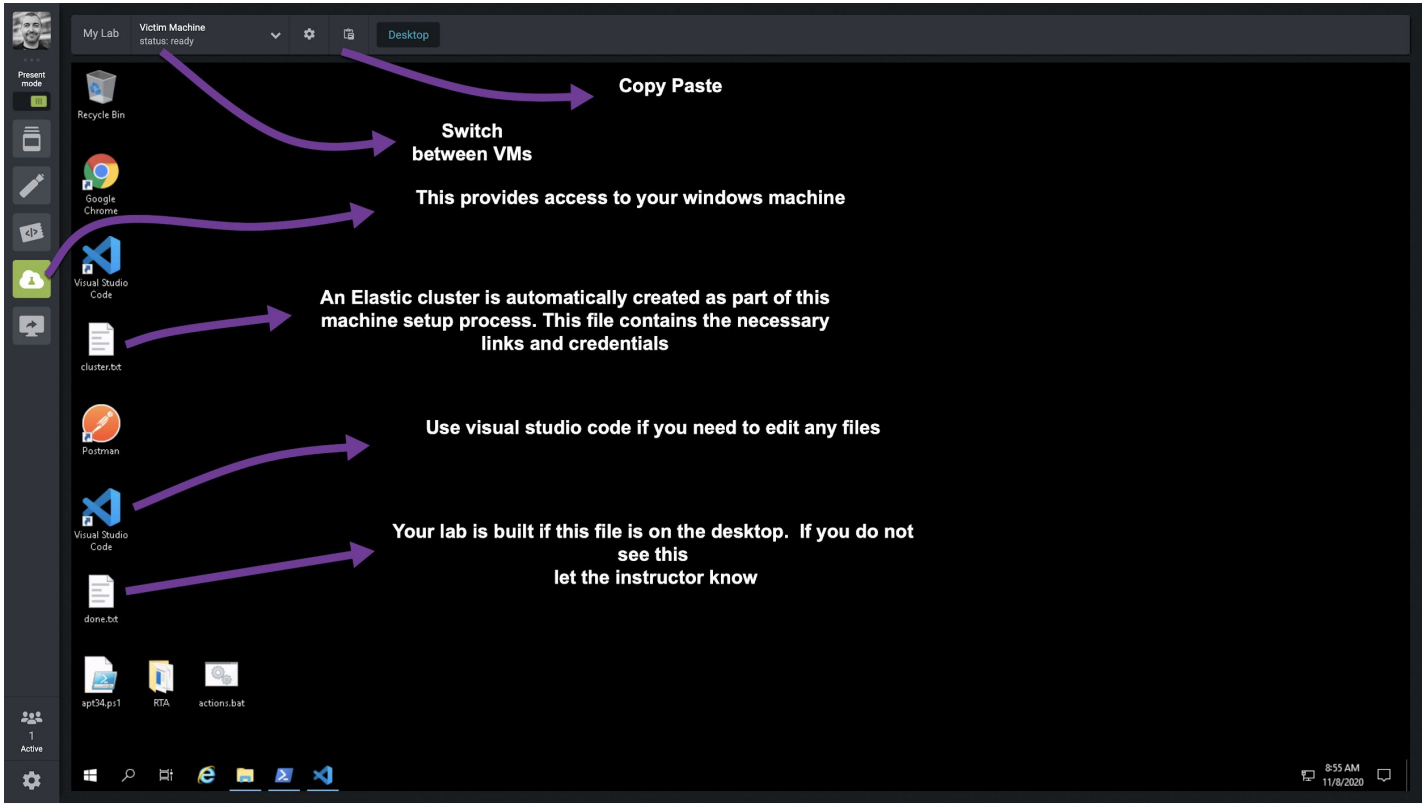
Adversary Emulation Labs

Lab 1 - Data Collection

20 Minutes
Overview and Preparation

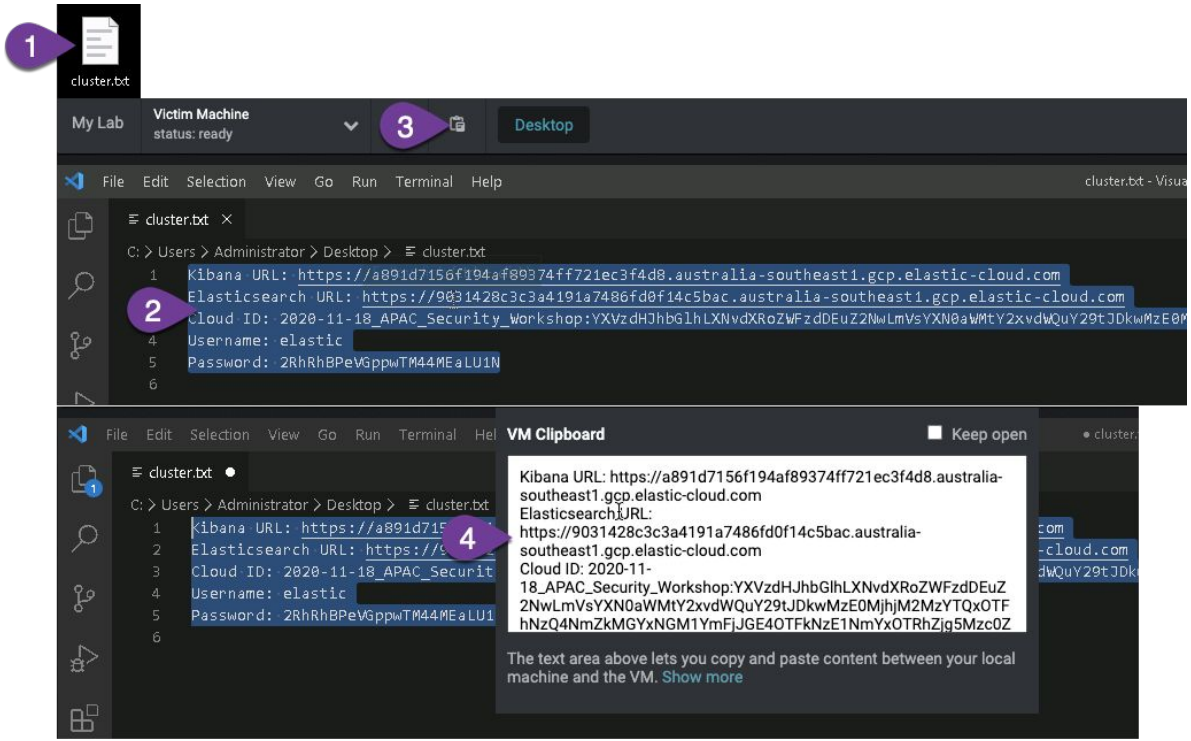
Strigo Overview



Login to Kibana

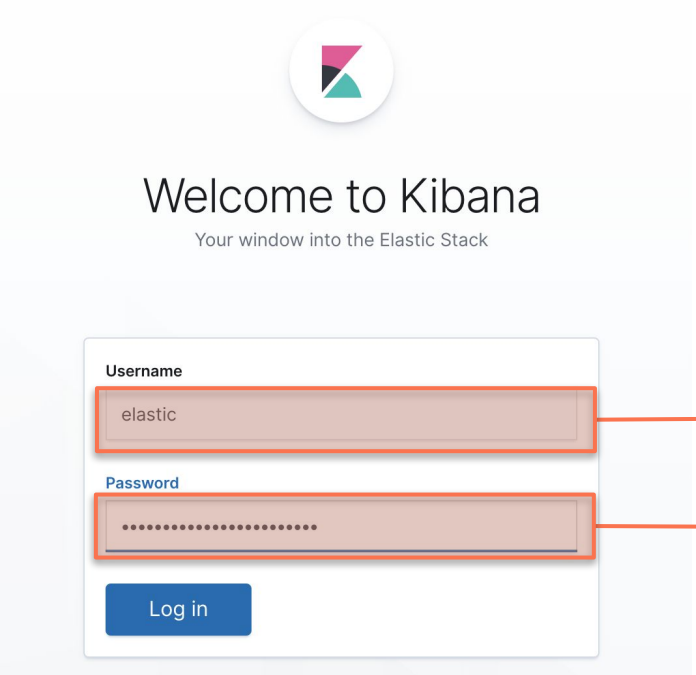
Open **cluster.txt** on your desktop and copy the credentials

On a Mac use “Control + C” not “Command + C”



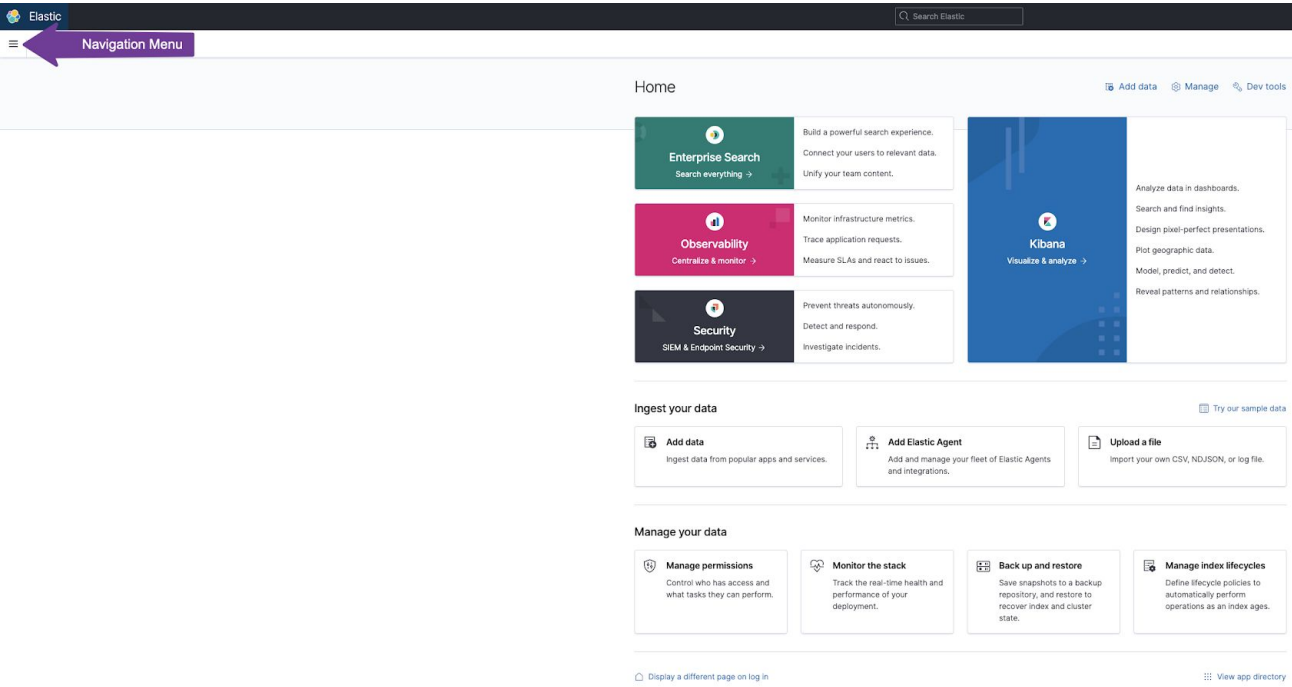
Open browser on your machine and log into Kibana

As user ‘elastic’



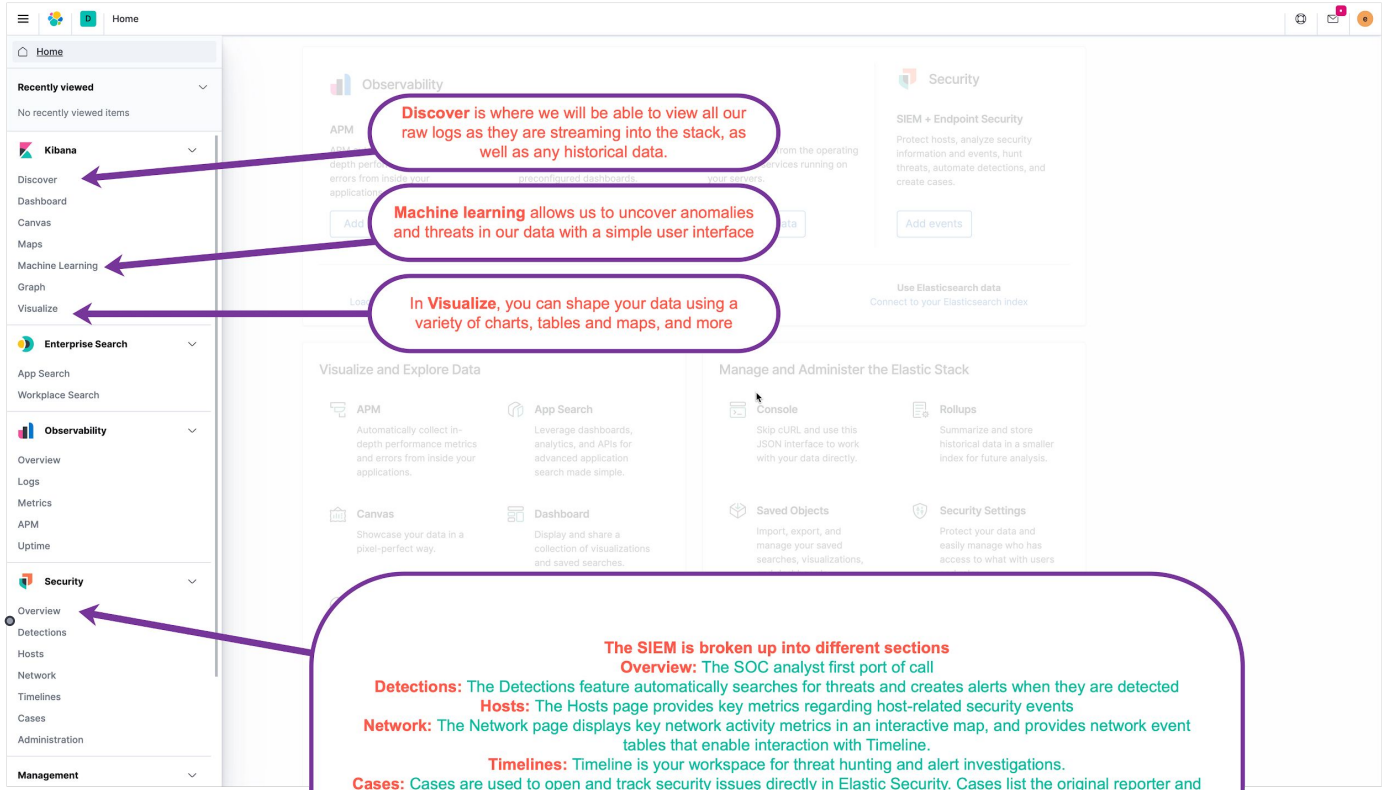
1. Username is: elastic
2. Copy-n-Paste the Cloud elastic user password copied from slide before

Open Navigation Menu



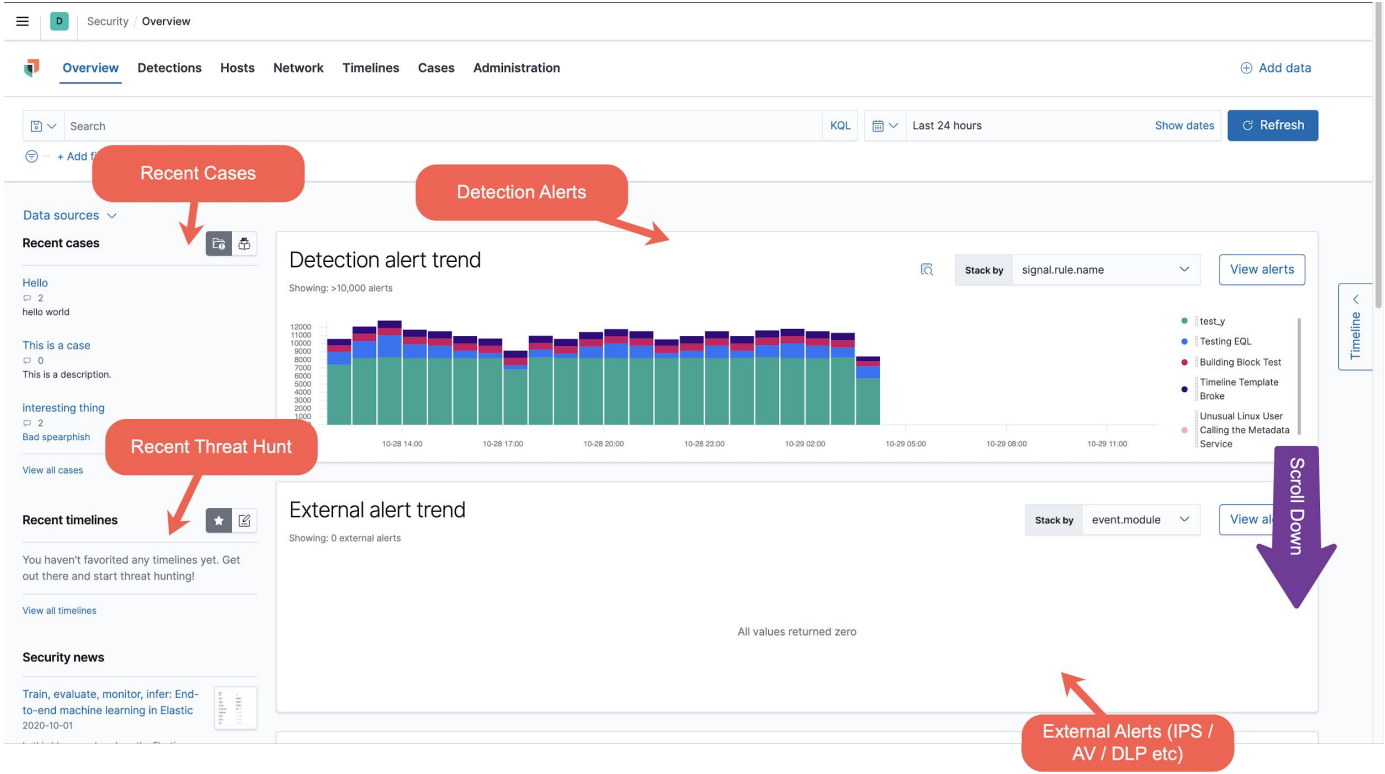
Kibana Menu

Click Overview

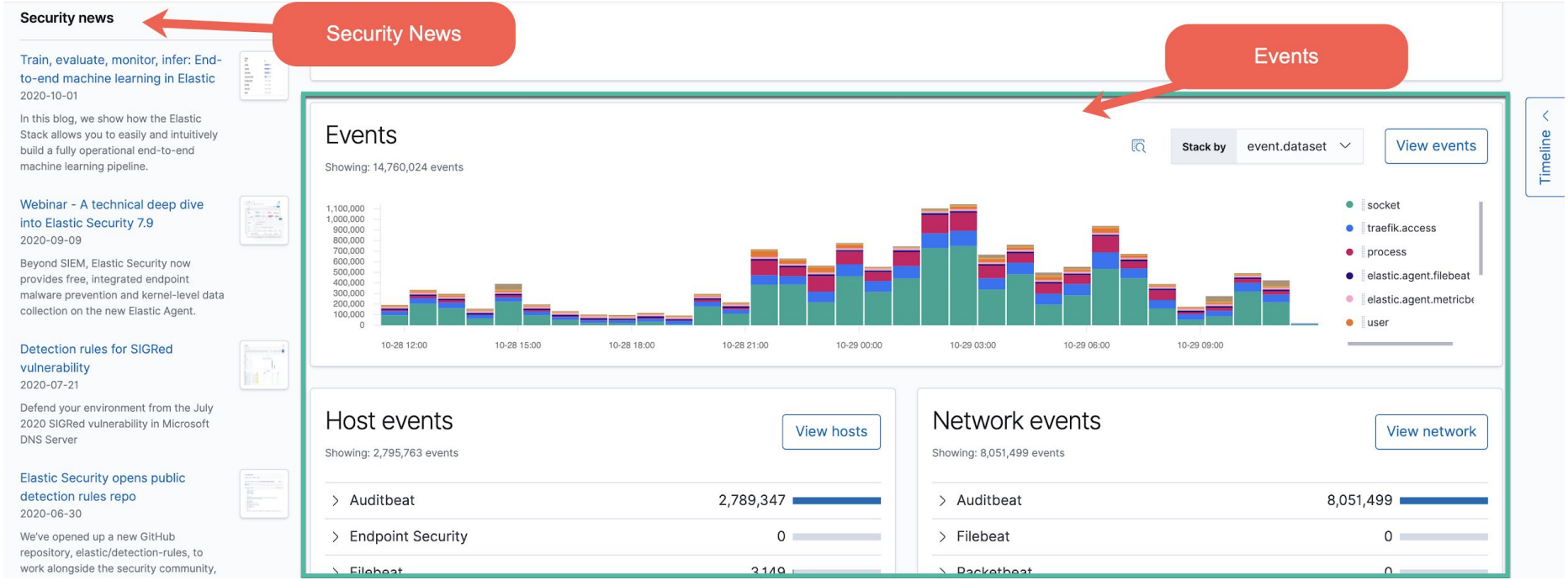


elastic

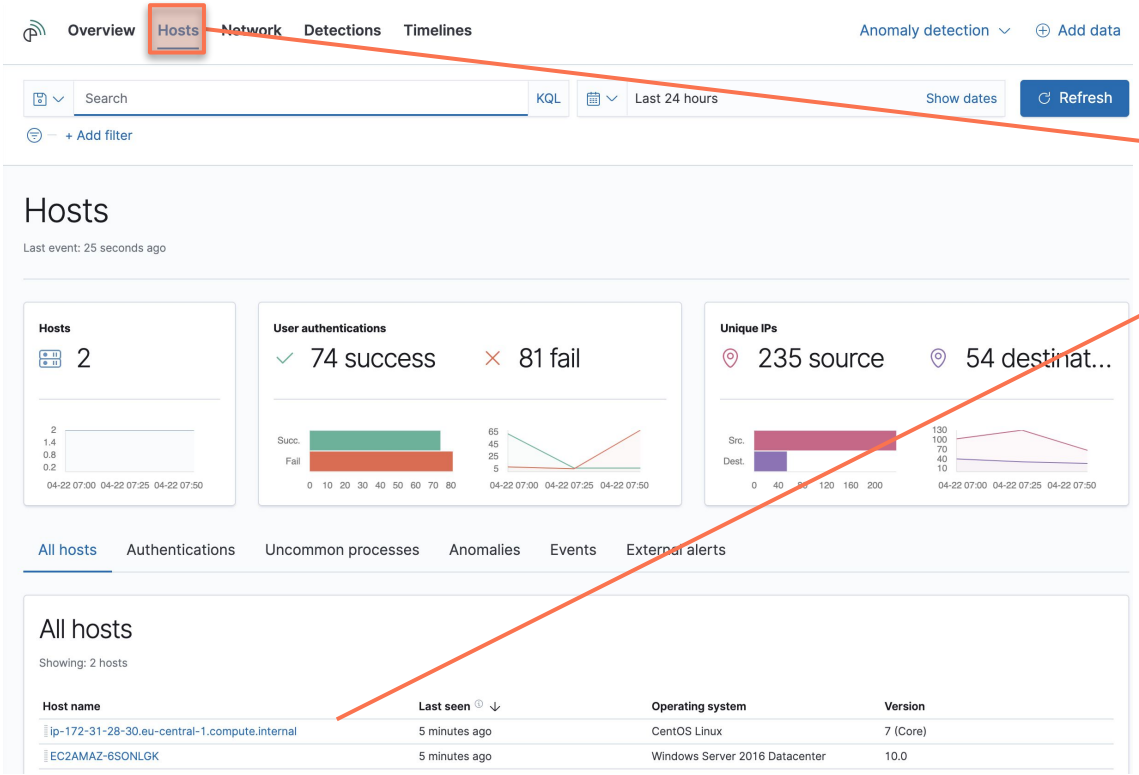
SIEM Overview



SIEM Overview



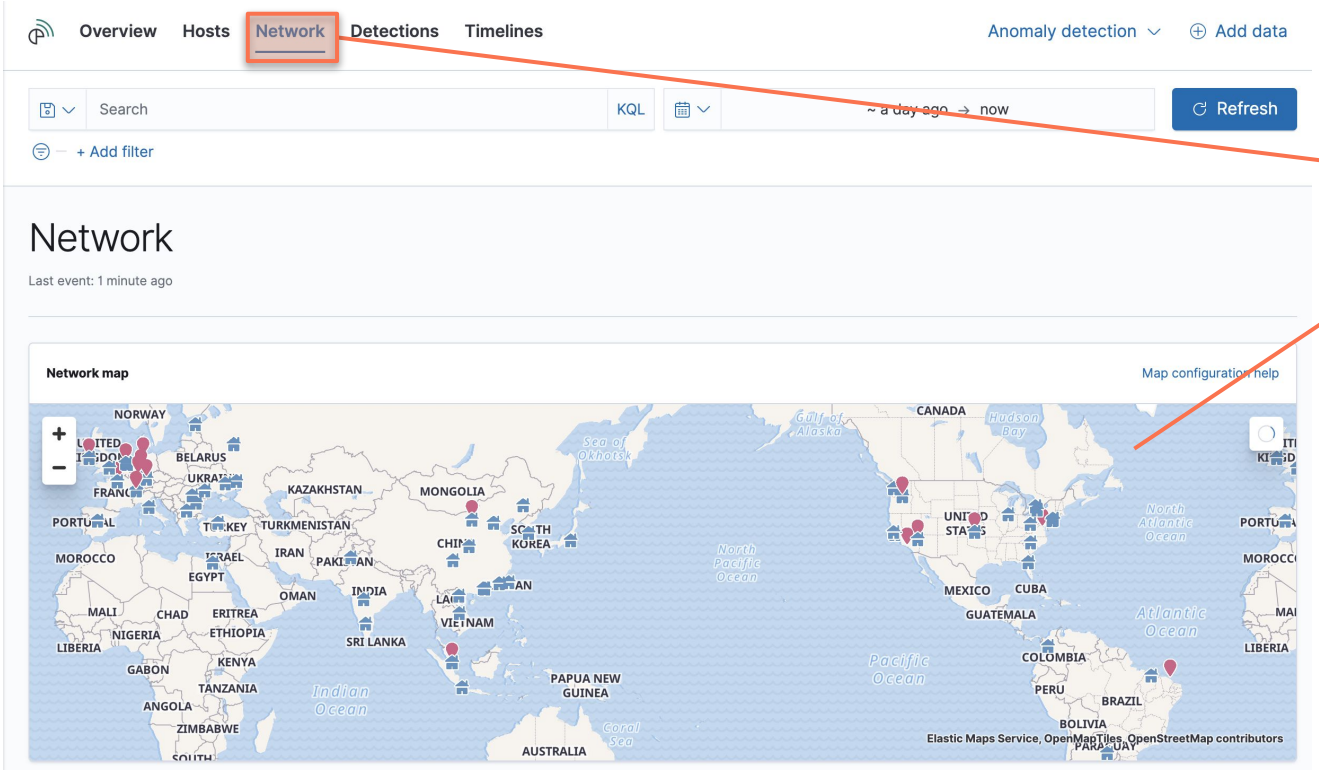
Hosts Overview



1 Click on the Hosts Tab

2 Notice you have VM's available to interrogate. Click on any of the hosts to filter the view on the specific host.

Network Overview



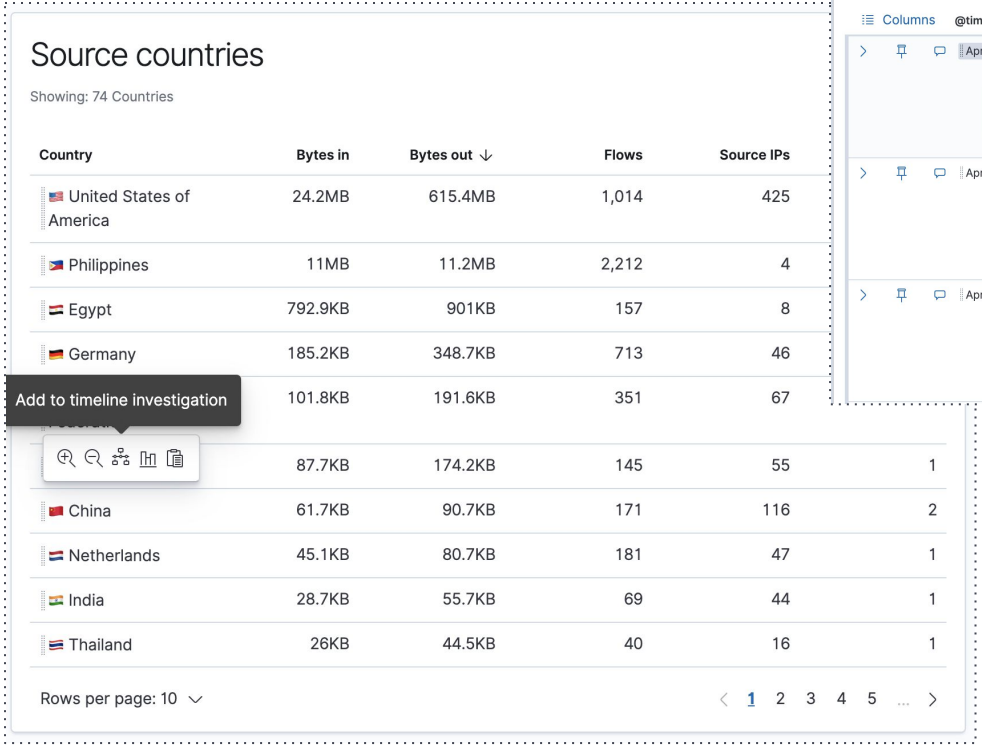
1 Click on the Network Tab

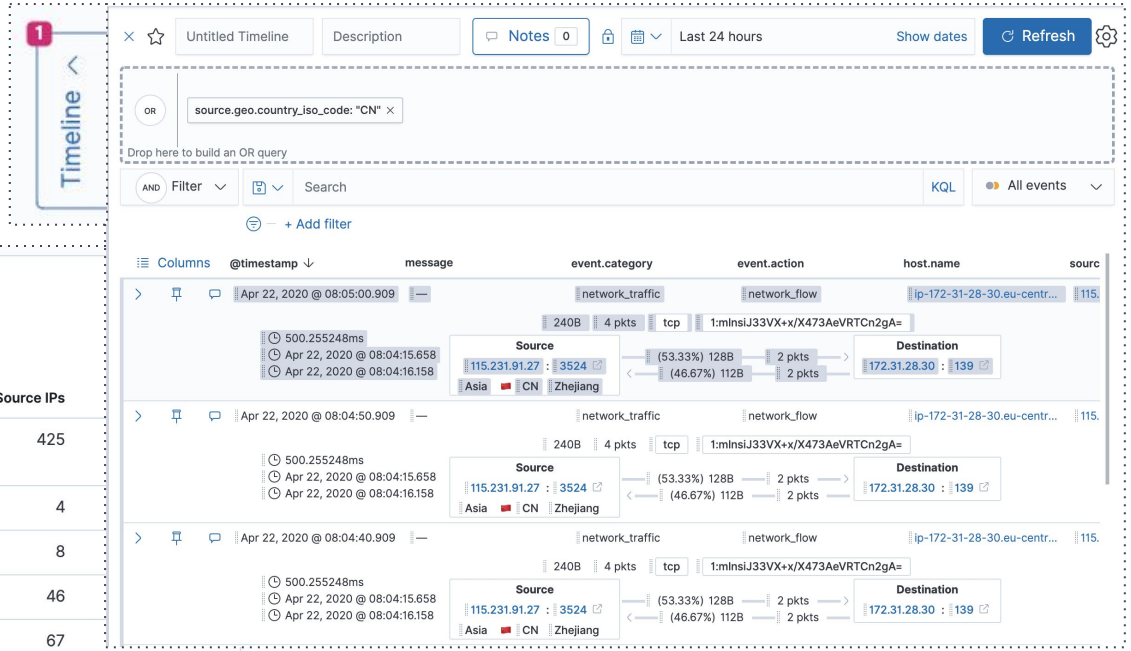
2 Notice the rich network information displayed thanks to geo-IP enrichment at ingest..
Scroll Down to Bottom

elastic

Timeline

Create an Investigation

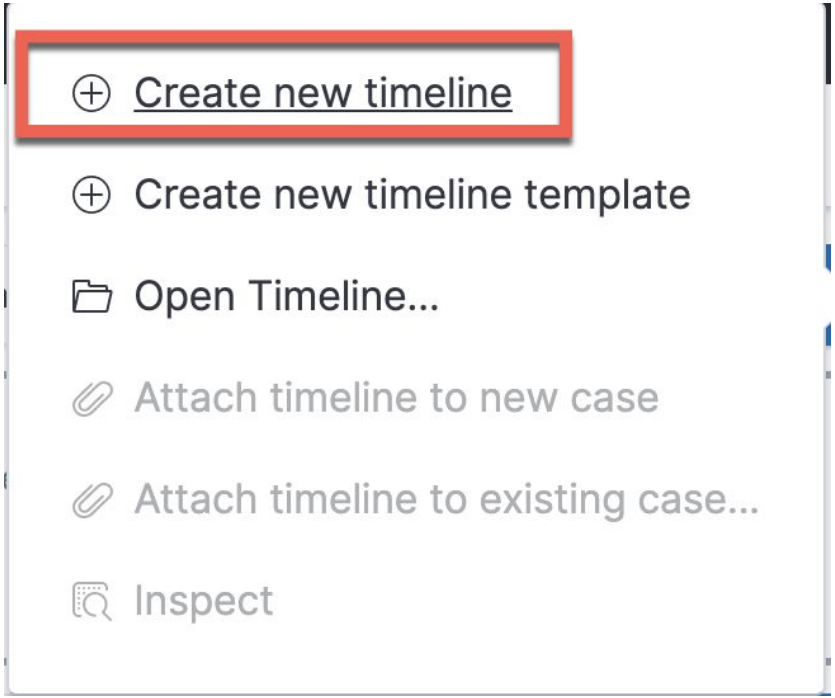




Hover over any field (e.g, Source Country United States of America) then select add to timeline investigation and click the Timeline button

Timeline

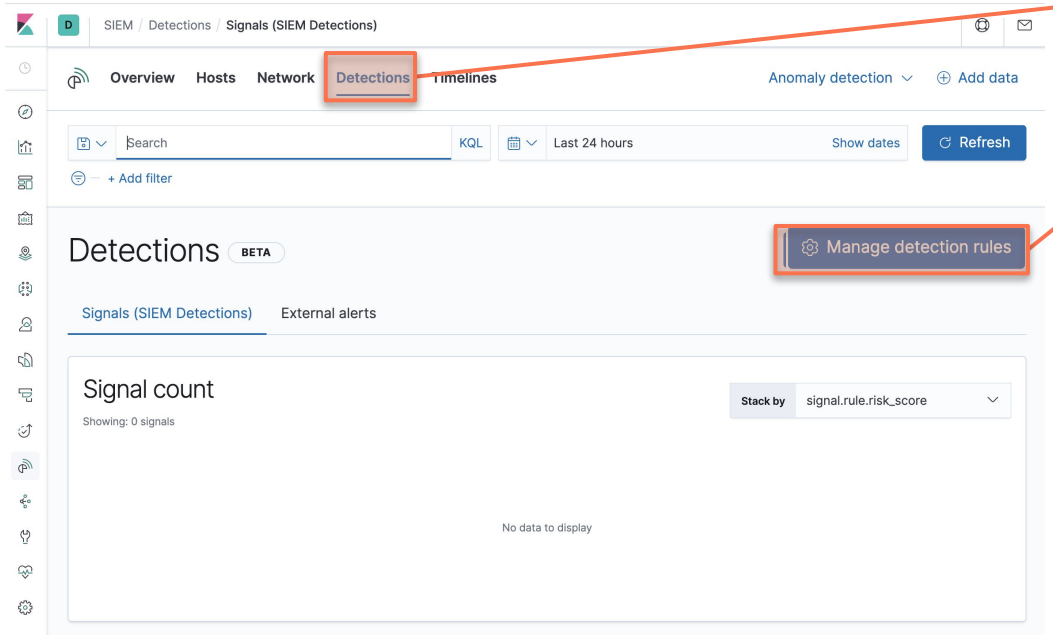
Create new timeline to clear view



elastic

Detections

Enable OOTB Detections

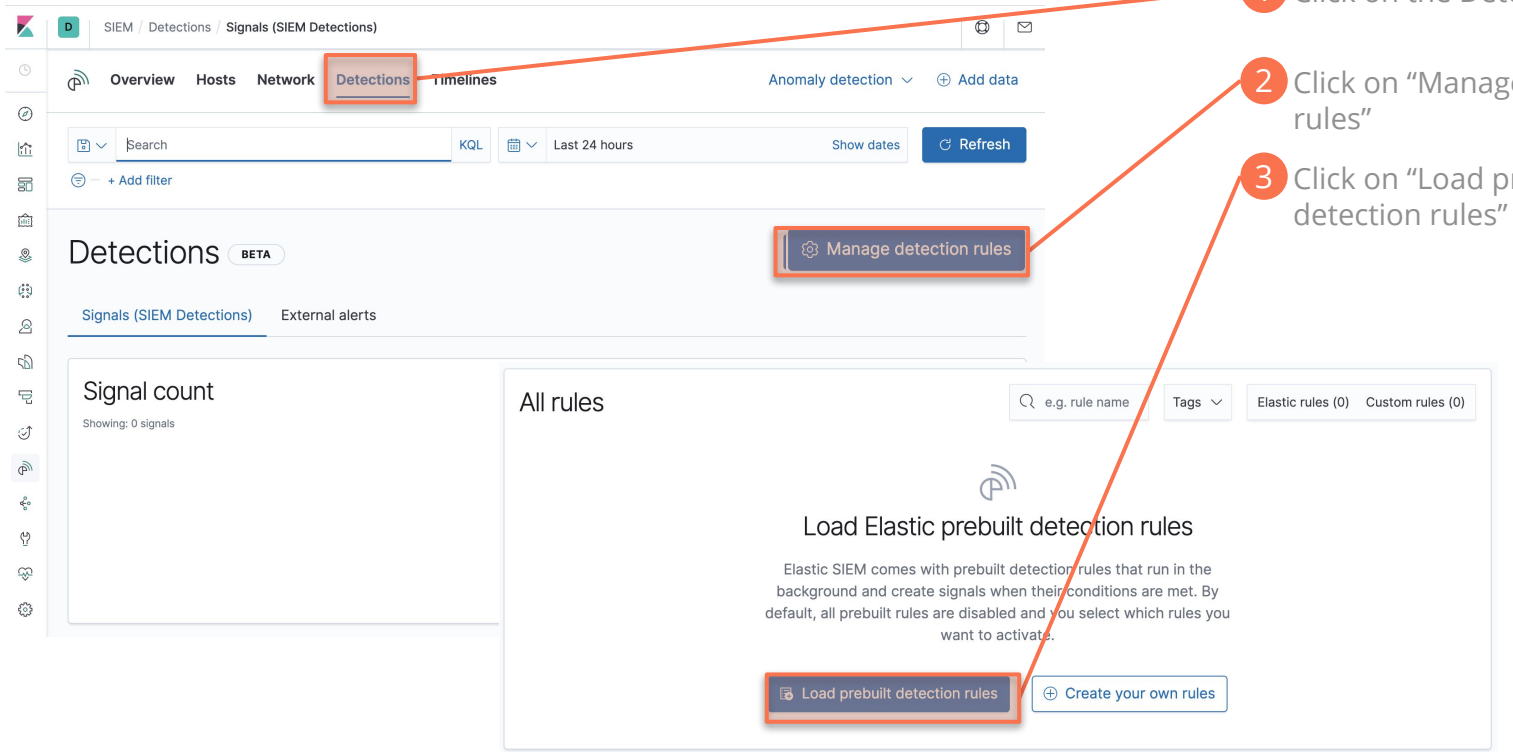


1. Click on the Detections Tab
2. Click on “Manage detection rules”

elastic

Detections

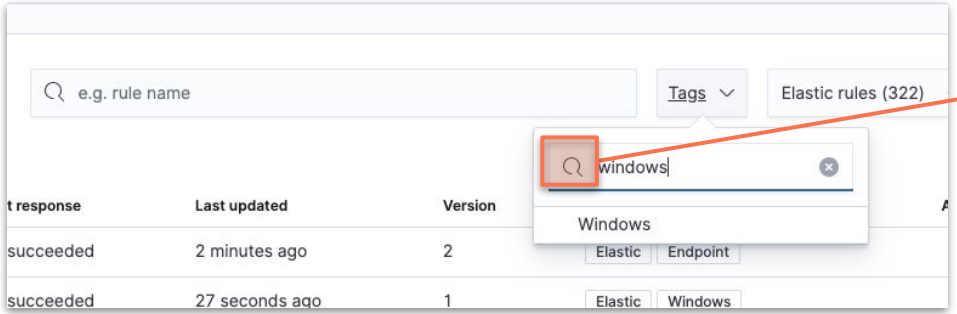
Enable OOTB Detections



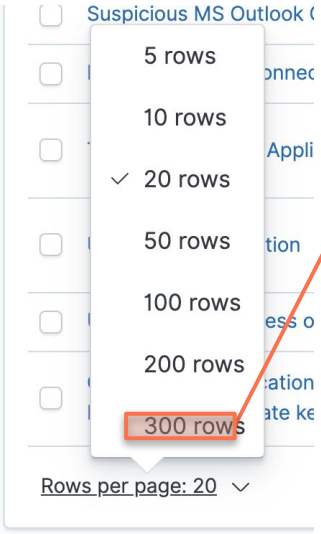
1. Click on the Detections Tab
2. Click on “Manage detection rules”
3. Click on “Load pre-build detection rules”

Detection

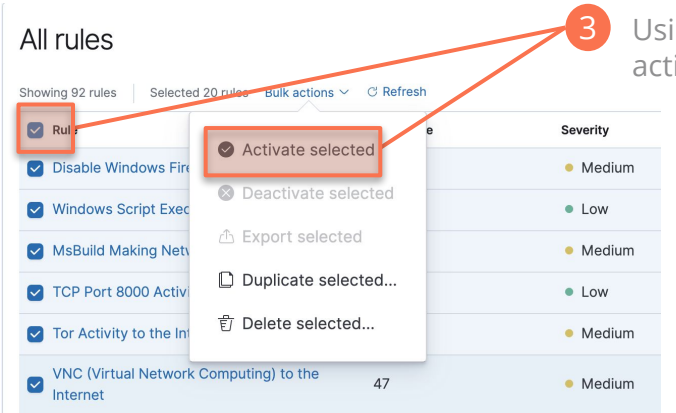
Enable OOTB Detection Rules for **Windows**



1 After spending some time going through the OOTB rules, click the tags **Windows**



2 Select “300 rows”

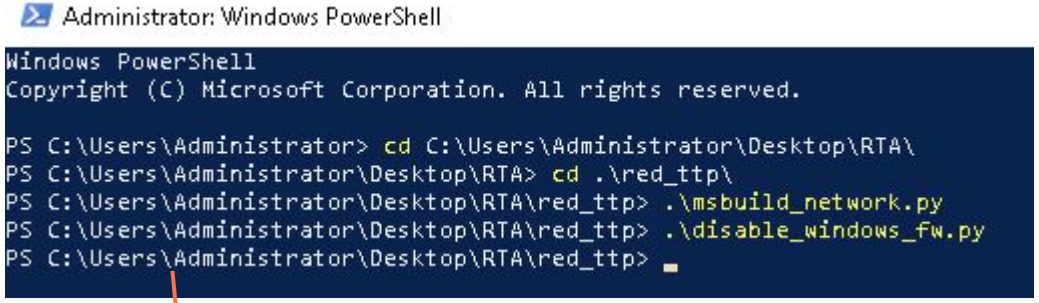


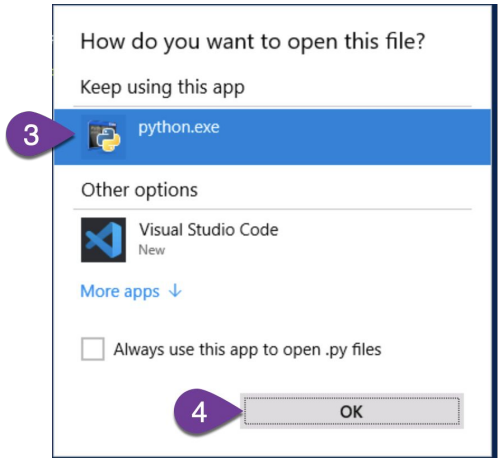
3 Using “Bulk Actions” activate all rules

elastic

Run RTAs on the Windows VM

To generate Signals





1 On your Windows VM in Strigo, execute two of the RTA scripts: msbuild_network.py and disable_windows_fw.pw

2 Within a few minutes, notice the Signals generated in the Detections view of the SIEM app

Apr 22, 2020 @ 07:16:18.890	Trusted Developer Application Usage	1	query	low	21	sysmon
Apr 22, 2020 @ 07:15:37.021	MsBuild Making Network Connections	1	query	medium	47	sysmon
Apr 22, 2020 @ 07:13:24.567	Disable Windows Firewall Rules via Netsh	1	query	medium	47	sysmon

elastic

Useful Fields

Common field names you will interact with

The Easy Ones

source.address
- Source IP Address

source.port
- Source Port

destination.address
- Destination IP Address

destination.port
- Source IP Address

process.pid
- Process ID

process.ppid
- Process parent ID

process.args
- Process Arguments

The Gnarly Ones

process.entity_id
- Unique process ID

process.Ext.ancestry
- A collection of each of the unique Process ID's per host

_id
- A unique reference for the document you are looking at

process.code_signature.status
- Whether a process executable is signed

Try some searches in timeline

K

Q

L

powershell.exe - Free Text Search

process.name: powershell.exe - Field Search

(powershell.exe and event.module: sysmon) - Boolean AND / OR

process.name: powershell.exe and not (event.action: network_flow or event.action: log_on) - NOT with OR

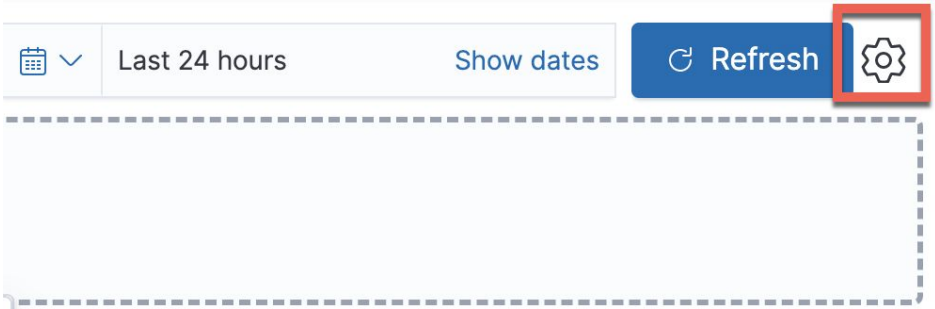
process.pid >= 1000 and process.pid <= 1500 - Range query

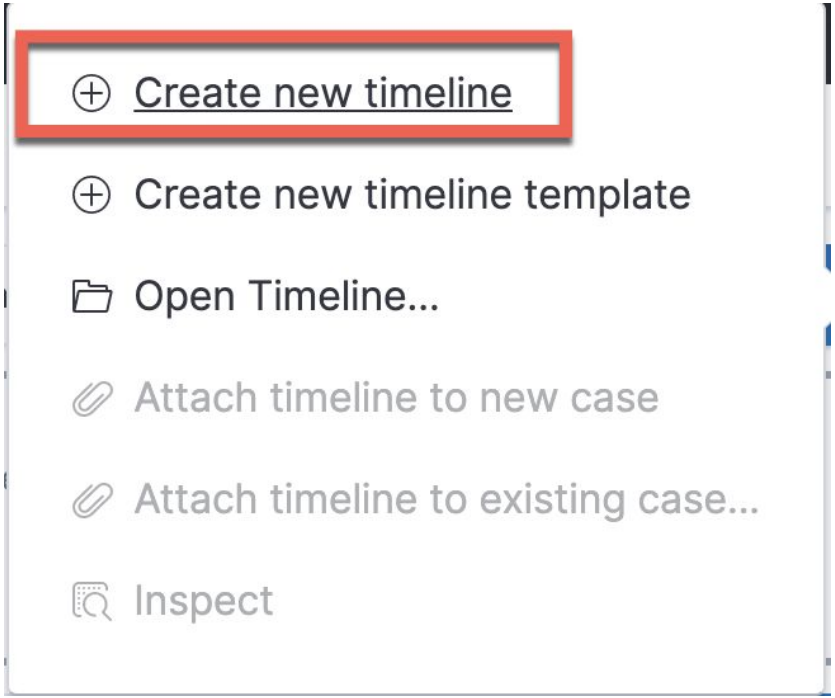
process.name: powersh* - Wildcard Search

host.os*:windows - Wildcard field match

Timeline

Create new timeline to clear view





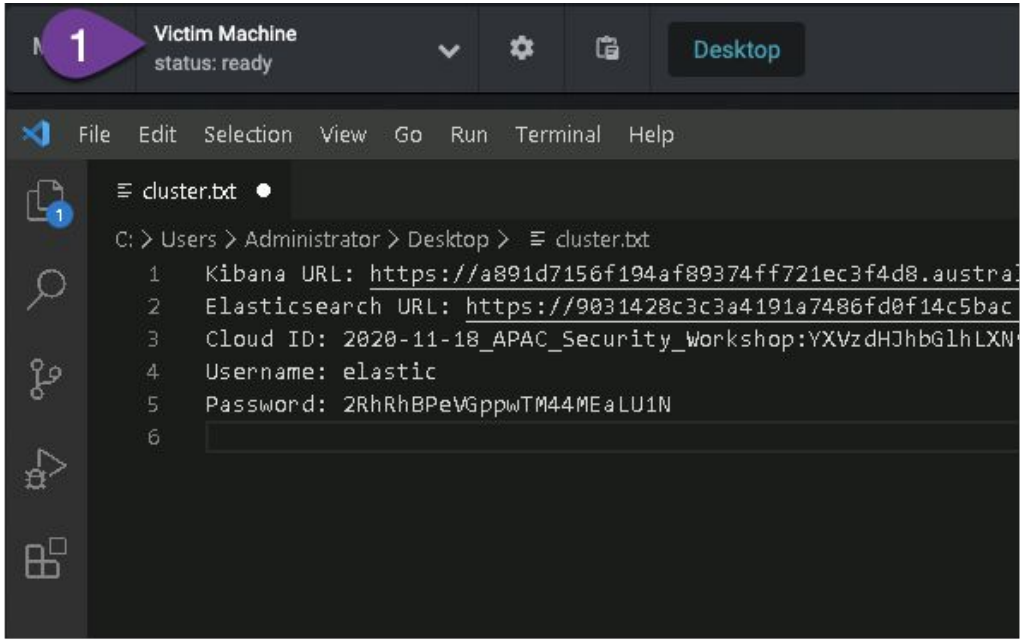
elastic

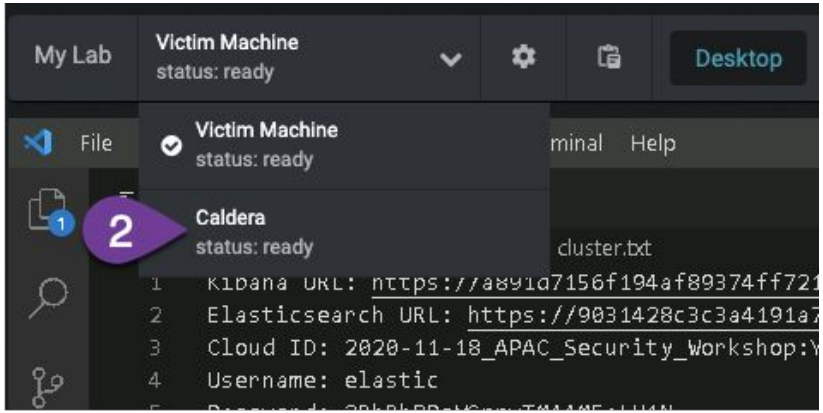
End Lab 1

Lab 2 - Implant Deployment & Adversary Execution

20 Minutes

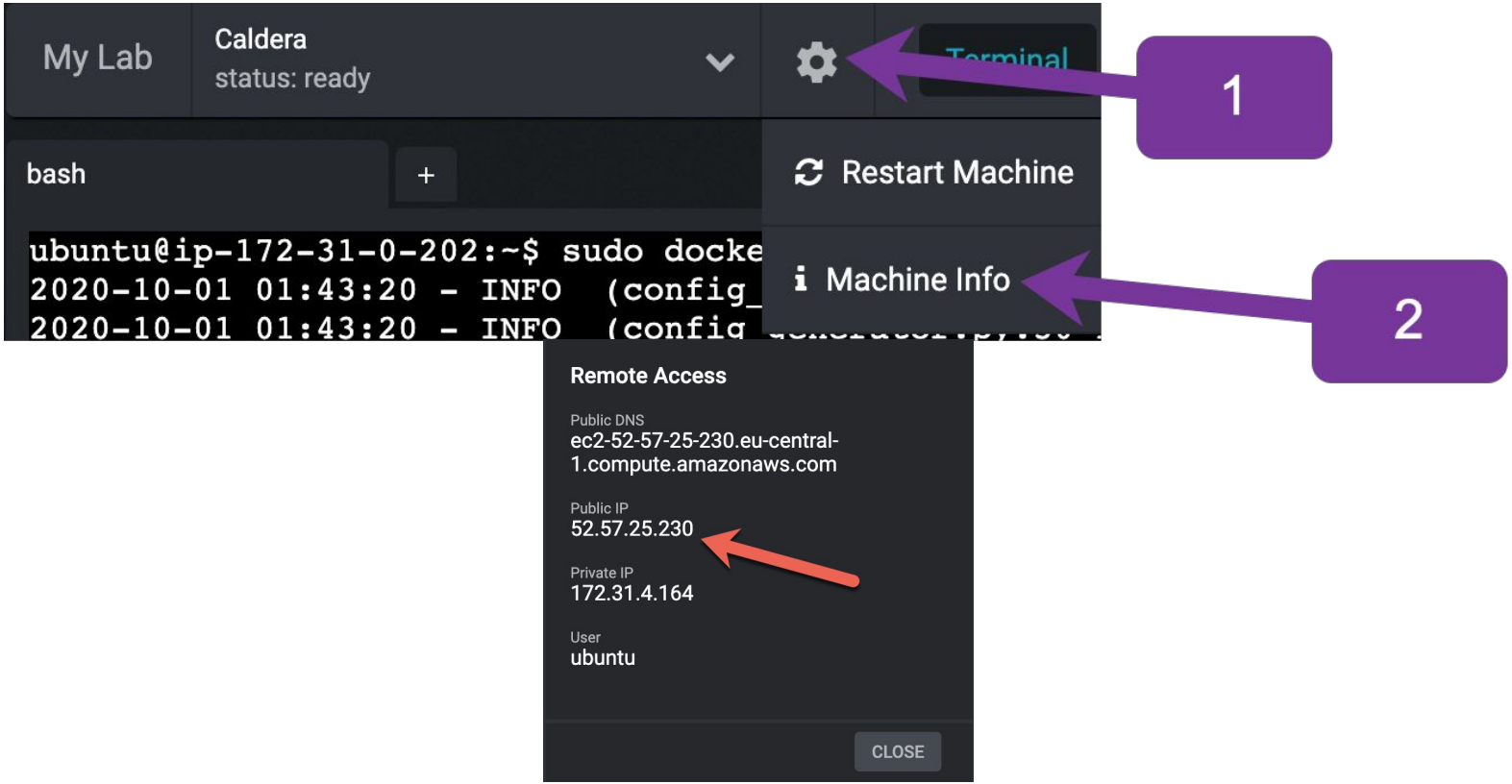
Switch to Caldera





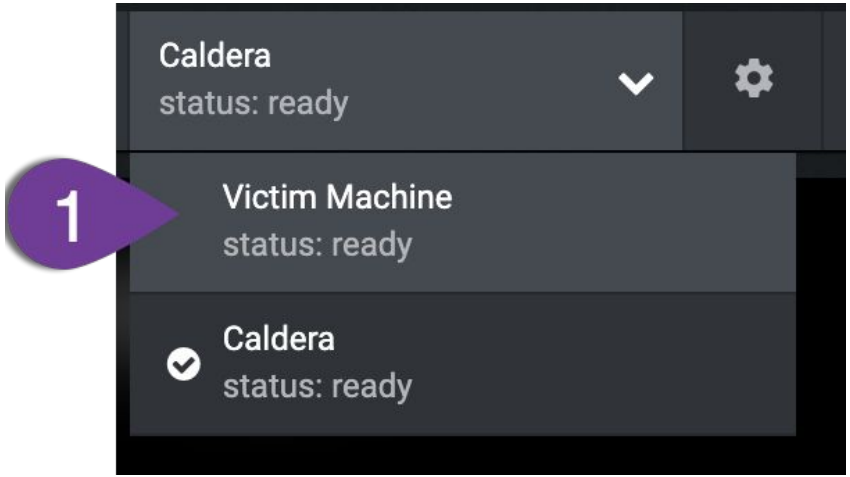
Retrieve IP For Caldera Server

Copy the Public IP address, this will be used for the implant

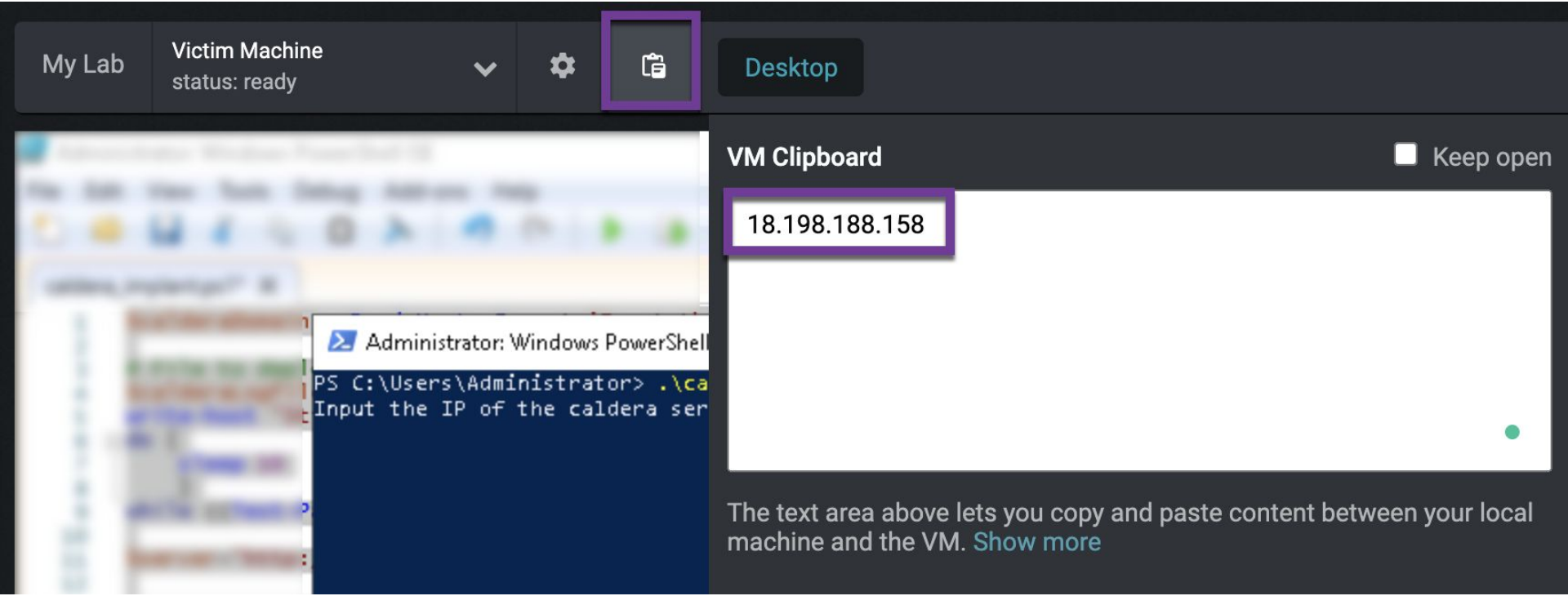


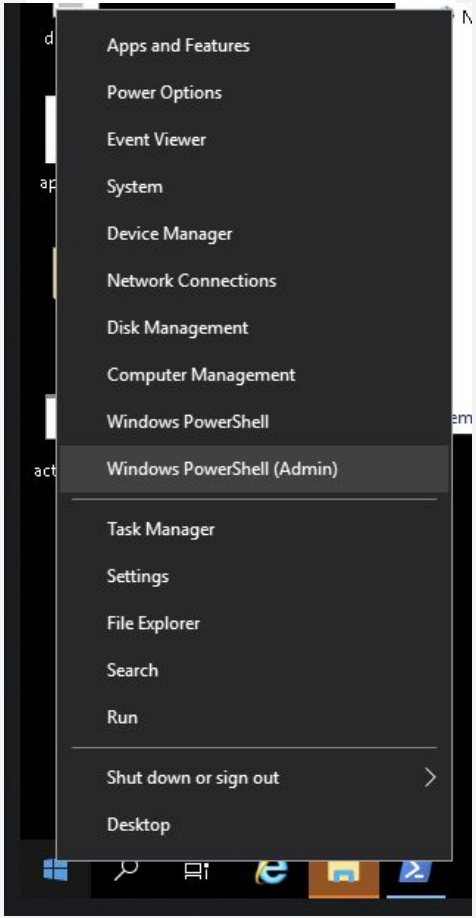
elastic

Switch back to the victim machine



Copy Clipboard

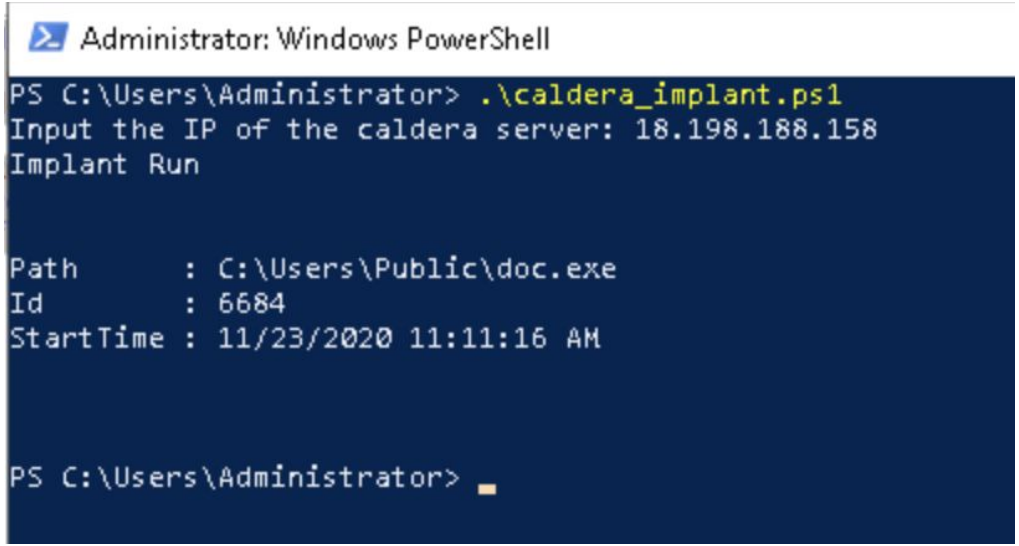




Run powershell in **admin mode** by **right clicking** the windows flag icon

Run Caldera Implant.ps1

To generate Signals

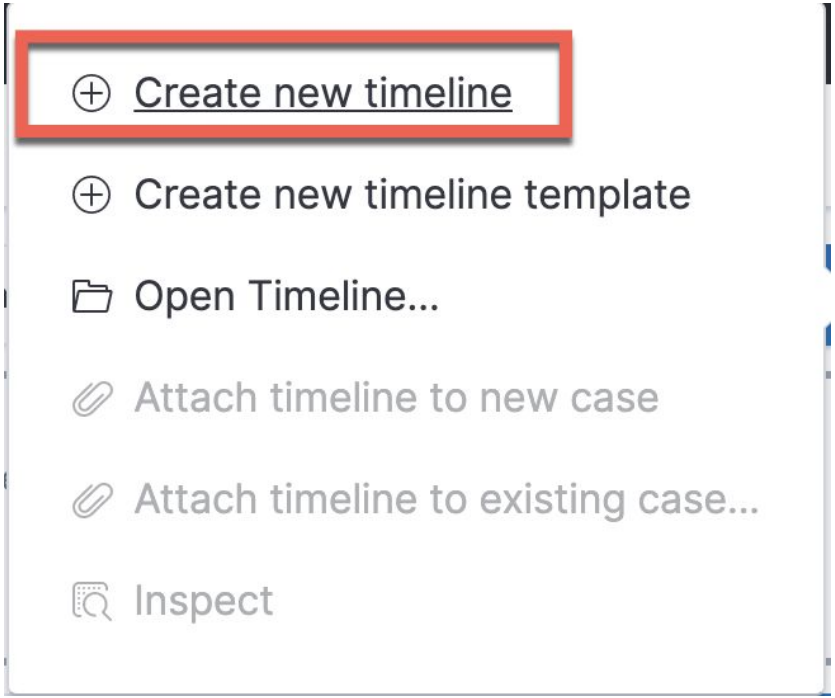


On your Windows VM in Strigo, execute **.\caldera_implant.ps1**
From **C:\Users\Administrator**
Paste in your IP from Caldera here

elastic

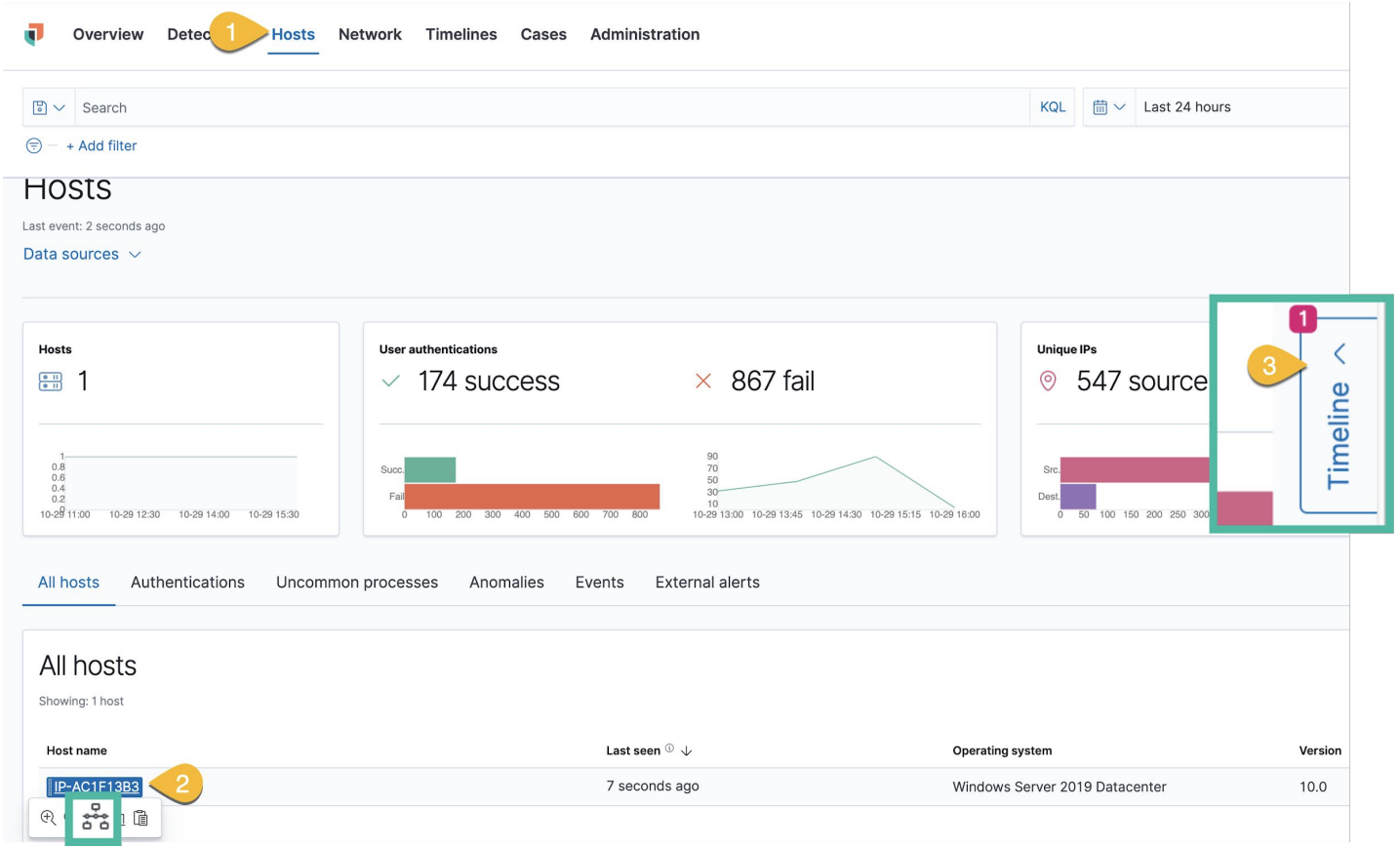
Timeline

Create new timeline to clear view



elastic

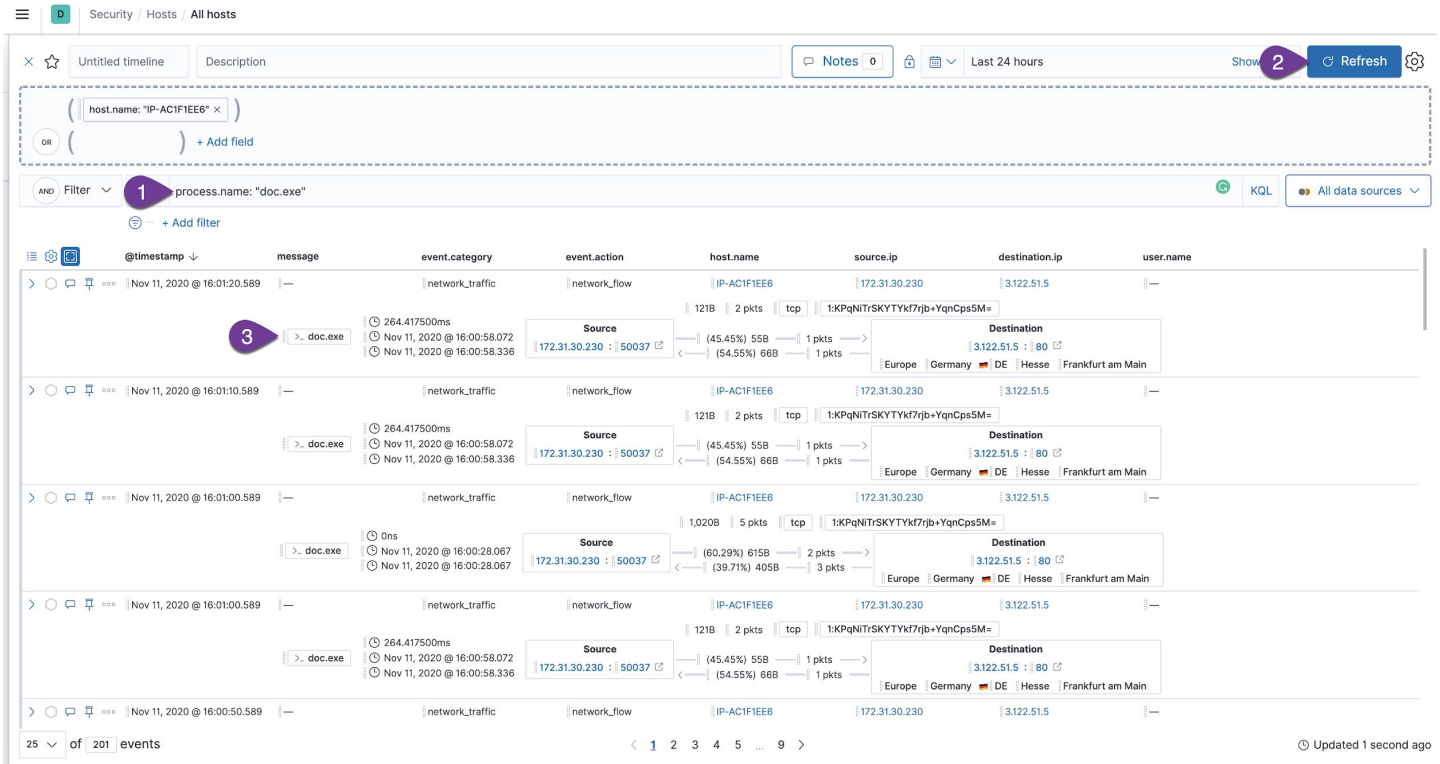
Confirm Eyes On in Elastic



elastic

Search for the process

process.name: **doc.exe**

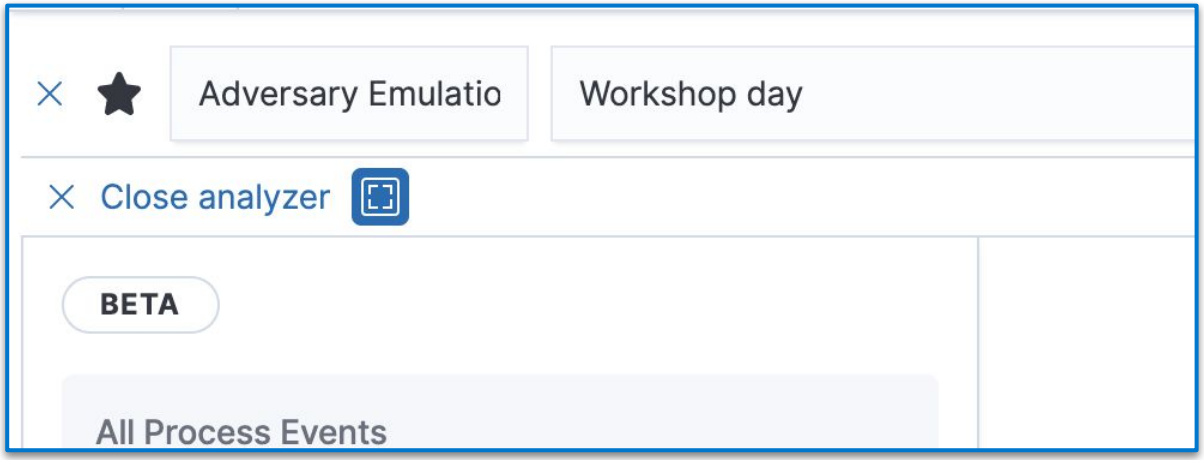


Save timeline

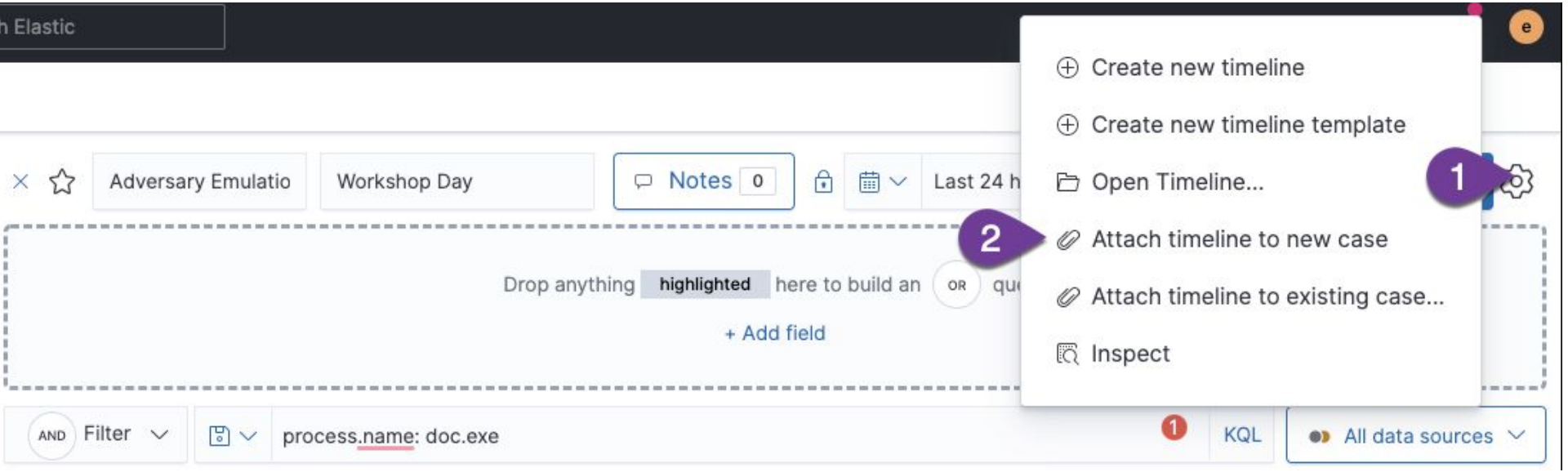
Enter a title and description. No save button required :)

Title: Adversary Emulation

Description: Workshop Day



Create A New Case



elastic

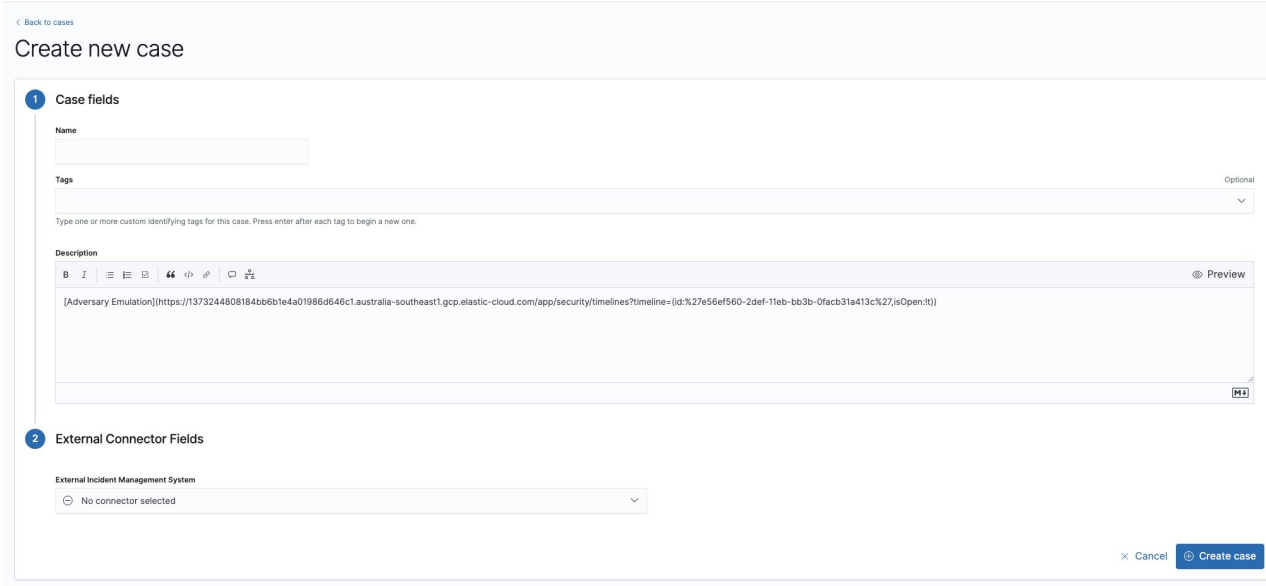
Create A New Case Continued

Enter a title and description. No save button required :)

Name: Adversary Emulation

Tags: emulation

Click **Create Case**



End Lab 2

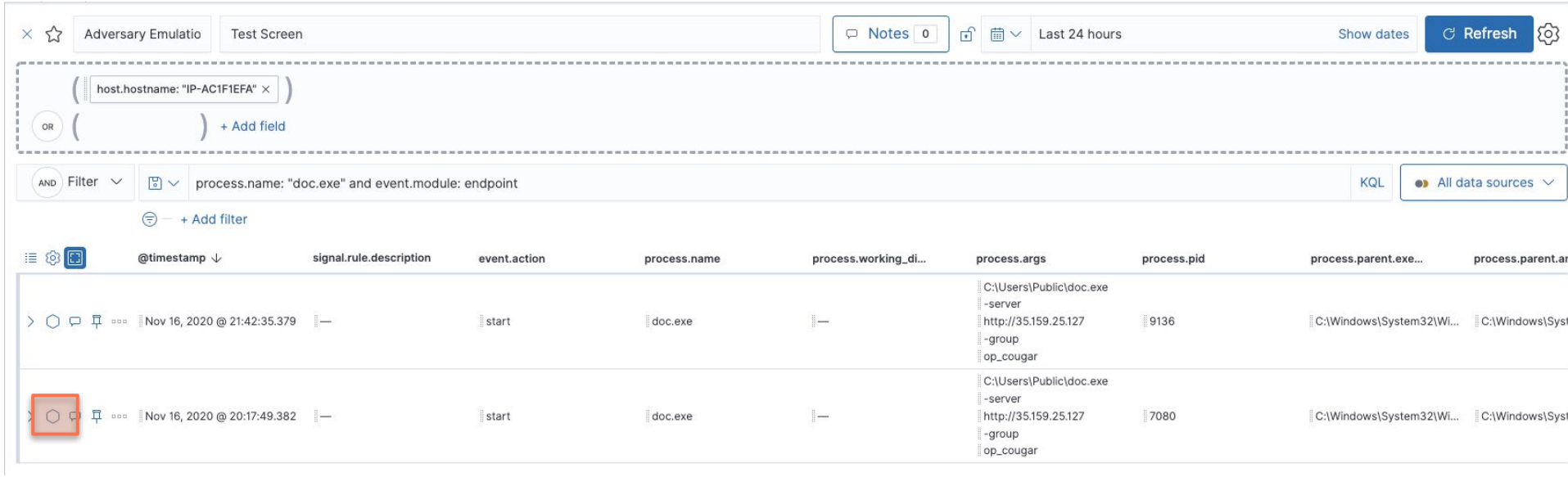
Lab 3 - Detection

Rule creation

Review dataset in timeline

Look at the last event by time

Filter: **process.name: “doc.exe” and event.module: “endpoint”**



elastic

Process Tree View

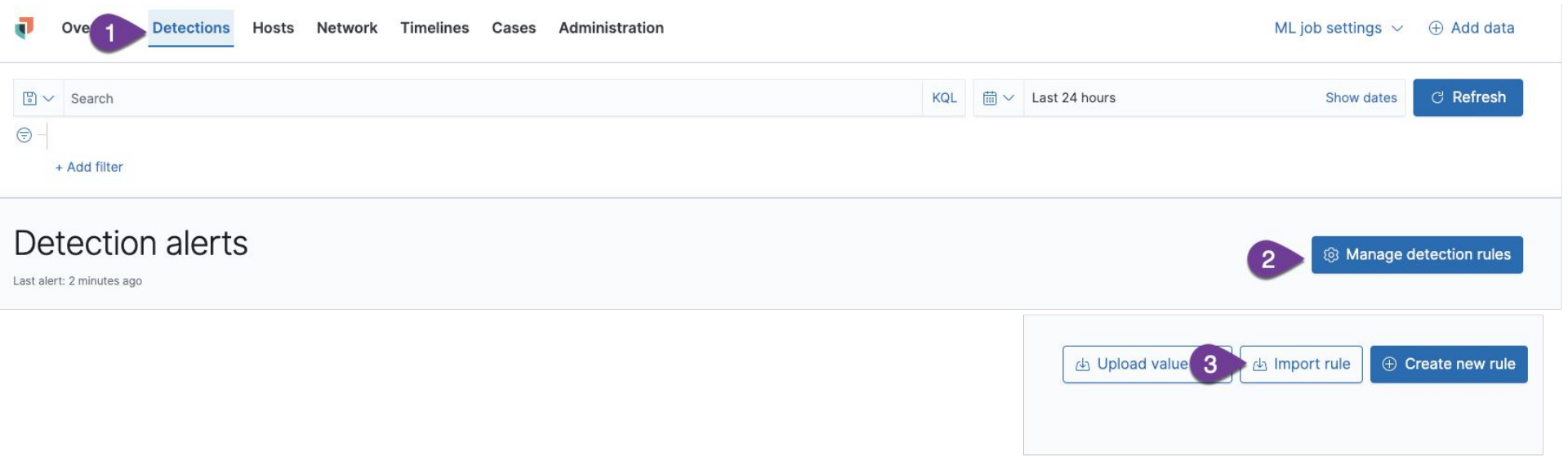
Your view may be different

Download Rule Set

https://ela.st/aptelk-rules

elastic

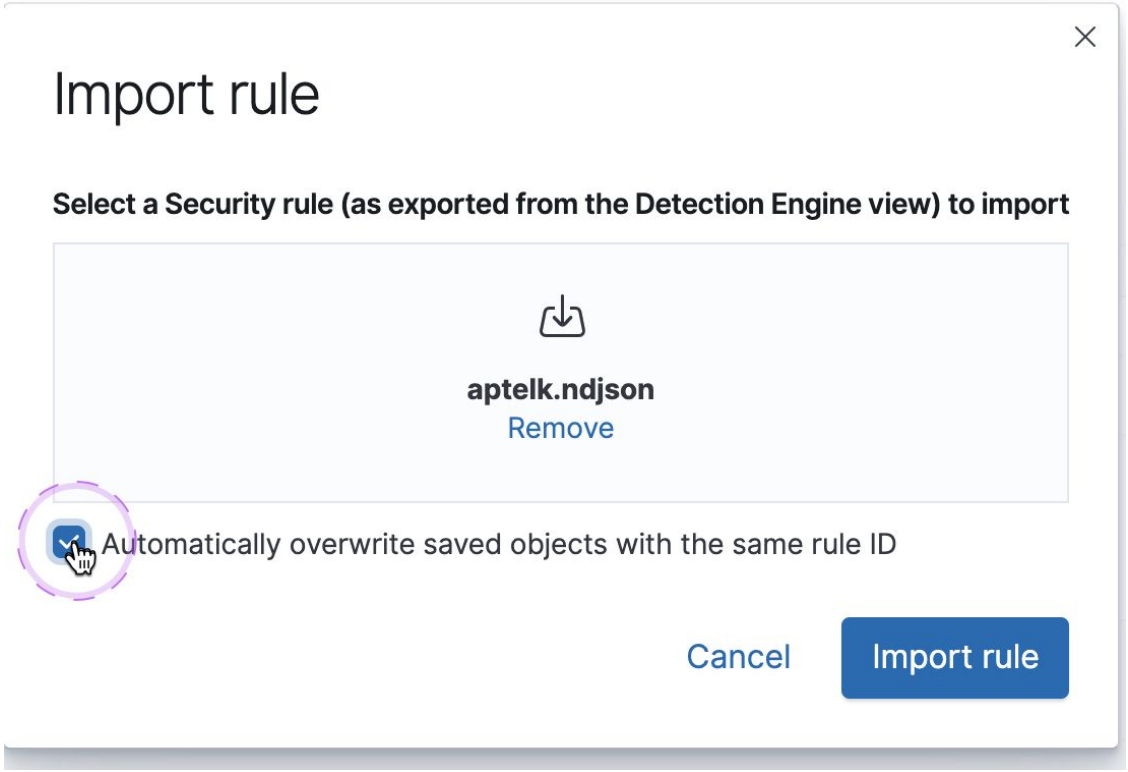
Upload Rules

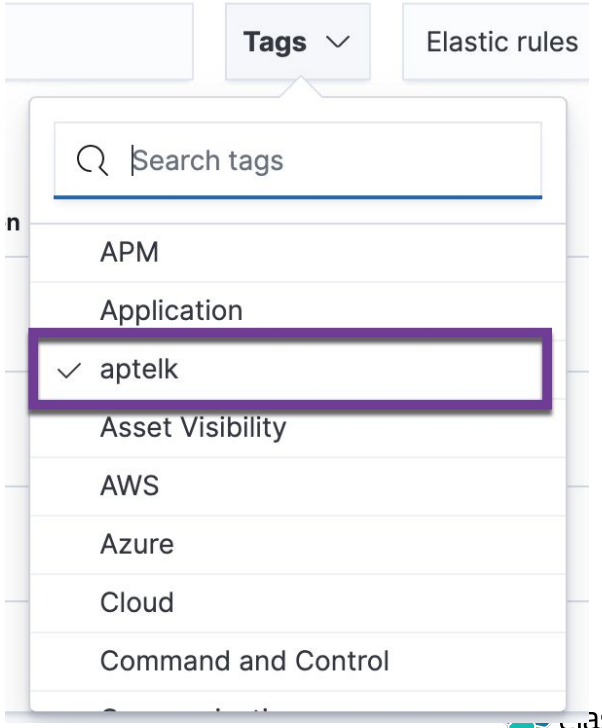


elastic

Import Rules

Import the rule set aptelk.ndjson





Adversary Emulation - Powershell with Network Connection - High Threshold

Threshold

Detection:

- Process name is powershell.exe
- Network connection exists
- Confirmed geo lookup to a public address

Search:

```
process.name: "powershell.exe"  and event.category : network* and
destination.geo.country_name : *
```

Adversary Emulation - Powershell Writing a File

EQL

Detection:

- OS signed binaries used by attackers to evade detection
- File write event
- File execution where code signing signature is not trusted and the process is started
- Network connection is made

EQL:

```
sequence by host.name
  [process where event.type == "start"
    and process.name in ("powershell.exe", "mshta.exe", "installutil.exe",
"msxsl.exe", "rundll32.exe") ]
[file where file.extension == "exe"
[process where process.code_signature.status != "trusted" and event.type==
"start"
  [network where true]
```

Adversary Emulation - Powershell Writing a File Until Adversary Tool Is Executed

EQL

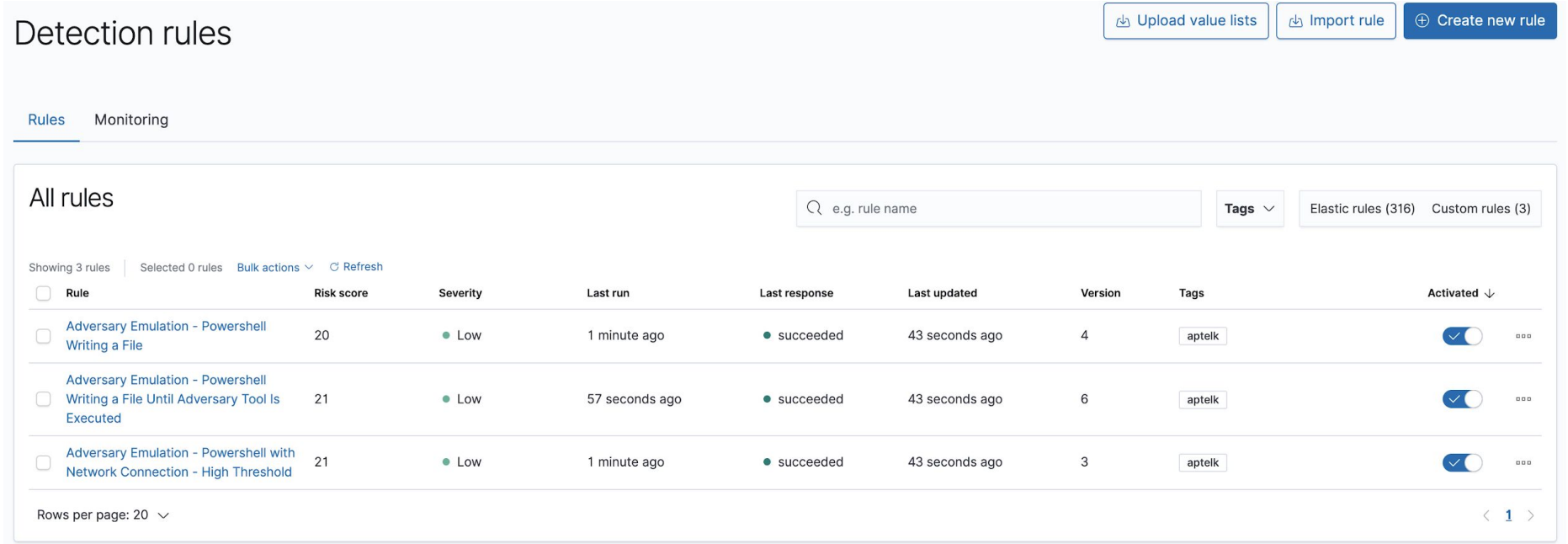
Detection:

- OS signed binaries used by attackers to evade detection
- File write event
- File execution where code signing signature is not trusted and the process is started
- Until we see process conhost.exe being executed

EQL:

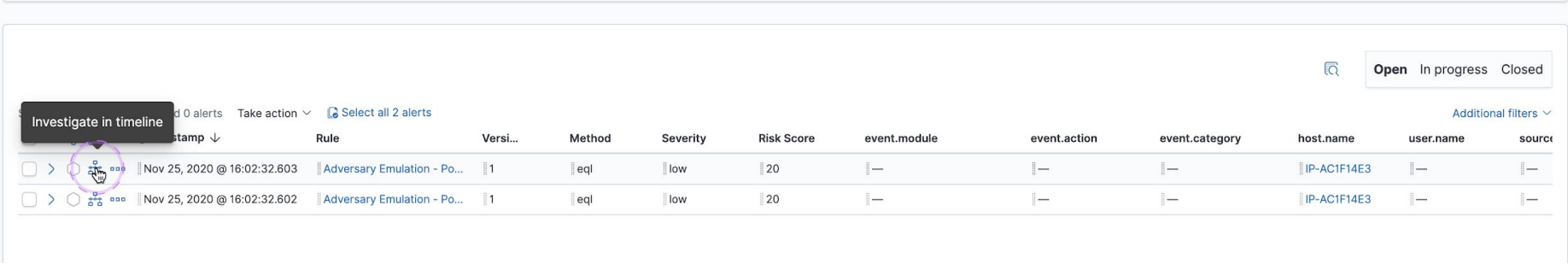
```
sequence by host.name
  [process where event.type == "start"
    and process.name in ("powershell.exe", "mshta.exe", "installutil.exe",  "msxsl.exe",
"rundll32.exe") ]
[file where file.extension == "exe"]
[process where process.code_signature.status != "trusted" and event.type== "start"]
  until
[ process where process.name in ("conhost.exe", "wmic.exe", "whoami.exe")]
```

Click on each of the rules



Investigate

Scroll Down and Investigate in Timeline



elastic

End Lab 3