

Day 29 -Elastic Defend Setup Tutorial

INSTALLAZIONE DELL'EDR DI ELASTIC (ELASTIC DEFEND)

Day 29 - Elastic Defend Setup Tutorial

Per procedere con l'installazione di **Elastic Defend** andiamo su **Kibana** , sezione Management->Integrations. Clicchiamo su 'Add Elastic Defend'.
Diamo un nome ed una descrizione configurazione dell'immagine di fianco.

Select configuration settings

Use quick settings to configure the integration to **protect your traditional endpoints or dynamic cloud environments**. You can make configuration changes after you create the integration.

Select the type of environment you want to protect:

Traditional Endpoints (desktops, laptops, virtual machines) ▼

- ☐ Data Collection
Augment your existing anti-virus solution with advanced data collection and detection
- ☐ Next-Generation Antivirus (NGAV)
Machine learning malware, ransomware, memory threat, malicious behavior, and credential theft preventions, plus process telemetry
- ☐ Essential EDR (Endpoint Detection & Response)
Everything in NGAV, plus file and network telemetry
- ☒ Complete EDR (Endpoint Detection & Response)
Everything in Essential EDR, plus full telemetry

2

Where to add this integration?

New hosts Existing hosts

Agent policy

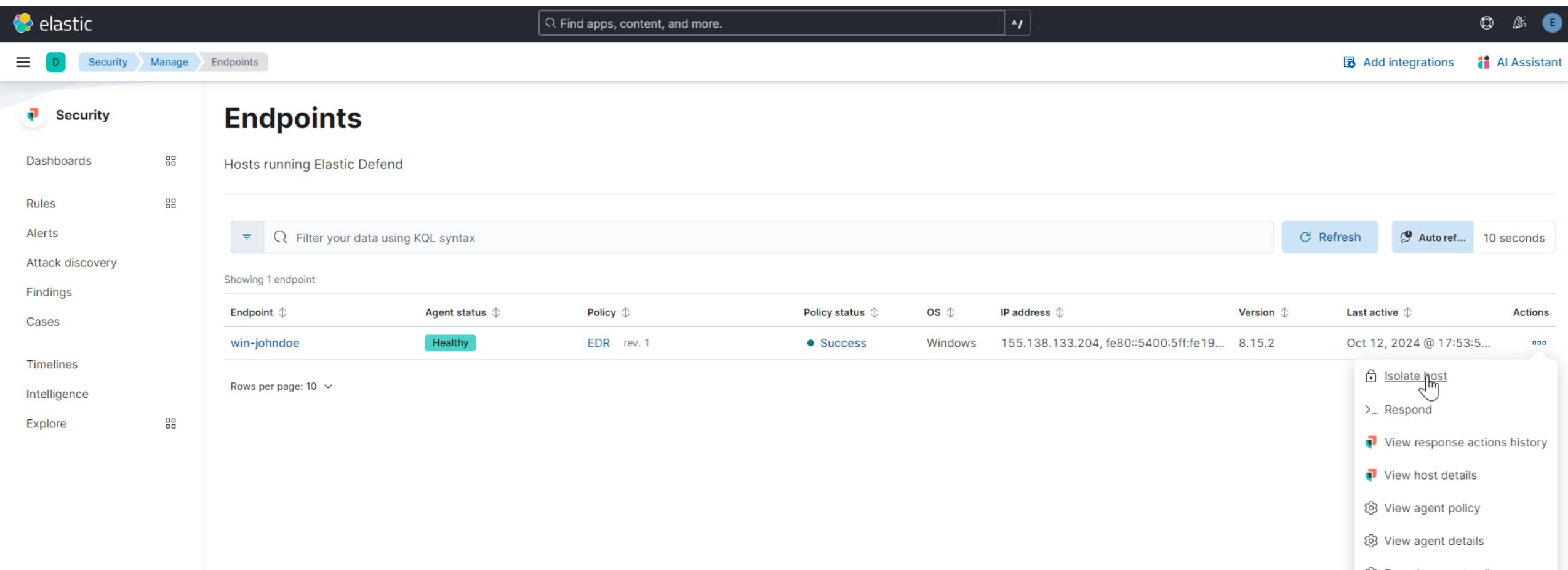
Agent policies are used to manage a group of integrations across a set of agents.

Agent policy

Windows-Policy ▼

2 agents are enrolled with the selected agent policies.

Dalla sezione Security->Management-Endpoints posso vedere gli endpoint su cui è installato **Elastic Defend** e per esempio isolare l'host.



The screenshot displays the Elastic Defend interface. The top navigation bar includes the Elastic logo, a search bar, and user profile information. The left sidebar shows the 'Security' section with various sub-panels. The main content area is titled 'Endpoints' and shows 'Hosts running Elastic Defend'. A table lists the endpoints, with one entry 'win-johndoe' highlighted. A context menu is open for this entry, showing actions like 'Isolate host', 'Respond', 'View response actions history', 'View host details', 'View agent policy', and 'View agent details'.

Endpoints

Hosts running Elastic Defend

Filter your data using KQL syntax

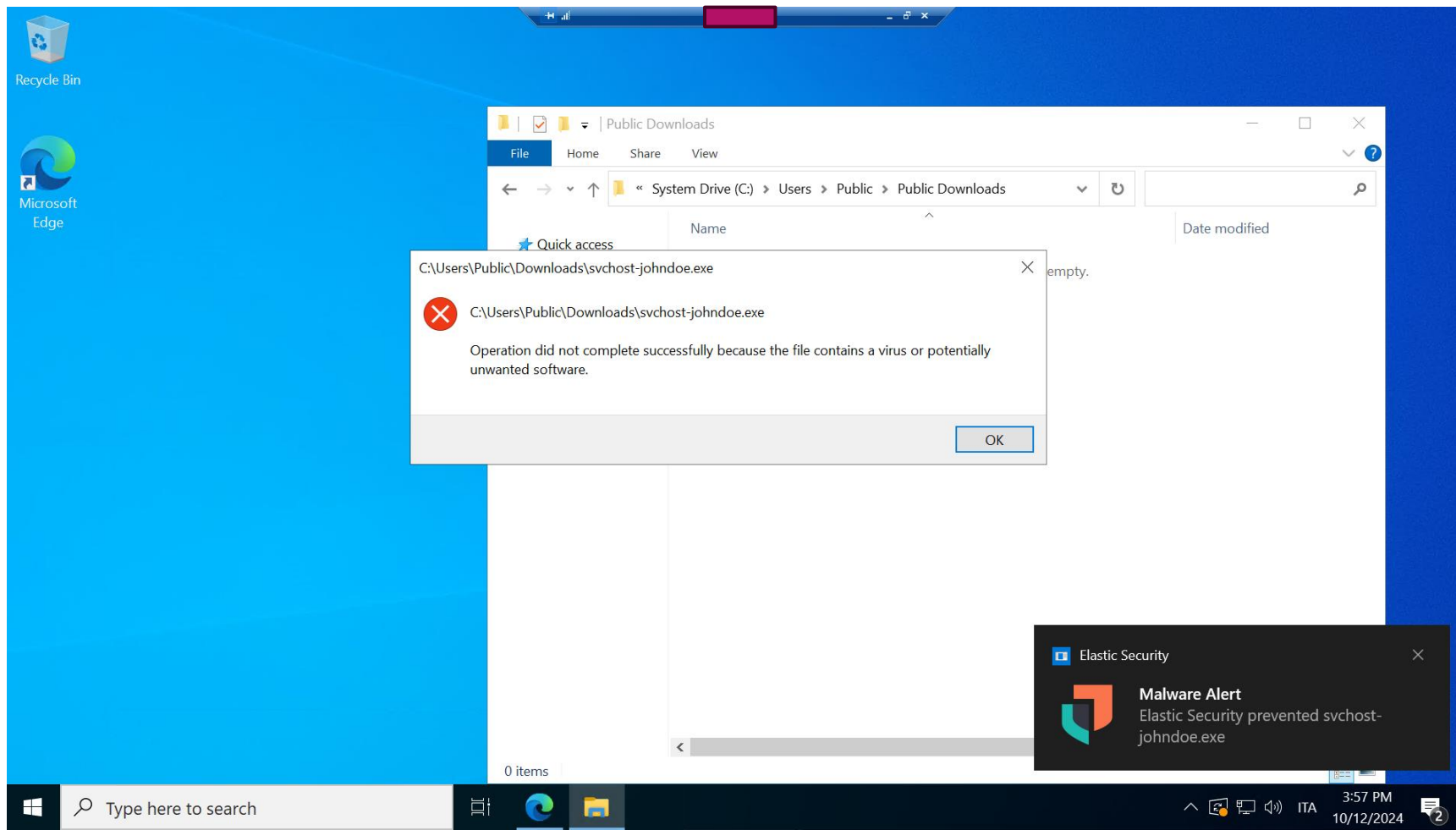
Refresh Auto ref... 10 seconds

Showing 1 endpoint

Endpoint	Agent status	Policy	Policy status	OS	IP address	Version	Last active	Actions
win-johndoe	Healthy	EDR rev. 1	Success	Windows	155.138.133.204, fe80::5400:5ff:fe19...	8.15.2	Oct 12, 2024 @ 17:53:5...	<ul style="list-style-type: none">Isolate host> RespondView response actions historyView host detailsView agent policyView agent details

Rows per page: 10

Infatti se provo ora ad avviare il payload per avviare la callback su **Mythic** verrà istantaneamente bloccato ed eliminato dall'EDR.



Day 29 -Elastic Defend Setup Tutorial

Vediamo la telemetria generata da **Elastic Defend**, possiamo osservare l'alert che ha rilevato il payload.

The screenshot displays the Elastic Defend interface. At the top, the Elastic logo and a search bar are visible. The main navigation bar includes 'Discover' and 'Alerts'. The search bar contains the query 'malware'. The left sidebar shows 'Popular fields' and 'Available fields'. The main content area features a bar chart showing event frequency over time, with a peak around 17:55. Below the chart, the 'Documents (41)' tab is active, displaying a list of documents. The first document is expanded, showing details about a malware prevention alert. The right sidebar shows the 'Document' view with a table of fields and values.

Documents (41) | Patterns | Field statistics

Sort fields 1

Document | 1 of 41

Actions: [Icon] [Icon]

Table | JSON

Search field names

Field	Value
kibana.alert.workflow_status	open
kibana.space_ids	default
kibana.version	8.15.1
message	Malware Prevention Alert
process.args	C:\Users\Public\Downloads\svchost-john doe.exe

In questo caso l'alert è stato creato in automatico dall'integrazione, possiamo osservare delle info importanti quali il processo relativo all'alert e l'hash del payload.

elastic

Find apps, content, and more.

Security Alerts

Security

Dashboards

Rules

Alerts

Attack discovery

Findings

Cases

Timelines

Intelligence

Explore

Alerts

Filter your data using KQL syntax

Status open 1 Severity User

Summary Trend Counts Treemap

Severity levels

Levels	Count ↓
Low	71
Critical	5
High	2

78 alerts

Alerts by name

Rule name
SSH Brute Force Attempt - johndoe
Mythic-C2-Apollo-Agent-Detected
Malware Prevention Alert

Columns 12 Sort fields 1 78 alerts Fields

Actions	@timestamp	Rule	Assignees	Severity
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Oct 12, 2024 @ 18:02:43.426	Malware Prevention Alert		high
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Oct 12, 2024 @ 17:57:46.404	Mythic-C2-Apollo-Agent-D...		critical
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Oct 12, 2024 @ 17:57:46.402	Mythic-C2-Apollo-Agent-D...		critical

Expand details

High

Oct 12, 2024 @ 18:02:43.426

Malware Prevention Alert

Status Open Risk score 73 Assignees +

Overview Table JSON

explorer.exe, file svchost-johndoe.exe, by Administrator on win-johndoe created high alert Malware Prevention Alert.

Investigation

Investigation guide

There's no investigation guide for this rule.

Highlighted fields

Field	Value
host.name	win-johndoe
agent.status	Healthy
user.name	Administrator
process.executable	C:\Users\Public\Downloads\svchost-johndoe.exe
file.path	C:\Users\Public\Downloads\svchost-johndoe.exe
kibana.alert.rule.type	query
file.name	svchost-johndoe.exe
file.hash.sha256	b63410488b190e512926bb617a11a71e502b1eadf85ea11d4c5ed950eec894a6
file.directory	C:\Users\Public\Downloads

Get started



Day 29 -Elastic Defend Setup Tutorial

Possiamo anche impostare una risposta automatica dell'**EDR** dalle regole dell'alert come visto anche in precedenza.

Quindi sempre da 'Edit Rule Settings' imposteremo nel seguente modo:

Response Actions


Response actions are run on each rule execution.

▼  Elastic Defend 

Response action

isolate ▼

Select an endpoint response action. The response action only runs on hosts with Elastic Defend installed. [Learn more](#)



 **Proceed with caution**

Only select this option if you're certain that you want to automatically block communication with other hosts on your network until you release this host.

Comment (optional)

prova

Leave a note that explains or describes the action. Your comment is included in the response actions history.

 Osquery  Elastic Defend

Grazie alla regola siamo riusciti a bloccare il download!

