Automate IOA alerts to shared mailbox

Fusion SOAR workflows

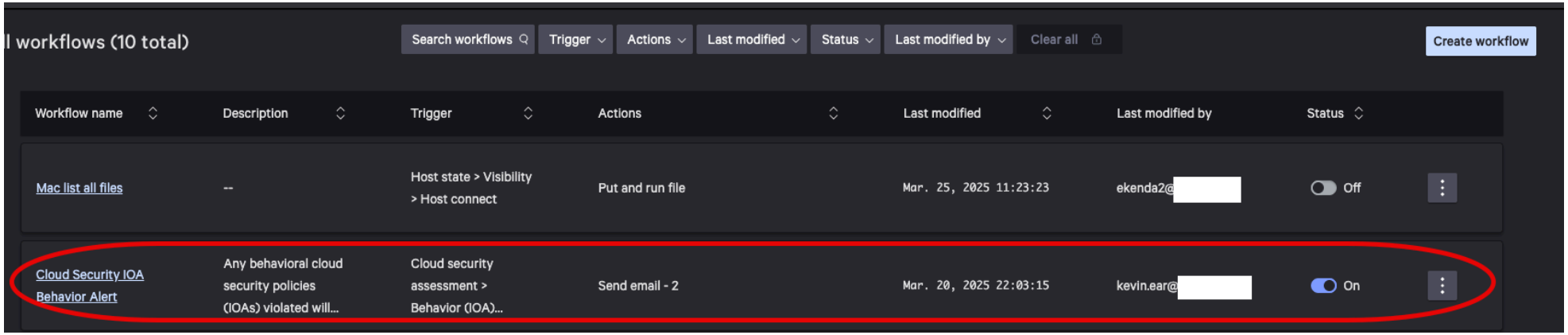
Purpose: Falcon Fusion SOAR workflows help streamline analyst workflows by automating actions around specific and complex scenarios. We can create workflows to define the actions you want Falcon to perform in response to incidents, detections, policies, cloud security findings, and more.

Use Case: Streamline investigation and remediation by automating alerts from Falcon to send emails to our Digital Cloud Security Mailbox each time a IOA behavioral policy is triggered. Instead of manually navigating to the Cloud Security Dashboard and clicking on each alert, SOAR workflows will consolidate the required data and provide you with the necessary information to accelerate investigation and remediation.

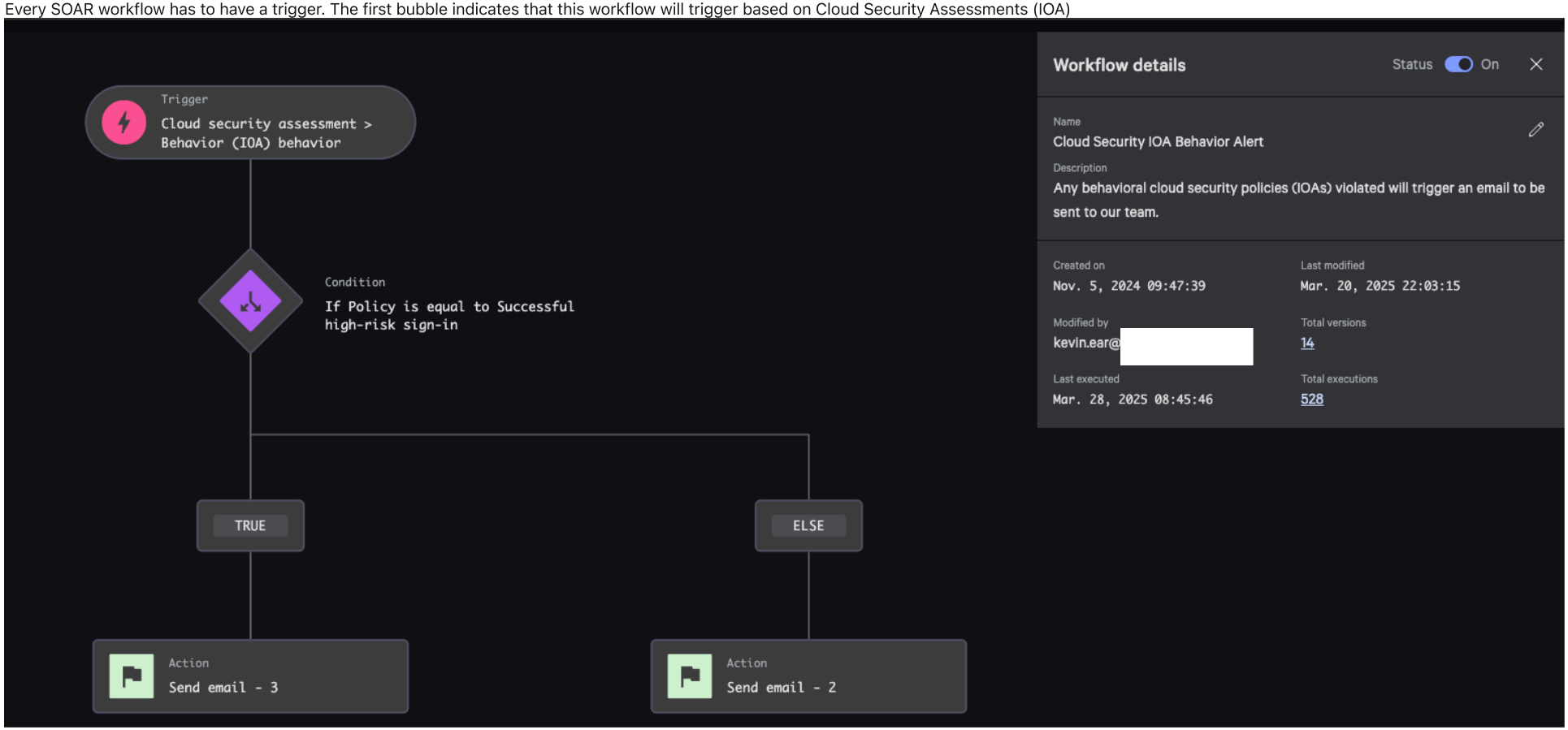
Locating the specific policy that is configured to automate IOA alerts to send to our shared mailbox

Next-Gen SIEM > Fusion SOAR > Workflows

1. The specific workflow is called "Cloud Security IOA Behavior Alert"



2. Every SOAR workflow has to have a trigger. The first bubble indicates that this workflow will trigger based on Cloud Security Assessments (IOA)



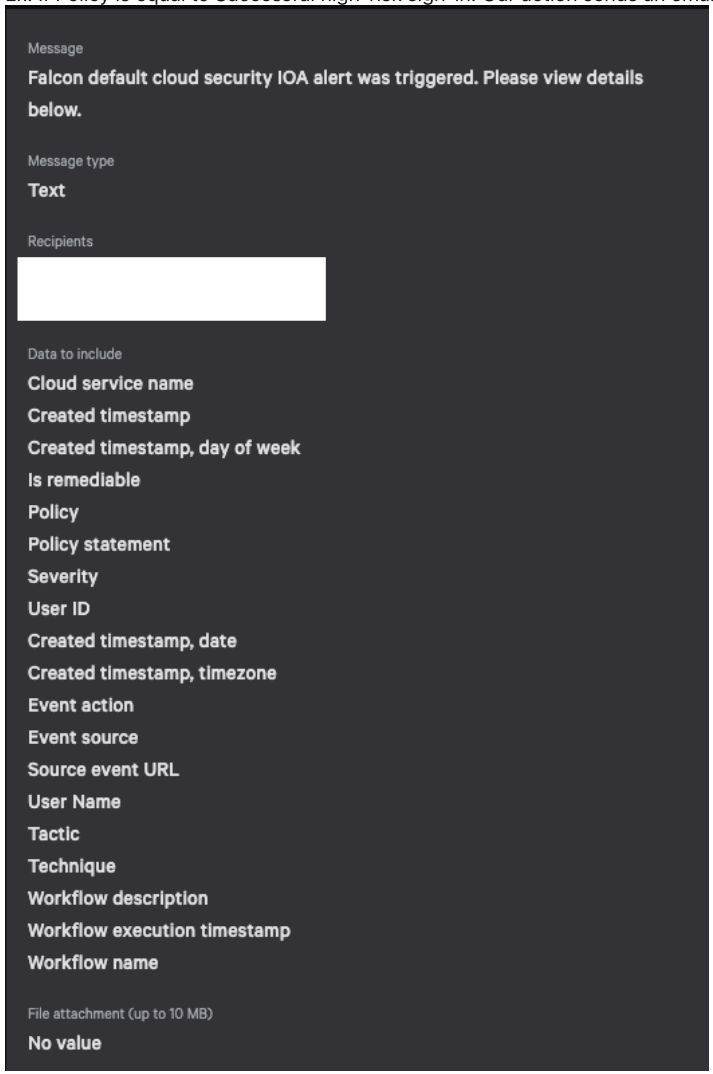
3. **Routing specific policy alerts to another team**

- If we want to send alerts pertaining to a specific policy to another team, we can leverage "Conditions," and we will be given parameters/attributes to select.
- Select "Policy" parameter and select which policy you want.

4. Based on our condition, we need to configure an action. Since our end goal is to send an email, select/search for "Send email"

- When you select send email, you will be required to enter the email addresses of the recipients and select the data you want to include in the email.

Ex: If Policy is equal to Successful high-risk sign-in. Our action sends an email to infosec-alerts@



5. Else statement (If condition is NOT true)

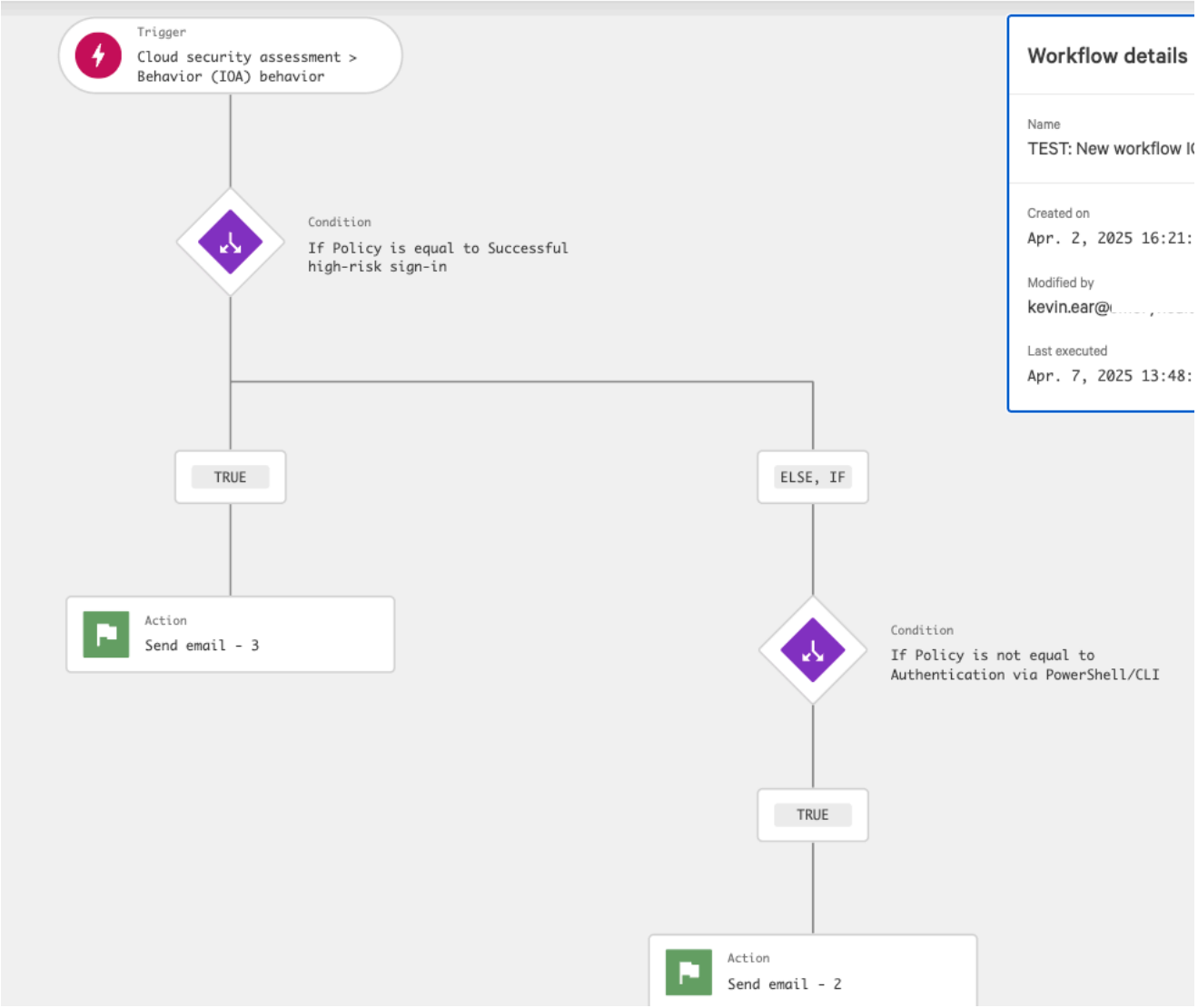
- If the condition, If Policy is equal to Successful high-risk sign-in, is not true, we will send all the other IOA alerts to e

New Workflow:

1. Trigger Cloud Security Assessment > Behavior (IOA) means this workflow will trigger when there is an indicator of alert policy triggered
2. Conditions: 1st condition "If policy is equal to Successful High-Risk Sign In", send these alerts to Elliot's team
3. Else, if:

- Else send all the other IOA alerts to
- There is "Else, If" because we also want the ability to keep the policy "If Policy is not equal to Authentication via PowerShell/CLI" enabled and see those alerts on the Cloud Security Dashboard but prevent it from going to our ED Cloud Security mailbox. Note: You can see the policy is still enabled in Falcon.

Note: This new workflow will be beneficial for us in the event we need to exclude other IOA alerts from going to our shared mailbox and keep the policy enabled.


Trigger
Cloud security assessment > Behavior (IOA) behavior
Condition
If Policy is equal to Successful high-risk sign-in
TRUE
ELSE, IF
Action
Send email - 3
Condition
If Policy is not equal to Authentication via PowerShell/CLI
TRUE
Action
Send email - 2
Workflow details
Name
TEST: New workflow I
Created on
Apr. 2, 2025 16:21:
Modified by
kevin.ear@
Last executed
Apr. 7, 2025 13:48: