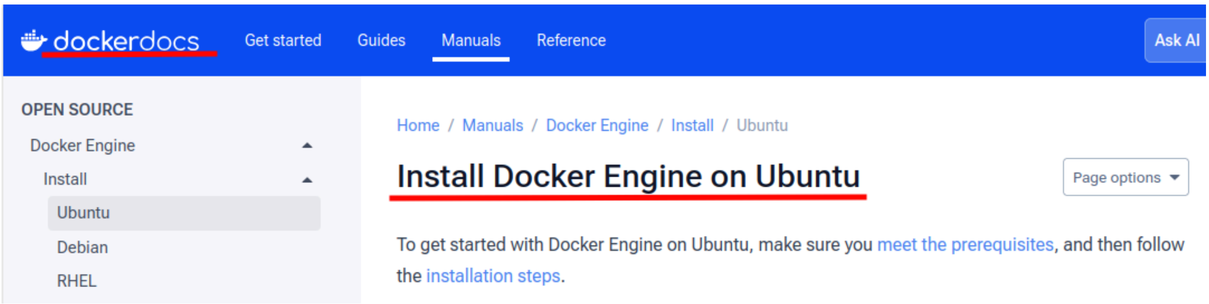
Brandon Gracy *08/12/2025*

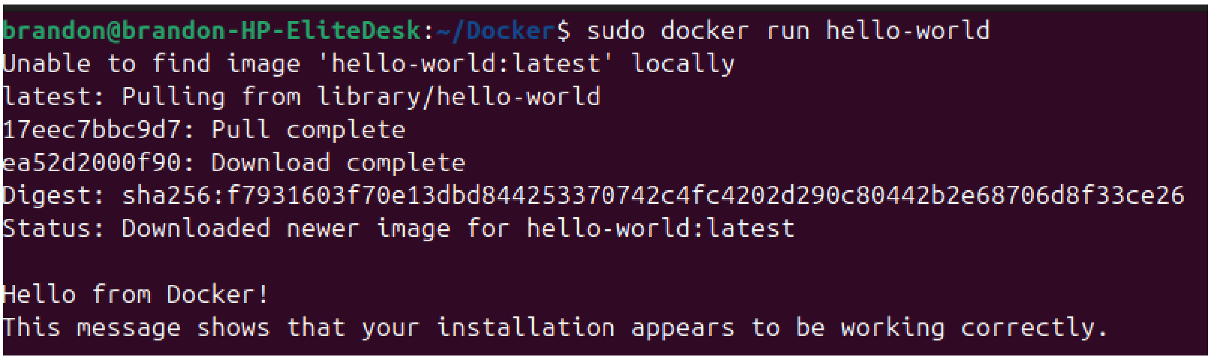
In this task, we are going to see how to installing Docker and Elastic on an Ubuntu
machine, followed by verifying network activity through ping and nmap scans.



Install Docker Engine on Ubuntu

To get started with Docker Engine on Ubuntu, make sure you meet the prerequisites, and then follow the installation steps.

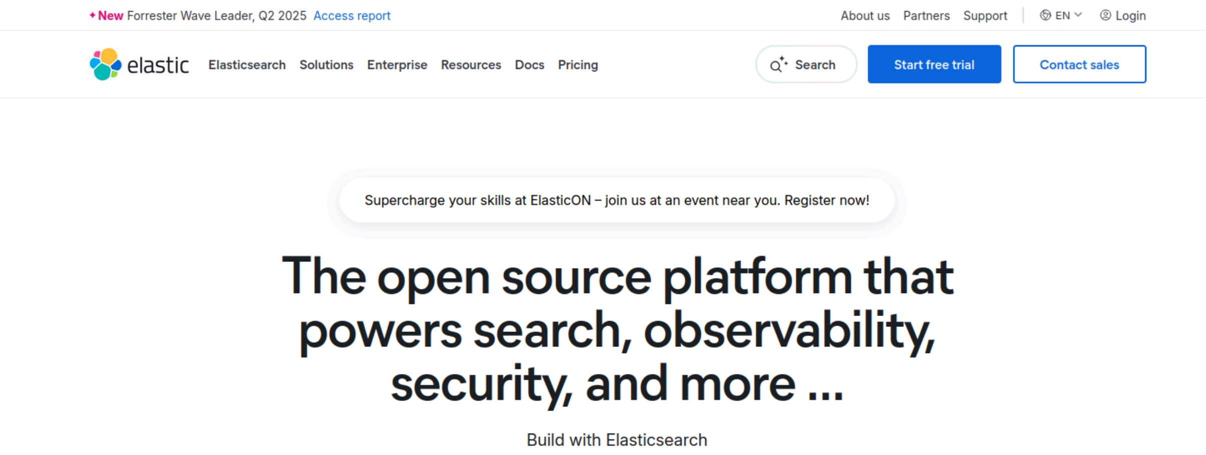
We received a document that teaches how to install Docker in ubuntu, let's just follow the document.



```
brandon@brandon-HP-EliteDesk:~/Docker$ sudo docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
17eec7bbc9d7: Pull complete
ea52d2000f90: Download complete
Digest: sha256:f7931603f70e13dbd844253370742c4fc4202d290c80442b2e68706d8f33ce26
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.
```

When you finish installing Docker, you'll see this image.

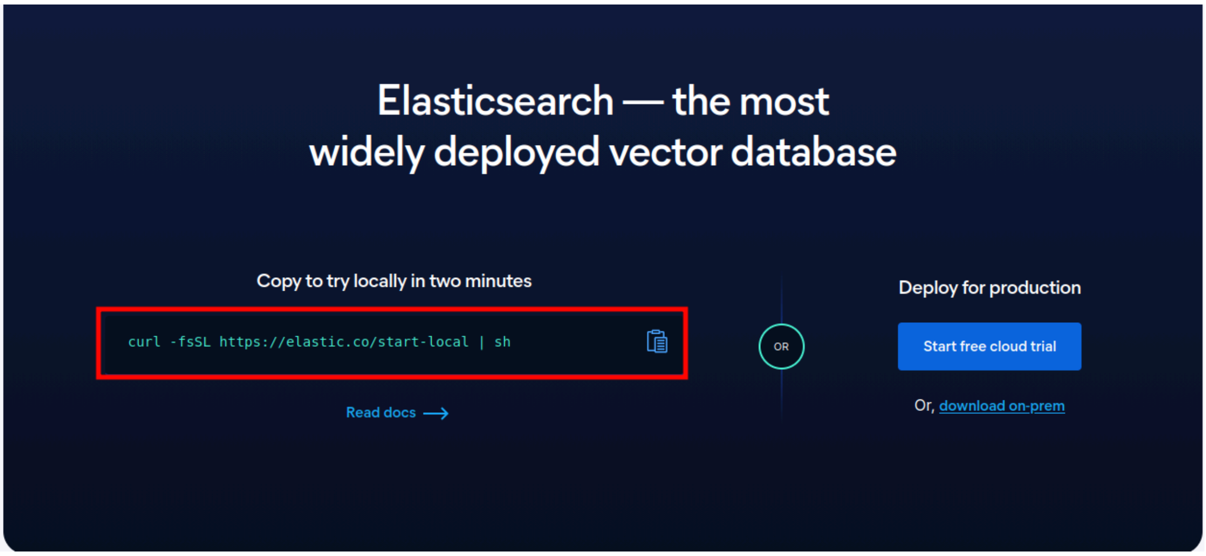
In the next step, we have to install the Elastic stack, It is a research, logging, and observability platform widely used in security, DevOps, and data analytics.


✦New Forrester Wave Leader, Q2 2025 Access report
About us
Partners
Support
EN
Login
elastic
Elasticsearch
Solutions
Enterprise
Resources
Docs
Pricing
Search
Start free trial
Contact sales
Supercharge your skills at ElasticON – join us at an event near you. Register now!

The open source platform that powers search, observability, security, and more ...

Build with Elasticsearch

That’s the interface of the site that we need.

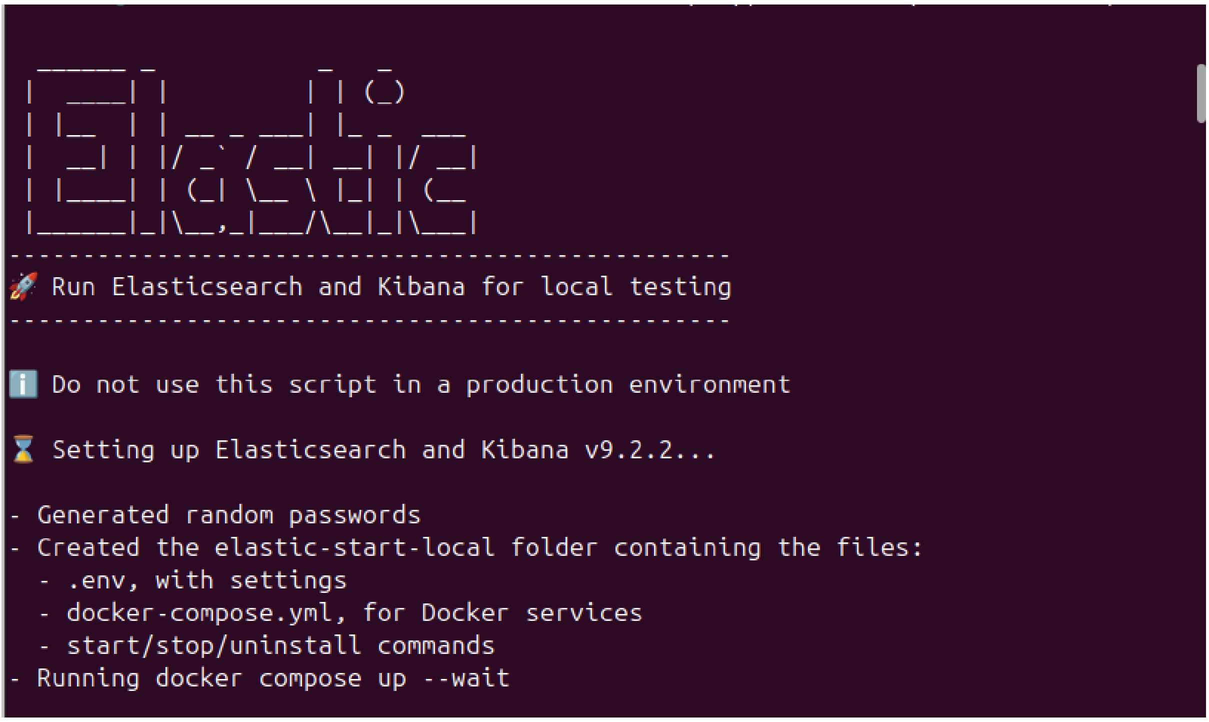


Elasticsearch — the most widely deployed vector database

Copy to try locally in two minutes

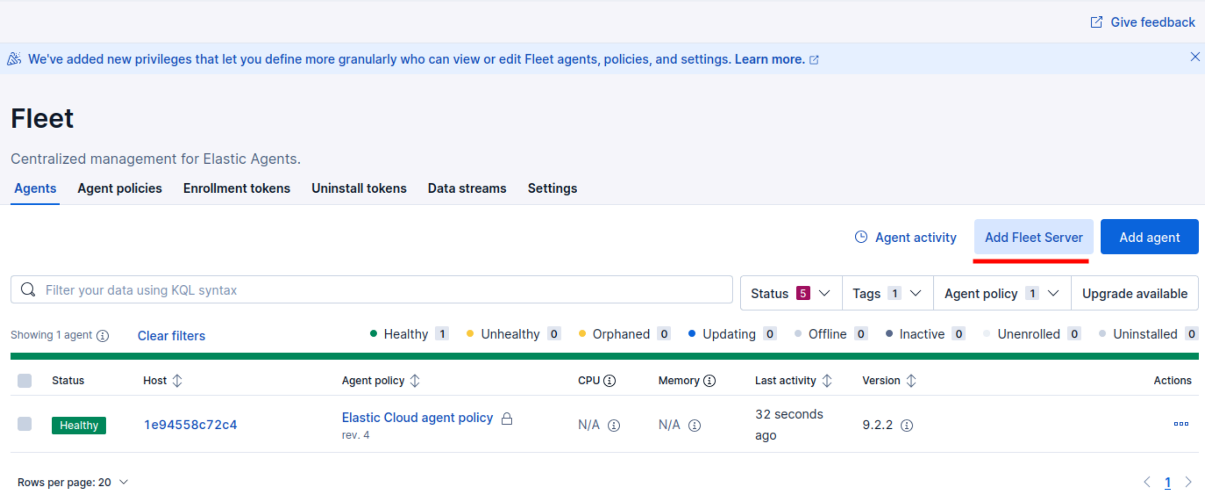
```
curl -fsSL https://elastic.co/start-local | sh
```

We just have to scroll down to the bottom of the website, copy and paste this code into our terminal.



```
  ______ _           _   _
 |  ____| |         | | (_)
 | |__  | | __ _ ___| |_ _  ___
 |  __| | |/ _` / __| __| |/ __|
 | |____| | (_| \__ \ |_| | (__
 |______|_|\__,_|___/\__|_|\___|
-------------------------------------------------
🚀 Run Elasticsearch and Kibana for local testing
-------------------------------------------------

ℹ️ Do not use this script in a production environment

⌛ Setting up Elasticsearch and Kibana v9.2.2...

- Generated random passwords
- Created the elastic-start-local folder containing the files:
  - .env, with settings
  - docker-compose.yml, for Docker services
  - start/stop/uninstall commands
- Running docker compose up --wait
```

When you run the command, you will see this image.



Give feedback

We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. Learn more.

Fleet

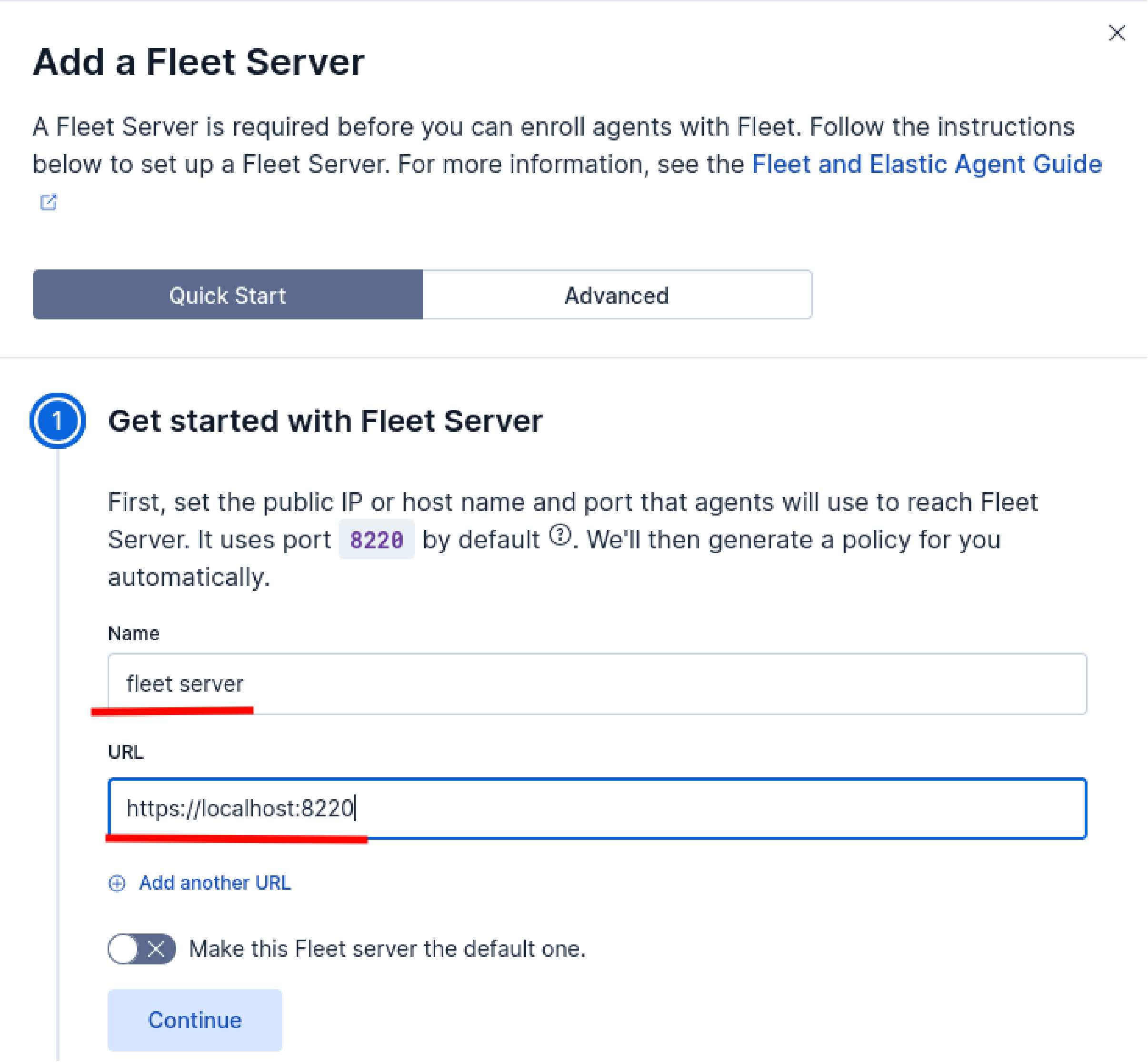
Centralized management for Elastic Agents.

Showing 1 agent   Clear filters   ● Healthy 1 ● Unhealthy 0 ● Orphaned 0 ● Updating 0 ● Offline 0 ● Inactive 0 ● Unenrolled 0 ● Uninstalled 0

□	Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
□	Healthy	1e94558c72c4	Elastic Cloud agent policy rev. 4	N/A	N/A	32 seconds ago	9.2.2	•••

Rows per page: 20   1

Now, let's add an agent in our pc, we have to go to feet in the bweb-site and click in add feet server.



Add a Fleet Server

A Fleet Server is required before you can enroll agents with Fleet. Follow the instructions below to set up a Fleet Server. For more information, see the Fleet and Elastic Agent Guide

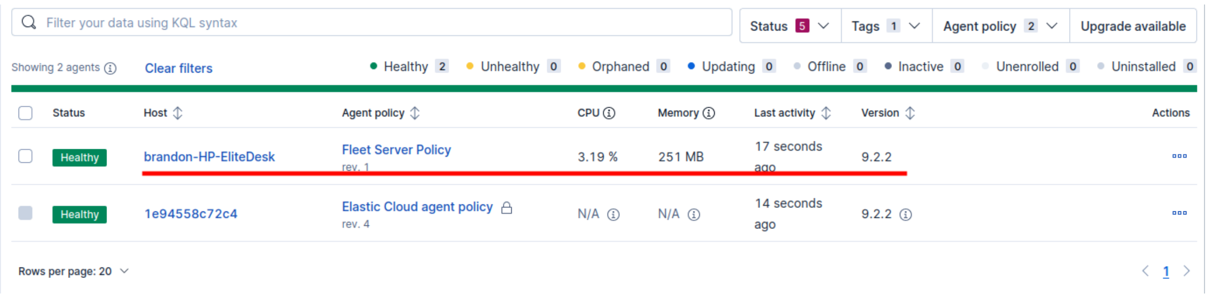
1 Get started with Fleet Server

First, set the public IP or host name and port that agents will use to reach Fleet Server. It uses port `8220` by default. We'll then generate a policy for you automatically.

Name: fleet server

URL: https://localhost:8220

We have to add a new server for our agent, just give a name and put this url.

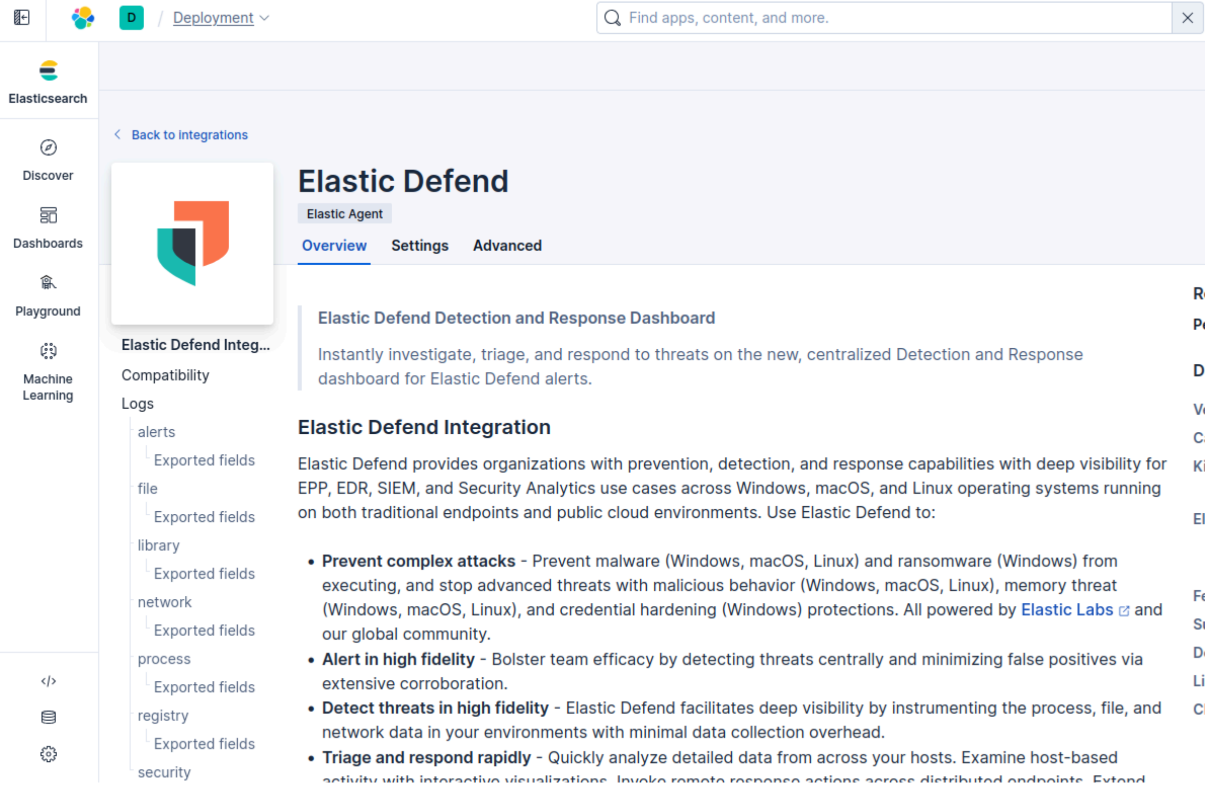


Showing 2 agents Clear filters ● Healthy 2 ● Unhealthy 0 ● Orphaned 0 ● Updating 0 ● Offline 0 ● Inactive 0 ● Unenrolled 0 ● Uninstalled 0

□	Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
□	Healthy	brandon-HP-EliteDesk	Fleet Server Policy rev. 1	3.19 %	251 MB	17 seconds ago	9.2.2	···
□	Healthy	1e94558c72c4	Elastic Cloud agent policy rev. 4	N/A	N/A	14 seconds ago	9.2.2	···

Rows per page: 20

Here we can see our agent.



Elastic Defend

Elastic Defend Detection and Response Dashboard

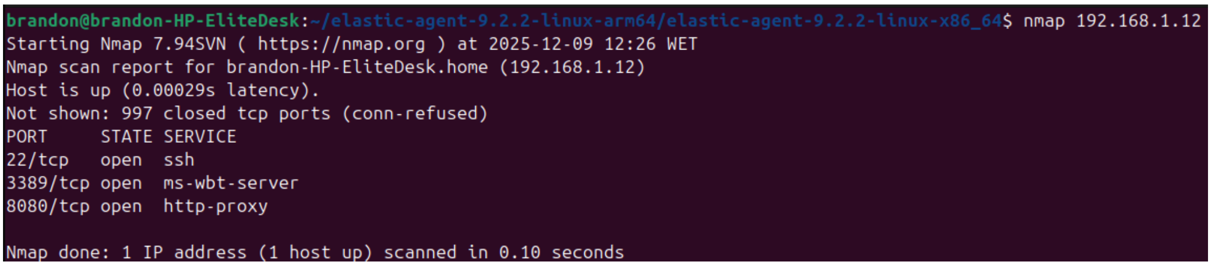
Instantly investigate, triage, and respond to threats on the new, centralized Detection and Response dashboard for Elastic Defend alerts.

Elastic Defend Integration

Elastic Defend provides organizations with prevention, detection, and response capabilities with deep visibility for EPP, EDR, SIEM, and Security Analytics use cases across Windows, macOS, and Linux operating systems running on both traditional endpoints and public cloud environments. Use Elastic Defend to:

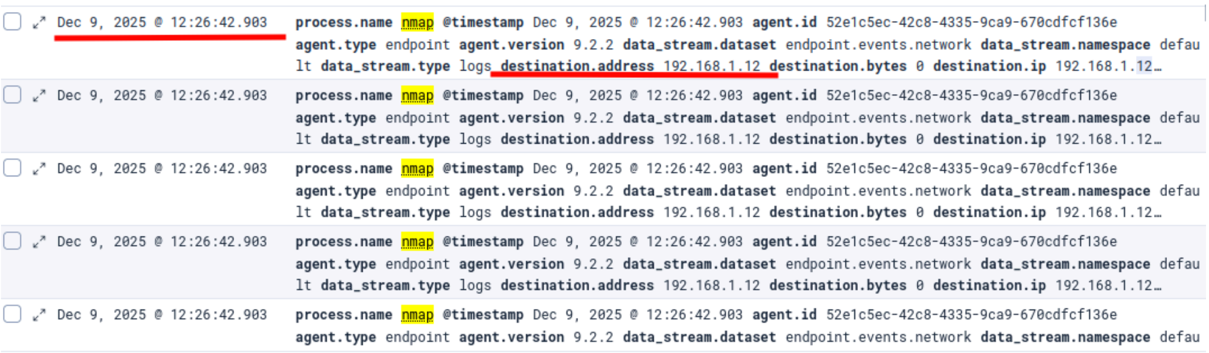
- **Prevent complex attacks** - Prevent malware (Windows, macOS, Linux) and ransomware (Windows) from executing, and stop advanced threats with malicious behavior (Windows, macOS, Linux), memory threat (Windows, macOS, Linux), and credential hardening (Windows) protections. All powered by Elastic Labs and our global community.
- **Alert in high fidelity** - Bolster team efficacy by detecting threats centrally and minimizing false positives via extensive corroboration.
- **Detect threats in high fidelity** - Elastic Defend facilitates deep visibility by instrumenting the process, file, and network data in your environments with minimal data collection overhead.
- **Triage and respond rapidly** - Quickly analyze detailed data from across your hosts. Examine host-based activity with interactive visualizations. Invoke remote response actions across distributed endpoints. Extend

We have to look for Elastic-defend and do the download.



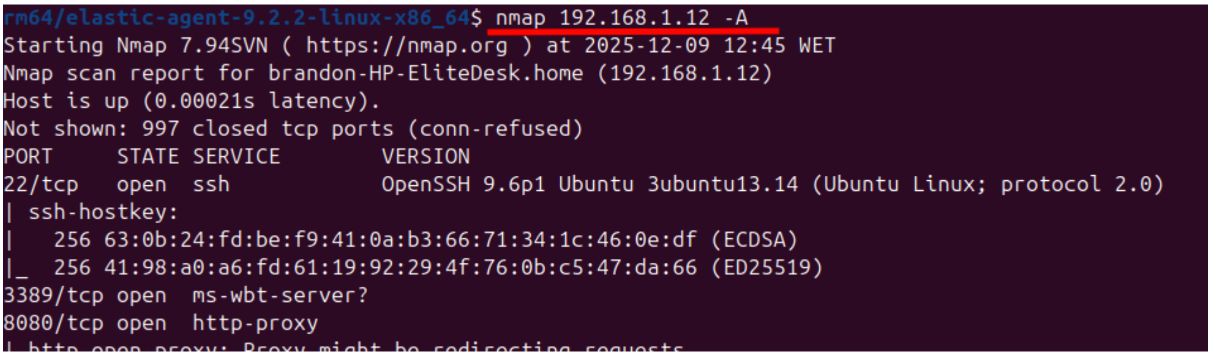
```
brandon@brandon-HP-EliteDesk:~/elastic-agent-9.2.2-linux-arm64/elastic-agent-9.2.2-linux-x86_64$ nmap 192.168.1.12
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-09 12:26 WET
Nmap scan report for brandon-HP-EliteDesk.home (192.168.1.12)
Host is up (0.00029s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

Let’s do a scan with nmap to see if it will appear in Elastic application.



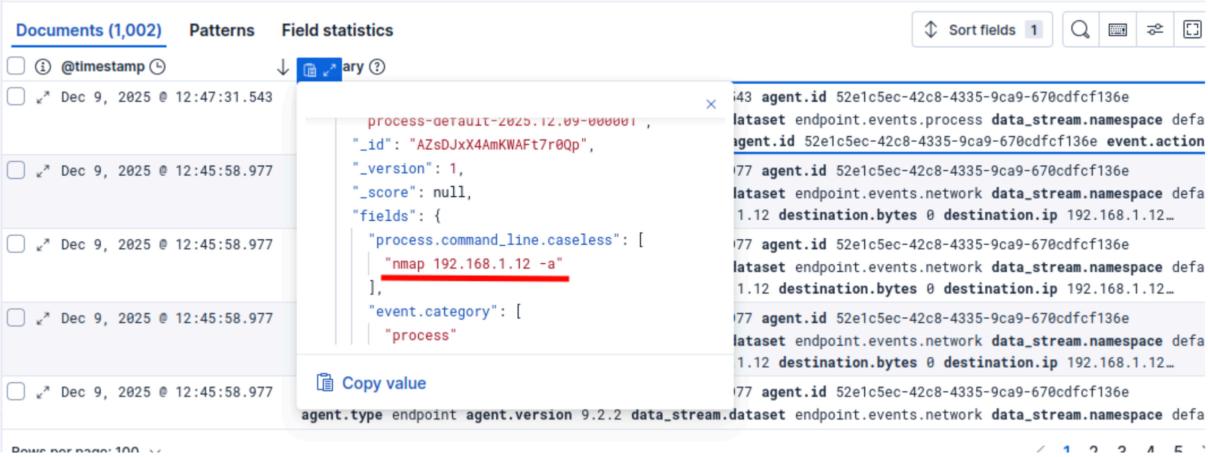
```
☐ ⤢ Dec 9, 2025 @ 12:26:42.903  process.name nmap @timestamp Dec 9, 2025 @ 12:26:42.903 agent.id 52e1c5ec-42c8-4335-9ca9-670cdfcf136e
                                agent.type endpoint agent.version 9.2.2 data_stream.dataset endpoint.events.network data_stream.namespace defau
                                lt data_stream.type logs destination.address 192.168.1.12 destination.bytes 0 destination.ip 192.168.1.12…
☐ ⤢ Dec 9, 2025 @ 12:26:42.903  process.name nmap @timestamp Dec 9, 2025 @ 12:26:42.903 agent.id 52e1c5ec-42c8-4335-9ca9-670cdfcf136e
                                agent.type endpoint agent.version 9.2.2 data_stream.dataset endpoint.events.network data_stream.namespace defau
                                lt data_stream.type logs destination.address 192.168.1.12 destination.bytes 0 destination.ip 192.168.1.12…
☐ ⤢ Dec 9, 2025 @ 12:26:42.903  process.name nmap @timestamp Dec 9, 2025 @ 12:26:42.903 agent.id 52e1c5ec-42c8-4335-9ca9-670cdfcf136e
                                agent.type endpoint agent.version 9.2.2 data_stream.dataset endpoint.events.network data_stream.namespace defau
                                lt data_stream.type logs destination.address 192.168.1.12 destination.bytes 0 destination.ip 192.168.1.12…
☐ ⤢ Dec 9, 2025 @ 12:26:42.903  process.name nmap @timestamp Dec 9, 2025 @ 12:26:42.903 agent.id 52e1c5ec-42c8-4335-9ca9-670cdfcf136e
                                agent.type endpoint agent.version 9.2.2 data_stream.dataset endpoint.events.network data_stream.namespace defau
                                lt data_stream.type logs destination.address 192.168.1.12 destination.bytes 0 destination.ip 192.168.1.12…
☐ ⤢ Dec 9, 2025 @ 12:26:42.903  process.name nmap @timestamp Dec 9, 2025 @ 12:26:42.903 agent.id 52e1c5ec-42c8-4335-9ca9-670cdfcf136e
                                agent.type endpoint agent.version 9.2.2 data_stream.dataset endpoint.events.network data_stream.namespace defau
```

Perfect, we can check the scan, and others details, like date, hour and destination.



```
rm64/elastic-agent-9.2.2-linux-x86_64$ nmap 192.168.1.12 -A
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-09 12:45 WET
Nmap scan report for brandon-HP-EliteDesk.home (192.168.1.12)
Host is up (0.00021s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 63:0b:24:fd:be:f9:41:0a:b3:66:71:34:1c:46:0e:df (ECDSA)
|_  256 41:98:a0:a6:fd:61:19:92:29:4f:76:0b:c5:47:da:66 (ED25519)
3389/tcp open  ms-wbt-server?
8080/tcp open  http-proxy
|_http-open-proxy: Proxy might be redirecting requests
```

Now, we are going to use a filter -A to see what happens in the Elastic logs.



```
Dec 9, 2025 @ 12:47:31.543
Dec 9, 2025 @ 12:45:58.977
Dec 9, 2025 @ 12:45:58.977
Dec 9, 2025 @ 12:45:58.977
Dec 9, 2025 @ 12:45:58.977
```

```
    process-default-2025.12.09-000001",
  "_id": "AZsDJxX4AmKWAFt7r0Qp",
  "_version": 1,
  "_score": null,
  "fields": {
    "process.command_line.caseless": [
      "nmap 192.168.1.12 -a"
    ],
    "event.category": [
      "process"
```

```
543 agent.id 52e1c5ec-42c8-4335-9ca9-670cdfcf136e
lataset endpoint.events.process data_stream.namespace defa
agent.id 52e1c5ec-42c8-4335-9ca9-670cdfcf136e event.action
977 agent.id 52e1c5ec-42c8-4335-9ca9-670cdfcf136e
lataset endpoint.events.network data_stream.namespace defa
1.12 destination.bytes 0 destination.ip 192.168.1.12…
977 agent.id 52e1c5ec-42c8-4335-9ca9-670cdfcf136e
lataset endpoint.events.network data_stream.namespace defa
1.12 destination.bytes 0 destination.ip 192.168.1.12…
977 agent.id 52e1c5ec-42c8-4335-9ca9-670cdfcf136e
lataset endpoint.events.network data_stream.namespace defa
1.12 destination.bytes 0 destination.ip 192.168.1.12…
977 agent.id 52e1c5ec-42c8-4335-9ca9-670cdfcf136e
agent.type endpoint agent.version 9.2.2 data_stream.dataset endpoint.events.network data_stream.namespace defa
```

If we expand the log, we can check the command that was used and his filter.