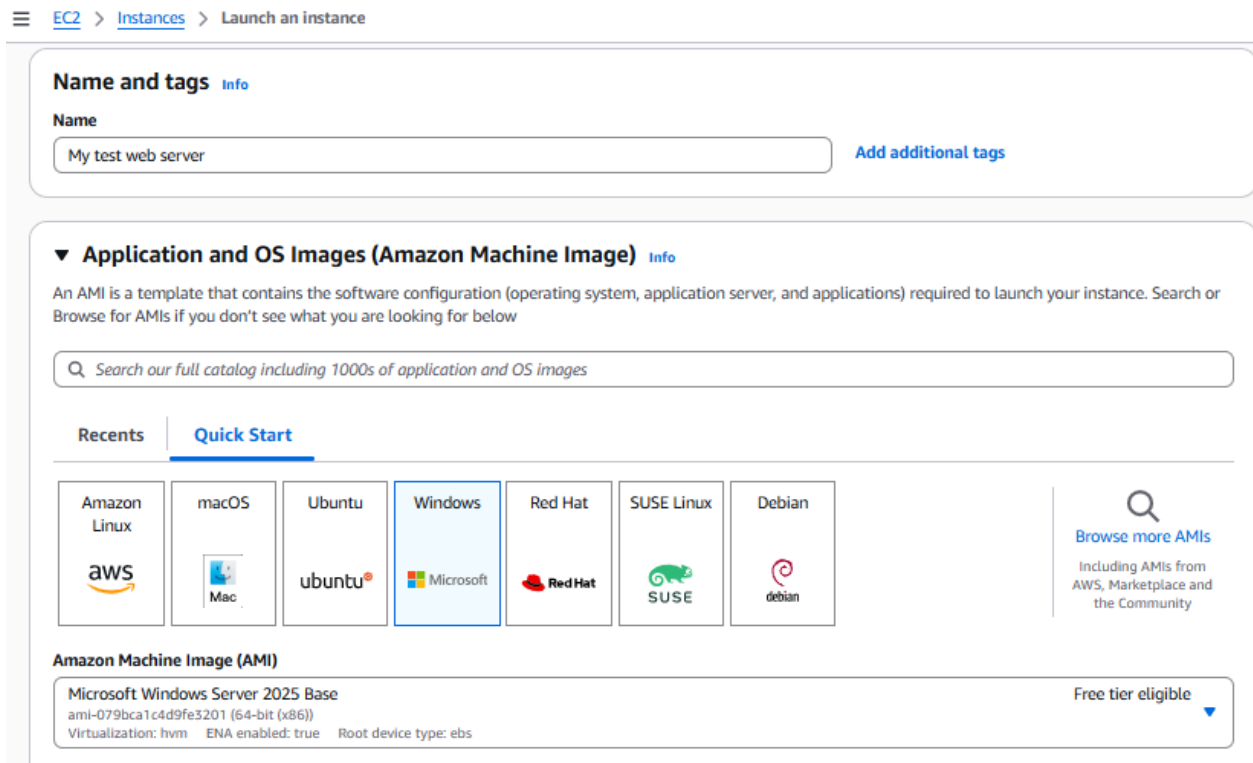


A.I and SIEM Integration

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

Create key pair

Key pair name
Key pairs allow you to connect to your instance securely.

Key 10

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☒ RSA
RSA encrypted private and public key pair

☐ ED25519
ED25519 encrypted private and public key pair (Not supported for Windows instances)

Private key file format

☒ .pem
For use with OpenSSH

☐ .ppk
For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. [Learn more](#)

Cancel Create key pair

- 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 on the right side select “Actions” then “Security” and “Get windows password”

Instance summary for i-0f8eea68e5a38b249 (My test web server)

Updated 2 minutes ago

Instance ID
i-0f8eea68e5a38b249

IPv6 address
-

Hostname type
IP name: ip-10-0-246-us-east-2.compute.internal

Answer private resource DNS name
IPv4 (A)

Auto-assigned IP address
[Redacted] (Public IP)

IAM Role
-

IMDSv2
Required

Operator
-

Public IPv4 address
[Redacted] [Open address](#)

Instance state
Running

Private IP DNS name (IPv4 only)
ip-[Redacted]-us-east-2.compute.internal

Instance type
t3.medium

VPC ID
vpc-019873dbd67e7045d

Subnet ID
subnet-02c9675a0be3426f

Instance ARN
arn:aws:ec2:us-east-2:022687721466:instance/i-0f8eea68e5a38b249

Private IPv4 addresses
[Redacted]

Public DNS
[Redacted]

Elastic IP addresses
-

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | [Learn more](#)

Auto Scaling Group name
-

Managed
false

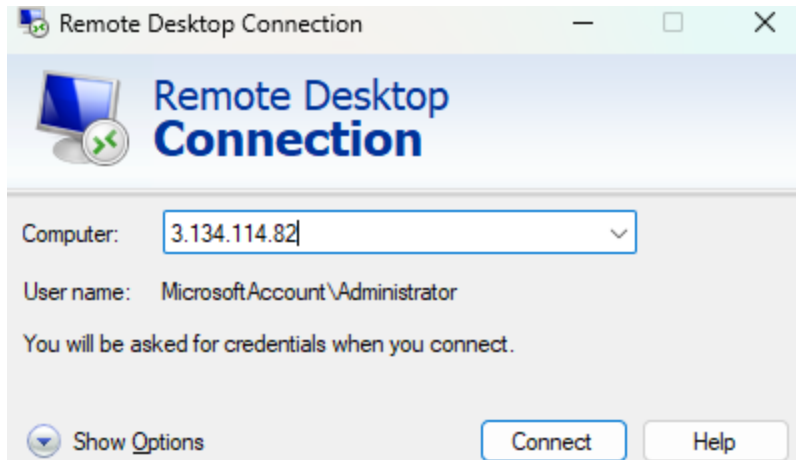
Actions

- Instance diagnostics
- Instance settings
- Networking
- Security
- Image and templates
- Monitor and troubleshoot

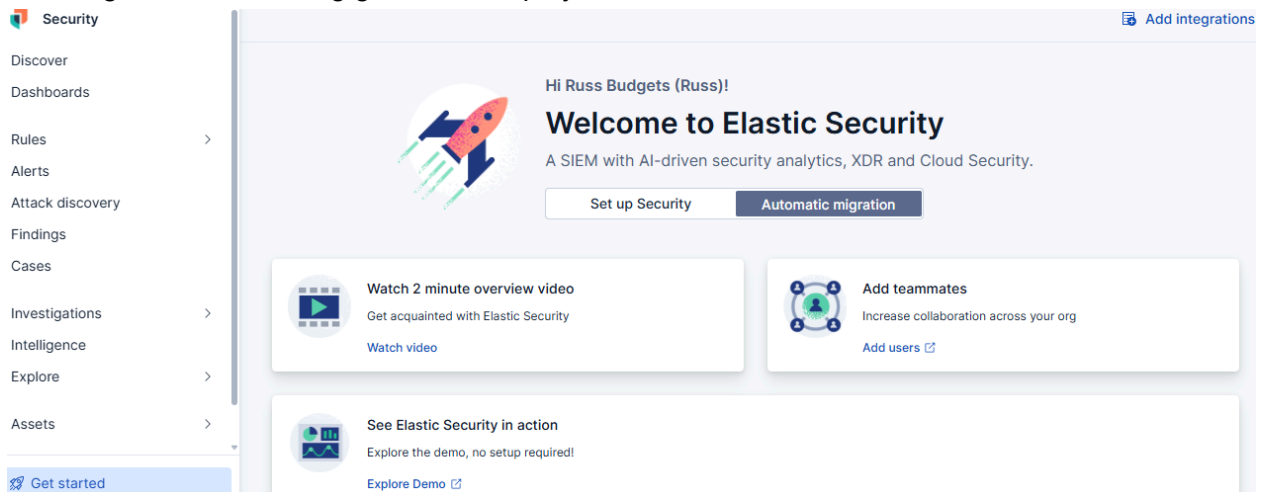
Details Status and alarms Monitoring **Security** Networking Storage Tags

▼ Security details

- 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.

Add agent

Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

1 What type of host do you want to monitor?

Settings for the monitored host are configured in the [agent policy](#).
Create a new agent policy to get started.

[Create policy](#)☒ Collect system logs and metrics ⓘ[Advanced options](#)

2 Enroll in Fleet?

To install Elastic Agent without root privileges, add the `--unprivileged` flag to the `elastic-agent install` command below.
For more information, see the [Fleet and Elastic Agent Guide](#).

Linux aarch... MacOS aarch... DEB aarch... RPM aarch... .. 1 ▾

```
$ProgressPreference = 'SilentlyContinue'
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/elastic-agent-9.0.3-build202507110136-windows-x86_64.zip
Expand-Archive .\elastic-agent-9.0.3-build202507110136-windows-x86_64.zip
cd elastic-agent-9.0.3-build202507110136-windows-x86_64
.\elastic-agent.exe install --url=https://c0f70...
```

Kubernetes
Windows x86_64
Windows MSI
Linux x86_64
MacOS x86_64
DEB x86_64
RPM x86_64

Confirm agent enrollment

- 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 Elastic agent.

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

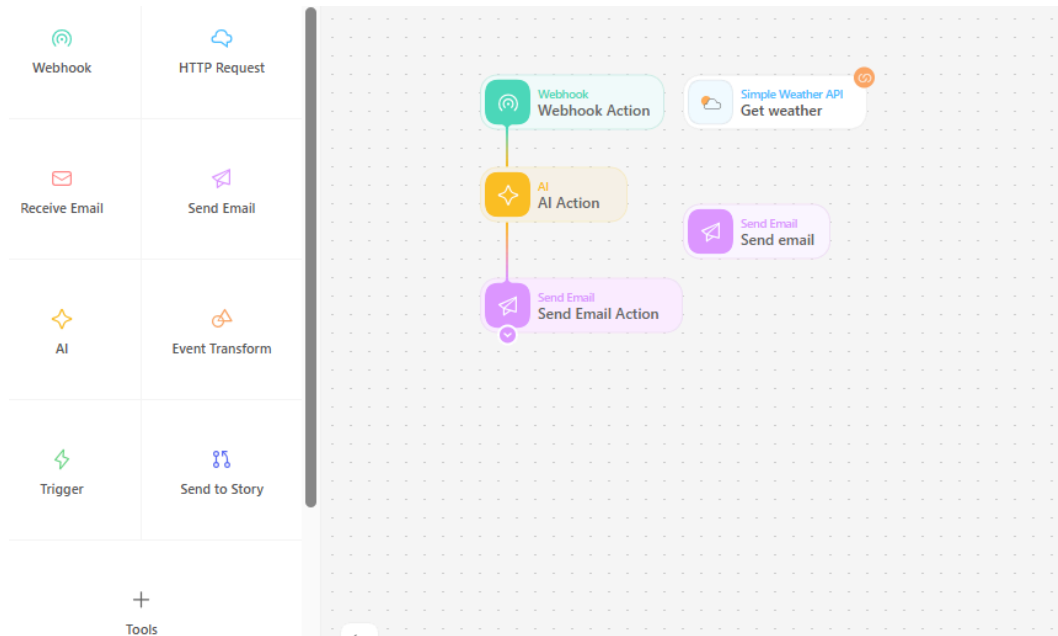
The screenshot shows the Elastic Agents management interface. The left sidebar contains navigation links: Rules, Alerts, Attack discovery, Findings, Cases, Investigations, Intelligence, Explore, and Assets (highlighted). The main panel is titled 'Agents' and includes tabs for Agent policies, Enrollment tokens, Uninstall tokens, Data streams, and Settings. Below these are links for Ingest Overview Metrics and Agent Info Metrics, along with an 'Agent activity' link and an 'Add agent' button. A search bar prompts 'Filter your data using KQL syntax'. Filter bars show 'Status' with 5 items, 'Tags' with 1 item, 'Agent policy' with 1 item, and 'Upgrade available'. A summary bar indicates 'Showing 1 agent' with a 'Clear filters' button and status counts: Healthy (1), Unhealthy (0), Orphaned (0), Updating (0), Offline (0), Inactive (0), Unenrolled (0), and Uninstallable (0). A table lists agent details with columns: Status, Host, Agent policy, CPU, Memory, Last activity, and Version. One agent is listed with status 'Healthy', host 'EC2AMAZ-AFVHPV6', agent policy 'Agent policy 1 rev. 1', CPU 'N/A', Memory '419 MB', last activity '41 seconds ago', and version '9.0.3+build202507110136'. At the bottom, there's a 'Rows per page: 20' dropdown and pagination controls.

- 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”

The image shows two informational boxes from the Elastic Defend integration setup. The top box is yellow and contains the text: 'Requires root privileges' and 'Elastic Agent needs to be run with root/administrator privileges for this integration.' The bottom box is blue and contains the text: 'This package has 2 transform assets which will be created and started with the same roles as the user installing the package.'

The screenshot shows the 'Select integration' step in the Elastic Defend setup. It features a search bar with 'Elastic Defend' entered. Below the search bar, there's a message 'Your integration policy has errors.' and buttons for 'Cancel' and 'Add integration'.

- 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

Webhook connector

Send a request to a web service.

Compatibility: **Alerting Rules** Security Solution

connector name

Test Tines webhook

connector settings

Method URL

POST

authentication

☒ None

☐ Basic 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

Source

Use Kibana [Data Views](#) or specify individual [index patterns](#) as your rule's data source to be searched.

✓ Index Patterns
Data View

Index patterns

apm-*-transaction* ×
auditbeat-* ×
endgame-* ×
filebeat-* ×
logs-* ×
packetbeat-* ×
traces-apm* ×
winlogbeat-* ×
-*elastic-cloud-logs-* ×

Enter the pattern of Elasticsearch indices where you would like this rule to run. By default, these will include index patterns defined in Security Solution advanced settings.

Custom query Import query from saved timeline

⋮
+

×

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

Test Tines webhook

Action frequency

Summary of alerts

Per rule run

☐ If alert matches a query

☐ If alert is generated during timeframe

Body

```

1  {
2    "rule_name": "{{context.rule.name}}",
3    "description": "{{context.rule.description}}"
4  }
```

- 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”

Name

AI Action

Description

Prompt ⓘ

Summarize the following data into one sentence. Provide some next action steps for the analyst to take when reviewing the alert. Format the data into bullet points to make it easier to read.

{ } 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.

The screenshot displays the Tines interface. On the left, a search bar with a plus icon and the text "Filter your data using KQL syntax" is visible. Below it, a list of host names is shown, with "ec2amaz-afvhpv6" highlighted in red. On the right, a detailed view of a rule is shown. The rule is named "Test admin rule" and has a status of "Open". It has a risk score of 21 and is assigned to "Assignees". The rule description is "Test admin rule" and the alert reason is "Test admin rule". The interface also shows a table of alerts with columns for Actions, @timestamp, and Rule. The table contains two rows of alerts, both with a timestamp of "Jul 14, 2025 @ 16:28:45.901" and "Test admin rule".

Low

Jul 14, 2025 @ 16:28:45.901

⚠️ [Test admin rule](#)

Status
Open

Risk score
21

Assignees
+

Notes
+ Add note

Overview Table JSON

About

Rule description [Show rule summary](#)

Test admin rule

Alert reason [Show full reason](#)

Alert reason

Columns 18 Sort fields 1 2 alerts Updated 2 minutes

Fields

Actions	@timestamp	Rule
	Jul 14, 2025 @ 16:28:45.901	Test admin rule
	Jul 14, 2025 @ 16:28:45.895	Test admin rule



Russ Geisler <mail@tines.io>

to me ▼



4:58 PM (7 minutes ago)

A new event has been detected.

-