



Search. Observe. Protect.

Leverage System Protection With Elastic Security

elastic.co

TABLE OF CONTENTS

- INTRODUCTION.....1
- CREATING A DEPLOYMENT2
- ADD DATA WITH FLEET AND ELASTIC AGENT3
- ADD DATA THREAT INTELLEGENT9
- PREVENT ATTACK TEST8

INTRODUCTION

Kibana is your window into the Elastic Stack. Kibana enables you to:

- **Analyze and visualize your data.** Search for hidden insights, compile a dashboard of charts, gauges, maps and other visualizations that show what you found, and share it with others.
- **Search, observe, and protect your data.** Add a search box to your app or website, analyze logs metrics, and find security vulnerabilities.
- **Manage, monitor, and secure the Elastic Stack.** Manage your indices and ingest pipelines, monitor the health of your Elastic Stack cluster, and control which users have access to which features and data.

In these labs, you will learn how to add data security, how to prevent attack, and manage endpoint.

CREATING A DEPLOYMENT

You will start by creating a deployment on Elastic Cloud. Next you will access Kibana, and load the data from your environment.

Creating a cloud deployment

1. Go to cloud.elastic.co
2. Click **Sign up**.
3. Enter your email and choose a password.
4. Click **Start free trial**. This brings you to the Cloud console. Here, you can create a deployment to start a 14-day free trial.
5. Enter a name for the deployment, for example `security-workshop`.
6. Leave the other settings to their default values and click **Create deployment**. It will take a few minutes for the Elastic Stack to initialize.
7. You won't need the password that's shown to you. You will use your Elastic Cloud account to access Kibana. Click **Skip**.
8. Wait a couple of minutes and click **Continue** when the button turns blue. This brings you to the Kibana home.

Getting to know Kibana

Click the menu button in the top left (it looks like three horizontal lines). This button opens Kibana's main menu. This menu has five sections:

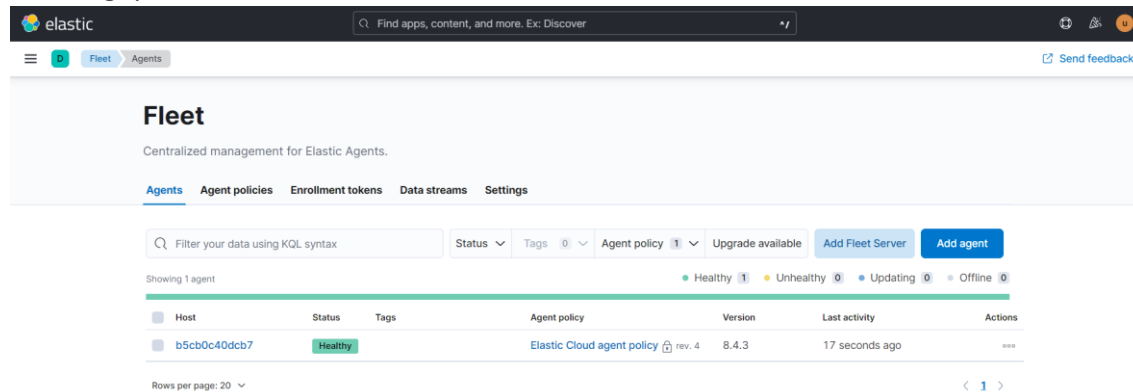
- **Analytics**, where you find the tools to analyze and visualize the data.
- **Enterprise Search**, **Observability**, and **Security**, the homes for the three Elastic solutions.
- **Management**, where you can manage your deployment.

We will focus on the **Security and Management**.

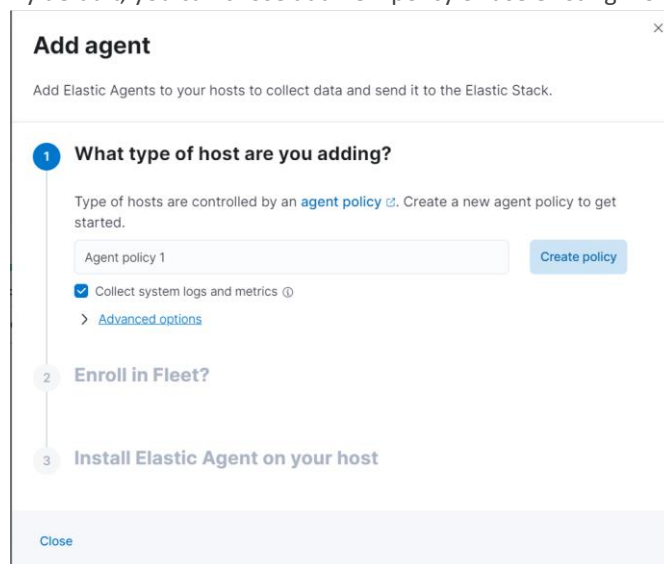
ADD DATA WITH FLEET AND ELASTIC AGENT

Let's get started install Elastic Agent in local computer.

1. Open the main menu by clicking the menu button located at the top left. Select **Fleet** from the **Management** section.
2. This brings you to the Fleet view:



3. Select the **Add agent** to add elastic agent.
4. By default, you can chose add new policy or use existing. For first time set name policy and select **Create policy**.



5. At point 3 select operating system like you use. Copy all script and run in your computer.

Add agent

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

3 Install Elastic Agent on your host

Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our [downloads page](#). For additional guidance, see our [installation docs](#).

Linux TarMacWindowsRPMDEBKubernetes

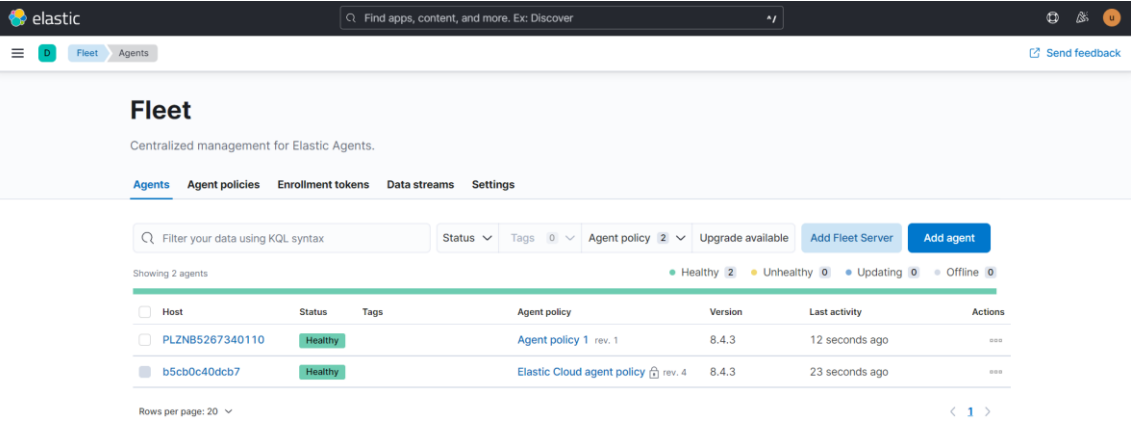
```
$ProgressPreference = 'SilentlyContinue'  
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.4.3-windows-x86_64.zip -OutFile elastic-agent-8.4.3-windows-x86_64.zip  
Expand-Archive .\elastic-agent-8.4.3-windows-x86_64.zip -DestinationPath .  
cd elastic-agent-8.4.3-windows-x86_64  
.\elastic-agent.exe install --url=https://93c640b142e04c41ac895fc8d5e3750d.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=SUC5UU1vUUJtRm9GSF1VeVViMm46bC1mVTcyM09TUy1a0XFPdY9nY1dPQQ==
```

Close

6. In Windows you can open Power shell and run it. If show question continues, press y and enter. Wait until finish.

```
Administrator: Windows PowerShell  
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
  
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows  
  
PS C:\WINDOWS\system32> $ProgressPreference = 'SilentlyContinue'  
PS C:\WINDOWS\system32> Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.4.3-windows-x86_64.zip -OutFile elastic-agent-8.4.3-windows-x86_64.zip  
PS C:\WINDOWS\system32> Expand-Archive .\elastic-agent-8.4.3-windows-x86_64.zip -DestinationPath .  
PS C:\WINDOWS\system32> cd elastic-agent-8.4.3-windows-x86_64  
PS C:\WINDOWS\system32\elastic-agent-8.4.3-windows-x86_64> .\elastic-agent.exe install --url=https://93c640b142e04c41ac895fc8d5e3750d.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=SUC5UU1vUUJtRm9GSF1VeVViMm46bC1mVTcyM09TUy1a0XFPdY9nY1dPQQ==  
Elastic Agent will be installed at C:\Program Files\Elastic\Agent and will run as a service. Do you want to continue? [Y/n]:y  
{ "log.level": "info", "@timestamp": "2022-11-01T15:34:03.830+0700", "log.origin": { "file.name": "cmd/enroll_cmd.go", "file.line": 471 }, "message": "Starting enrollment to URL: https://93c640b142e04c41ac895fc8d5e3750d.fleet.us-central1.gcp.cloud.es.io:443/", "ecs.version": "1.6.0" }  
{ "log.level": "info", "@timestamp": "2022-11-01T15:34:06.636+0700", "log.origin": { "file.name": "cmd/enroll_cmd.go", "file.line": 273 }, "message": "Successfully triggered restart on running Elastic Agent.", "ecs.version": "1.6.0" }  
Successfully enrolled the Elastic Agent.  
Elastic Agent has been successfully installed.  
PS C:\WINDOWS\system32\elastic-agent-8.4.3-windows-x86_64>
```

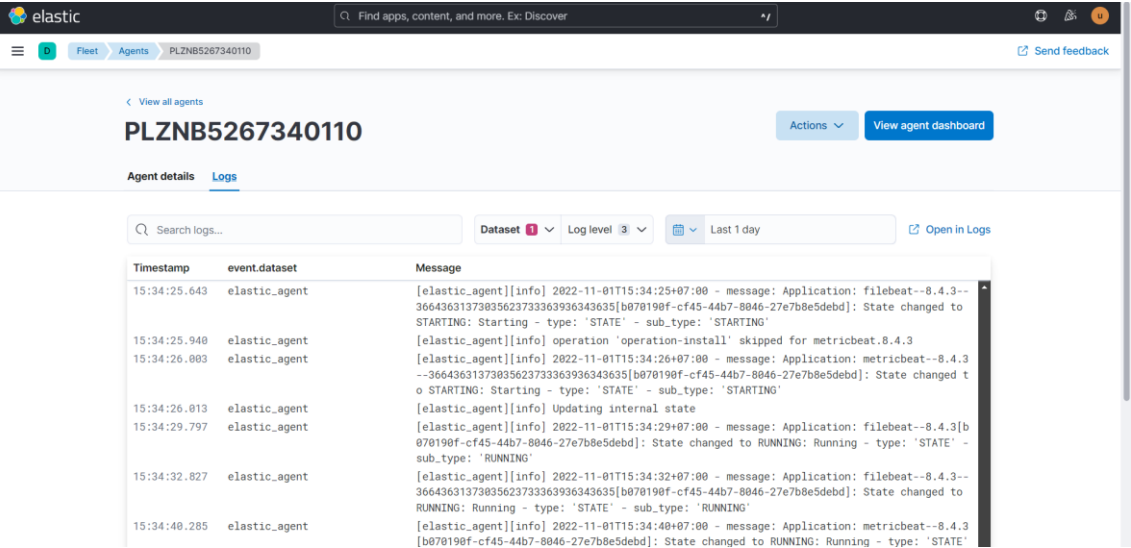
7. You will see hostname the computer at list fleet.



The screenshot shows the Elastic Fleet management interface. At the top, there's a search bar and navigation tabs for Fleet and Agents. Below the header, the 'Fleet' section is active, showing 'Centralized management for Elastic Agents.' and tabs for Agents, Agent policies, Enrollment tokens, Data streams, and Settings. A filter bar allows searching by KQL syntax, with filters for Status, Tags, Agent policy, and Upgrade available. Below this, a table lists agents with columns for Host, Status, Tags, Agent policy, Version, Last activity, and Actions. Two agents are listed: PLZNB5267340110 and b5cb0c40dcb7, both with a 'Healthy' status. The bottom of the page shows 'Rows per page: 20' and a pagination link.

Host	Status	Tags	Agent policy	Version	Last activity	Actions
PLZNB5267340110	Healthy		Agent policy 1 rev. 1	8.4.3	12 seconds ago	...
b5cb0c40dcb7	Healthy		Elastic Cloud agent policy rev. 4	8.4.3	23 seconds ago	...

8. At fleet select **hostname** and select **Logs** tab for make sure the logs send to Elasticsearch.



The screenshot shows the Elastic Fleet interface with the 'Agents' tab selected. The specific agent 'PLZNB5267340110' is highlighted. Below the agent name, there are tabs for 'Agent details' and 'Logs'. The 'Logs' tab is active, displaying a list of logs with columns for Timestamp, event.dataset, and Message. The logs show the agent's startup sequence, including state changes from 'STARTING' to 'RUNNING' for both filebeat and metricbeat. The 'Message' column contains detailed log entries with timestamps and application names.

Timestamp	event.dataset	Message
15:34:25.643	elastic_agent	[elastic_agent][info] 2022-11-01T15:34:25+07:00 - message: Application: filebeat--8.4.3--36643631373835623733363936343635[b070190f-cf45-44b7-8046-27e7b8e5debd]: State changed to STARTING: Starting - type: 'STATE' - sub_type: 'STARTING'
15:34:25.940	elastic_agent	[elastic_agent][info] operation 'operation-install' skipped for metricbeat.8.4.3
15:34:26.003	elastic_agent	[elastic_agent][info] 2022-11-01T15:34:26+07:00 - message: Application: metricbeat--8.4.3--36643631373835623733363936343635[b070190f-cf45-44b7-8046-27e7b8e5debd]: State changed to STARTING: Starting - type: 'STATE' - sub_type: 'STARTING'
15:34:26.013	elastic_agent	[elastic_agent][info] Updating internal state
15:34:29.797	elastic_agent	[elastic_agent][info] 2022-11-01T15:34:29+07:00 - message: Application: filebeat--8.4.3[b070190f-cf45-44b7-8046-27e7b8e5debd]: State changed to RUNNING: Running - type: 'STATE' - sub_type: 'RUNNING'
15:34:32.827	elastic_agent	[elastic_agent][info] 2022-11-01T15:34:32+07:00 - message: Application: filebeat--8.4.3--36643631373835623733363936343635[b070190f-cf45-44b7-8046-27e7b8e5debd]: State changed to RUNNING: Running - type: 'STATE' - sub_type: 'RUNNING'
15:34:40.285	elastic_agent	[elastic_agent][info] 2022-11-01T15:34:40+07:00 - message: Application: metricbeat--8.4.3[b070190f-cf45-44b7-8046-27e7b8e5debd]: State changed to RUNNING: Running - type: 'STATE'

9. Back to fleet select **Agent policy 1** and select **Add integration**.

The screenshot shows the Elastic Agent policy page for 'Agent policy 1'. The breadcrumb navigation is 'Fleet > Agent policies > Agent policy 1'. The page header includes a search bar and a 'Send feedback' link. The main content area shows the policy name 'Agent policy 1' with tabs for 'Integrations' and 'Settings'. A summary bar displays 'Revision 1', 'Integrations 1', 'Agents 1 agent', and 'Last updated on Nov 01, 2022'. Below this is a table of integrations with columns for Name, Integration, Namespace, and Actions. The table contains one entry: 'system-1' with integration 'System v1.20.4' and namespace 'default'. An 'Add integration' button is visible in the top right of the table area.

Name	Integration	Namespace	Actions
system-1	System v1.20.4	default	...

10. Select **Endpoint and Cloud Security** and select **Add Endpoint and Cloud Security**.

The screenshot shows the Elastic Agent 'Endpoint and Cloud Security' integration page. The breadcrumb navigation is 'Integrations > Endpoint and Cloud Security'. The page header includes a search bar and a 'View deployment details' link. The main content area features the Elastic Agent logo, the title 'Endpoint and Cloud Security', and a version '8.4.1'. A blue button 'Add Endpoint and Cloud Security' is in the top right. Below the title are tabs for 'Overview', 'Settings', and 'Advanced'. The 'Overview' tab is active, showing a description: 'This integration sets up templates and index patterns required for Endpoint and Cloud Security.' It also includes sections for 'Compatibility', 'Logs', and 'alerts'. On the right side, there is a 'Details' section with a table of integration details.

Details	
Version	8.4.1
Category	Cloud, Security
Elasticsearch assets	Index templates 2, Transforms 2, Ingest pipelines 13
Features	logs, metrics
License	basic

11. At integration name set name like picture and make sure Agent policy use existing policy.
Then select **Save and continue**

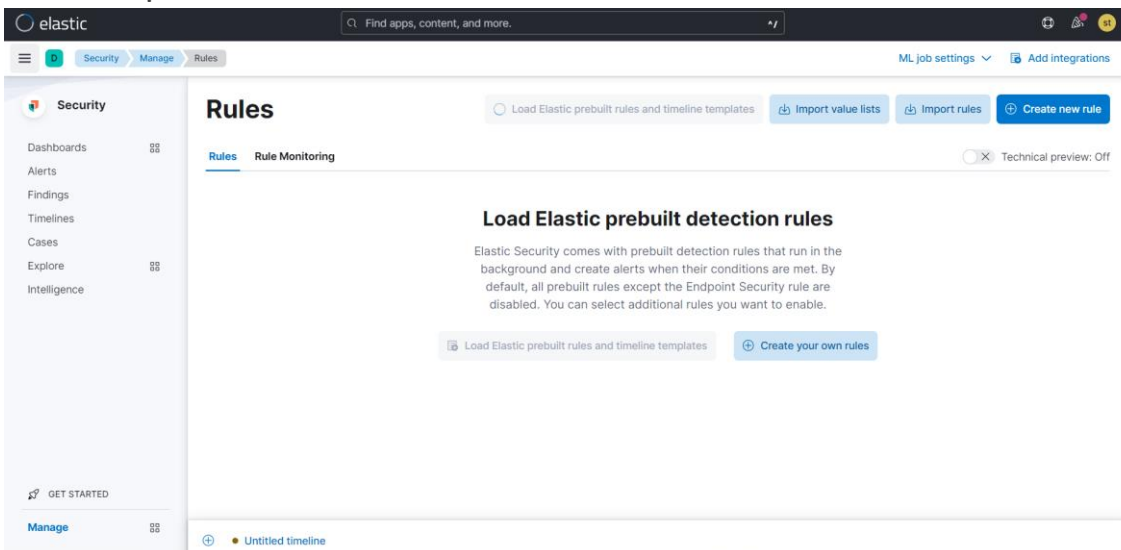
The screenshot shows the Elastic UI interface for configuring an integration. The breadcrumb navigation at the top indicates the path: Integrations > Endpoint and Cloud Security > Add integration. The main heading is '1 Configure integration'. Below this, the 'Integration settings' section prompts the user to choose a name and description. The 'Integration name' field contains 'EDR-1', and the 'Description' field is empty with a note that it is optional. A link for 'Advanced options' is provided. A blue informational box states that the integration will be saved with recommended defaults. The second section, '2 Where to add this integration?', has two tabs: 'New hosts' and 'Existing hosts', with 'Existing hosts' being the active tab. Under 'Existing hosts', the 'Agent policy' section explains that agent policies manage groups of integrations. A dropdown menu for 'Agent policy' shows 'Agent policy 1' selected, with a note indicating that 1 agent is enrolled with this policy. At the bottom right, there are 'Cancel' and 'Save and continue' buttons.

12. List policy will show Endpoint and Cloud Security.

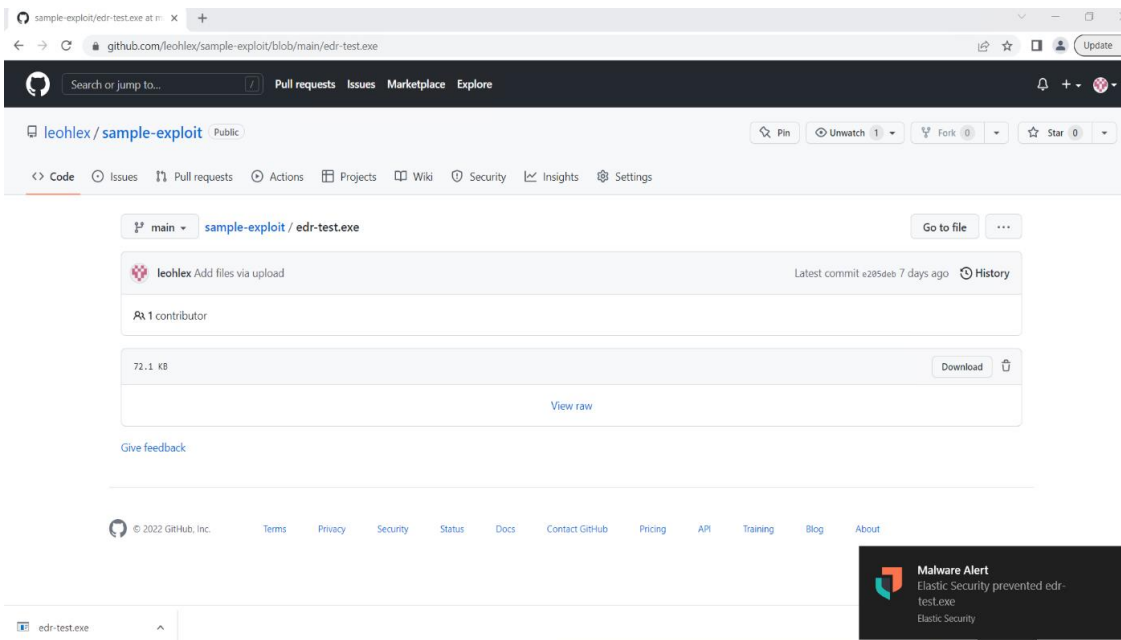
PREVENT ATTACK TEST

Let's try Endpoint Security to detect some file infected.

1. Open Kibana select menu security and sub menu alert, then manage rule. Select **Load Elastic prebuilt rules and timeline templates.**



2. Open in browser this link and download the file.
<https://github.com/leohlex/sample-exploit/blob/main/edr-test.exe>
3. After download Elastic Endpoint security will terminate and send information about the proses to Elasticsearch and we can see in Kibana.



ADD DATA THREAT INTELLIGENT

Let's add some data from Threat Intelligent for more enrich information and analytic.

1. Open the main menu by clicking the menu button located at the top left. Select **Fleet** from the **Management** section.
2. This brings you to the Fleet view:

The screenshot shows the Elastic Fleet management page. At the top, there's a search bar with the text "Find apps, content, and more. Ex: Discover". Below the search bar, there's a navigation bar with "Fleet" and "Agents" tabs. The "Fleet" tab is selected. The main heading is "Fleet" with the subtitle "Centralized management for Elastic Agents". Below this, there's a navigation bar with "Agents", "Agent policies", "Enrollment tokens", "Data streams", and "Settings". The "Agents" tab is selected. There's a search bar with the text "Filter your data using KQL syntax". To the right of the search bar, there are filters for "Status", "Tags", "Agent policy", and "Upgrade available". There are also buttons for "Add Fleet Server" and "Add agent". Below the filters, there's a table showing 2 agents. The table has columns for "Host", "Status", "Tags", "Agent policy", "Version", "Last activity", and "Actions". The first agent is "PLZNB5267340110" with status "Healthy", agent policy "Agent policy 1 rev. 1", version "8.4.3", and last activity "12 seconds ago". The second agent is "b5cb0c40dcb7" with status "Healthy", agent policy "Elastic Cloud agent policy rev. 4", version "8.4.3", and last activity "23 seconds ago".

Host	Status	Tags	Agent policy	Version	Last activity	Actions
PLZNB5267340110	Healthy		Agent policy 1 rev. 1	8.4.3	12 seconds ago	...
b5cb0c40dcb7	Healthy		Elastic Cloud agent policy rev. 4	8.4.3	23 seconds ago	...

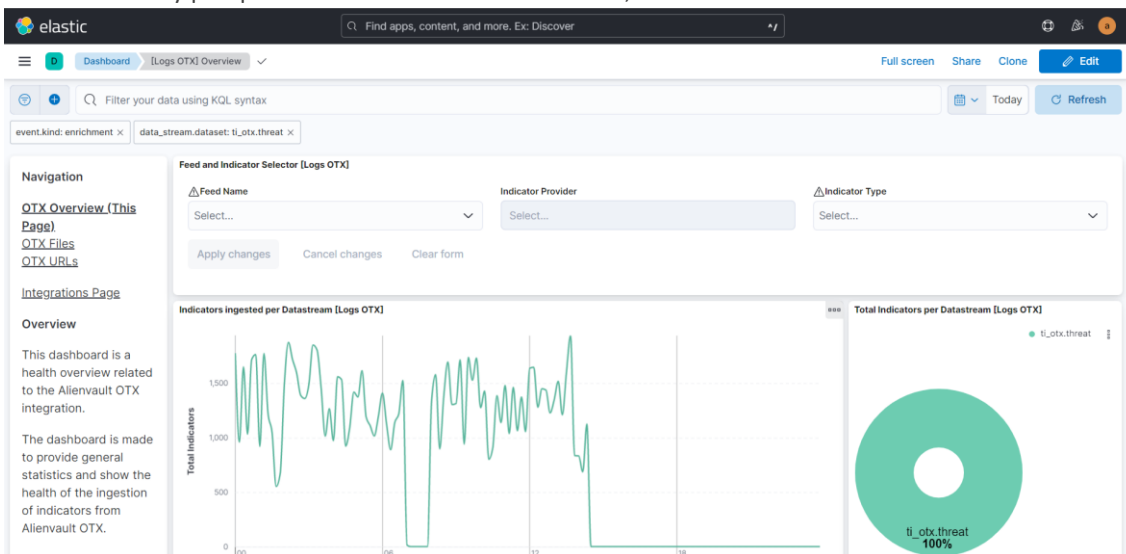
3. Select the **Agent policy 1** to add Threat Intelligent.
4. Select **Add Integration** then search **Threat** and select **AlienVault OTX**.

The screenshot shows the Elastic Integrations page. At the top, there's a search bar with the text "Find apps, content, and more. Ex: Discover". Below the search bar, there's a navigation bar with "Integrations" and "Browse integrations" tabs. The "Integrations" tab is selected. The main heading is "Integrations". Below this, there's a search bar with the text "Search". To the right of the search bar, there are filters for "Status", "Tags", "Agent policy", and "Upgrade available". There are also buttons for "Add Fleet Server" and "Add agent". Below the filters, there's a table showing 2 integrations. The table has columns for "Host", "Status", "Tags", "Agent policy", "Version", "Last activity", and "Actions". The first integration is "Web crawler" with status "Healthy", agent policy "Agent policy 1 rev. 1", version "8.4.3", and last activity "12 seconds ago". The second integration is "b5cb0c40dcb7" with status "Healthy", agent policy "Elastic Cloud agent policy rev. 4", version "8.4.3", and last activity "23 seconds ago".

Host	Status	Tags	Agent policy	Version	Last activity	Actions
Web crawler	Healthy		Agent policy 1 rev. 1	8.4.3	12 seconds ago	...
b5cb0c40dcb7	Healthy		Elastic Cloud agent policy rev. 4	8.4.3	23 seconds ago	...

5. Select **Add AlienVault OTX** put required value like Name, API Token, and set Policy for put integration. After finish select **Save and continue**.

6. Cek data already pump to elasticsearch. Go to Dashboard, search and select **OTX Overview**.



Version: 8.x

© 2015-2022 Elasticsearch BV. All rights reserved. Decompiling, copying, publishing and/or distribution without written consent of Elasticsearch BV is strictly prohibited.