Technical documentation

This document contains high-level technical information about the use cases and the different components developed for the POC.

Some of this documentation has been developed using the SDK of the Cortex XSOAR solution. The SDK has made possible the generation of different markdown files for each one of the playbooks and automation developed. We used the generated markdown files to build this document.

Orquestación y respuesta ante incidentes de ciberseguridad

Sergio Sánchez Palma
Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
M1.749 - TFM-Seguridad empresarial

Manuel Jesús Mendoza Flores
Cristina Romero Tris

28/12/2021

Index

Use Cases

Acceso no autorizado (Fuerza bruta)

Playbook: Acceso no autorizado (Fuerza bruta)

The use case is designed to address brute force alerts from a SIEM trigger (Splunk). With the use of security events generated by the domain controller, an alert has been created that detects failed logins (more than 3 in one minute for the POC) of access to an "ftp" service that only allows access to users registered in the domain controller. The playbook will determine if the attack is coming from an existing user on the domain controller and if there is a possibility that the credential is leaked. If all conditions are met, the SOC will notify and request approval for an automatic password rotation. Otherwise, a notification will simply be sent to the SOC. As for the user, in case he/she has the phone number registered on the domain controller, the user is notified by mail and an SMS to the phone. Finally, the investigation is classified and closed.

Dependencies

This playbook uses the following sub-playbooks, integrations, and scripts.

Sub-playbooks

This playbook does not use any sub-playbooks.

Integrations

- SlackV3
  - Send messages and notifications to your Slack team.
- Have I Been Pwned? V2
  - Uses the Have I Been Pwned? service to check whether email addresses, domains, or usernames were compromised in previous breaches
- Mail Sender (New)
  - Send emails implemented in Python with embedded image support
- Twilio
  - send an SMS
- Active Directory Query v2
  - Active Directory Query integration enables you to access and manage Active Directory objects (users, contacts, and computers).

Automations

- GeneratePassword
  - This function generates a password and allows various parameters to customize the properties of the password depending on the use case (e.g. password complexity requirements). The default behavior is to generate a password of *random length* including all four character classes (upper, lower, digits, symbols) with at least five and at most ten characters per class.

- Set
  - Set a value in context under the key you entered.
- DeleteContext
  - Delete field from context.
- SetTiposCiberdelitosLegislacion
- TimeStampCompare
  - Compares a single timestamp to a list of timestamps.
- IncreaseIncidentSeverity
  - Optionally increases the incident severity to the new value if it is greater than the existing severity.

Commands

- TwilioSendSMS
  - send an SMS
- ad-get-user
  - Retrieves detailed information about a user account. The user can be specified by name, email address, or as an Active Directory Distinguished Name (DN). If no filter is specified, all users are returned.
- send-notification
  - The message content. When mentioning another slack user, make sure to do so in the following format: <@user_name>.
- send-mail
  - Send an email
- pwned-email
  - Checks if an email address was compromised.
- ad-set-new-password
  - Sets a new password for an Active Directory user. This command requires a secure connection (SSL, TLS).
- closeInvestigation
  - Close the current incident

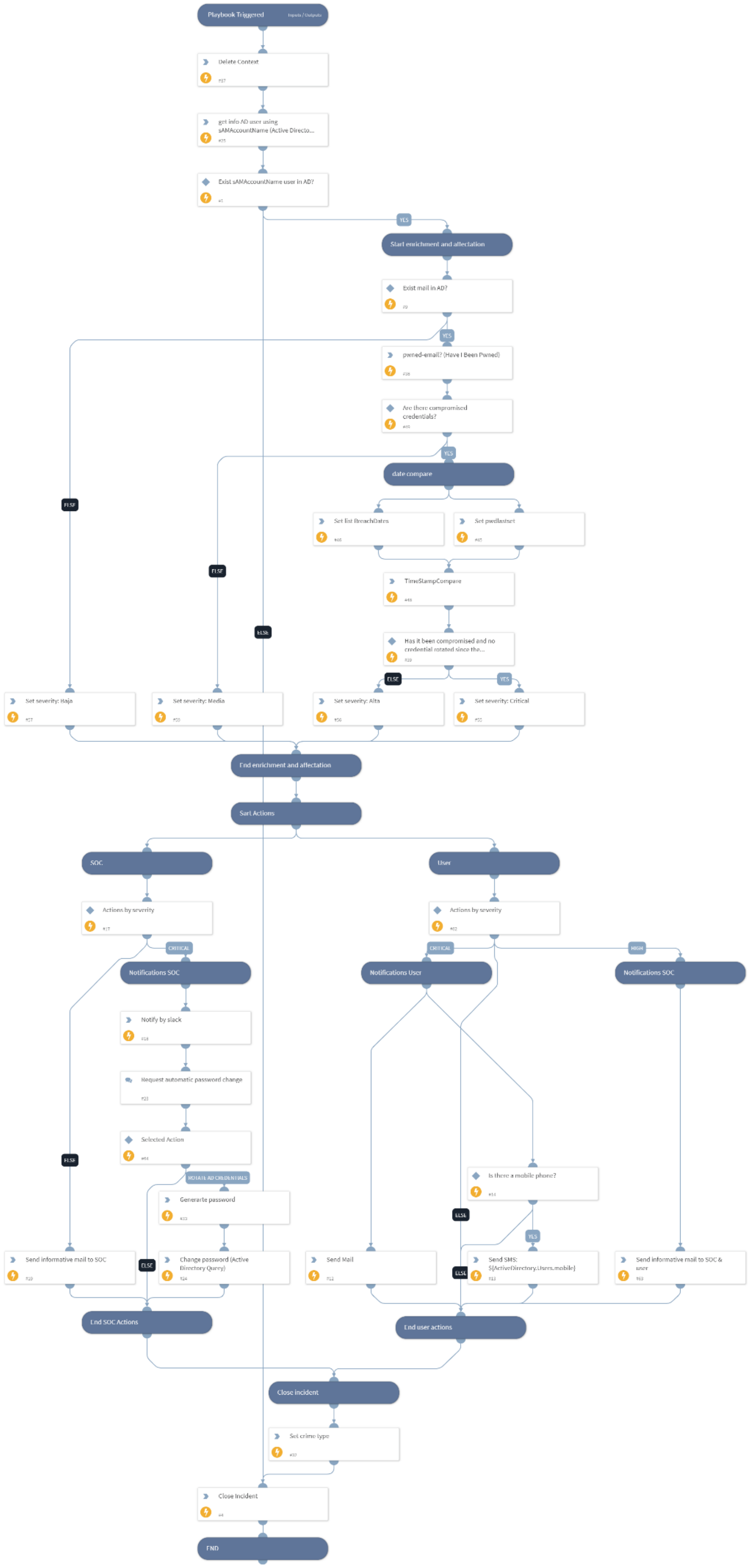
Playbook Inputs

There are no inputs for this playbook.

Playbook Outputs

There are no outputs for this playbook.

Playbook Image


Playbook Triggered
Inputs / Outputs
Delete Context
#37
get info AD user using sAMAccountName (Active Directo...
#25
Exist sAMAccountName user in AD?
#1
YES
Start enrichment and affectation
Exist mail in AD?
#9
YES
pwned-email? (Have I Been Pwned)
#36
Are there compromised credentials?
#49
YES
date compare
Set list BreachDates
#46
Set pwdlastset
#45
TimeStampCompare
#48
Has it been compromised and no credential rotated since the...
#39
ELSE
ELSE
ELSE
ELSE
YES
Set severity: Baja
#57
Set severity: Media
#59
Set severity: Alta
#56
Set severity: Critical
#55
End enrichment and affectation
Sart Actions
SOC
User
Actions by severity
#17
Actions by severity
#62
CRITICAL
CRITICAL
HIGH
Notifications SOC
Notifications User
Notifications SOC
Notify by slack
#18
Request automatic password change
#23
Selected Action
#64
ROTATE AD CREDENTIALS
Generarte password
#33
ELSE
ELSE
ELSE
ELSE
YES
Is there a mobile phone?
#14
Send informative mail to SOC
#19
Change password (Active Directory Query)
#24
Send Mail
#12
Send SMS: ${ActiveDirectory.Users.mobile}
#13
Send informative mail to SOC & user
#63
End SOC Actions
End user actions
Close incident
Set crime type
#37
Close Incident
#4
END

Malware (C2)

Playbook: Malware (C2)

The use case is designed to address malware C&C syslog alerts, which are sent directly to the SOAR tool for processing. In case that the origin machine is on an automatic action whitelist, the asset manager will be notified to acknowledge the event and the answer will be sent directly to the SOAR. In the case that the Origin machine is on an automatic action whitelist, the asset manager will be notified to expand on the event and service information. That response will be provided to the SOC service to determine the most appropriate actions to be taken. On the other hand, in case of a virtualized computer and not considered as a critical asset, the network cards will be automatically disconnected. In case of a critical asset, the SOC will be notified through a form, to determine the actions to be taken (computer shutdown and/or disconnection of network cards and/or snapshot). Finally, the investigation is classified and closed.

Dependencies

This playbook uses the following sub-playbooks, integrations, and scripts.

Sub-playbooks

This playbook does not use any sub-playbooks.

Integrations

- VMware
    - VMware vCenter server is a centralized management application that lets you manage virtual machines and ESXi hosts centrally.
- Mail Sender (New)
    - Send emails implemented in Python with embedded image support
- AnsibleVMware
    - Manage VMware vSphere Server, Guests, and ESXi Hosts
- SlackV3
    - Send messages and notifications to your Slack team

Automations

- DeleteContext
    - Delete field from context.
- Print
    - Prints text to war room (Markdown supported)
- SetTiposCiberdelitosLegislacion
- Set
    - Set a value in context under the key you entered.

Commands

- vmware-create-snapshot

    - Creates VM snapshot
- vmware-poweroff
    - Powers off a powered-on or suspended virtual machine.
- send-notification
    - Sends a message to a user, group, or channel.
- vmware-get-vms
    - Returns all virtual machines on a system.
- send-mail
    - Send an email
- vmware-guest-info
    - Gather info about a single VM
- closeInvestigation
    - Close the current incident
- vmware-change-nic-state
    - Changes the state of a VM NIC.

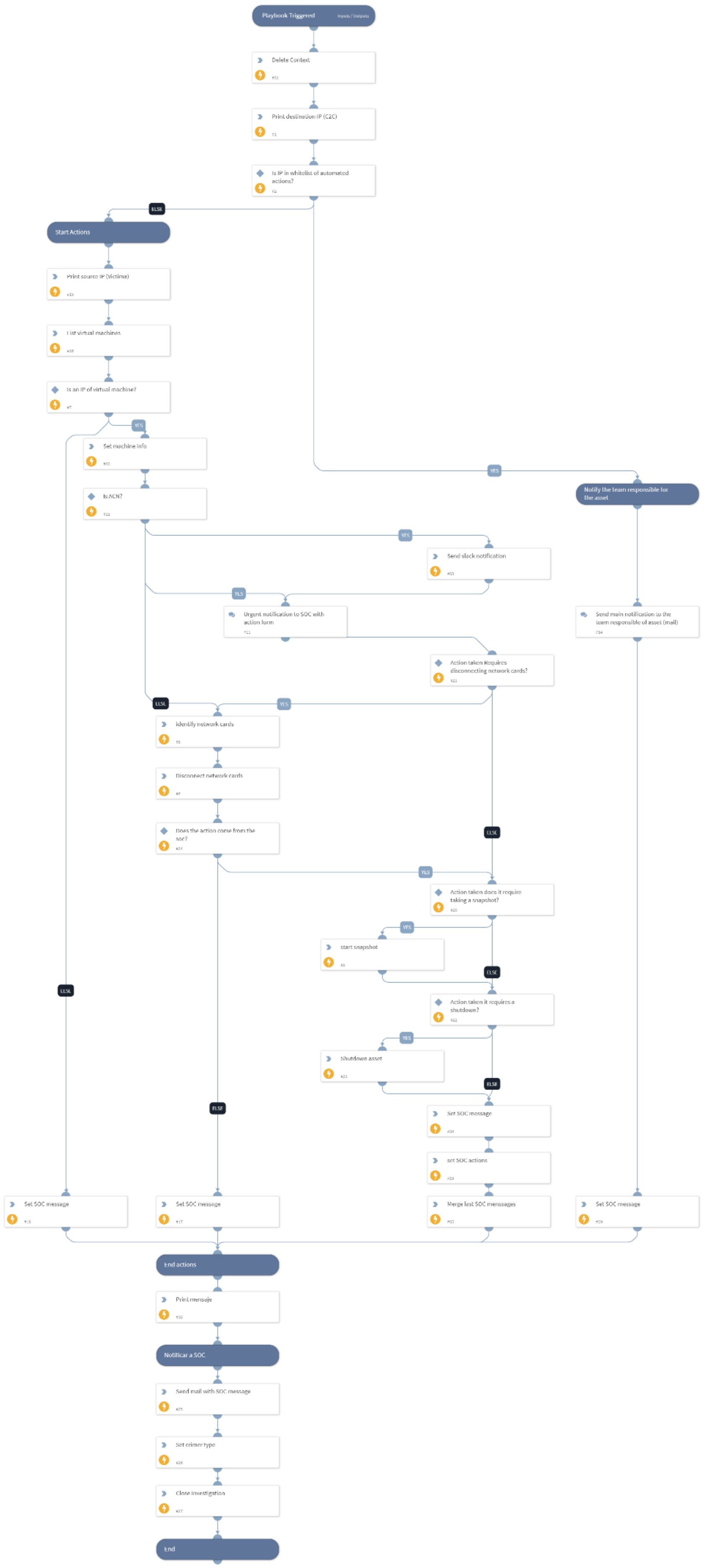
Playbook Inputs

There are no inputs for this playbook.

Playbook Outputs

There are no outputs for this playbook.

Playbook Image


Playbook Triggered
Inputs / Outputs
Delete Context
#31
Print destination IP (C2C)
#1
Is IP in whitelist of automated actions?
#2
ELSE
Start Actions
Print source IP (Victima)
#15
List virtual machines
#16
Is an IP of virtual machine?
#7
YES
Set machine info
#30
Is ACN?
#32
YES
Notify the team responsible for the asset
YES
Send slack notification
#33
YES
Urgent notification to SOC with action form
#11
Send main notification to the team responsible of asset (mail)
#14
Action taken Requires disconnecting network cards?
#23
ELSE
YES
identify network cards
#6
Disconnect network cards
#8
Does the action come from the soc?
#24
ELSE
YES
Action taken does it require taking a snapshot?
#20
YES
start snapshot
#5
ELSE
Action taken it requires a shutdown?
#22
YES
Shutdown asset
#21
ELSE
ELSE
ELSE
Set SOC message
#34
set SOC actions
#19
Set SOC message
#18
Set SOC message
#17
Merge last SOC menssages
#35
Set SOC message
#29
End actions
Print mensaje
#36
Notificar a SOC
Send mail with SOC message
#25
Set crimer type
#28
Close investigation
#27
End

Robo de credenciales (Data Leak)

Playbook: Robo de credenciales (Data Leak)

The use case is designed to address leaked credentials of existing users in AD from an e-mail and not rotated before the leak date. The "have I been pwned" service will be used to obtain this information and also the information on the domain controller. In case there is evidence of a potential breach, a separate incident is opened in the SOAR tool for analysis.

Dependencies

This playbook uses the following sub-playbooks, integrations, and scripts.

Sub-playbooks

This playbook does not use any sub-playbooks.

Integrations

- Active Directory Query v2
    - Active Directory Query integration enables you to access and manage Active Directory objects (users, contacts, and computers).
- Have I Been Pwned? V2
    - Uses the Have I Been Pwned? service to check whether email addresses, domains, or usernames were compromised in previous breaches.

Automations

- Set
    - Set a value in context under the key you entered.
- SearchIncidentsV2
    - Searches Demisto incidents.
- DeleteContext
    - Delete field from context.
- TimeStampCompare
    - Compares a single timestamp to a list of timestamps.

Commands

- createNewIncident
    - Create a new incident
- pwned-email
    - Checks if an email address was compromised.
- ad-get-user
    - Retrieves detailed information about a user account. The user can be specified by name, email address, or as an Active Directory Distinguished Name (DN). If no filter is specified, all users are returned.

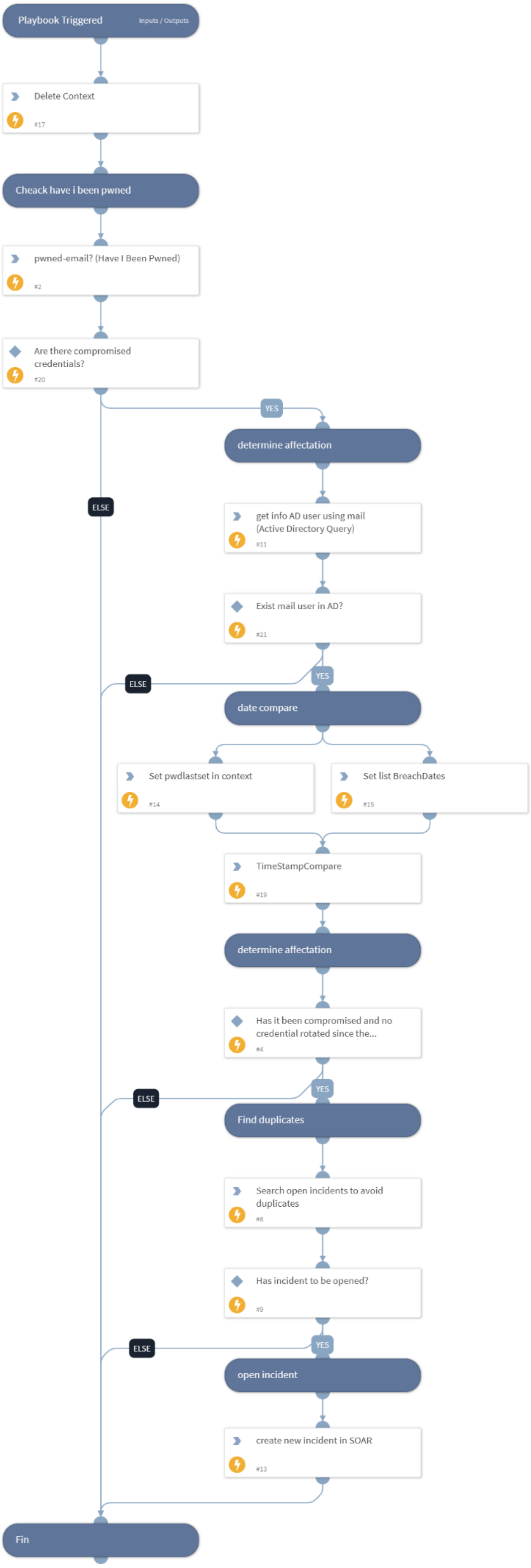
Playbook Inputs

Name	Description	Default Value	Required
mail	Insert email to verify		Required

Playbook Outputs

There are no outputs for this playbook.

Playbook Image


Playbook Triggered
Inputs / Outputs
Delete Context
#17
Cheack have i been pwned
pwned-email? (Have I Been Pwned)
#2
Are there compromised credentials?
#20
YES
ELSE
determine affectation
get info AD user using mail (Active Directory Query)
#11
Exist mail user in AD?
#21
ELSE
YES
date compare
Set pwdlastset in context
#14
Set list BreachDates
#15
TimeStampCompare
#19
determine affectation
Has it been compromised and no credential rotated since the...
#4
ELSE
YES
Find duplicates
Search open incidents to avoid duplicates
#8
Has incident to be opened?
#9
ELSE
YES
open incident
create new incident in SOAR
#13
Fin

Playbook: Robo de credenciales (Data Leak) - email

The playbook's objective is to capture all detected emails in the body of an email message into a SOAR-managed mailbox. The playbook will then send them as an input to the credentials leak playbook for analysis and investigation if necessary.

Dependencies

This playbook uses the following sub-playbooks, integrations, and scripts.

Sub-playbooks

- Robo de Credenciales (Data Leak) - Core

Integrations

This playbook does not use any integrations.

Automations

- Print
  - Prints text to war room (Markdown supported)

Commands

- closeInvestigation
  - Close the current incident
- extractIndicators
  - Extract indicators from a text-based file. Indicators that can be extracted: * IP * Domain * URL * File Hash * Email Address

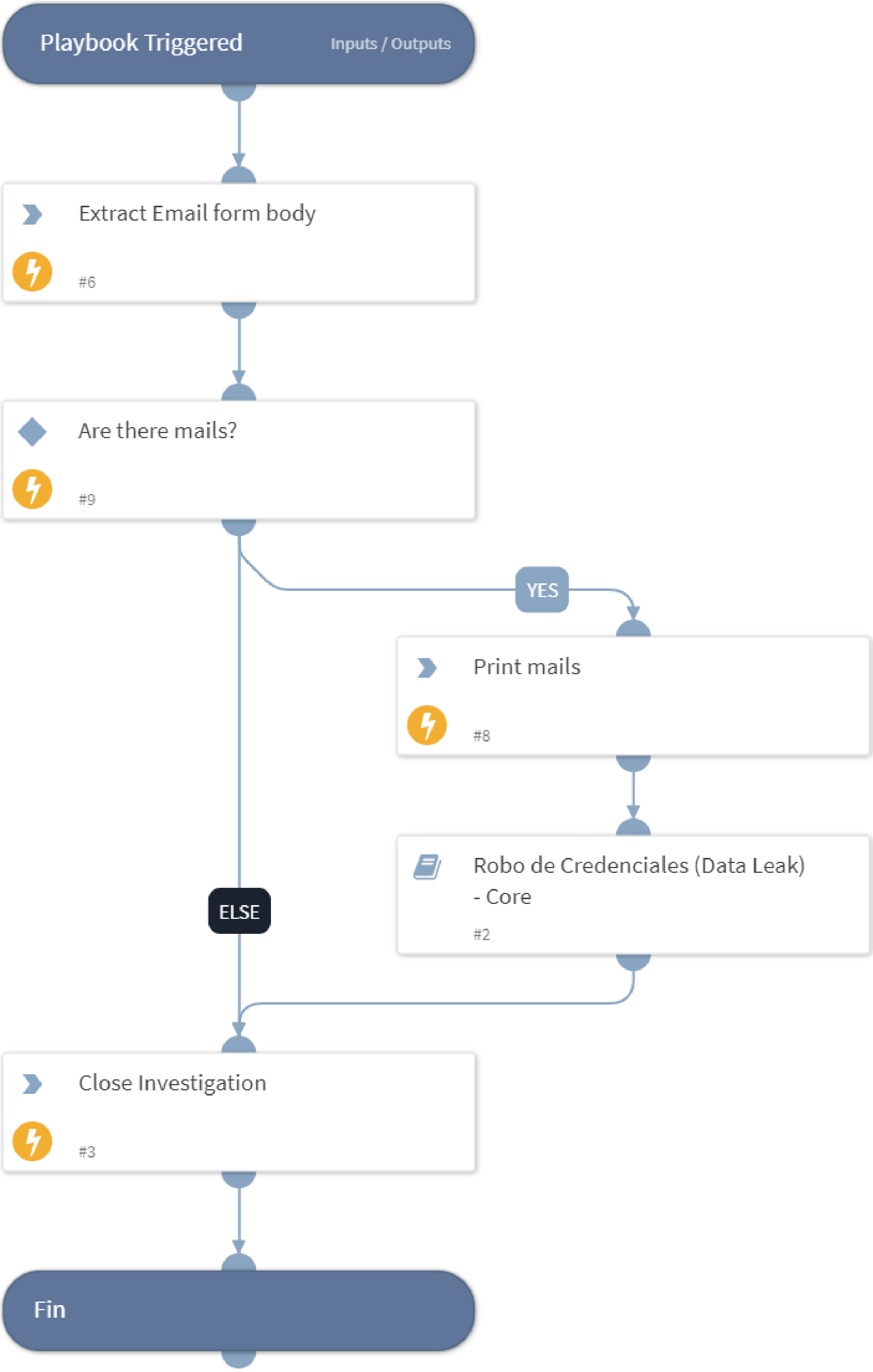
Playbook Inputs

There are no inputs for this playbook.

Playbook Outputs

There are no outputs for this playbook.

Playbook Image


Playbook Triggered
Inputs / Outputs
Extract Email form body
#6
Are there mails?
#9
YES
Print mails
#8
Robo de Credenciales (Data Leak) - Core
#2
ELSE
Close Investigation
#3
Fin

Playbook: Robo de credenciales (Data Leak) - job

The objective of the playbook is to capture all users from AD VIP groups and domain administrators on a scheduled basis. The playbook will then send them as an input to the credentials leak playbook for analysis and investigation if necessary.

Dependencies

This playbook uses the following sub-playbooks, integrations, and scripts.

Sub-playbooks

- Robo de Credenciales (Data Leak) - Core

Integrations

This playbook does not use any integrations.

Automations

- Print
  - Prints text to war room (Markdown supported)
- Set
  - Set a value in context under the key you entered.

Commands

- closeInvestigation
  - Close the current incident
- ad-get-group-members
  - Retrieves the list of users or computers that are members of the specified group.

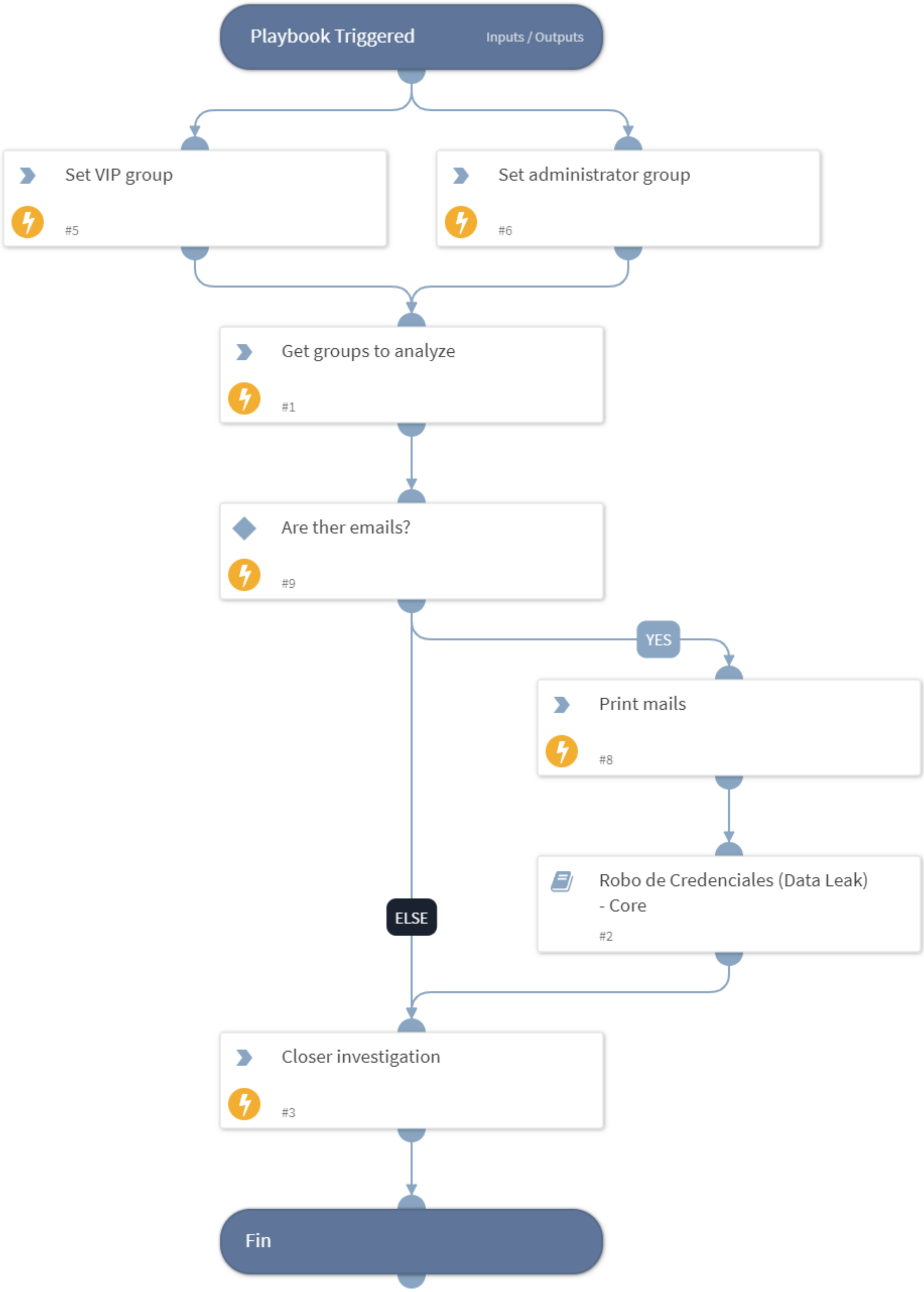
Playbook Inputs

There are no inputs for this playbook.

Playbook Outputs

There are no outputs for this playbook.

Playbook Image


Playbook Triggered
Inputs / Outputs
Set VIP group
#5
Set administrator group
#6
Get groups to analyze
#1
Are ther emails?
#9
YES
Print mails
#8
Robo de Credenciales (Data Leak) - Core
#2
ELSE
Closer investigation
#3
Fin

Playbook: Robo de credenciales (Data Leak) - manual

The objective of the playbook is to capture all emails detected in the self-contained form in this playbook. The playbook will then send them as an input to the credentials leak playbook for analysis and investigation if necessary.

Dependencies

This playbook uses the following sub-playbooks, integrations, and scripts.

Sub-playbooks

- Robo de Credenciales (Data Leak) - Core

Integrations

This playbook does not use any integrations.

Automations

- Print:
    - Prints text to war room (Markdown supported)

Commands

- closeInvestigation
    - Close the current incident
- extractIndicators
    - Extract indicators from a text-based file. Indicators that can be extracted: * IP * Domain * URL * File Hash * Email Address

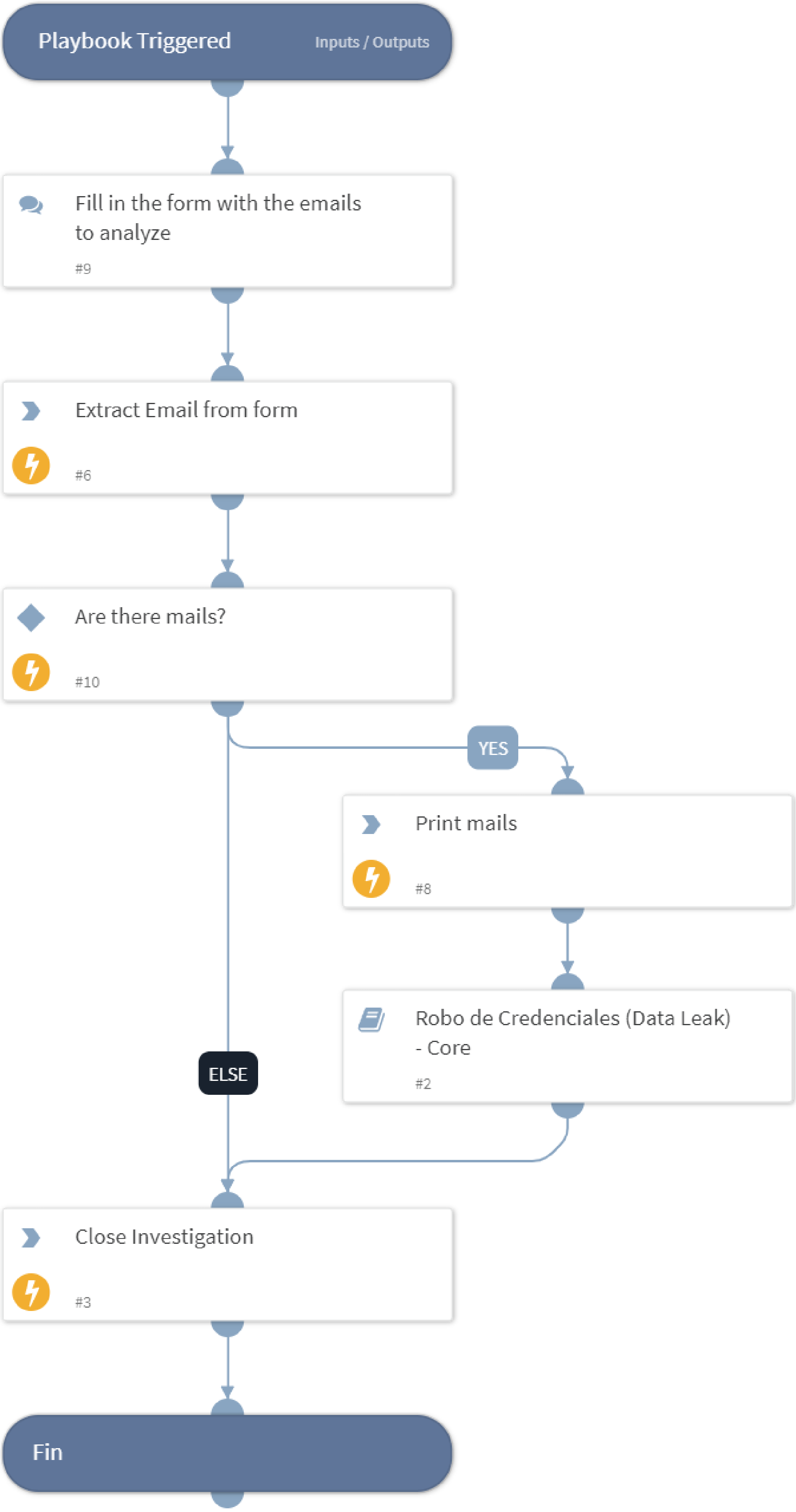
Playbook Inputs

There are no inputs for this playbook.

Playbook Outputs

There are no outputs for this playbook.

Playbook Image


Playbook Triggered
Inputs / Outputs
Fill in the form with the emails to analyze
#9
Extract Email from form
#6
Are there mails?
#10
YES
Print mails
#8
Robo de Credenciales (Data Leak) - Core
#2
ELSE
Close Investigation
#3
Fin

Automations

Automation: SetTiposCiberdelitosLegislacion

Determine type of crime

Script Data

Name	Description
Script Type	python3
Tags	Utility

Inputs

Argument Name	Description
tipoDelito	Set the name of the incident custom field of type of crime

Outputs

There are no outputs for this script.

Incident fields

Incident

Field name	type	description	Incident type
Count	Short text	Number of alert events	Fuerza bruta
Action	Short text	Define actions to take	All types
Tipos ciberdelitos segun legislacion	Single select	Crime type classifier	All types

Incident Types

Incident

Name	playbook	description
C2	Malware (C2) - core	Malware use cases
Fuerza Bruta	Acceso no autorizado (Fuerza bruta) - core	Brute force use cases
Data Leak		Data Leak use cases

Data Leak - email	Robo de Credenciales (Data Leak) - email	Trigger data leak uses case whith email
Data Leak - Ticket		Data Leak investigation

Classifiers & mappers

Incident

name	type	description	integration
Splunk - Fuerza bruta	Classifier	Classifies Splunk events.	SplunkPy
Splunk - Fuerza bruta	Incoming Mapper	Maps Splunk logs fields.	SplunkPy
Syslog - Malware	Classifier	Classifies syslog events.	Syslog
Syslog - Malware	Incoming Mapper	Maps syslog logs fields.	Syslog
Mail Listener - Data Leak	Classifier	Classifies email messages.	Mail Listener v2
Mail Listener - Data Leak	Incoming Mapper	Maps incoming email messages fields.	Mail Listener v2

Concepts

Playbooks

Playbooks are self-contained, fully documented prescriptive procedures that query, analyze, and take action based on the gathered results. Playbooks enable you to organize and document security monitoring, orchestration, and response activities.

A key feature of Playbooks is the ability to structure and automate security responses, which were previously handled manually. You can reuse Playbook tasks as building blocks for new playbooks, saving you time and streamlining knowledge retention.

Integrations

Third-party tools and services that the SOAR platform orchestrates and automates SOC operations.

Automations

The Automation section is where you manage, create, and modify scripts. These scripts perform a specific action and are comprised of commands associated with an integration. Scripts are used as part of tasks, which are used in playbooks and commands. Scripts can access all information, including access to incidents, investigations, share data to the analyst,

Commands

Enable you to perform actions specific to an integration. For example, you can take a snapshot.

Incident fields

Incident Fields accept or populate incident data coming from incidents.

Incident types

Incident types are used to classify the events that are ingested into the SOAR system. Each incident type can be configured to work with a dedicated playbook, which can either run automatically when an event is ingested or can be triggered separately at a later point.

Inputs and Outputs

Depending on the task type that you select, and the script that you are running, your playbook task has inputs and outputs.

Inputs are data pieces that are present in the playbook or task. The inputs are often manipulated or enriched and they produce outputs. Outputs are objects whose entries will serve the tasks throughout the playbook, and they can be derived from the result of a task or command.

References

https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-5/cortex-xsoar-admin/cortex-xsoar-overview/cortex-xsoar-concepts.html

https://github.com/demisto/demisto-sdk