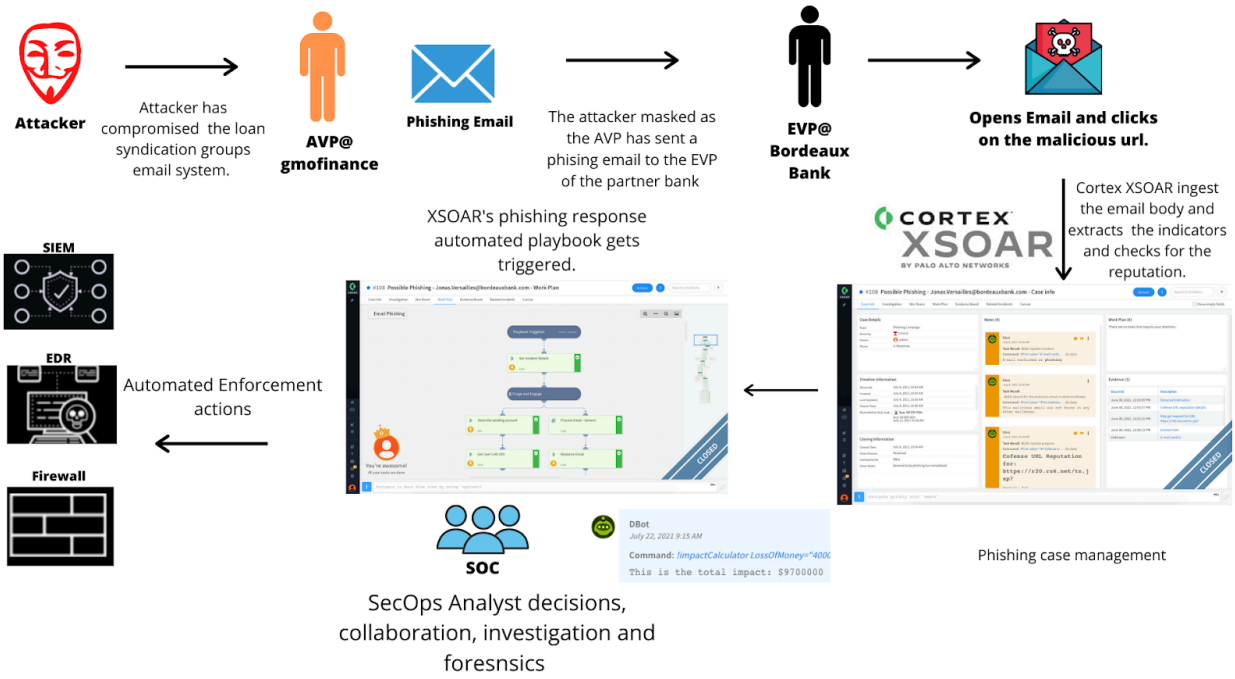
Sultan Taj

Automating Response to Phishing with XSOAR

In this lab we will run through an simulated case of email phishing and handling it with XSOAR's phishing response playbook.

This lab will run through a scenario of a spear phishing attack at a bank. The attacker intruded into the infrastructure of a loan syndication group, and hijacked the email server of the firm. The attacker has masked themself as the AVP of the loan syndication group, and has sent phishing emails to the EVP of corporation banking at the affiliate bank.



Task 1: Log in to the Cortex XSOAR instance

1. From the **Navigation menu**, click on **Compute Engine > VM instances.**
2. On the VM instances page, copy the **External IP** of the xsoar-phishing VM.

This IP is needed to access the lab instance

3. Next, open a new browser tab and enter the **External IP** address to access the lab instance formatted as the following: https://104.198.222.118
4. If you get a connection privacy warning, click **Advanced > Proceed**
5. Enter the credentials below in order to log into XSOAR
    a. Username: **admin**
    b. Password: **PQpV3vhhyWvnQS1vvMGs**

Task 2: Cortex XSOAR Playbook Overview

Phishing is an email-based form of social engineering. Disguised as legitimate communication, a fraudulent email used in a phishing attack is designed to trick its recipient into clicking a link, opening an attachment, or directly providing sensitive information. These actions are meant to either extract personal information from the target or infect the target's system with malware.

The process of responding to a phishing email is complex and time-consuming. Triage is often manual, as analysts have to go through mailboxes or phishing detection tools to classify emails as malicious. A typical process looks like this:

1. Analysts check the email address, IP address, and URL of the phishing email against threat intelligence tools. They may check indicator reputation through threat sources, collect context from the security information and event management (SIEM) system, etc.
2. If the email has an attachment, that file is scanned with a malware analysis tool.
3. The security analysts manually check URL misrepresentation, host-domain distance, and other minor telltale signs that the mail may be malicious.
4. If the email is deemed malicious, the analyst opens a ticket, and the security team sends an email to the affected employee directing them to not access the phishing email again.
5. All endpoints in the system are scanned for instances of the malicious email.
6. The malicious indicators are added to blacklists so that web and email gateways automatically block them going forward.

These actions—often performed across multiple tools—are manual, repetitive, and prone to error. Security analysts face numerous challenges while responding to phishing attacks, such as:

- Having to handle a large number of attacks without burning out
- Switching between multiple screens to coordinate response
- Avoiding errors while completing mundane tasks
- Standardizing response and reporting procedures

In this lab, you will see how Cortex XSOAR will help you through those challenges.

Task 3: Generate your first incident

1. On the homepage first change the date range to All times.
2. Click on the **My Dashboard** tab towards the top to view the data on all incidents.
3. Go to the incidents page by pressing the bomb icon on XSOAR navigation bar on the left.
4. Click on the **New Incident** button on the top right of the screen.

On the Incidents page you will see a list of generated incidents with information about them such as type, severity, and status. This page is useful for getting an overview of all the incidents in your instance.

5. Select **Phishing Campaign** from the workshopscenario and click **Create new incident**.

By clicking **New Incident** you will be able to choose the scenario that best fits your needs. On the actual XSOAR platform you will have more scenarios available to you.

6. Click on the most recent incident **ID** number to make sure that the **Playbook** is Email Phishing.

Email Phishing Playbook Description: This is an automated playbook to investigate suspected Phishing attempts. It picks up the required information from the incident metadata as created by the mail listener.

After pressing **Create new Incident** your incident will be automatically generated. You can view more details about your incident by selecting the correlating ID number.

Task 4: Incident information ingested into XSOAR

When generating a new incident, Cortex XSOAR will ingest the email body, extract the indicators, and check for reputation.

1. Click on the Work Plan tab to observe the playbook in action.

On the Investigation tab you can see the Rasterized image of the phishing email, the email body, email basic information and the indicators.

2. After viewing the investigation page, navigate back to the Case Info page.

Task 5: Completing Playbook tasks manually

The Case Info page consists of an overview of the incident you selected. For now, you will focus on completing the tasks under the **Work Plan**. These tasks must be completed by someone on your team in order to continue the automated playbook.

1. Click on the first task under the **Work Plan** pane on the right.

For this incident there will be a total of 4 tasks you need to complete manually. Before marking the task "complete" you have the option to write a completion note that you can review later.

However, writing a completion note is unnecessary to continue. The note can consist of new findings or thoughts you would like to reference later.

2. Click **Mark Completed** on the first task to Manually inspect the email for anything suspicious.
3. Click **Mark Completed** on the second task to Assign and involve appropriate personnel.
4. Click **Mark Completed** on the third task to Assess severity.
5. Click **Mark Completed** on the fourth task to confirm Are the hostnames in the urls being misrepresented?.
6. Once you have completed the manual tasks, verify you see the following:

Task 6: Closing the investigation

Once you have completed the manual tasks you will see the following screens. This means the playbook has finished running and a verdict has been reached.

1. Click on the Work Plan tab.

You can now scroll through the entire playbook to view the individual tasks. You always have the option to go back and review the incident.

Great! You have closed your first investigation on XSOAR. The XSOAR platform gives you the ability to generate an incident report which enables you to capture investigation-specific data and share it with team members.

2. Generate an incident report by navigating back to the Case Info page, pressing the Actions button in the top right.
3. Click on Report.

Here you have the opportunity to preview the report or generate it. You can generate the report manually or use XSOAR'S Investigation summary template.