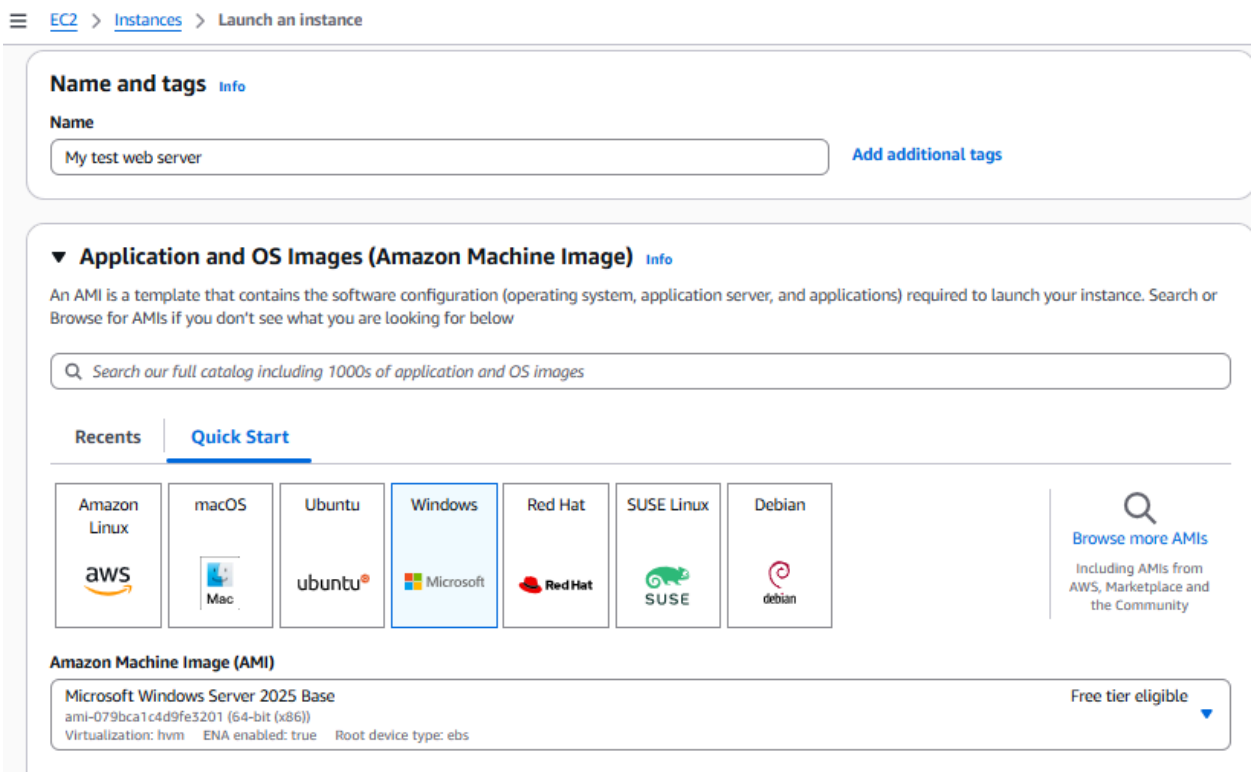
A.I and SIEM Integration

In this project, I will send Windows Server 2025 logs from an Elastic instance to the Tines automation tool to generate alerts and improve rules for the SIEM.

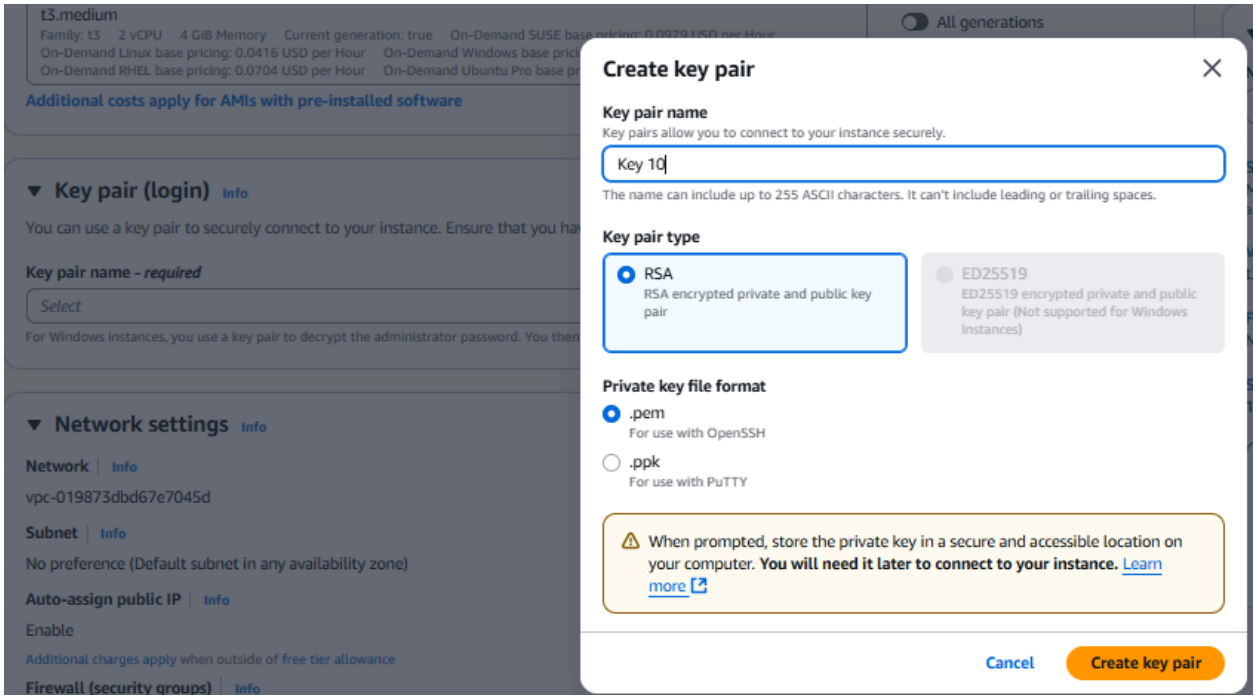
- The first step is to log into the AWS account to set up an EC2 instance.

- Type in EC2 in the search. Then on left column select “Instances” than click “Launch Instances” on right
- Name the instance and select “Windows” and “Microsoft Windows Server 2025”

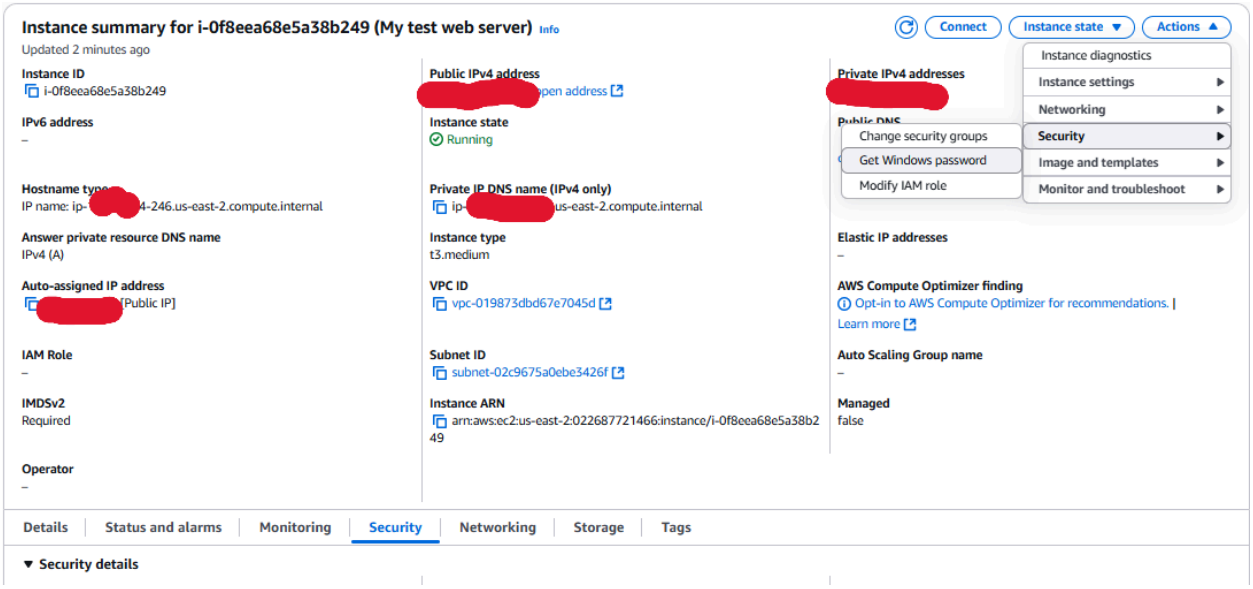


- Next select 4-8 gb of memory so the machine runs smoother (there is a small cost for this)

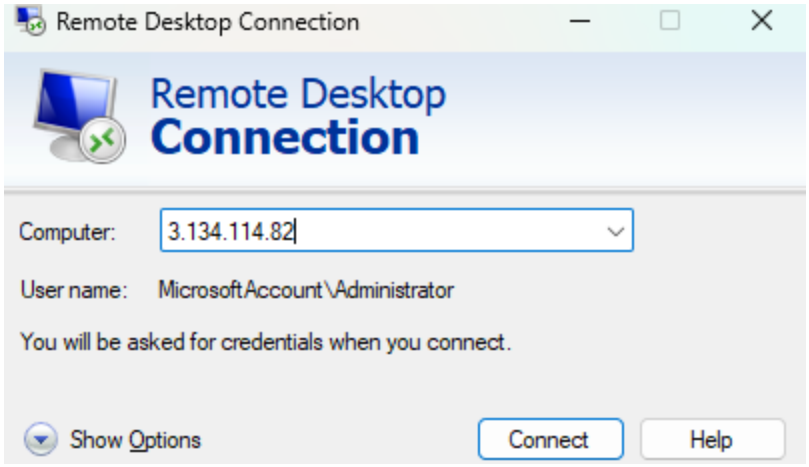
- The “Create New Key Pair” so we can connect to the instance

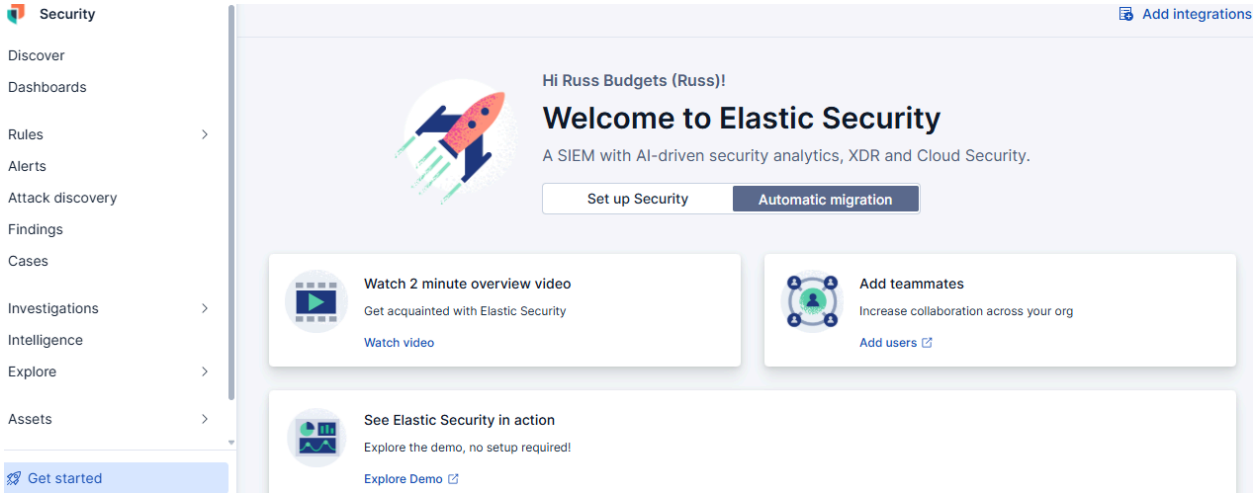


- Next, select “Create Security Group” then to allow RDP traffic and change the IP to your local IP instead of “Anywhere”.
- Then select “Launch Instance”
- Once it’s running, click the instance ID. Select the “Security” tab and one the right side select “Actions” then “Security” and “Get windows password”

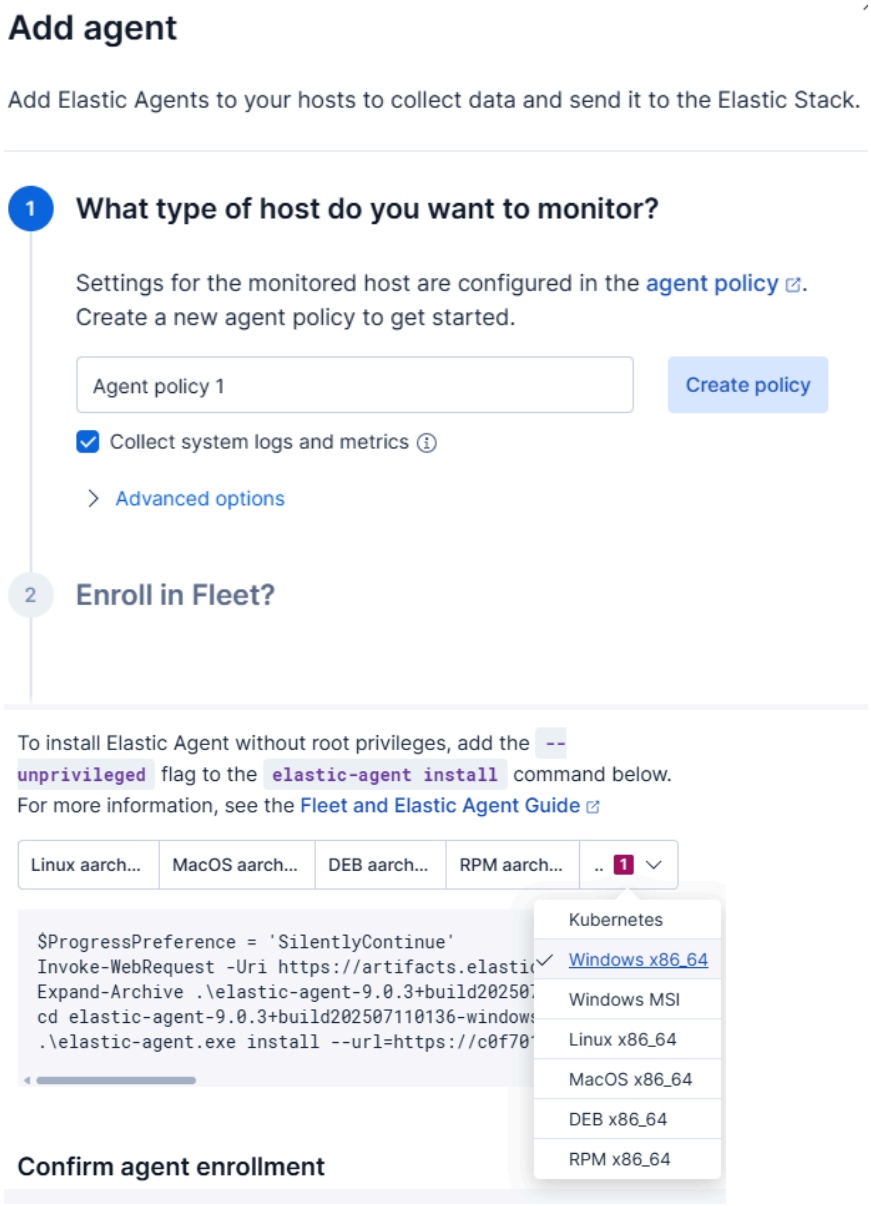


- Next upload the key pair file downloaded in the earlier step. Then click "Decrypt Password”.
- Copy the username and password showing at prompt window to use to RDP into the server.
- Open RDP and add the public IP of the instance

- 

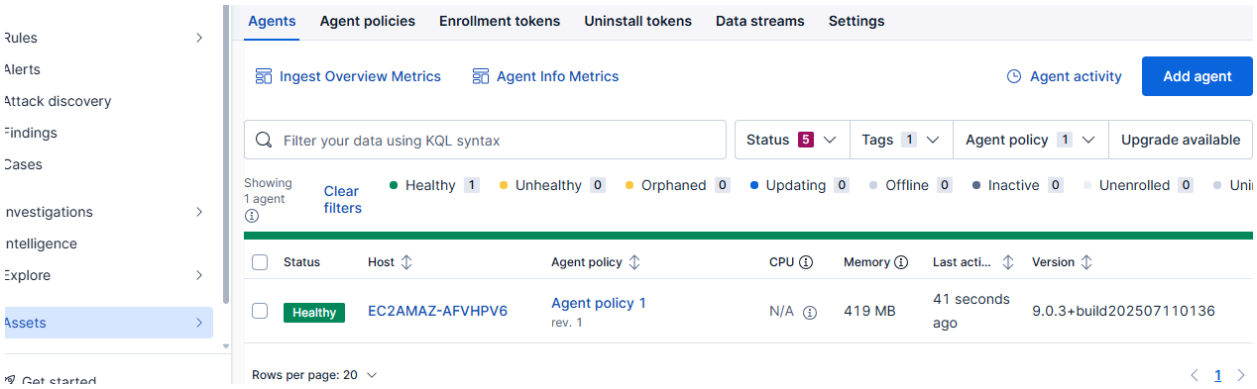
- The username will be Administrator and the password, whatever it gave at the prompt.
- Next, log into Elastic using gmail and deploy a cloud SIEM instance
- 

- On the left side select, “Assets”, then “Agents” then “Add Agents”.
- Name the policy and “Create Policy”. Then scroll down and select WIndows and copy the script.

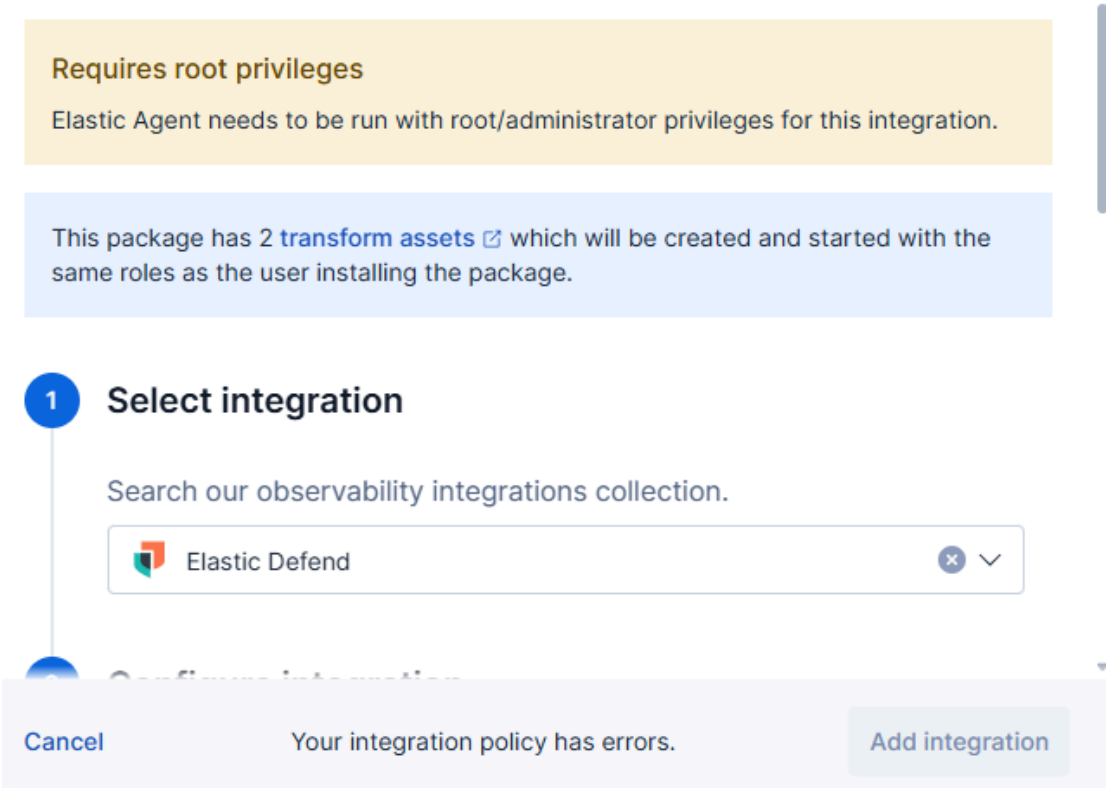


-
-
- Then go back to your RDP server instance and paste the script in terminal.
- After a few minutes, the terminal will verify you want to install Elasic agent.

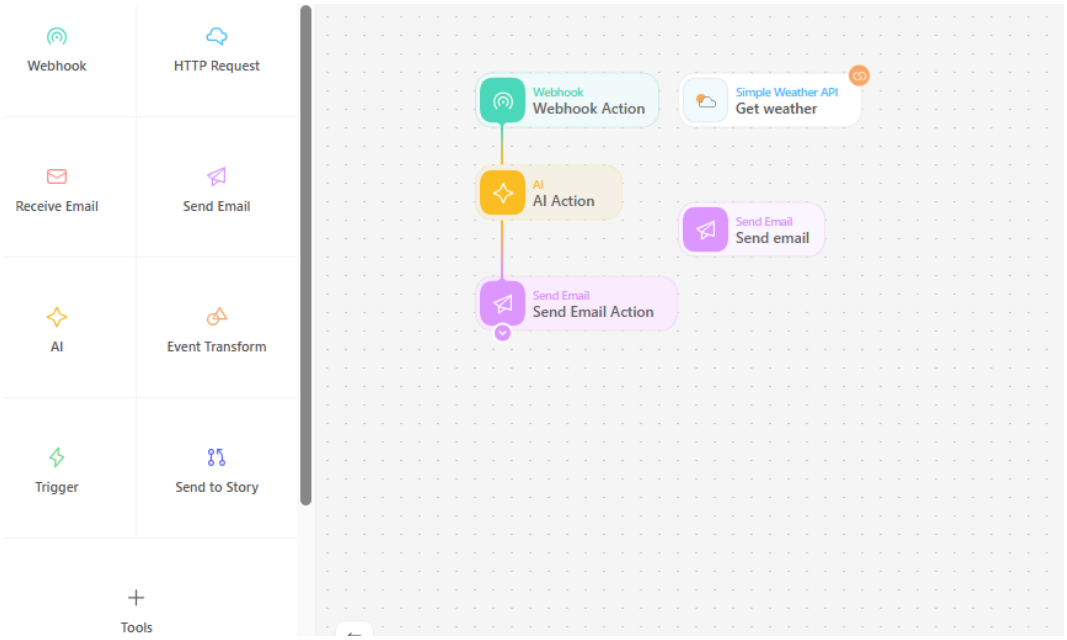
- After it installs, it will begin sending data to Elastic and can be viewed in “Assets” and “agents”



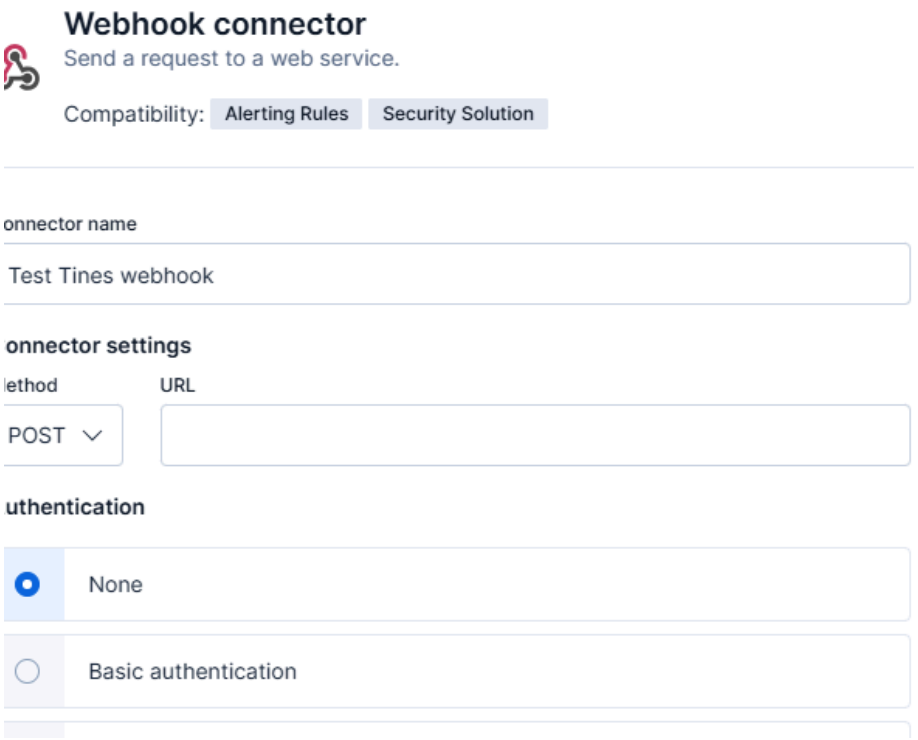
- Next, select the “Agent Policy 1” then “Add integration” button. Add “Elastic Defend”. Add a name and keep it as “traditional Endpoints” and “Complete EDR”



-
- Now log into Tines using gmail and set up an automation workflow. Drag the webhook, AI, and send email thumbnails into workflow and click dropdown arrow to draw line between them.
-

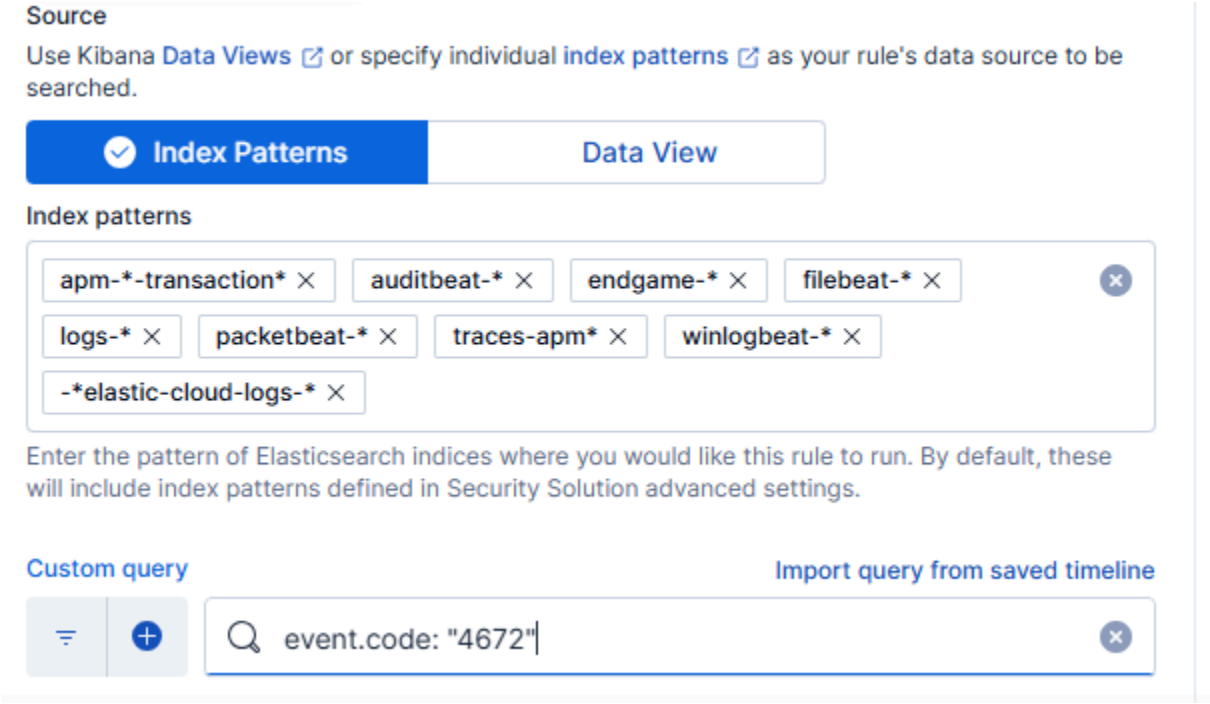


-
- Back in Elastic, select “Project Settings” Stack Management” and “Connectors”. Select to “Create Connector”
- Search for Webhook. Add title and select “none” for authentication

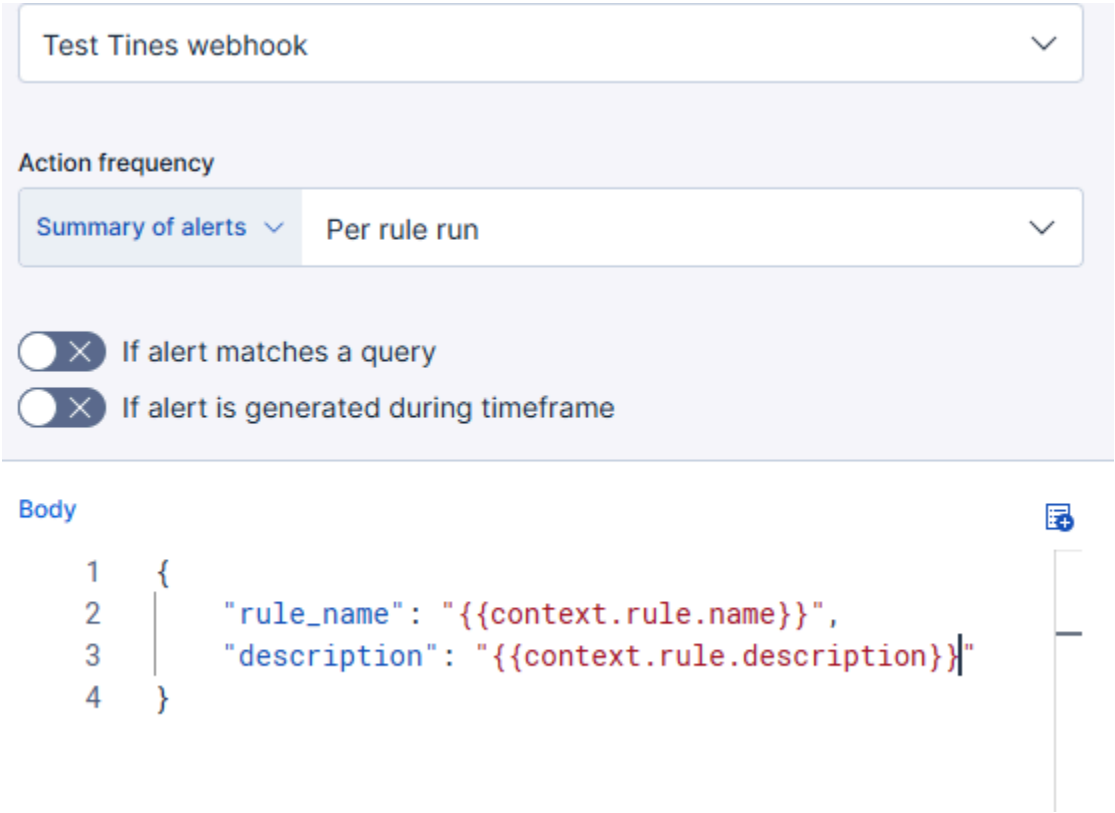


-
- Back in Tines, click the webhook thumbnail and copy the “Webhook URL” to paste into Elastic Connector.
- Now, in Elastic, we need to create a rule to detect malicious activity of an admin account being logged into.
- On the left select “Rules”, “Detection Rules” and select “custom query”

- For this rule we will add windows event code “4672”. All other settings can stay the same

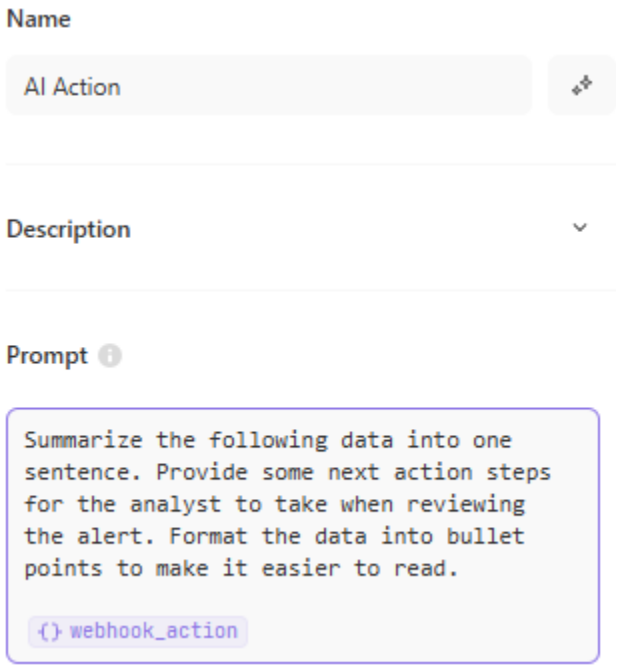


- Add name and description as “Test admin rule”. Under “Rule actions” select “webhook”. Then add the following:



- Then, “Create and enable rule”

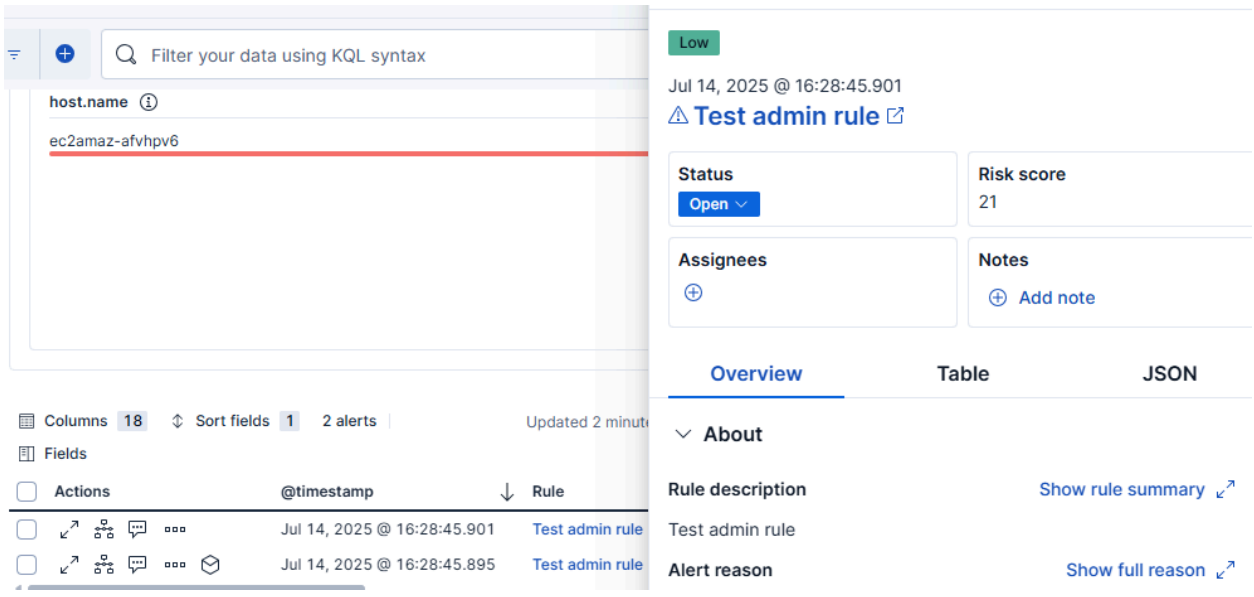
- In Tines, select the AI bubble and add the following to the prompt. Use the “+” to add the “webhook_action”



-
- Also, click to update the “send email” settings. Also, in the body email field, add summarize_webhook_data.

TESTING

- To test the rules, log out of the RDP connection, and back in using administrator. Then go into Elastic and click “alerts” to verify it detected an event.



-

Russ Geisler <mail@tines.io> 4:58 PM (7 minutes ago)

to me

A new event has been detected.

-