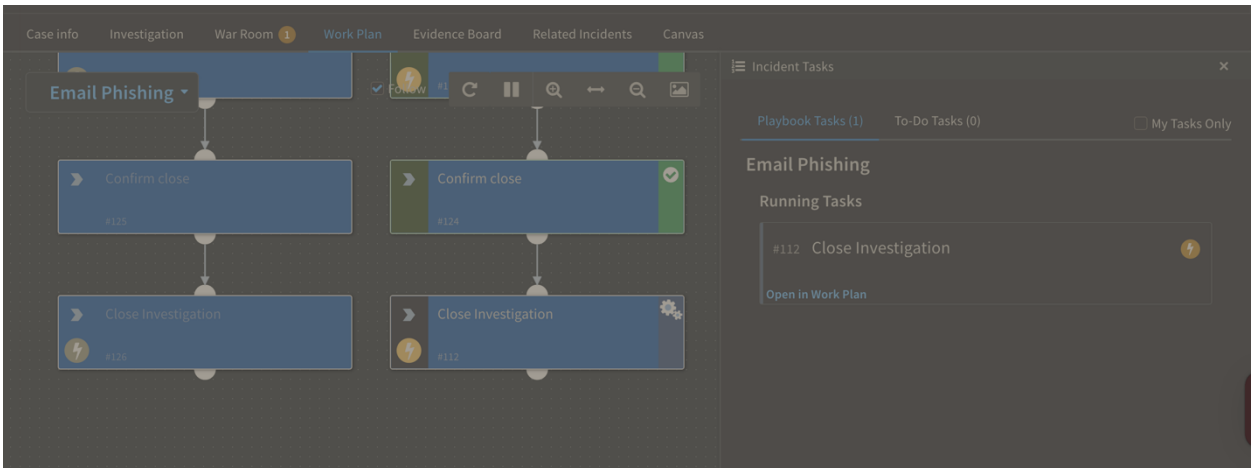

Email Phishing
Follow
Set Phishing Review Status
#113
Perform remediation task
#111
Ready to close Investigation
#114
Set Phishing Review Status
#110
Confirm close
#125
Confirm close
#124
Close Investigation
#126
Close Investigation
#112

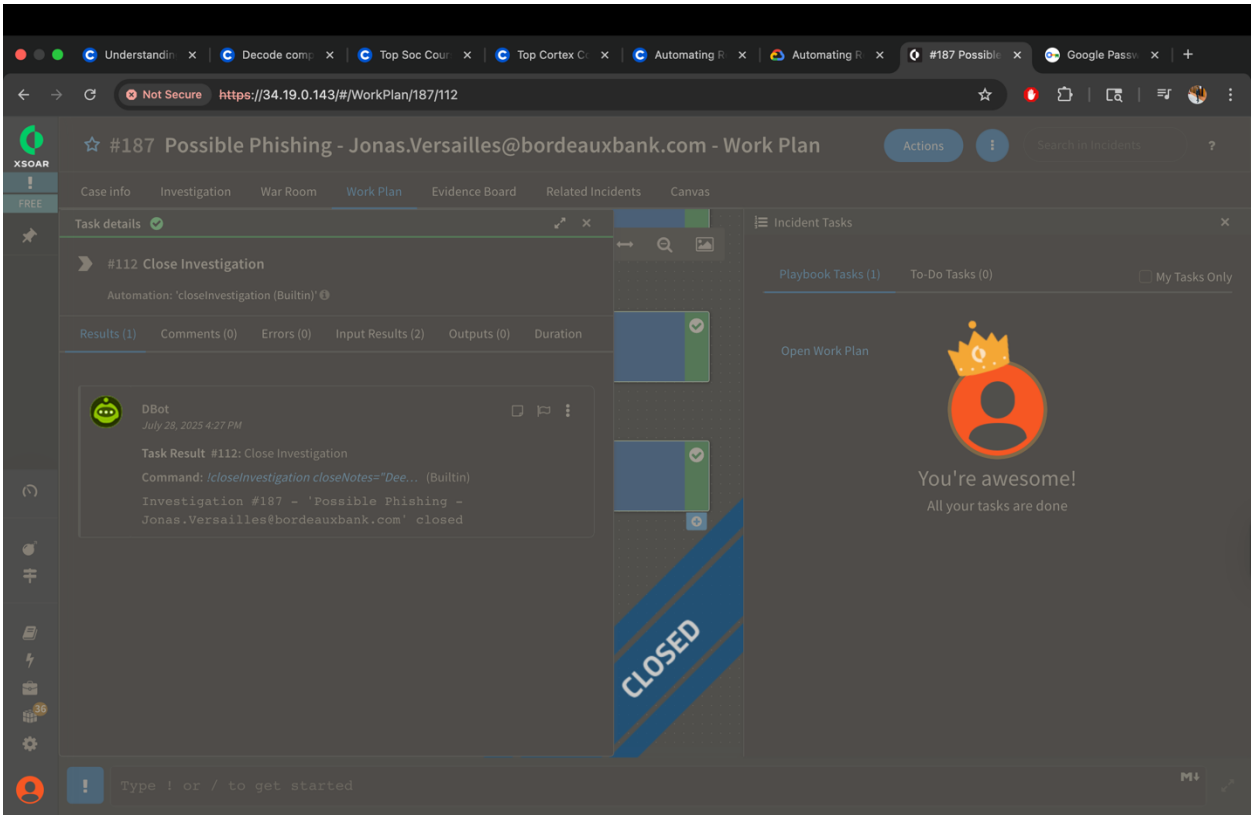

#187 Possible Phishing - Jonas.Versailles@bordeauxbank.com - War Room
Actions
Case info
Investigation
War Room
Work Plan
Evidence Board
Related Incidents
Canvas
No filter selected
Clear all
Add to Saved filters
July 28, 2025 4:14 PM
#30: Check sender domain distance
Command: !CheckSenderDomainDistance domain="paloal... (Scripts)
no
July 28, 2025 4:14 PM
Task Started #89: Is the distance really small
!Exists value="null"
July 28, 2025 4:14 PM
Task Result #89: Is the distance really small
Command: !Exists (Scripts)
no
DBot
July 28, 2025 4:14 PM
Execution paused, waiting for manual input
#31: Manually inspect the email for anything suspicious
Type ! or / to get started
Incident Tasks
Playbook Tasks (1)
To-Do Tasks (0)
My Tasks Only
Email Phishing
Waiting for action
#31 Manually inspect the email for anything suspic...
Hide description
Since automatic triage did not find anything wrong, please inspect it manually and see if something stands out
Complete task
Assign owner
Set due date
Completion note
Add more information or run commands related to the task (e.g. !command arg=1)
Cancel
Mark Completed
Open in Work Plan


Not Secure
https://34.19.0.143/#/WorkPlan/187/36
#187 Possible Phishing - Jonas.Versailles@bordeauxbank.com - Work Plan
Actions
Case info
Investigation
War Room
Work Plan
Evidence Board
Related Incidents
Canvas
Task details
Hide description
See if the URL text versus the hostname shown are different by hovering over the link. Also carefully inspected the URL for spelling spoofing which is typically a sign of phishing email.
Complete Task
No
Yes
Completion note
Add more information or run commands related to the task (e.g. !command arg=1)
Mark Completed
Add comment
John
Set due date
Results (0)
Comments (0)
Errors (0)
Input Results (0)
Duration
There are no results for this task
Type `:` to use Emojis
Incident Tasks
Playbook Tasks (1)
To-Do Tasks (0)
My Tasks Only
Email Phishing
Waiting for action
#36 Are the hostnames in the urls being misrepres...
Hide description
See if the URL text versus the hostname shown are different by hovering over the link. Also carefully inspected the URL for spelling spoofing which is typically a sign of phishing email.
Complete task
John
Set due date
Open in Work Plan


Email Phishing
Response
Follow
Search for the malicious email in other mailboxes
#102
Did we find an attachment inside the email and extract its hash?
#55
YES
SET Severity CRITICAL
#108
Sub playbook '101' is missing
Incident Tasks
Playbook Tasks (1)
To-Do Tasks (0)
My Tasks Only
Email Phishing
Waiting for action
#91 Confirmed Phishing?
Complete task
Assign owner
Set due date
else
Yes
Completion note
Add more information or run commands related to the task (e.g. !command arg=1)
Cancel
Mark Completed
Open in Work Plan

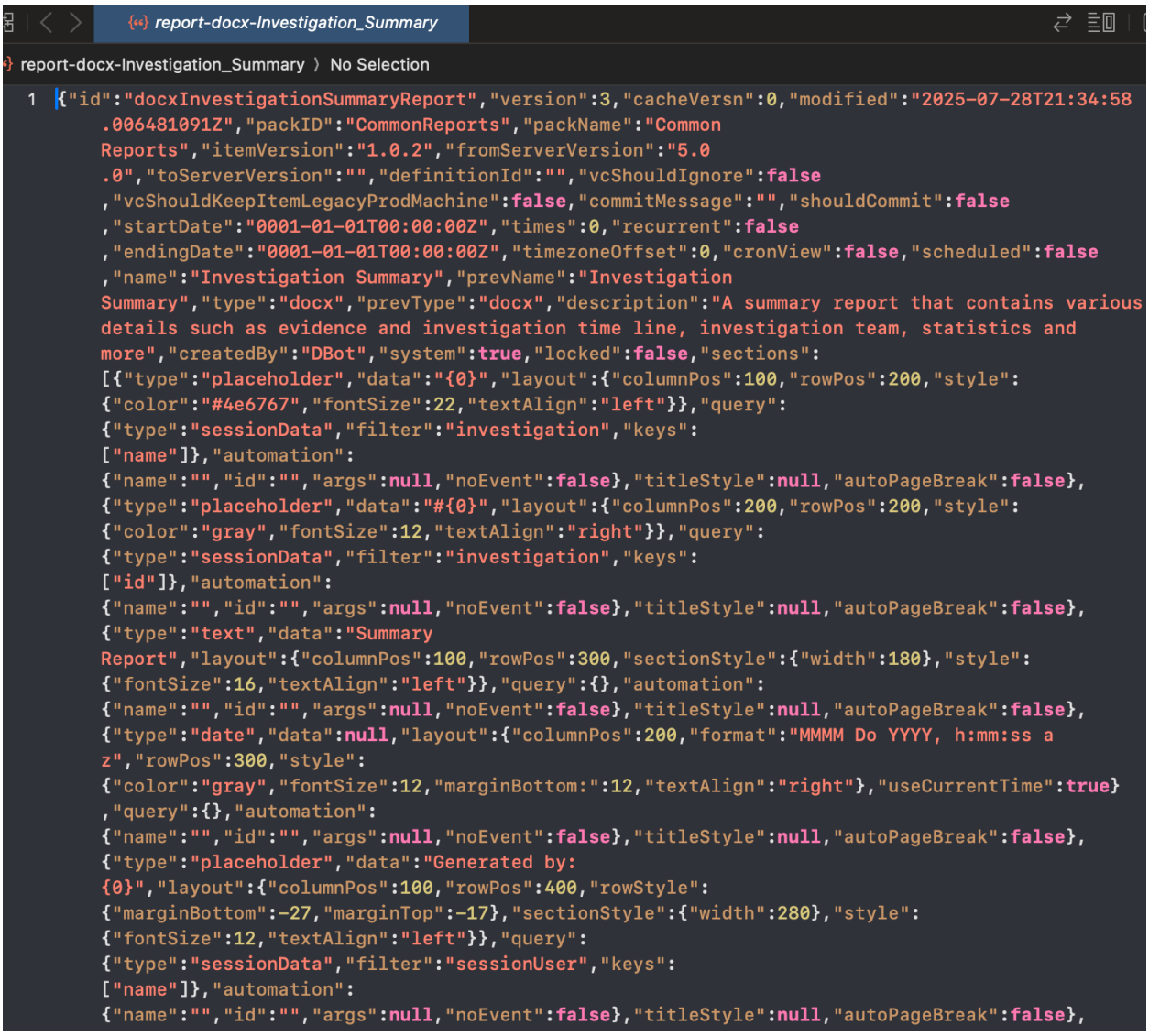

Email Phishing
#91
Follow
ELSE
YES
Update Incident
#130
Update Incident
#131
SET Severity Low
#118
SET Severity Critical
#117
Set Phishing Review Status
#113
Perform remediation tasks
#111
Ready to close Investigation
Set Phishing Review Status
Incident Tasks
Playbook Tasks (1)
To-Do Tasks (0)
My Tasks Only
Email Phishing
Waiting for action
#111 Perform remediation tasks
Complete task
Assign owner
Set due date
Open in Work Plan
Navigate to War Room view by using `option+2`





Step 3: (Optional) Generate a Report

1. **Create and Download the Report**:
    - Went to **Case Info → Actions → Report**
    - Set the "Select a tab to generate report from" option to **Case Info**
    - Clicked **Generate Report**
    - Downloaded the file from the **Reports** tab



Conclusion

In this lab, I learned how to use Cortex XSOAR to respond to phishing incidents, generate investigative reports, and work with the War Room, Work Plan, and automated playbooks. To continue learning, I explored additional resources like Cortex XSOAR Community Edition and Threat Intel Management.

For any technical issues with the lab, I contacted google-tech@paloaltonetworks.com.