Finding Evil with MITRE ATT&CK™ and the Elastic Stack

August 7, 2019

Abstract

Find out how Mitre's ATT&CK™ can be used as a baseline for threat hunting. Starting with data hygiene and ending with an example hunt, we'll show how the Elastic Stack can help you find bad actors in a standardized, auditable way.

Setup scripts and configuration for the Strigo environment can be found @ https://github.com/mrebeschini/2019BSidesLV

elastic

Kent Blake
Sr. Principal Solutions Architect
Security Specialist
@Elastic
kent@elastic.co

Matteo Rebeschini
Principal Solutions Architect
Security Specialist
@Elastic
matteo@elastic.co

elastic

Please setup your personal Elastic Lab Environment

You will need it for the workshop labs

Open the following Google Drive folder:

https://ela.st/2019BSidesLV

Follow instruction in the **Lab 1** PDF document.

elastic

Agenda

2:00 p.m.	Welcome, Check-In, Setup your Elastic Lab Environment
	Lab 1 - Create your Elastic Cloud Environment
2:30 p.m.	Introductions & Opening Remarks
	Elastic Stack Overview
3:00 p.m.	MITRE ATT&CK™ Overview
	Lab 2: Data Ingestion using Beats and MITRE ATT&CK
4:00 p.m.	Threat Hunting leveraging MITRE ATT&CK™ Host-level TTPs
	Lab 3: Finding Host-level TTPs using Kibana
4:30 p.m.	Introducing Elastic SIEM
	Lab 4: Interacting with the Elastic SIEM App
5:00 p.m.	Q&A Session & Group Discussions
5:30 p.m.	Workshop Concludes

elastic

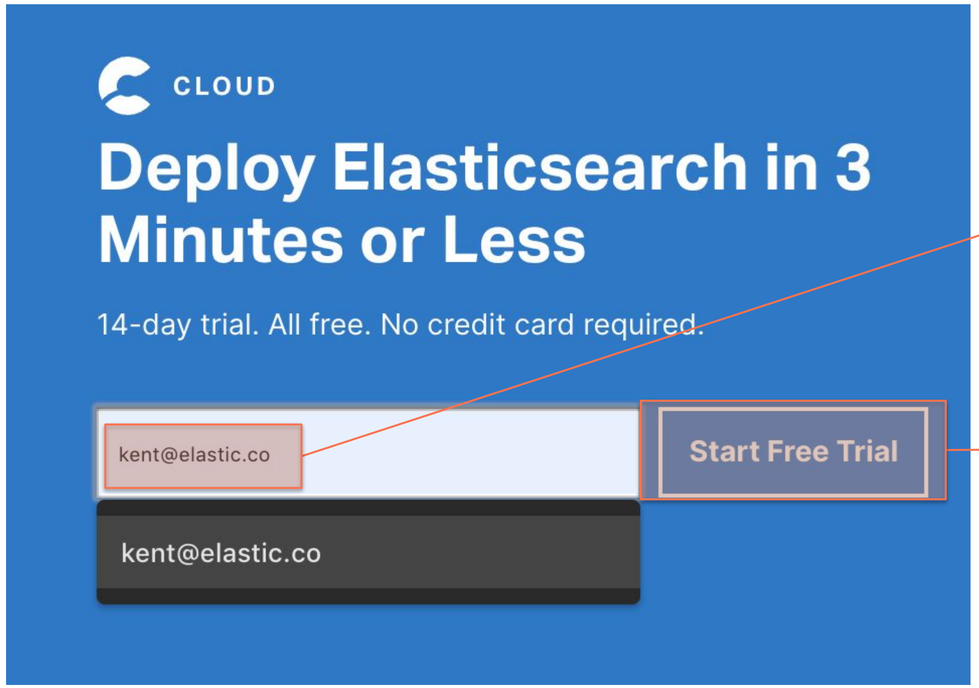
Lab 1

Elastic Cloud Setup

elastic

Sign up for the Elastic Cloud Trial

Go to https://cloud.elastic.co

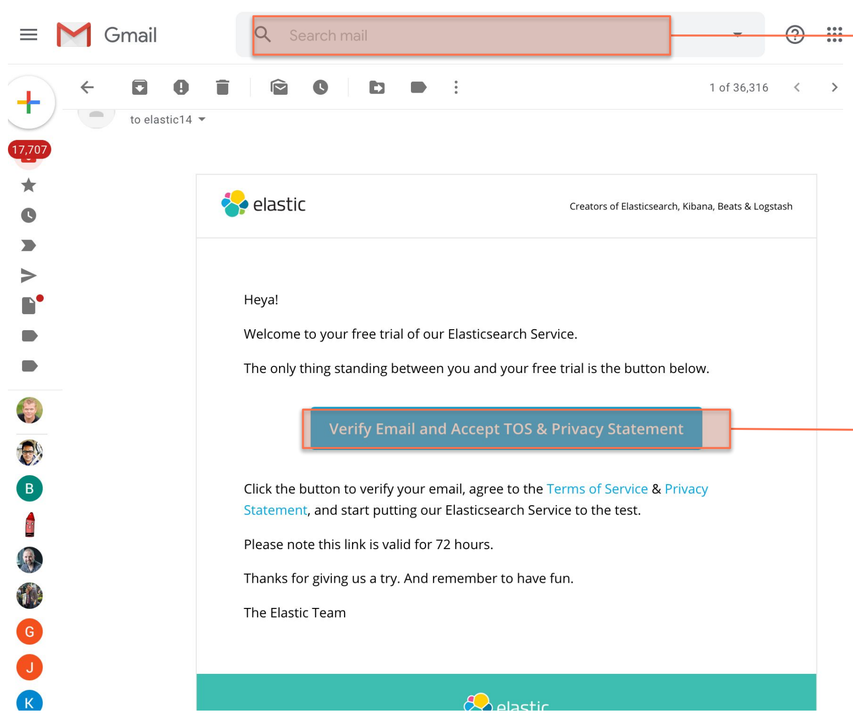


1. Enter your business email (no credit card is required)
2. Select ‘Start Free Trial’

elastic

Cloud account validation

Login to your business email

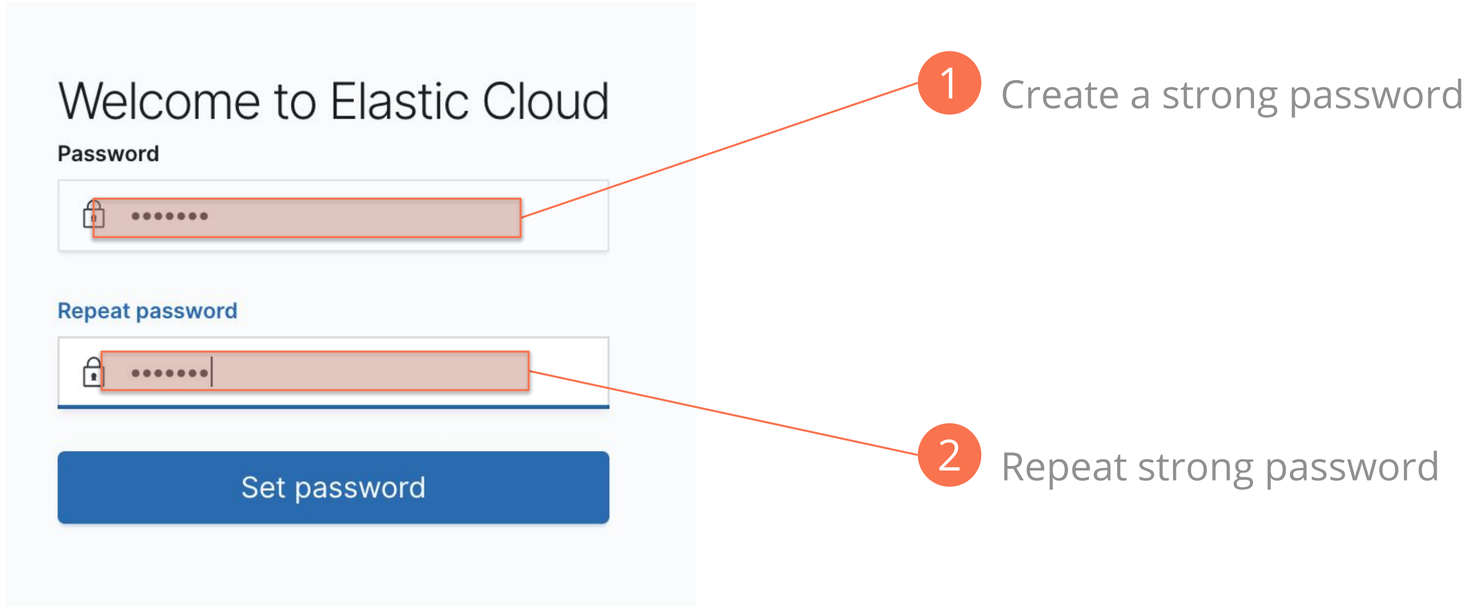


1 Find message with the Subject: '**[Action Required] It Worked! Your Elasticsearch Service Trial Awaits**.'

2 Select the 'Verify Email…' link

Set password

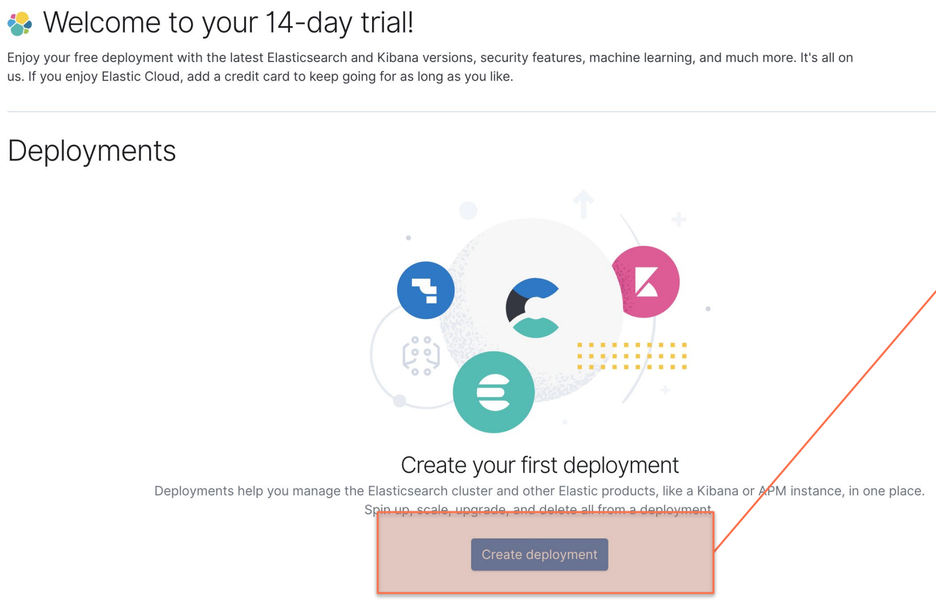
After the password is set, you will automatically be logged in



elastic

Create new trial cluster

Kibana has multiple indices, select auditbeat

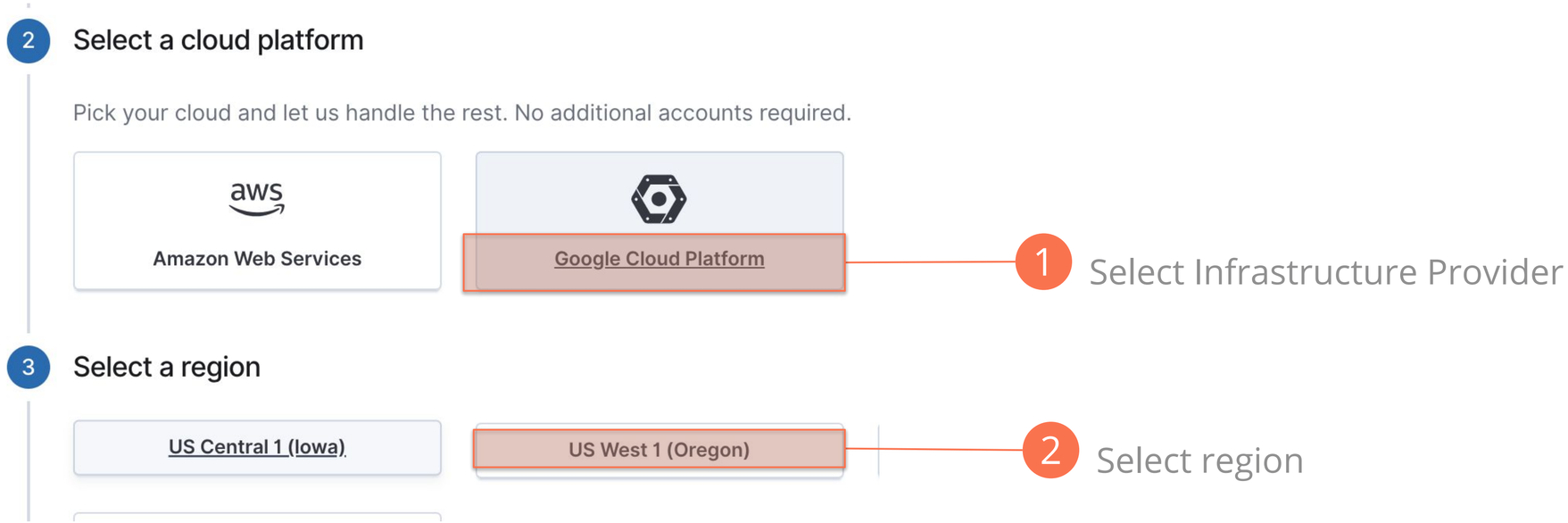


1 Select ‘Create deployment’

2 Name the deployment ‘workshop’

Deployment options

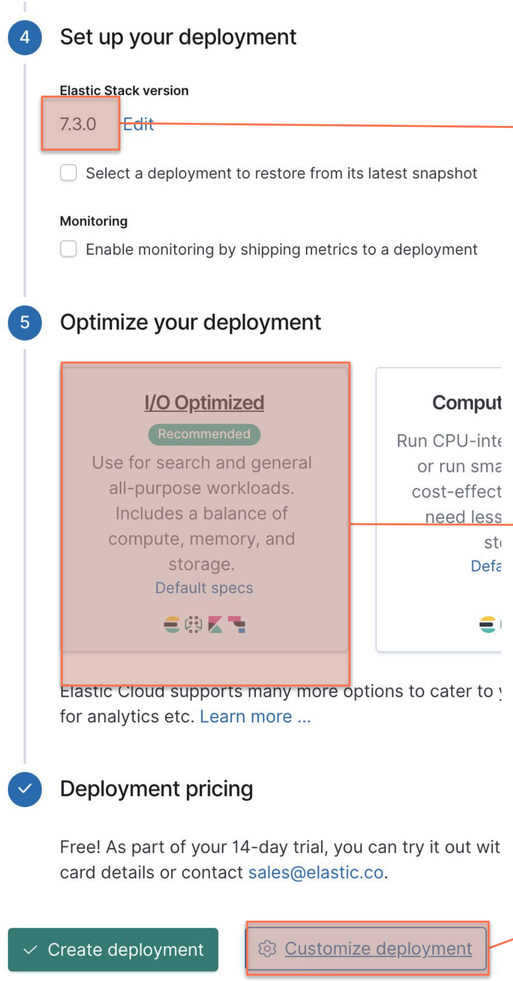
GCP in the US West region



elastic

Deployment options

Set deployment type and version



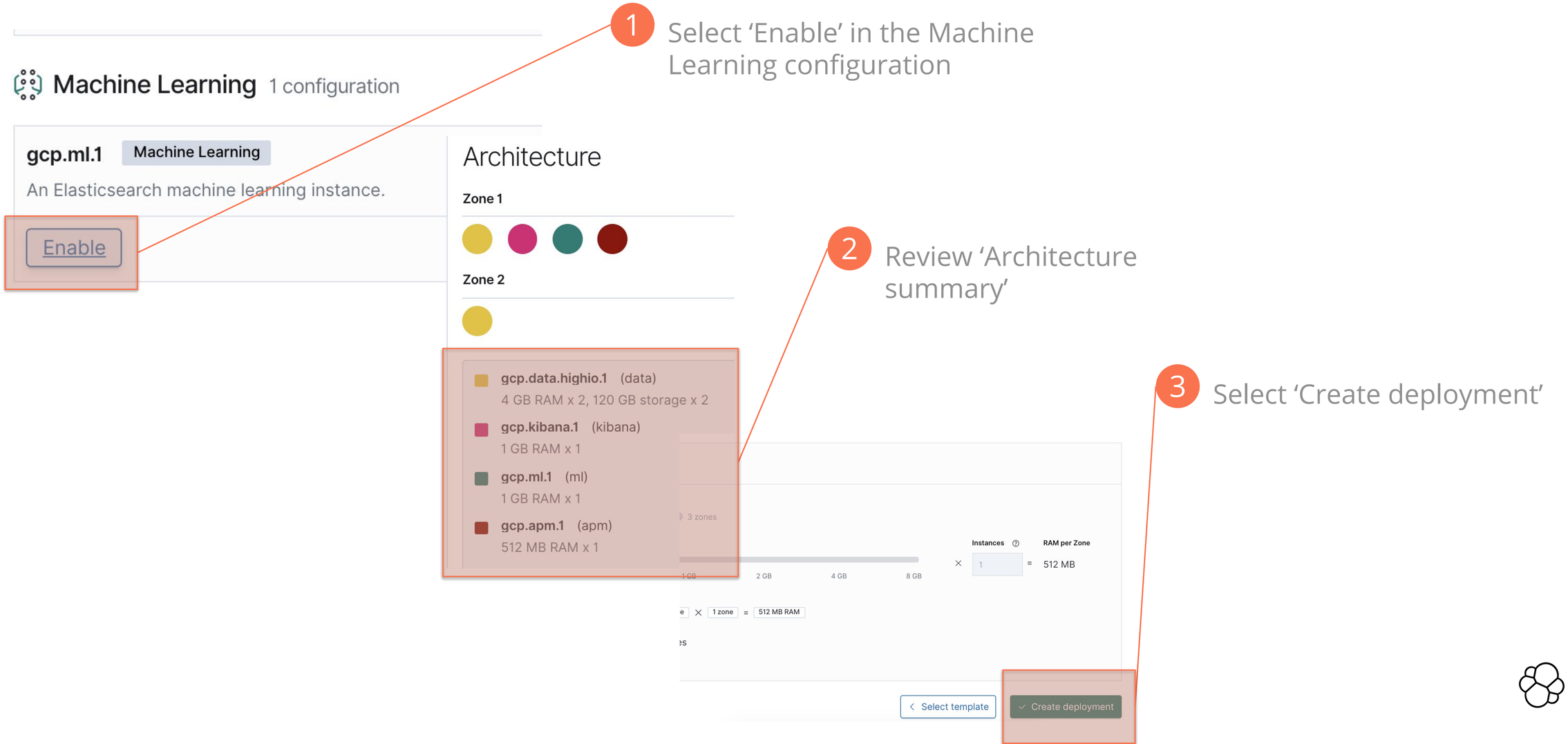
1 The version of the Elastic Stack to be deployed

2 Select 'I/O Optimized'

3 Select **'Customize Deployment'**

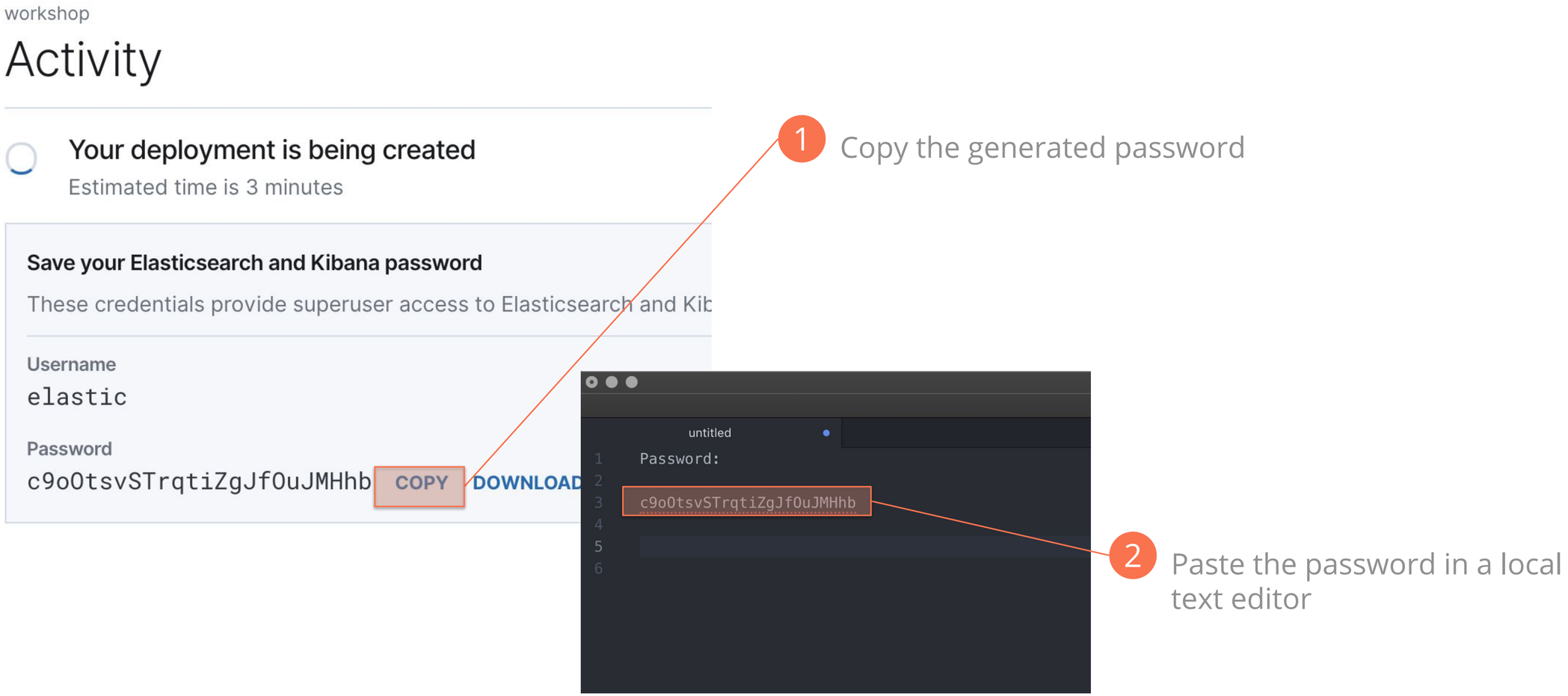
Create deployment

Enable Machine Learning



Cluster password

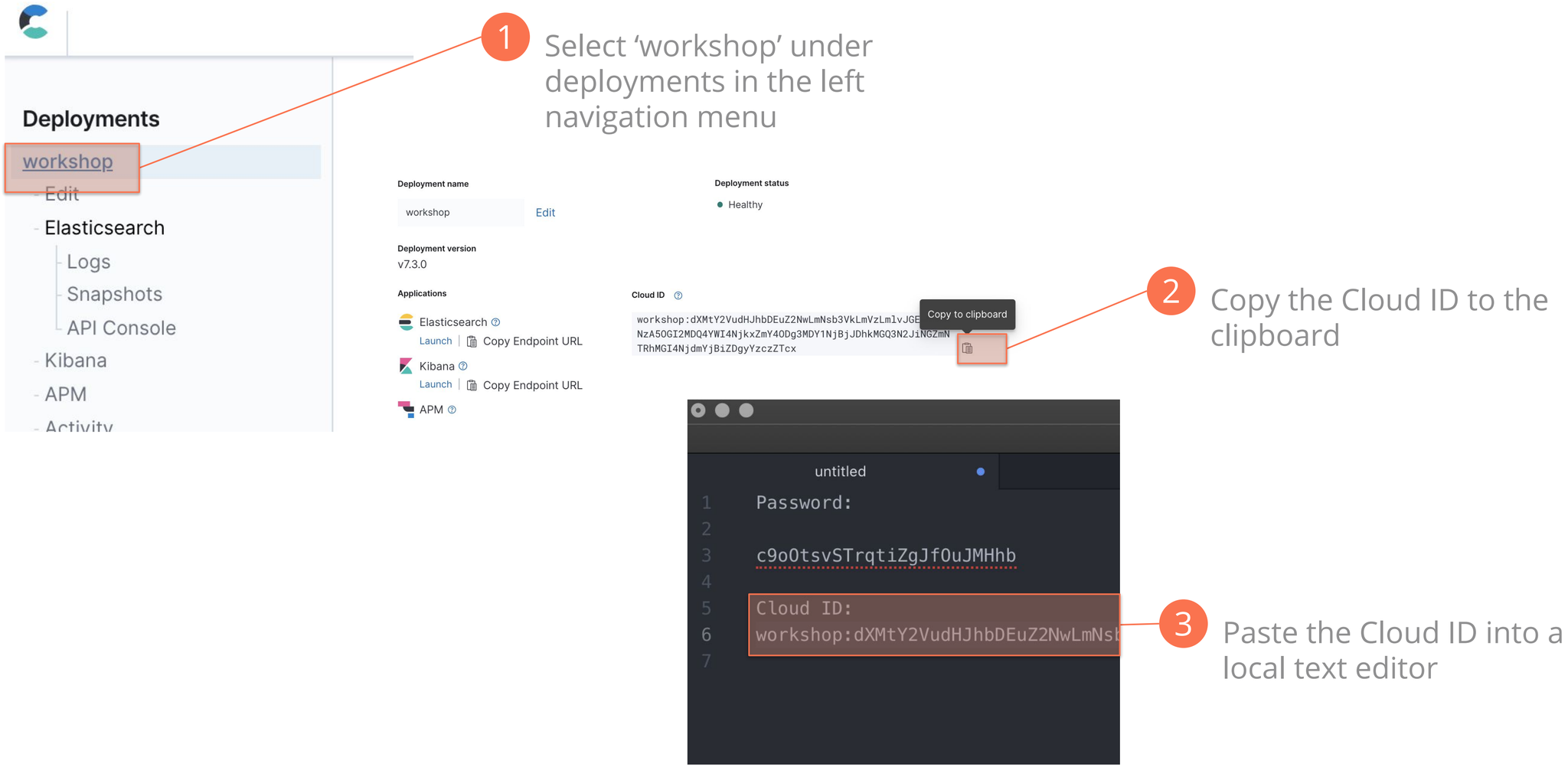
Save the password



elastic

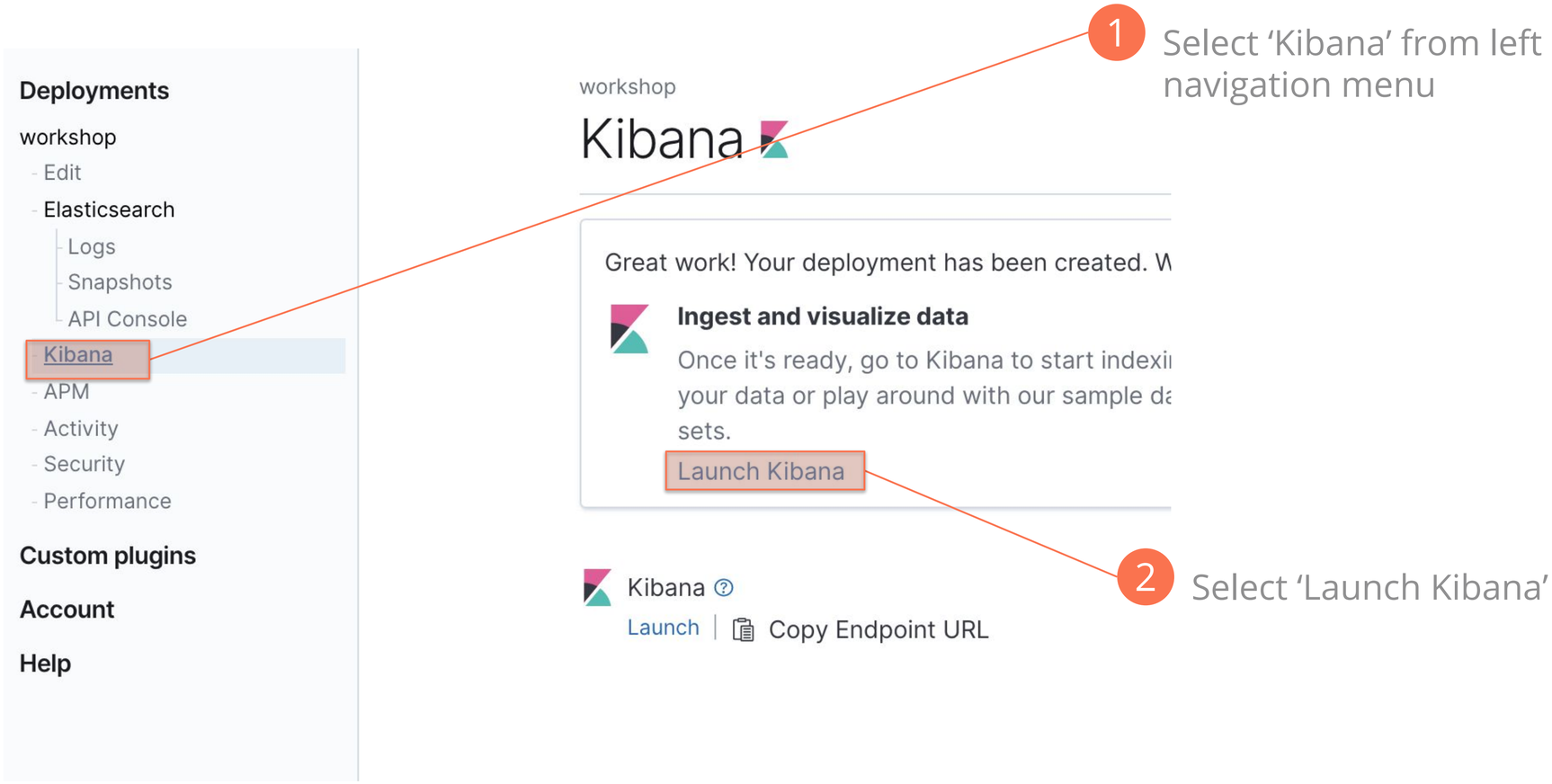
Cloud ID

Save the Cloud ID



Launch Kibana

Setup complete, time to launch Kibana



elastic

Elastic Stack Overview

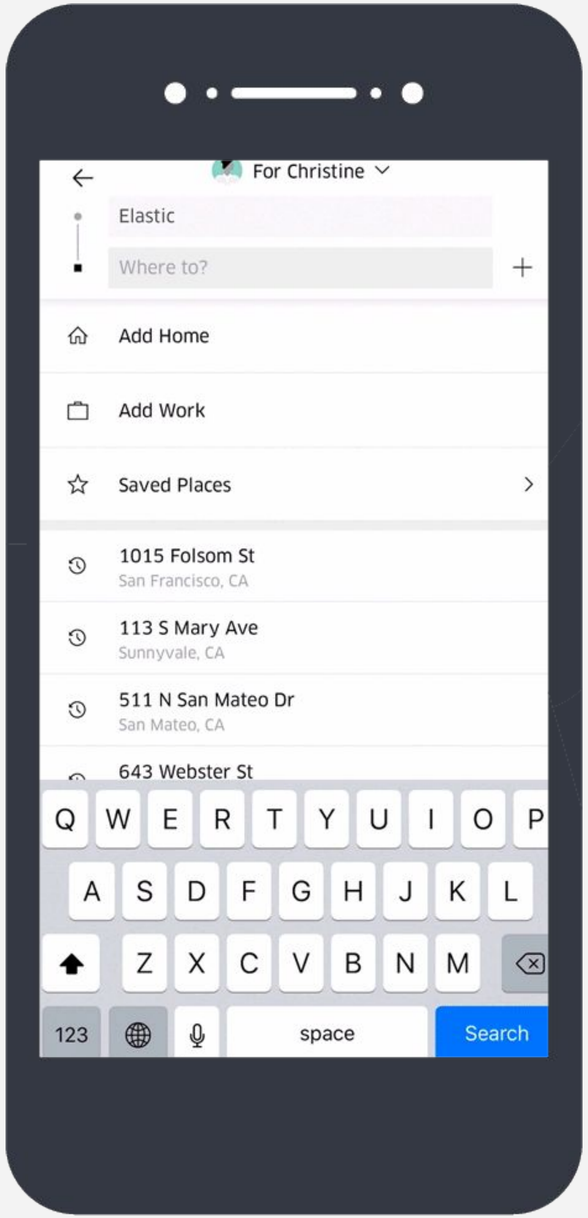
elastic

Elastic is a **search company**

SIEM & security analytics

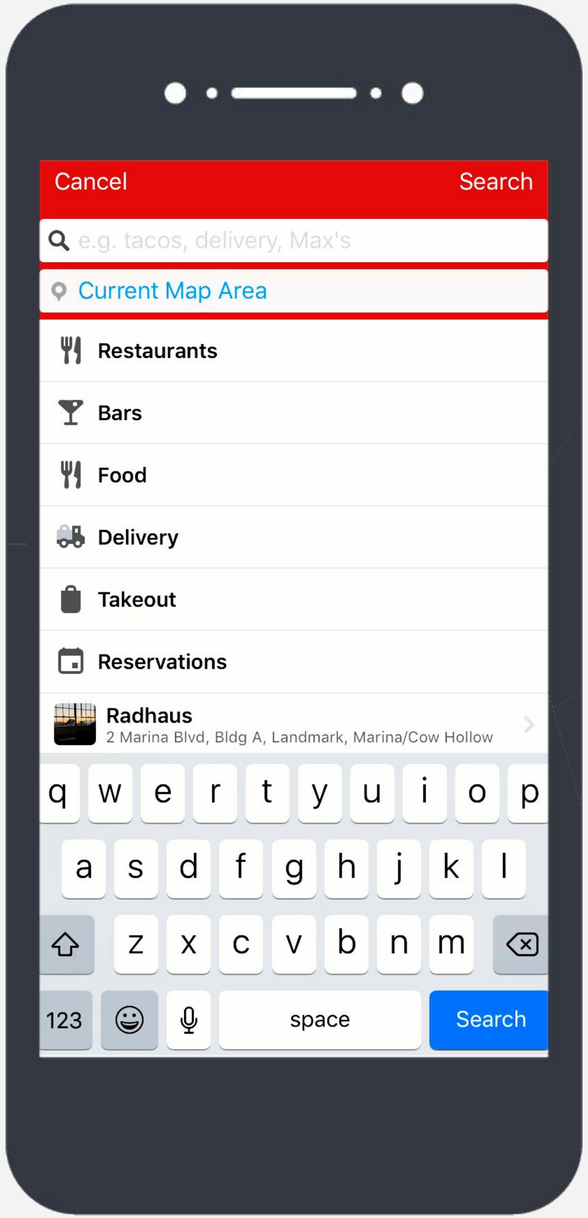
thrive on **search**

elastic



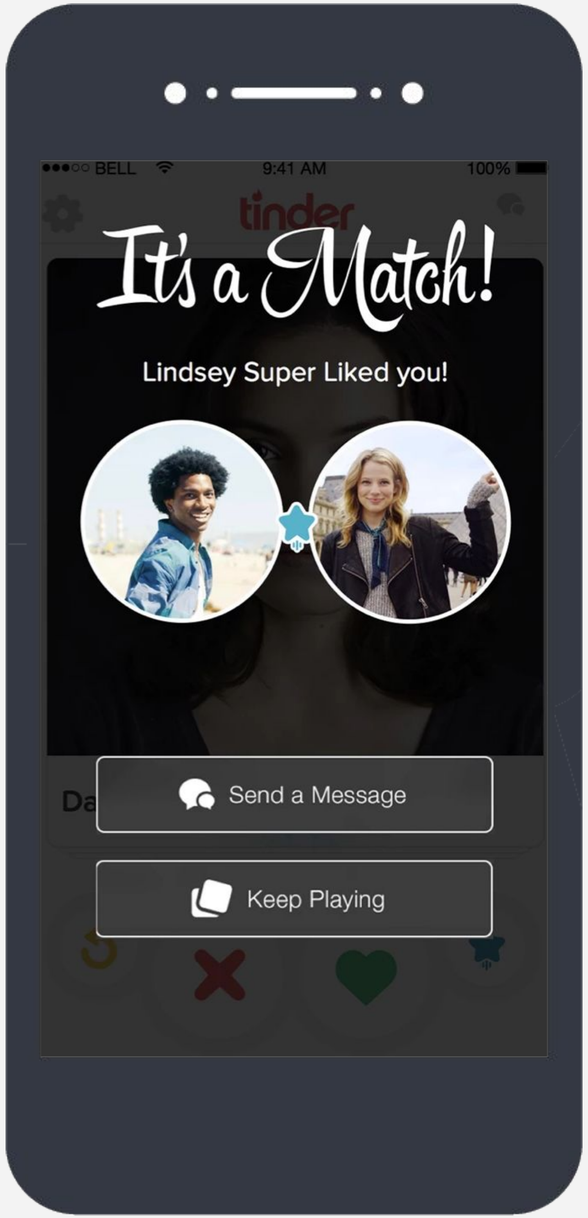
Uber

elastic



yelp®

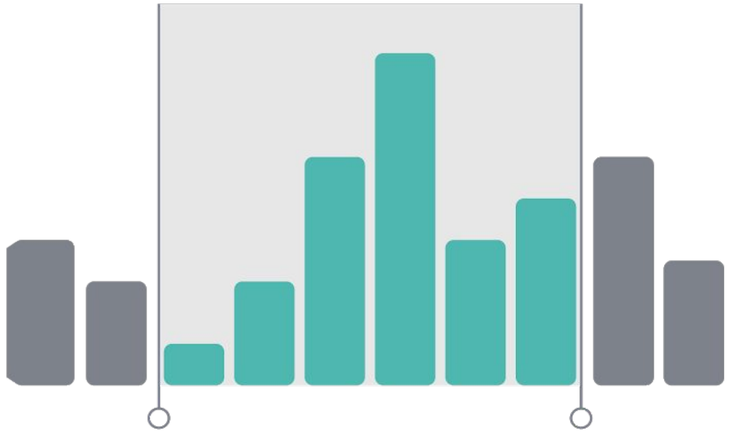
elastic

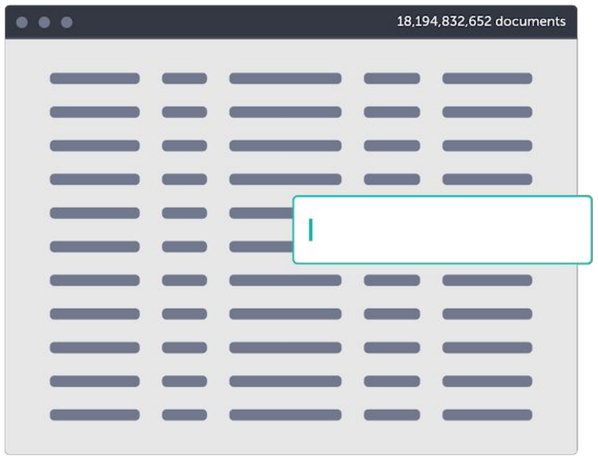


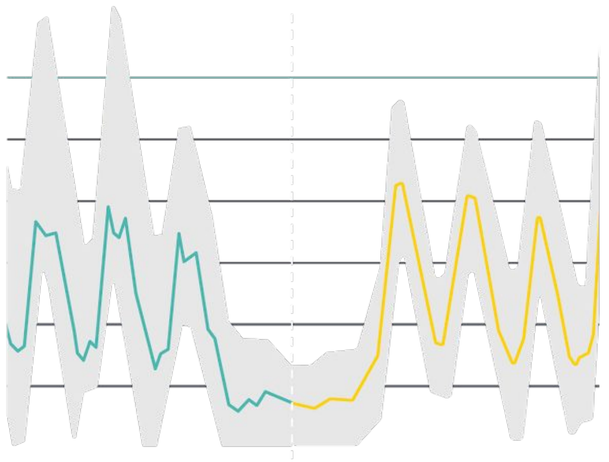
tinder™

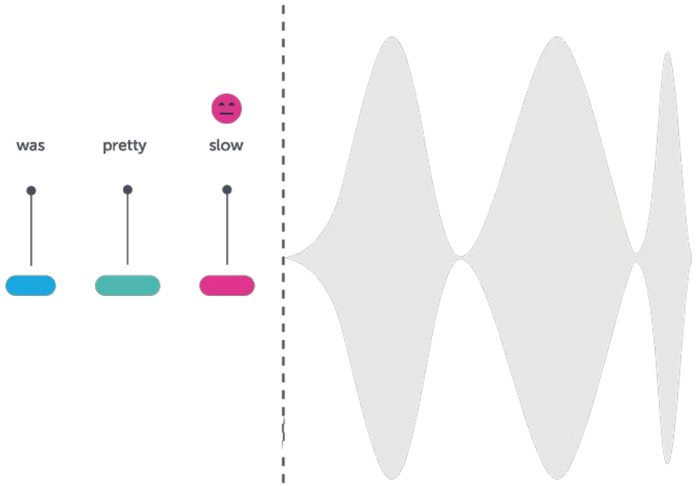
elastic

Search is a **constant/foundation**



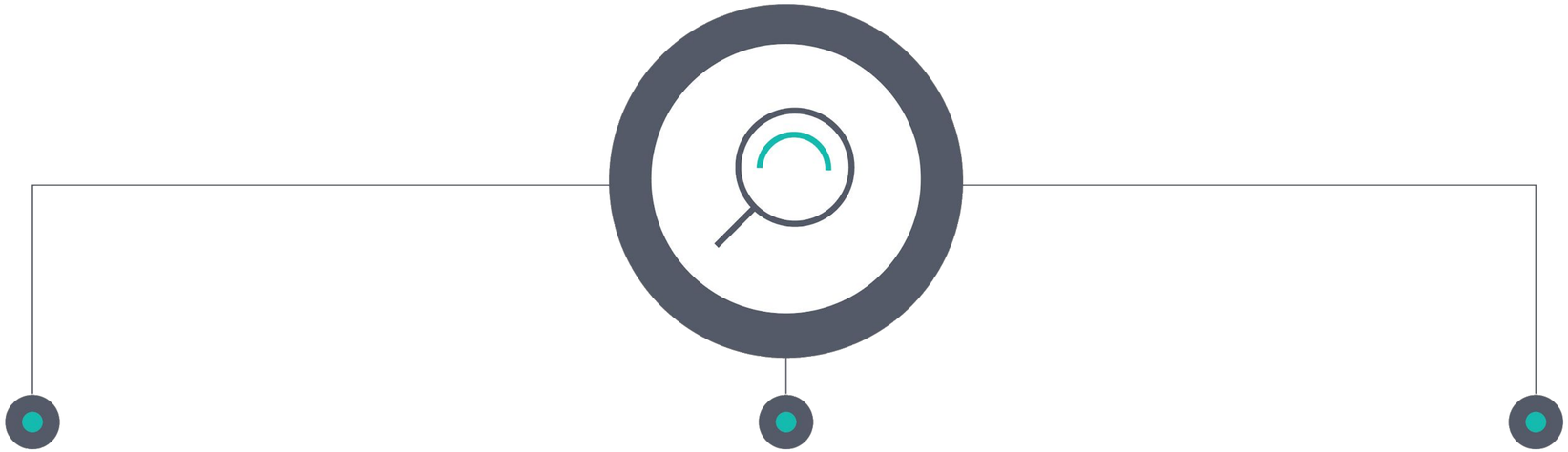






Elastic’s Heart: Elasticsearch

Technology **differentiation**



SCALE

Distributed by design

SPEED

Find matches in milliseconds

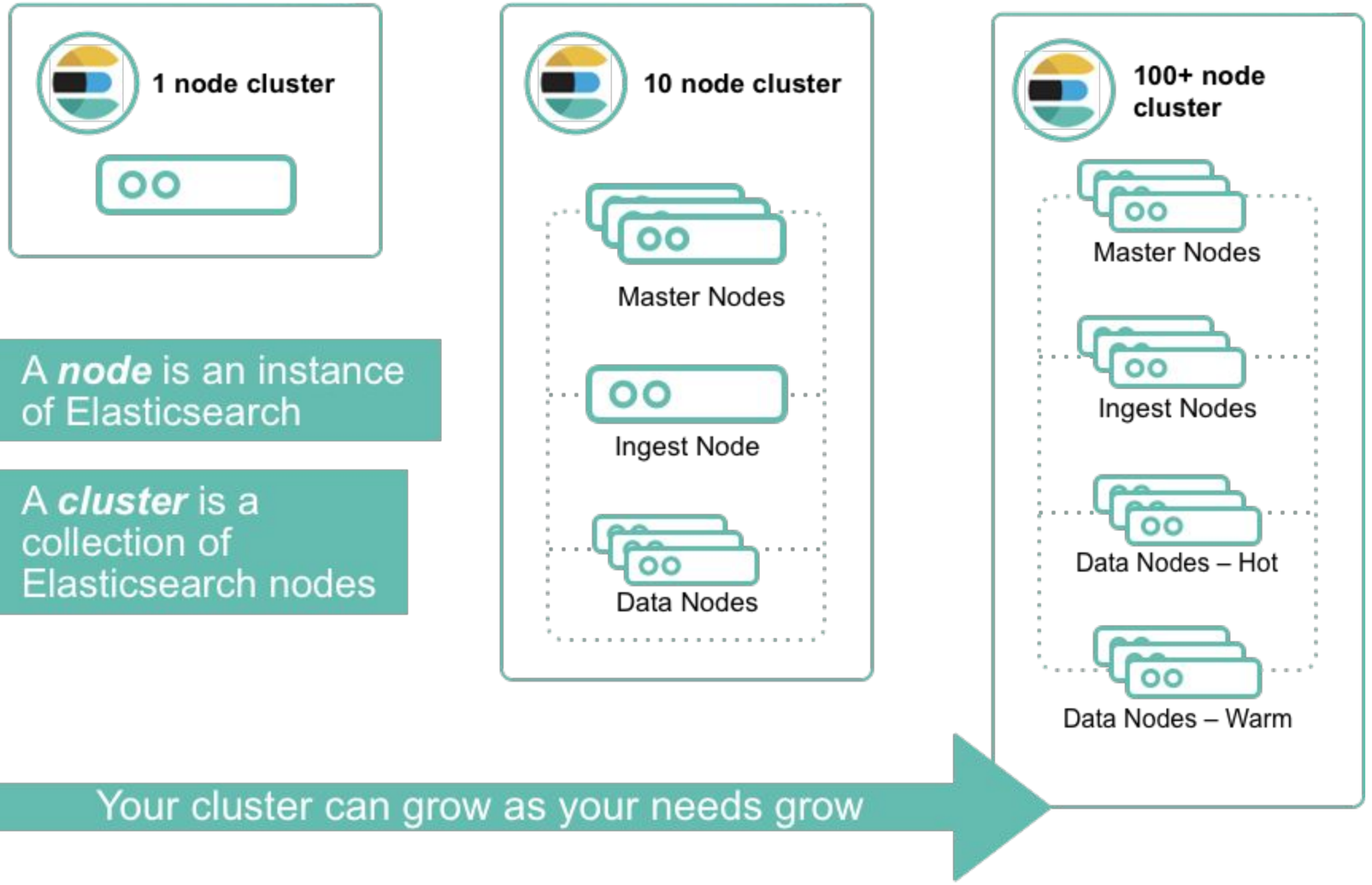
RELEVANCE

Get highly relevant results

elastic

Elasticsearch

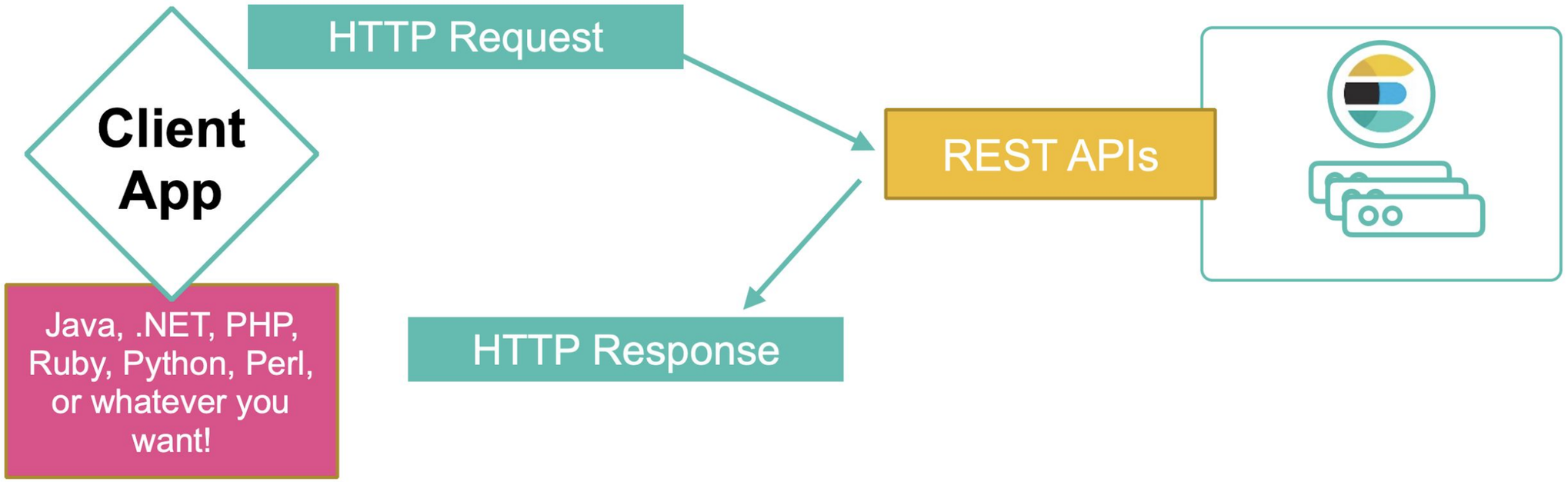
Distributed by design, scales horizontally



elastic

Elasticsearch is REST API First

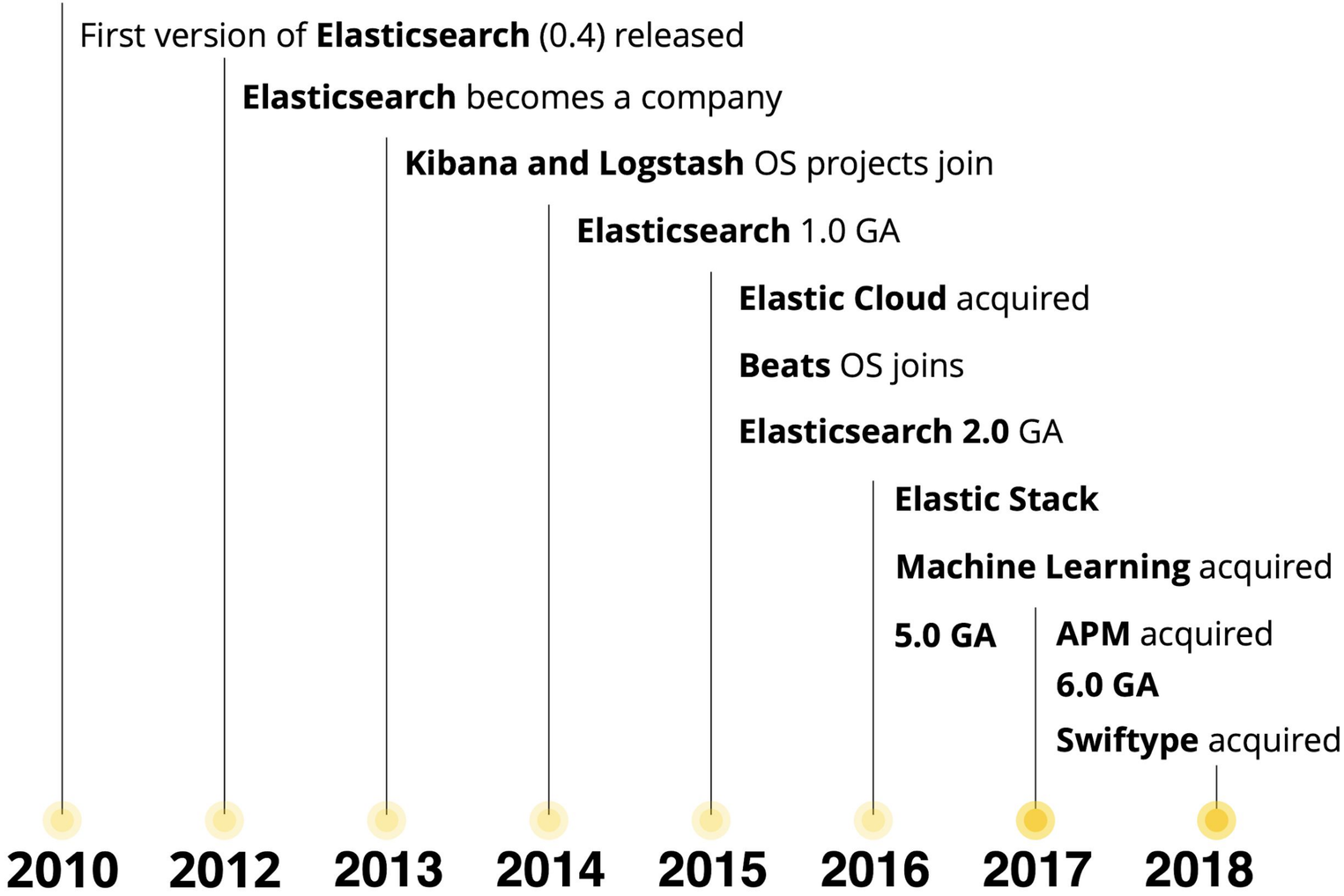
Developer Friendly...but not everyone is a developer



elastic

The Evolution of Elasticsearch

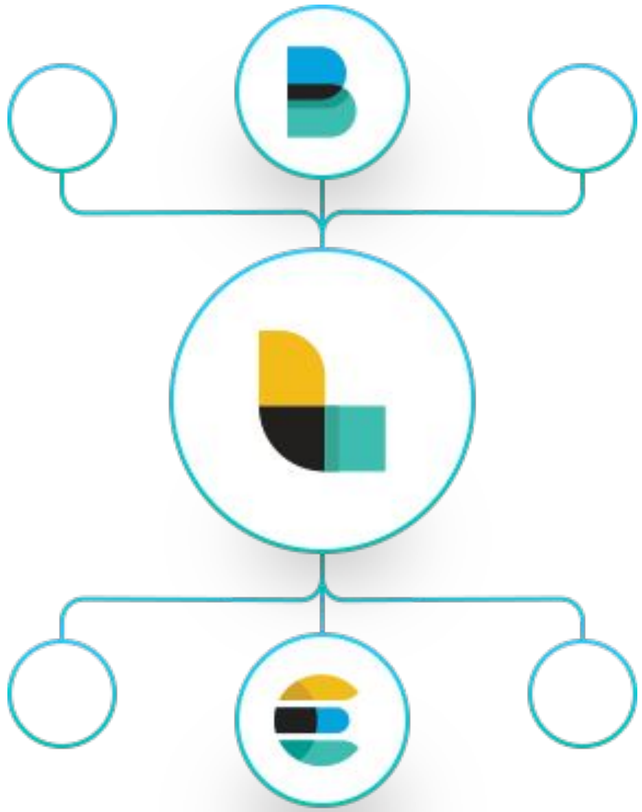
How community has contributed to Elastic's direction



elastic

Logstash

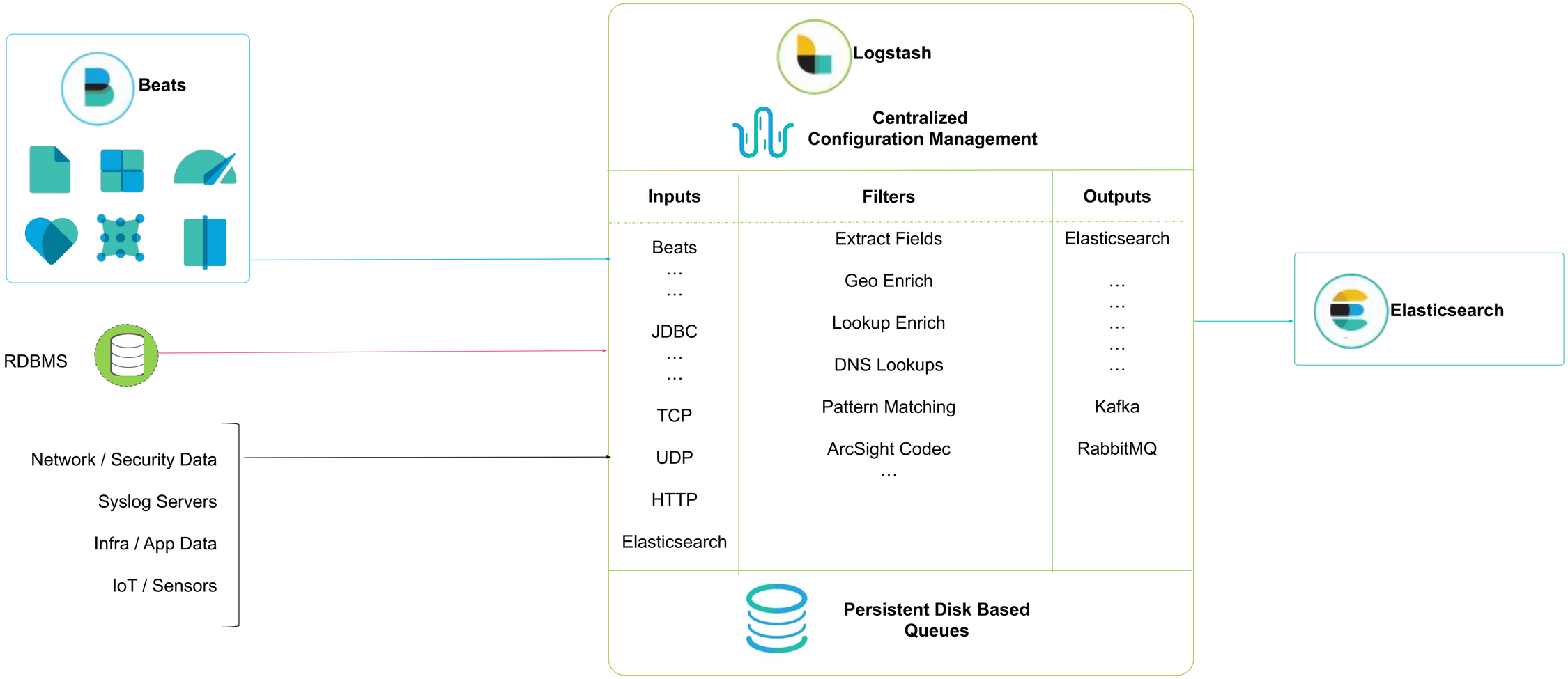
ETL for Elasticsearch



Ingest data of all shapes, sizes, and sources	Parse and dynamically transform data	Transport data to any output
Secure and encrypt data inputs	Build your own pipelines	Lots of plugins

Logstash Pipelines: Inputs + Filters + Outputs

Normalize and Enrich Data before Indexing



elastic

Normalization

Using Elastic Common Schema (ECS)

- Defines a **common** set of fields for ingesting data into Elasticsearch.
- Helps you **correlate** data from different log source types
- Designed to be **extensible**
- Details and **community** feedback @ https://github.com/elastic/ecs

Destination fields

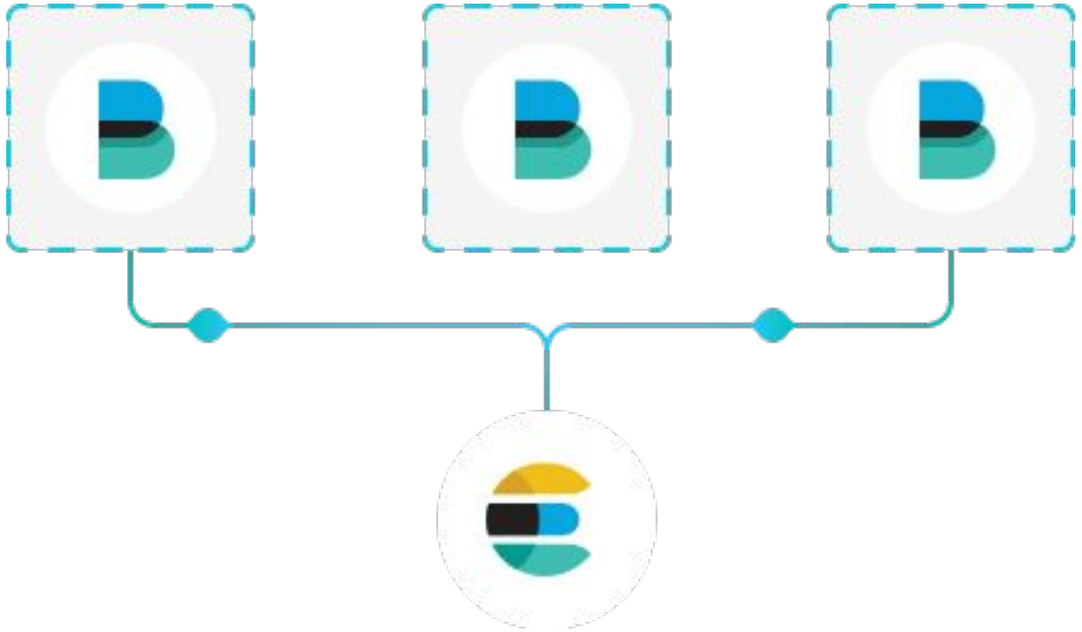
Destination fields describe details about the destination of a packet/event.

Field	Description	Type
`destination.ip`	IP address of the destination. Can be one or multiple IPv4 or IPv6 addresses.	ip
`destination.hostname`	Hostname of the destination.	keyword
`destination.port`	Port of the destination.	long
`destination.mac`	MAC address of the destination.	keyword
`destination.domain`	Destination domain.	keyword
`destination.subdomain`	Destination subdomain.	keyword

elastic

Beats

Lightweight data shippers



Ship data from the source	Ship and centralize in Elasticsearch	Ship to Logstash for transformation and parsing
Ship to Elastic Cloud	Libbeat: API framework to build custom beats	70+ community Beats

elastic

FileBeat
Log Files

MetricBeat
Metrics

PacketBeat
Network Data

WinLogBeat
Window Events

HeartBeat
Uptime Monitoring

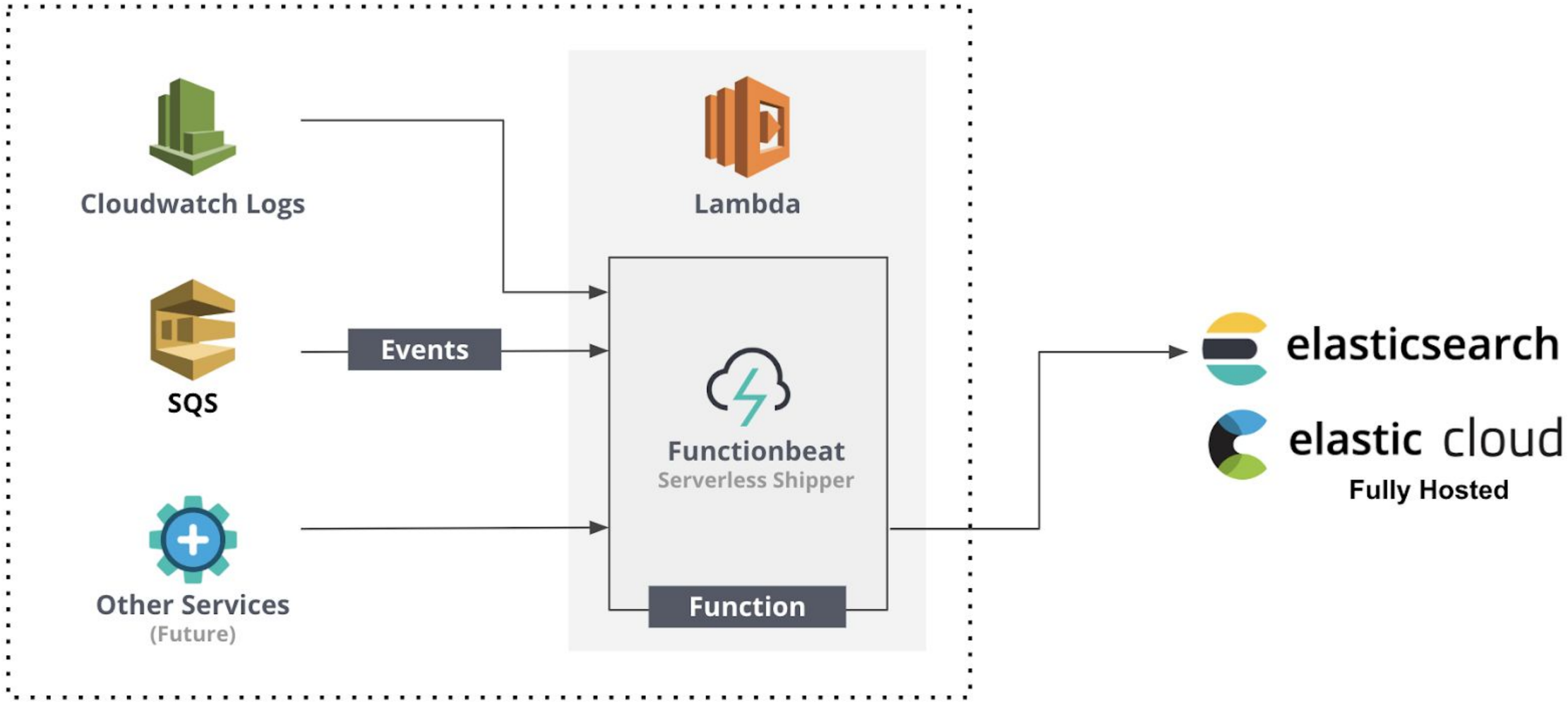
AuditBeat
Audit Data

FunctionBeat
Serverless Shipper

Plus, more than 70 community Beats and growing...

FunctionBeat - Serverless shipper for Cloud Data

Ingest from CloudWatch Logs & Amazon SQS

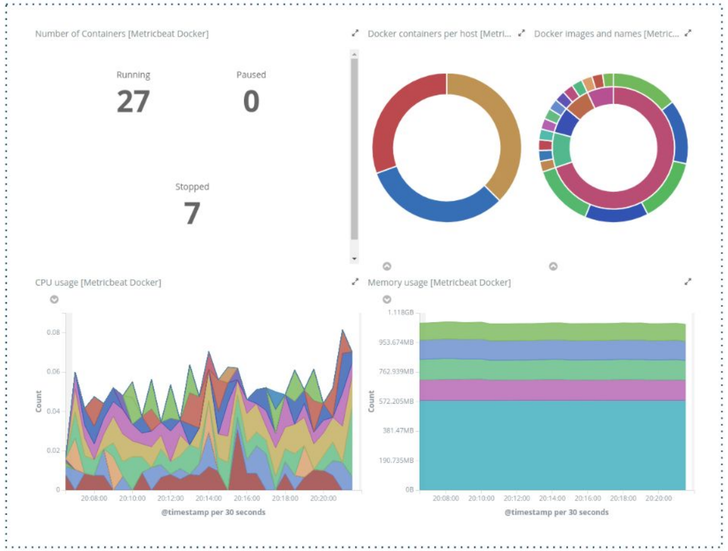


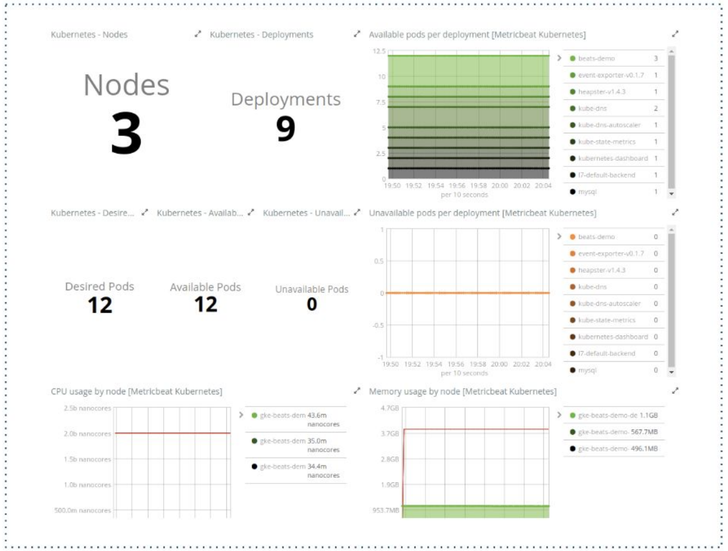
elastic

Beats Modules

Gain Immediate Visibility

- Turn-key insights for specific data types
- Data to dashboard in just one step
- Automated parsing and enrichment
- Default dashboards, alerts, ML jobs
- Autodiscovery for Kubernetes





Modules

Apache kafka mongoDB redis PostgreSQL NGINX docker kubernetes

RabbitMQ MySQL MEMCACHED HAPROXY Couchbase Prometheus vmware vSphere

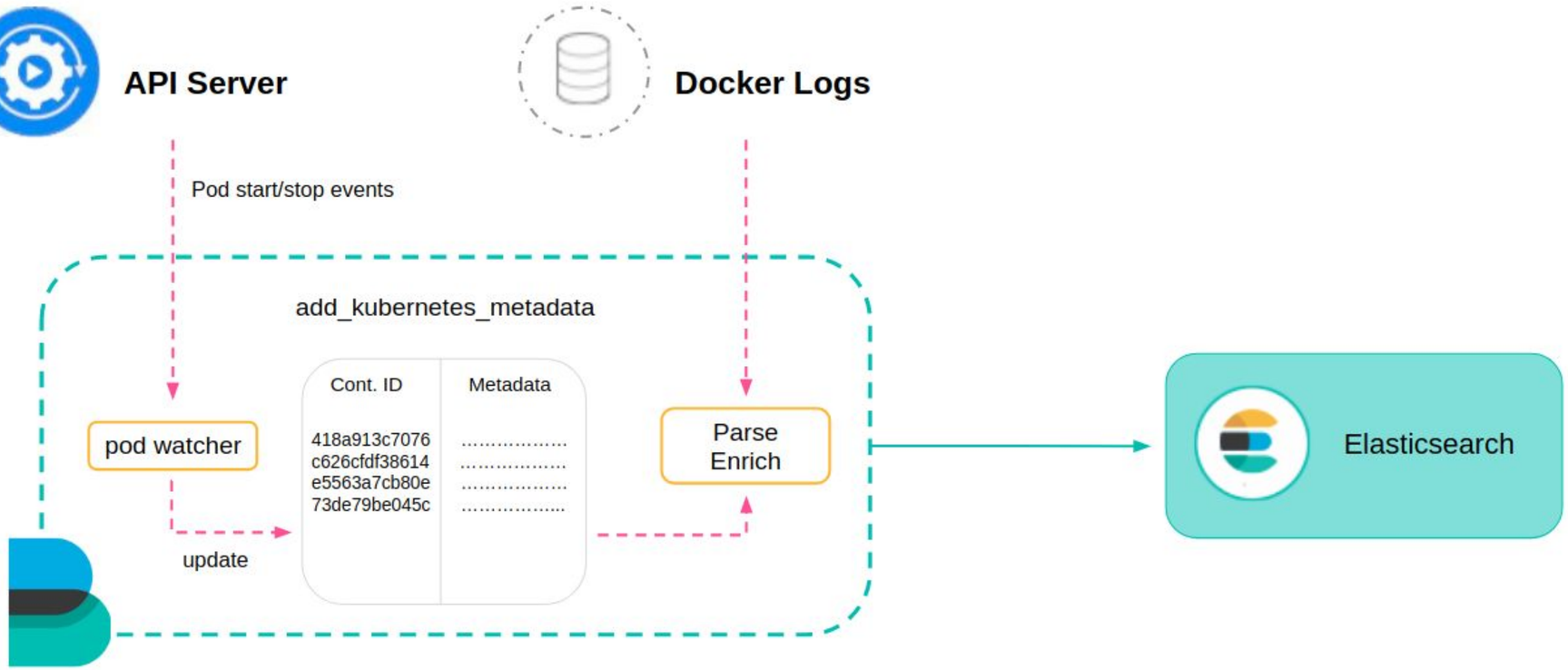
and more...

Checkout Beats dashboards at https://demo.elastic.co

elastic

Kubernetes Log Collection with Filebeat

Fluentd is great, but Filebeat is even better!




```
kubectl create -f filebeat-kubernetes.yaml
```


elastic

Kubernetes Metadata processors

Log Enrichment Example


```
{
  "@timestamp": "2017-11-17T00:53:33.759Z",
  "message": "2017/11/07 00:53:32.804991 client.go:651: INFO Connected to Elasticsearch version 6.0.0",
  "kubernetes": {
    "pod": {
      "name": "filebeat-vqf85"
    },
    "container": {
      "name": "filebeat"
    },
    "namespace": "kube-system",
    "labels": {
      "k8s-app": "filebeat",
      "kubernetes.io/cluster-service": "true"
    }
  },
  "meta": {
    "cloud": {
      "instance_id": "6959555125944564951",
      "instance_name": "gke-demo-default-pool-6b42dcb3-z2x7",
      "machine_type": "projects/865493543029/machineTypes/n1-standard-1",
      "availability_zone": "projects/865493543029/zones/europe-west1-b",
      "project_id": "carlosperez-163008",
      "provider": "gce"
    }
  },
}
```


elastic

Filebeat Auto-Discovery

Making logging dynamic as Kubernetes deployments are

```
filebeat.autodiscover:
  providers:
    - type: kubernetes
      templates:
        - condition:
            contains:
              kubernetes.container.image: "nginx"
          config:
            - module: nginx
              access: # For nginx access log
                prospector:
                  type: docker
                  containers.ids:
                    - "${data.kubernetes.container.id}"
```

A module contains:

- Log file path
- Ingest pipeline
- Field mappings
- Dashboards

Scraping Prometheus Metrics

Using the Metricbeat Prometheus Module

Gathering data directly from Prometheus Exporters

- The Metricbeat Prometheus module will query Prometheus exporters at the user-defined frequency.
- This method **does not require Prometheus server to be in place**, as the communication is directly between Metricbeat and Prometheus exporters.
- **Support for TLS** to ensure secure data transfer.

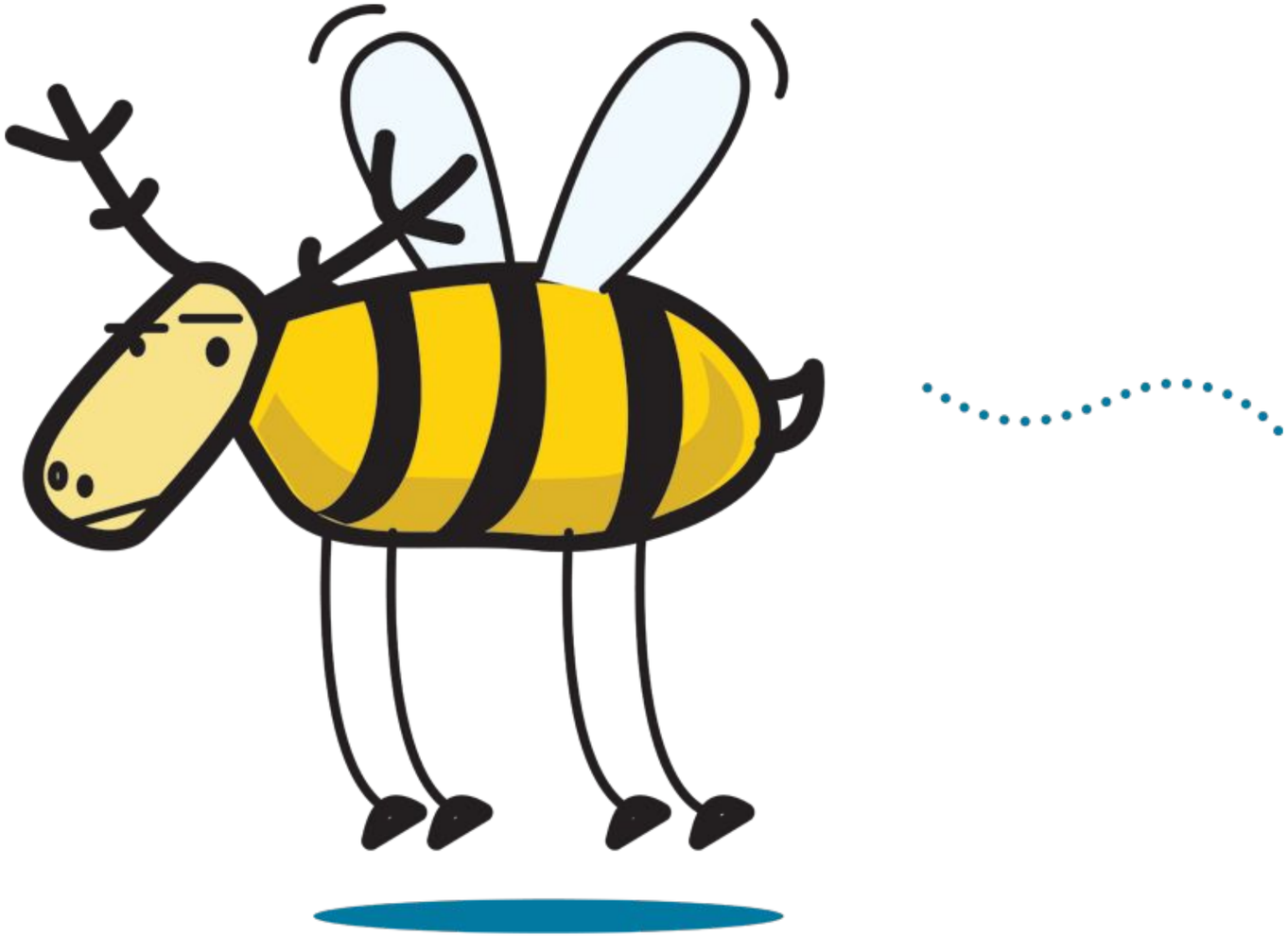
```
metricbeat.modules:
- module: prometheus
  metricsets: ["collector"]
  enabled: true
  period: 10s
  hosts: ["localhost:9090"]
  #metrics_path: /metrics
  #namespace: example

  # This can be used for service account based authorization:
  # bearer_token_file: /var/run/secrets/kubernetes.io/serviceaccount/token
  #ssl.certificate_authorities:
  # - /var/run/secrets/kubernetes.io/serviceaccount/service-ca.crt
```


elastic

Say hello to the Elastic Stack

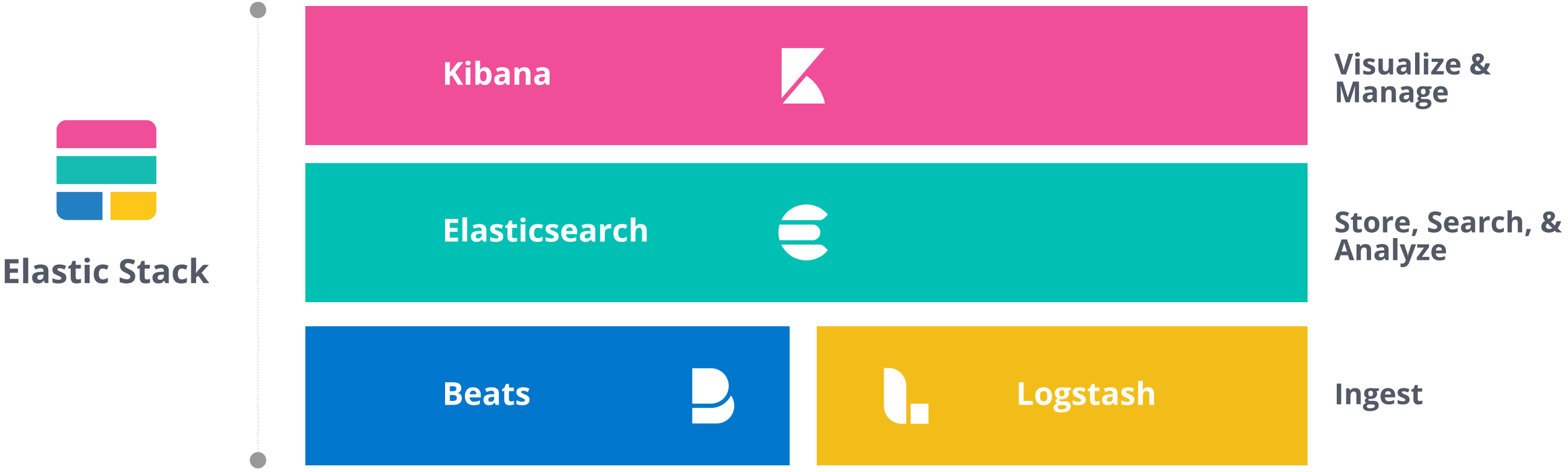
elastic

Say hello to (B)ELK!



elastic

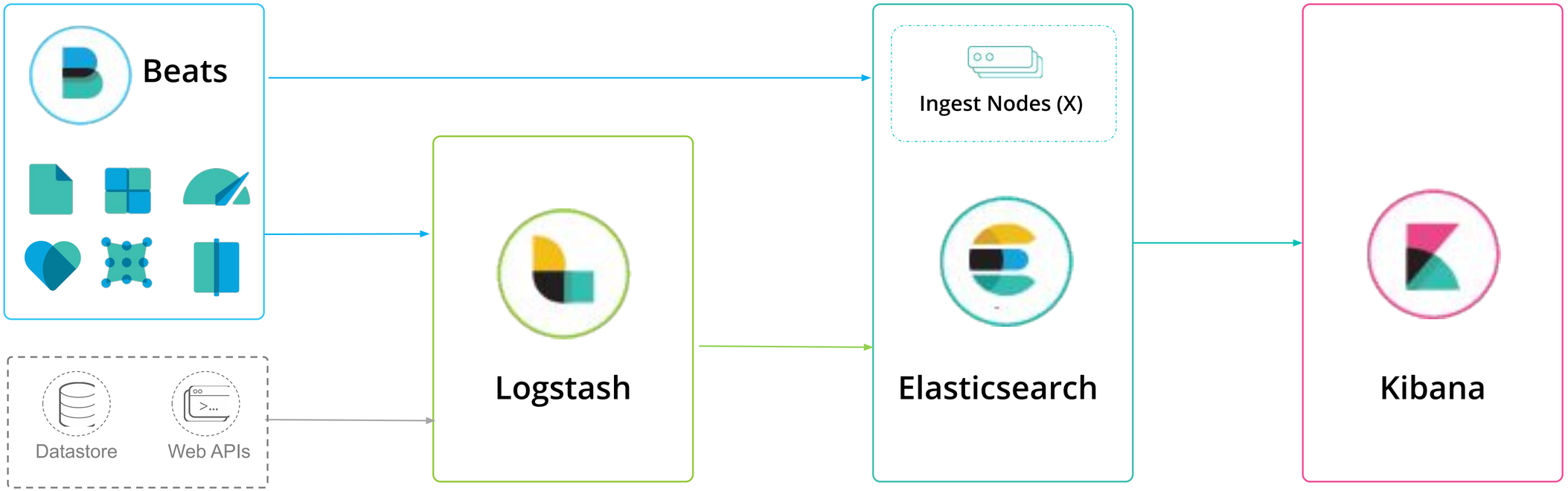
Elastic **Stack**



elastic

How Elastic Stack Components Work Together

Ingest data with Beats and/or Logstash. Manage/visualize with Kibana



elastic

Kibana

Demo

elastic

Elastic Stack

Deployment Models

elastic

Deployment **options**

SOLUTIONS

Elastic Stack

Kibana		Visualize & Manage
Elasticsearch		Store, Search, & Analyze
Beats	Logstash	Ingest

SaaS

Elastic Cloud

SELF-MANAGED

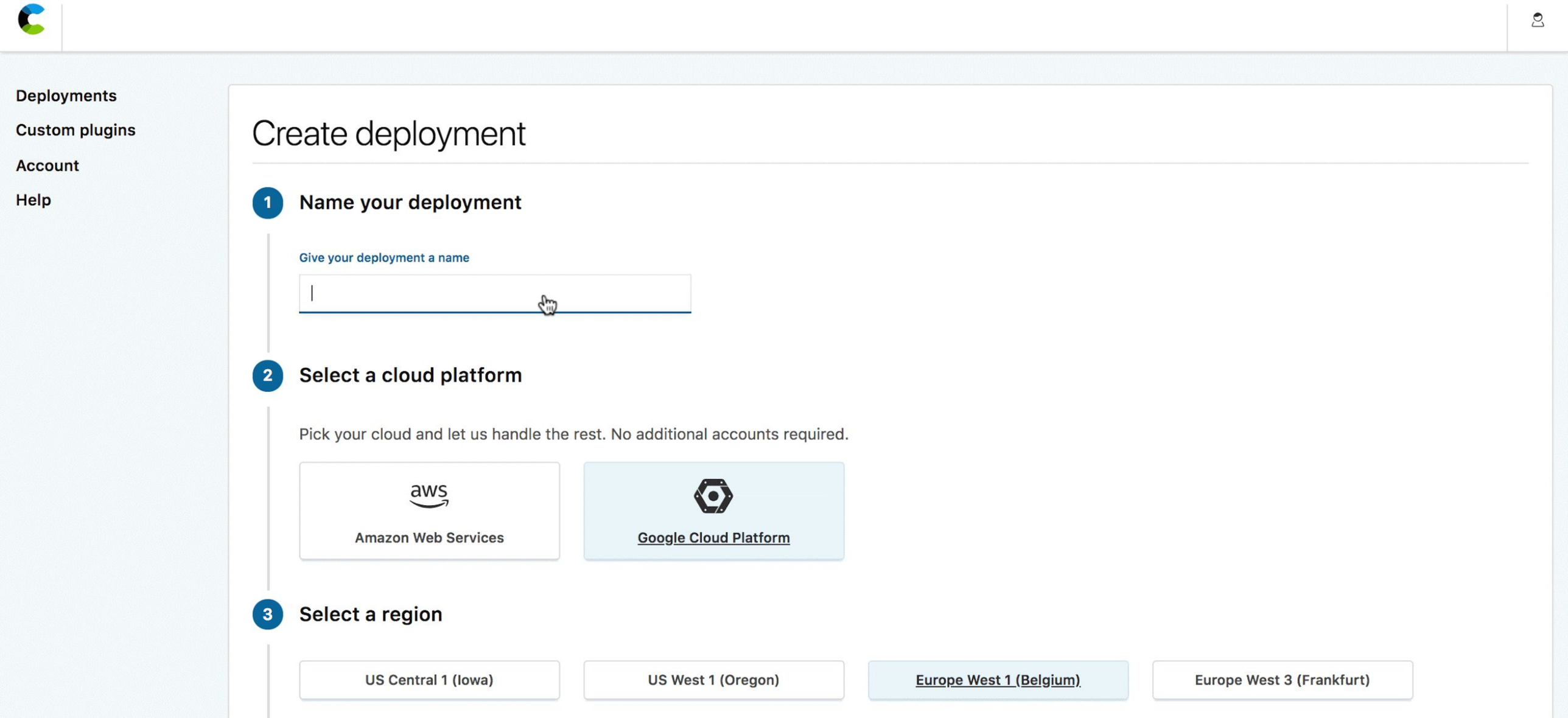
Elastic Cloud Enterprise

Standalone

elastic

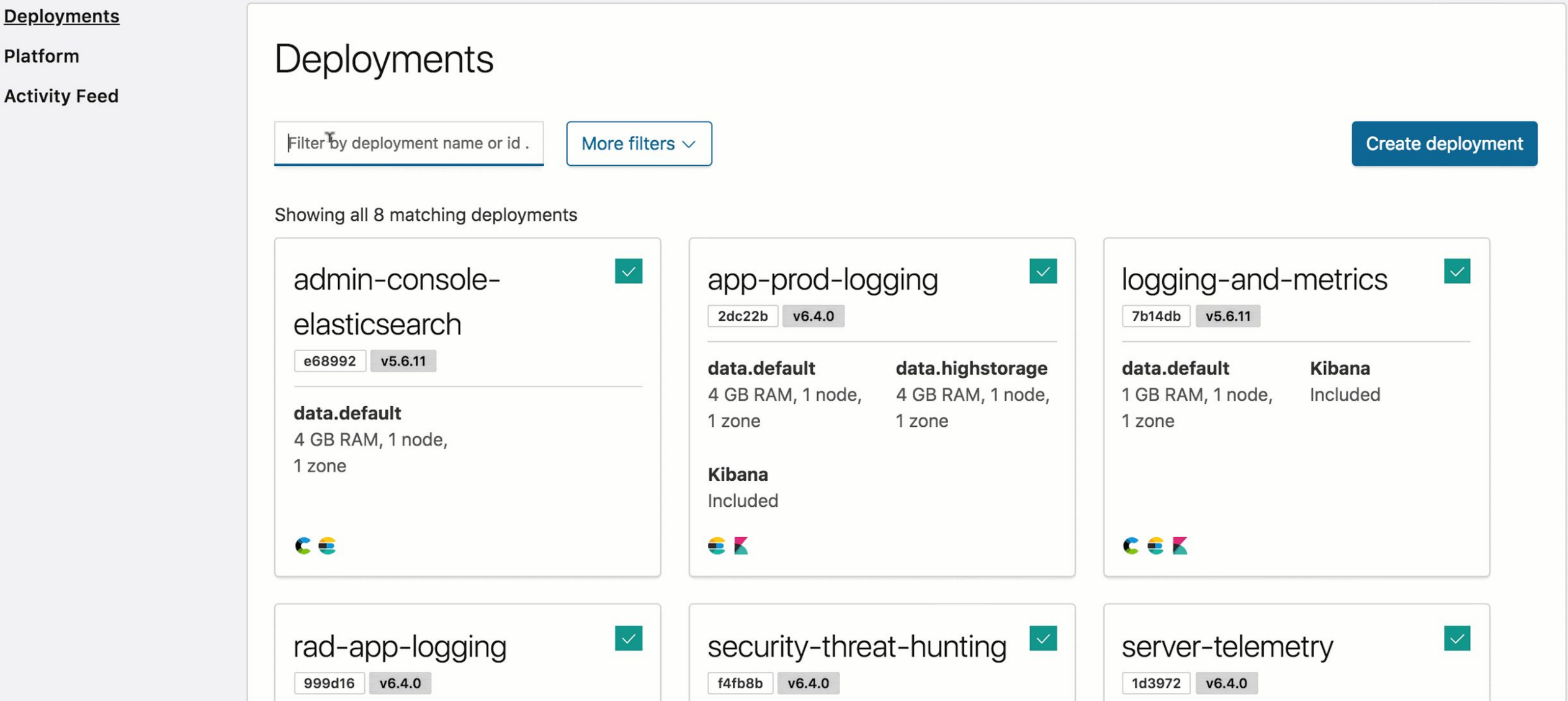
Elastic Cloud

Hosted Elasticsearch, from the creators. No one hosts it better.



Elastic Cloud Enterprise

Packaging years of SaaS experience into a product



Deploying Elastic on Kubernetes

Docker @ Elastic

At Elastic, we care about Docker. We provide Docker images for all the products in our stack, and we consider them a first-class distribution format.

https://www.docker.elastic.co/

Deploying Elastic on Kubernetes

Get started with official Elasticsearch and Kibana Helm charts:

1. Add the Elastic Helm Chart Repo: `helm repo add elastic https://helm.elastic.co`
2. Install Elasticsearch: `helm install --name elasticsearch elastic/elasticsearch`
3. Install Kibana: `helm install --name kibana elastic/kibana`
4. Install Filebeat: `helm install --name filebeat elastic/filebeat` (Recently Released!)

Elastic Cloud on Kubernetes (ECK)

Elastic's Operator for Kubernetes

AUTOMATE & ORCHESTRATE

Elastic Cloud on Kubernetes

Built on the Kubernetes Operator pattern, Elastic Cloud on Kubernetes extends the basic Kubernetes orchestration capabilities to support the setup and management of Elasticsearch and Kibana on Kubernetes.

With Elastic Cloud on Kubernetes, simplify the processes around deployment, upgrades, snapshots, scaling, high availability, security, and more for running Elasticsearch in Kubernetes.

elastic

Elastic Cloud on Kubernetes (ECK)

An Elasticsearch Operator, but so much more

EKS focuses on streamlining all those critical operations, such as:

- Managing and monitoring multiple clusters
- Upgrading to new stack versions with ease
- Scaling cluster capacity up and down
- Changing cluster configuration
- Dynamically scaling local storage
- Scheduling backups

More info @ https://www.elastic.co/elasticsearch-kubernetes

Elastic for

Security Analytics

elastic

Users Already Adopting the Elastic Stack for SIEM

Security Analytics Customers

elastic

Widely Deployed for Security Analytics

Beyond SIEM	Extended SecOps capabilities beyond SIEM **Existing SIEM hitting limits**
SIEM Alternative	Centralized log collection and security analysis **No existing SIEM**
Custom Security App	Platform for special security projects/apps **In-house app dev team creates app**
MSSP	Data store and search engine for security events **Service providers offer managed SIEM solution**
Vertical Security Solution	Data store, search engine, and analysis platform **Security vendor companies build an end-user product**

elastic

Agenda

2:00 p.m.	Welcome, Check-In, Setup your Elastic Lab Environment
	Lab 1 - Create your Elastic Cloud Environment
2:30 p.m.	Introductions & Opening Remarks
	Elastic Stack Overview
3:00 p.m.	MITRE ATT&CK™ Overview
	Lab 2: Data Ingestion using Beats and MITRE ATT&CK
4:00 p.m.	Threat Hunting leveraging MITRE ATT&CK™ Host-level TTPs
	Lab 3: Finding Host-level TTPs using Kibana
4:30 p.m.	Introducing Elastic SIEM
	Lab 4: Interacting with the Elastic SIEM App
5:00 p.m.	Q&A Session & Group Discussions
5:30 p.m.	Workshop Concludes

elastic

Lab 2

Data Ingestion using Beats and MITRE ATT&CK™

elastic

Setup Strigo

Your Training Environment

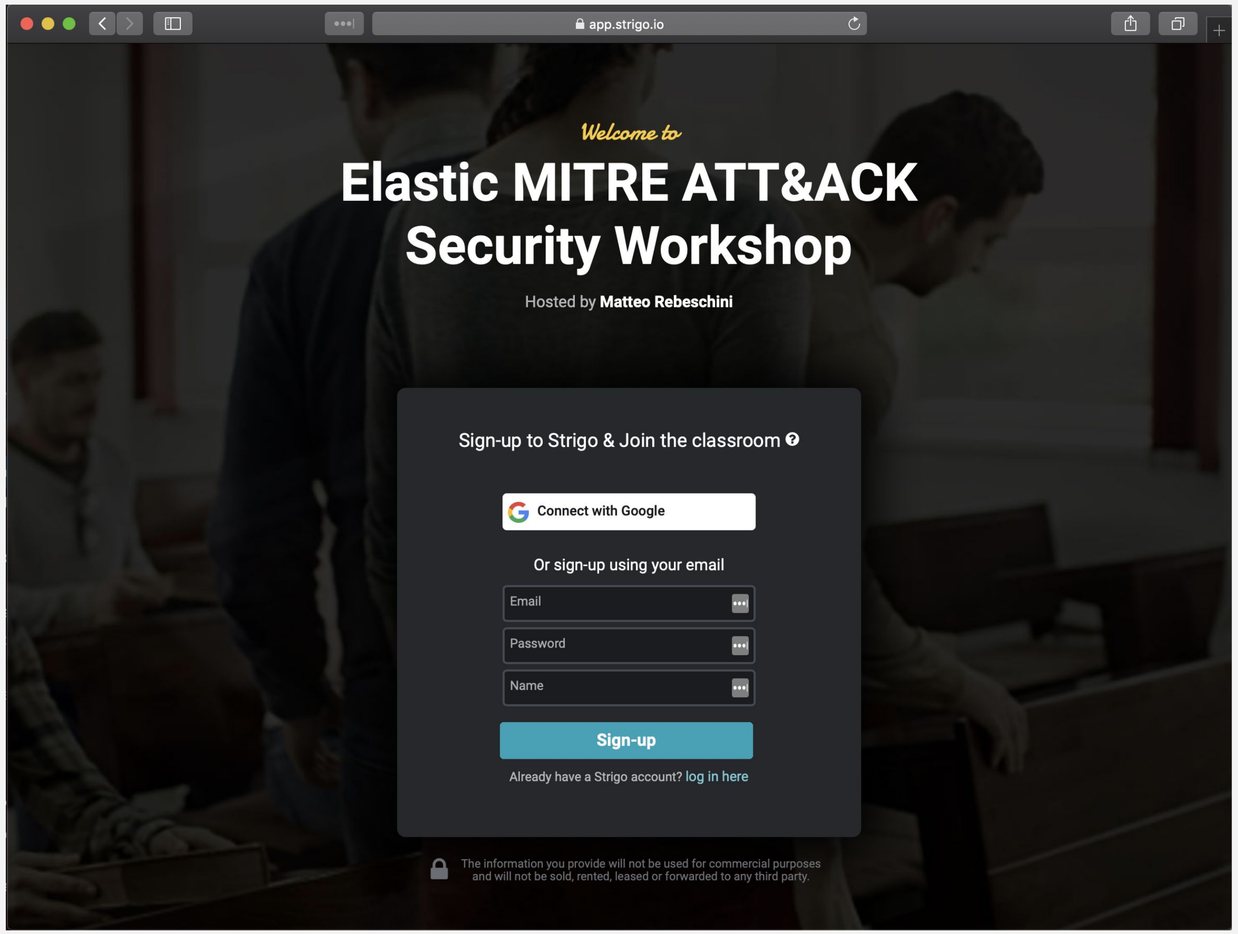
Class URL:

https://bit.ly/BSidesLV2019

Access Token:

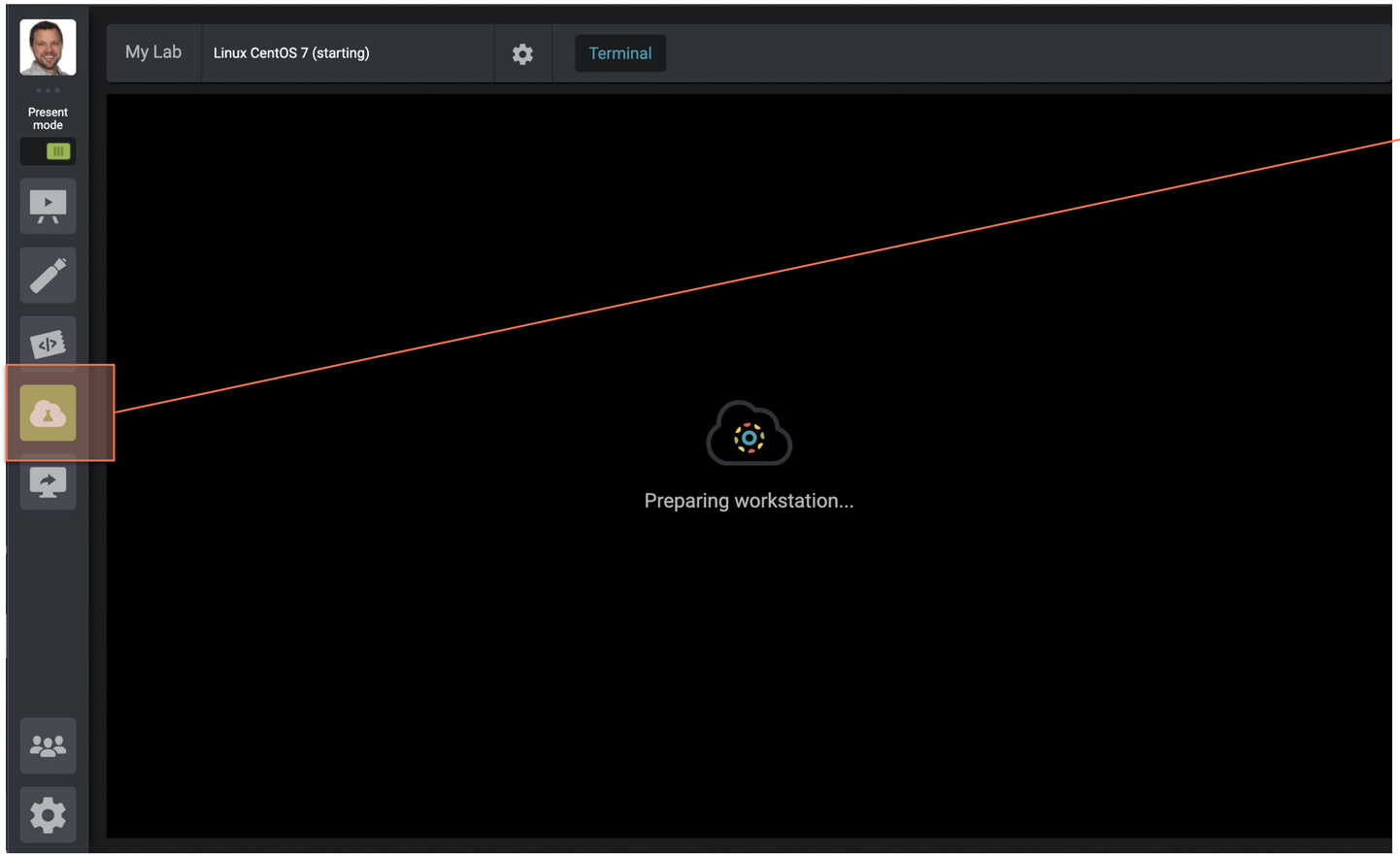
YK7M

Lab environment will stay active until 8/10 @ 5:00PM



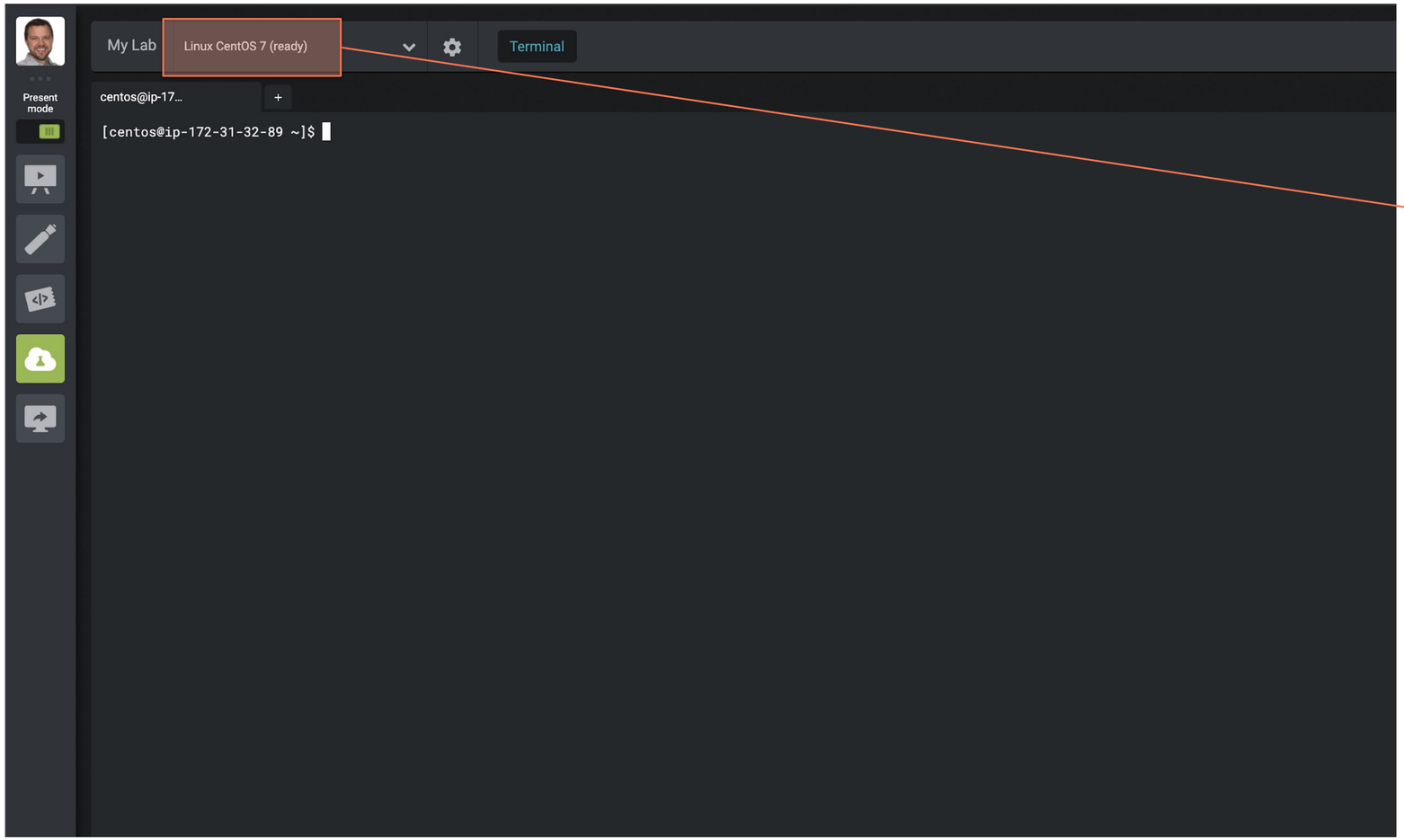
Linux Beats Scripted Install

Access “My Lab” (it will take a few minutes)



Linux Beats Scripted Install

You will see a CentOS Terminal when Lab Instance is Ready

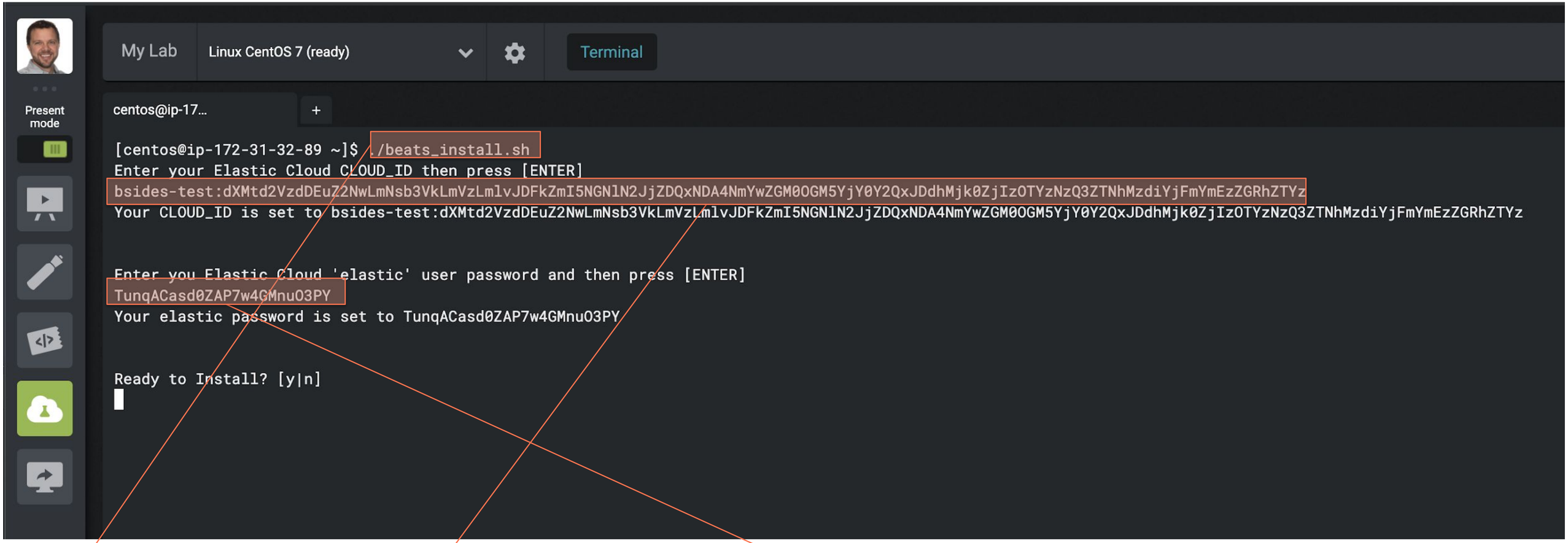


1 After a few minutes, a CentOS Linux instance should be available under ‘My Lab’

elastic

Linux Beats Scripted Install

Installation of MetricBeat, Filebeat, AuditBeat and PacketBeat



1 Type ‘./beats_install.sh’

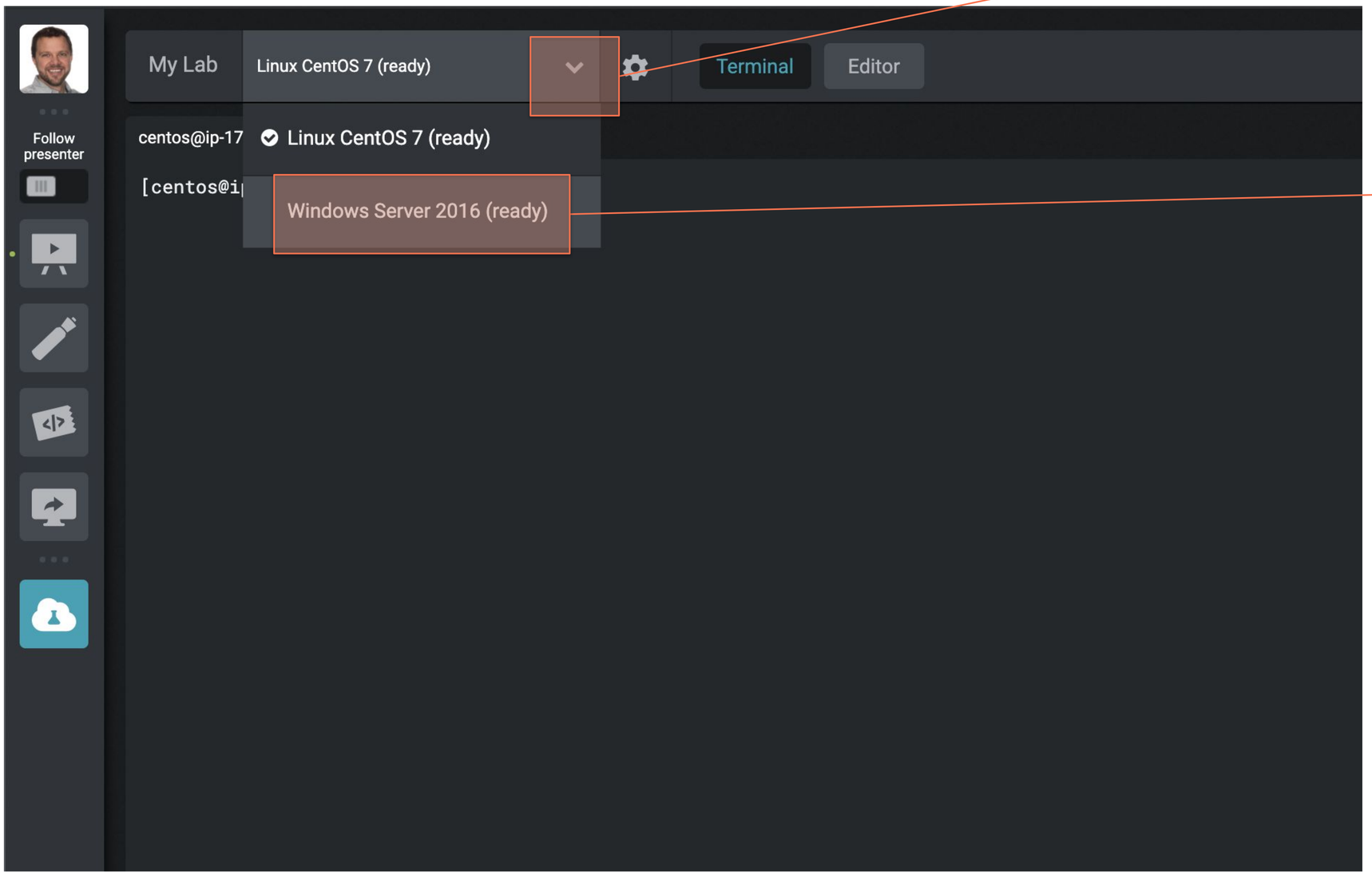
2 Copy-n-Paste the CLOUD ID created in Lab 1

3 Copy-n-Paste the elastic user’s password created in Lab 1

elastic

Windows Beats Scripted Install

Access your Windows Server 2016 Instance



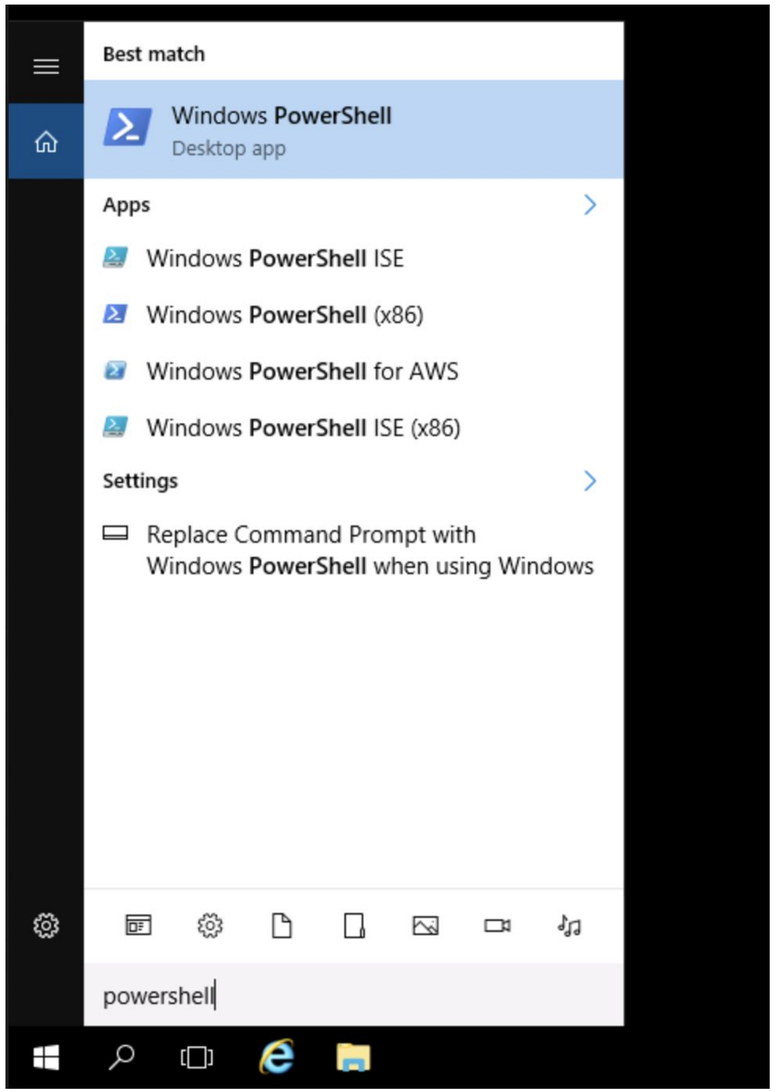
1 Select the arrow next to ‘My Lab’

2 Select ‘Windows Server 2016’

elastic

Windows Scripted Install

Install Sysmon with Custom Config Template



1 Type: cd ela <TAB> to autocomplete .\Elastic\> <RETRUN/ENTER>

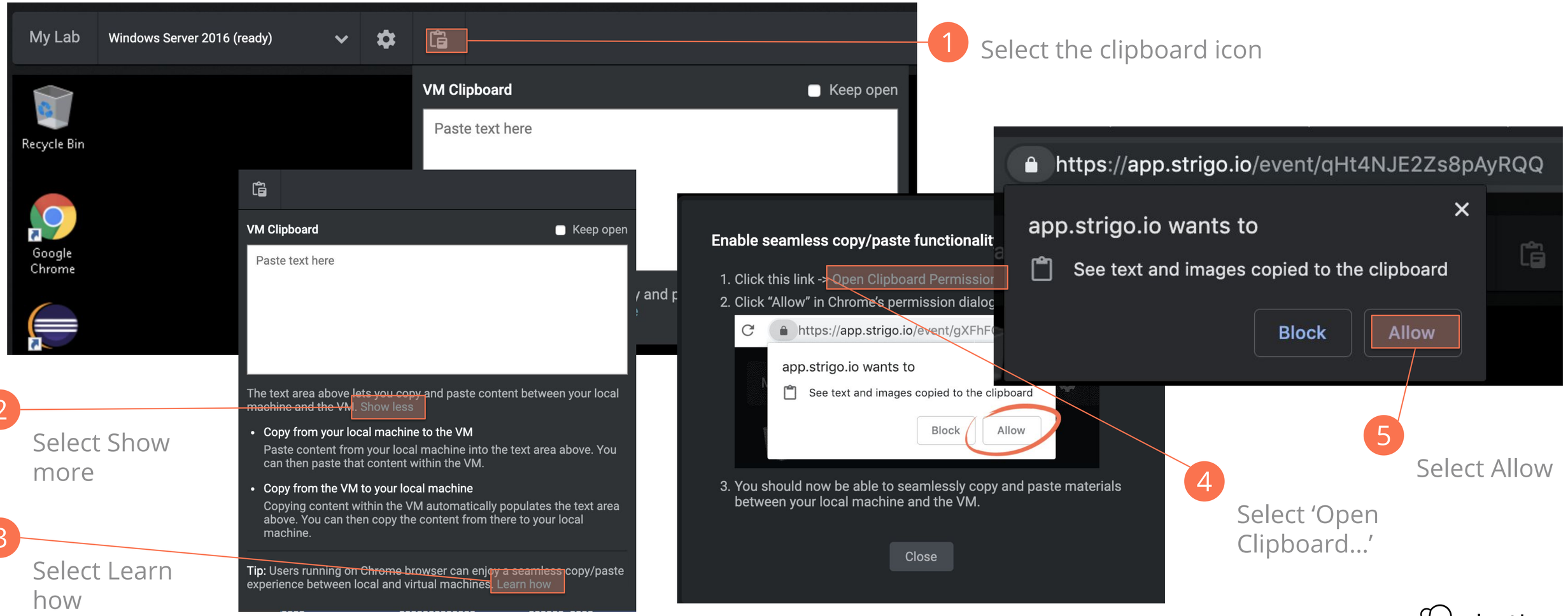
2 Type: sys <TAB> to autocomplete '.\sysmon-install.ps1' <RETURN/ENTER>

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cd .\Elastic\
PS C:\Users\Administrator\Elastic> .\sysmon-install.ps1
Installing Sysmon...


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         8/2/2019  12:55 PM                sysmon-temp
Installation Complete


PS C:\Users\Administrator\Elastic> _
```


elastic

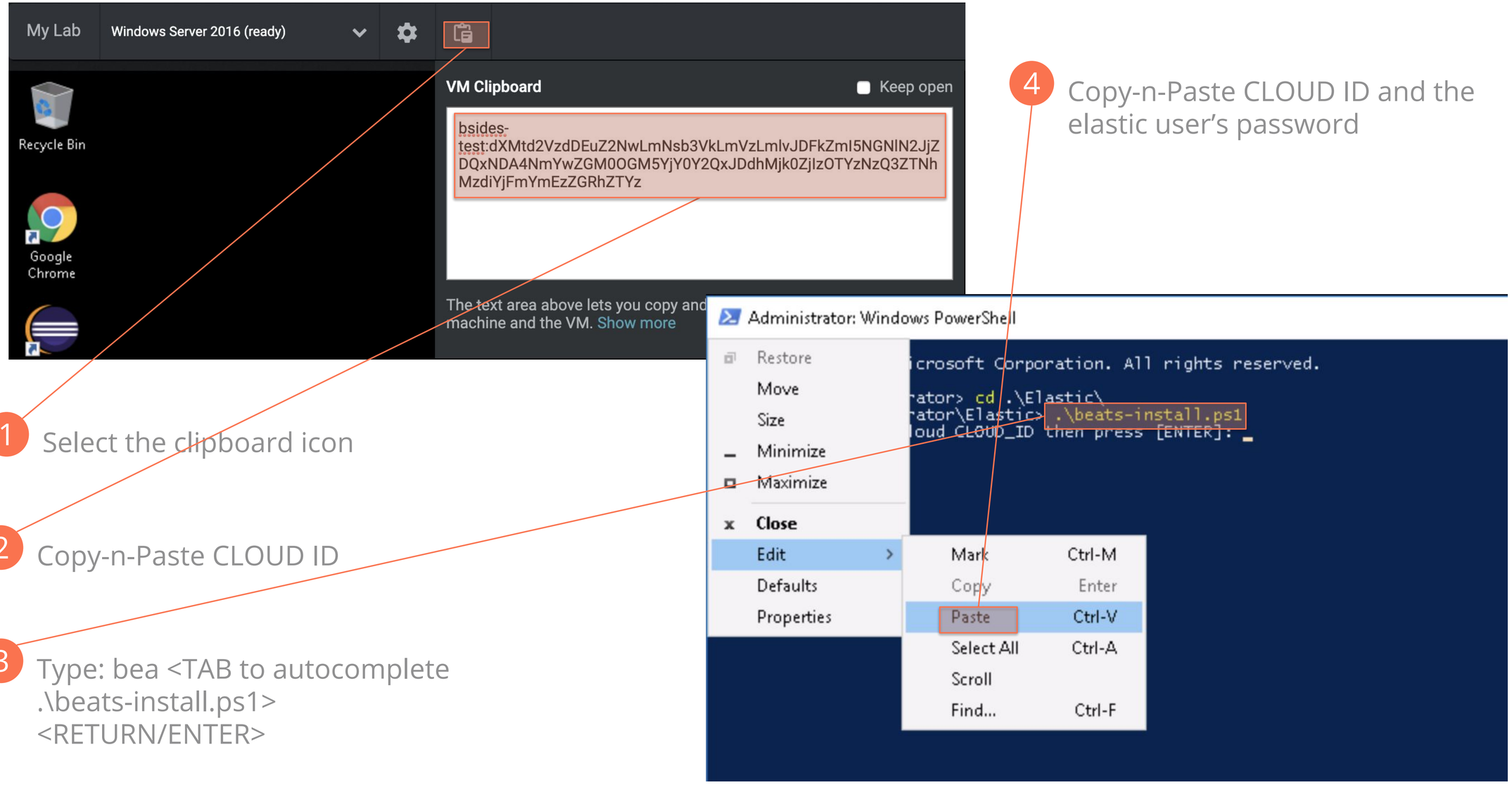
Windows Scripted Install

Seamless Clipboard Access using Google Chrome



Windows Scripted Install

You must use the Strigo VM Clipboard to Copy Text to the Instance



1 Select the clipboard icon

2 Copy-n-Paste CLOUD ID

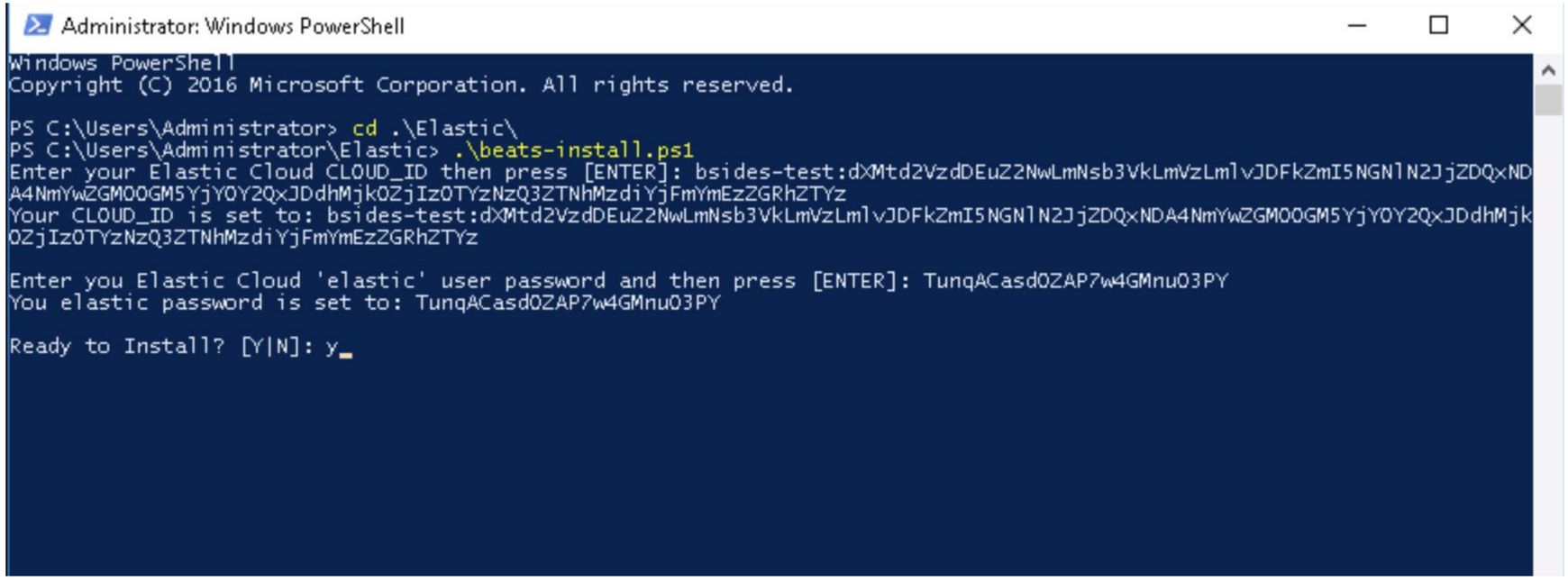
3 Type: bea <TAB to autocomplete .\beats-install.ps1> <RETURN/ENTER>

4 Copy-n-Paste CLOUD ID and the elastic user's password

elastic

Windows Scripted Install

Winlogbeat & Metricbeat Installation

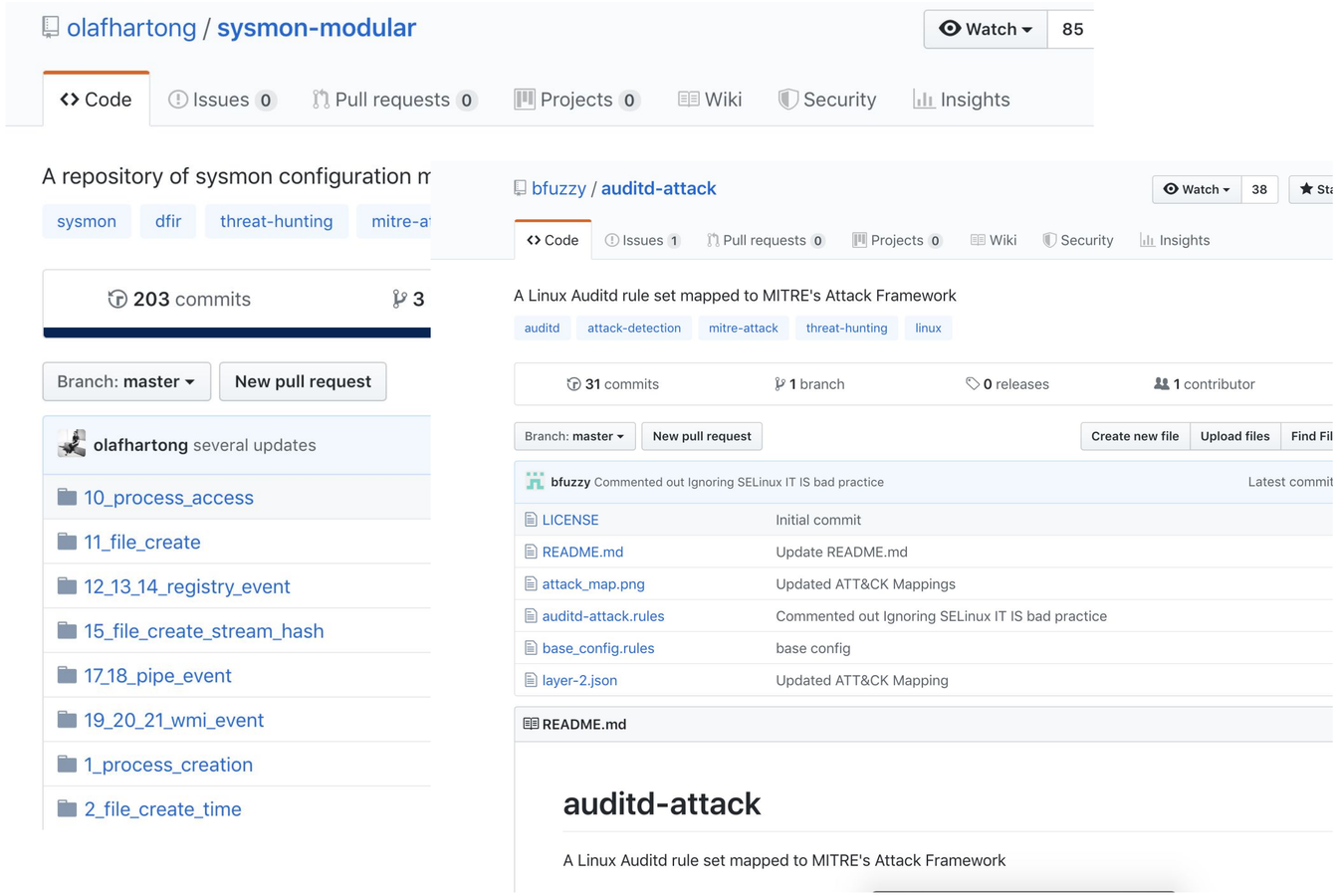


elastic

ATT&CK™ Beats Community

ATT&CK™ configs Thanks to the community

- olafhartong / sysmon-modular
- bfuzzy / auditd-attack



MITRE ATT&CK™ Overview

elastic

Prevention falls short

Prediction

Prevention

Retrospection

Detection

Focus on Detection

Prediction

Prevention

Retrospection

Detection

What to look for?

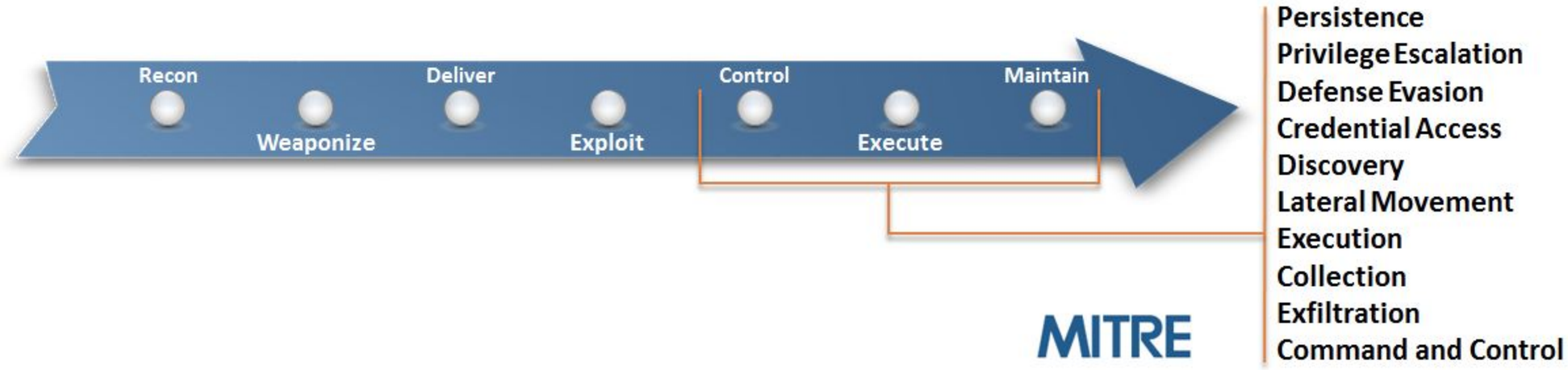
ATT&CK is a MITRE-developed, globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

MITRE

ATT&CK™

Adversarial Tactics, Techniques & Common Knowledge

ATT&CK is useful for understanding security risk against known adversary behavior, for planning security improvements, and verifying defenses work.



https://attack.mitre.org/wiki/Introduction_and_Overview

elastic

What’s in a name?

Nomenclature..should provide the names as soon as classification is made...if the names are unknown, knowledge of things also parishes.

For a single genus, a single name.

https://todayinsci.com/L/Linnaeus_Carolus/LinnaeusCarolus-Quotations.htm

Windows ATT&CK for Enterprise Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	AppCert DLLs	Accessibility Features	BITS Jobs	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Control Panel Items	AppInit DLLs	AppCert DLLs	Binary Padding	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	AppInit DLLs	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Logon Scripts	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Execution through API	Authentication Package	Application Shimming	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through Module Load	BITS Jobs	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Exploitation for Client Execution	Bootkit	DLL Search Order Hijacking	Component Firmware	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Remote File Copy	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Permission Groups Discovery	Remote Services	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Kerberoasting	Process Discovery	Replication Through Removable Media	Input Capture		Multi-Stage Channels
	Mshta	Component Object Model Hijacking	Hooking	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	Query Registry	Shared Webroot	Man in the Browser		Multi-hop Proxy
	PowerShell	Create Account	Image File Execution Options Injection	DLL Side-Loading	Network Sniffing	Remote System Discovery	Taint Shared Content	Screen Capture		Multiband Communication
	Regsvcs/Regasm	DLL Search Order Hijacking	New Service	Deobfuscate/Decode Files or Information	Password Filter DLL	Security Software Discovery	Third-party Software	Video Capture		Multilayer Encryption
	Regsvr32	External Remote Services	Path Interception	Disabling Security Tools	Private Keys	System Information Discovery	Windows Admin Shares			Remote Access Tools
	Rundll32	File System Permissions	Port Monitors	Exploitation for	Replication Through	System Network Configuration	Windows Remote			Remote File Copy

Example ATT&CK Technique

ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge

Page | Discussion | Read | View form | View history | Search enterprise

Last 5 Pages Viewed: Technique Matrix [object Object] Using the API [object Object] Rootkit [object Object] Group: Winnti Group, Blackfly [object Object] Process Discovery

- Main page
- Help
- Contribute
- References
- Using the API

Tactics
- Initial Access
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Execution
- Collection
- Exfiltration
- Command and Control

Techniques
- Technique Matrix
- All Techniques
- Windows

Process Discovery

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software running on systems within the network.

Contents [hide]

Process Discovery	
Technique	
ID	T1057
Tactic	Discovery
Platform	Linux, macOS, Windows
System Requirements	Administrator, SYSTEM may provide better process ownership details
Permissions Required	User, Administrator, SYSTEM
Data Sources	Process command-line parameters, Process monitoring
CAPEC ID	CAPEC-573

Windows

An example command that would obtain details on processes is "tasklist" using the Tasklist utility.

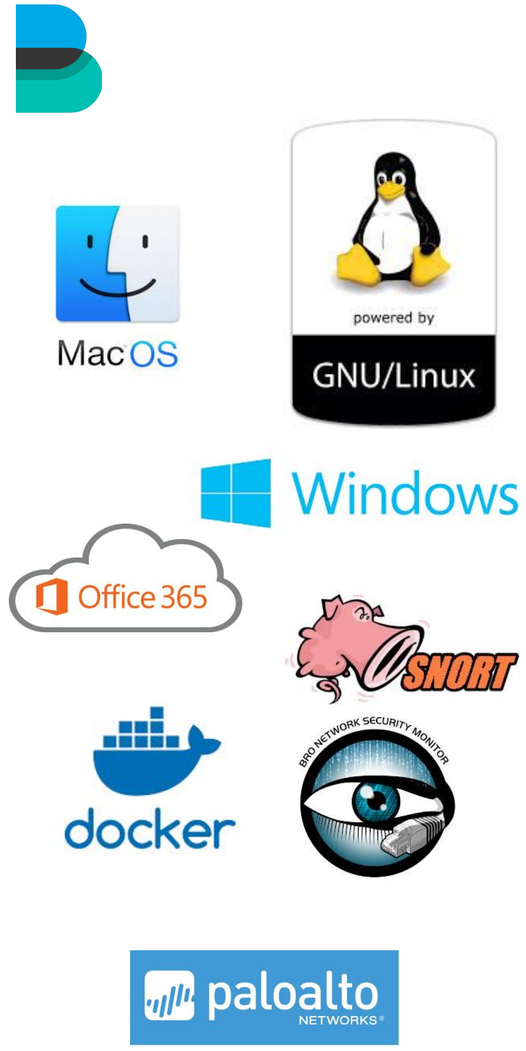
Mac and Linux

In Mac and Linux, this is accomplished with the `ps` command.

elastic

Data Quality

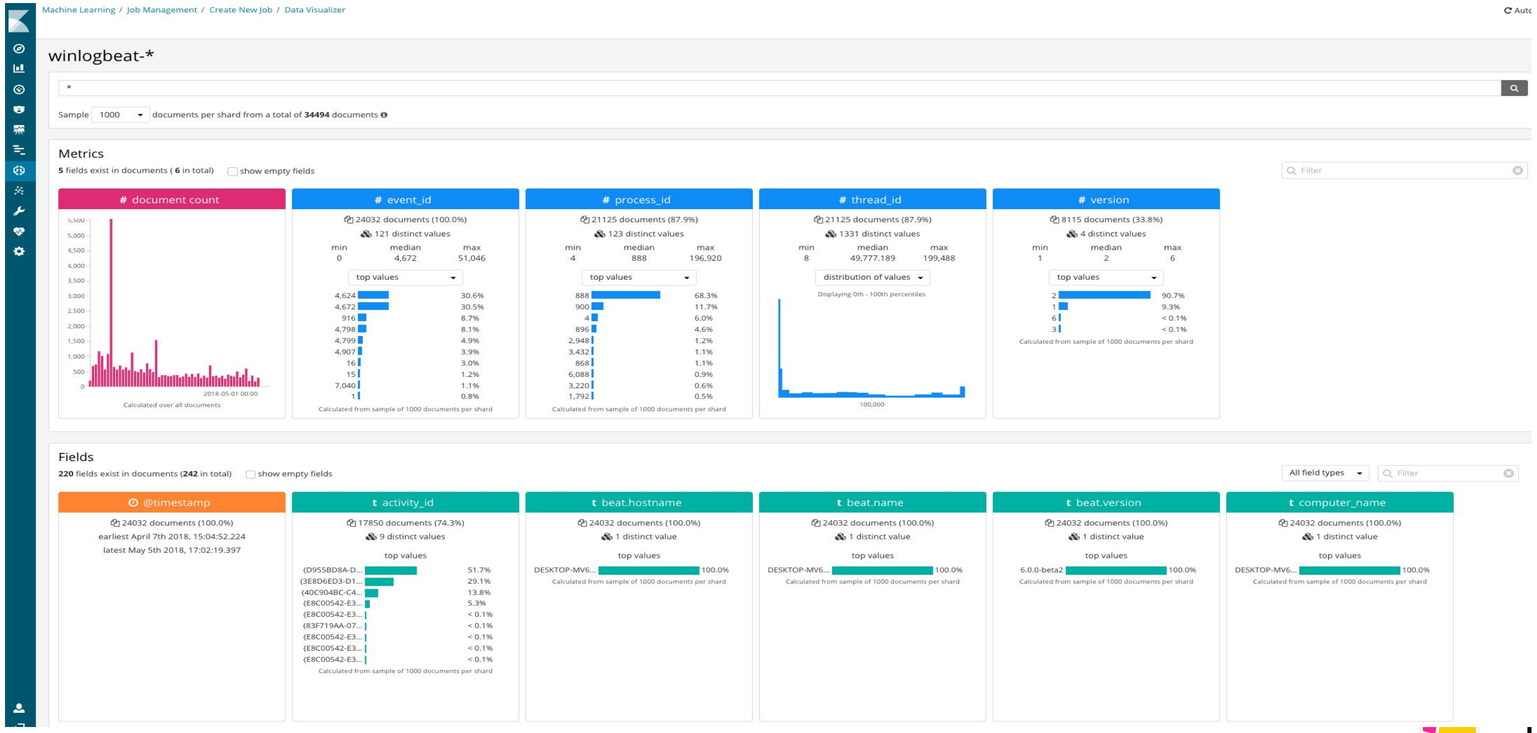
- What percentage of data is available?
- What percentage of the expected data is complete?
- How far back in time does the data go?
- What percentage of data is consistent over time?



elastic

Correlating Your Data with ATT&CK Analytics

- What field names are in your data?
- How do they correlate to one another?
- Are all ATT&CK data fields present?
- Does your data need to be transformed?
- Does your data need to be enriched?



elastic

Endpoint: Winlogbeat with Sysmon

- Command line arguments
- Networked Process
  - IP's
  - Port's
  - Parent
- Persistent across reboots
- Process creation
- FIle changes

Sysmon Events

Category	Event ID
Sysmon Service Status Changed	0
Process Create	1
File Creation Time Changed	2
Network Connection	3
Sysmon Service State Change	4
Process Terminated	5
Driver Loaded	6
Image Loaded	7
CreateRemoteThread	8
RawAccessRead	9

Category	Event ID
Process Access	10
File Create	11
Registry Object CreateDelete	12
Registry Value Create	13
Registry Object Rename	14
File Create Stream Hash	15
Sysmon Configuration Changed	16
Pipe Created	17
Pipe Connected	18
Error	255

v6

elastic

Agenda

2:00 p.m.	Welcome, Check-In, Setup your Elastic Lab Environment
	Lab 1 - Create your Elastic Cloud Environment
2:30 p.m.	Introductions & Opening Remarks
	Elastic Stack Overview
3:00 p.m.	MITRE ATT&CK™ Overview
	Lab 2: Data Ingestion using Beats and MITRE ATT&CK
4:00 p.m.	Threat Hunting leveraging MITRE ATT&CK™ Host-level TTPs
	Lab 3: Finding Host-level TTPs using Kibana
4:30 p.m.	Introducing Elastic SIEM
	Lab 4: Interacting with the Elastic SIEM App
5:00 p.m.	Q&A Session & Group Discussions
5:30 p.m.	Workshop Concludes

elastic

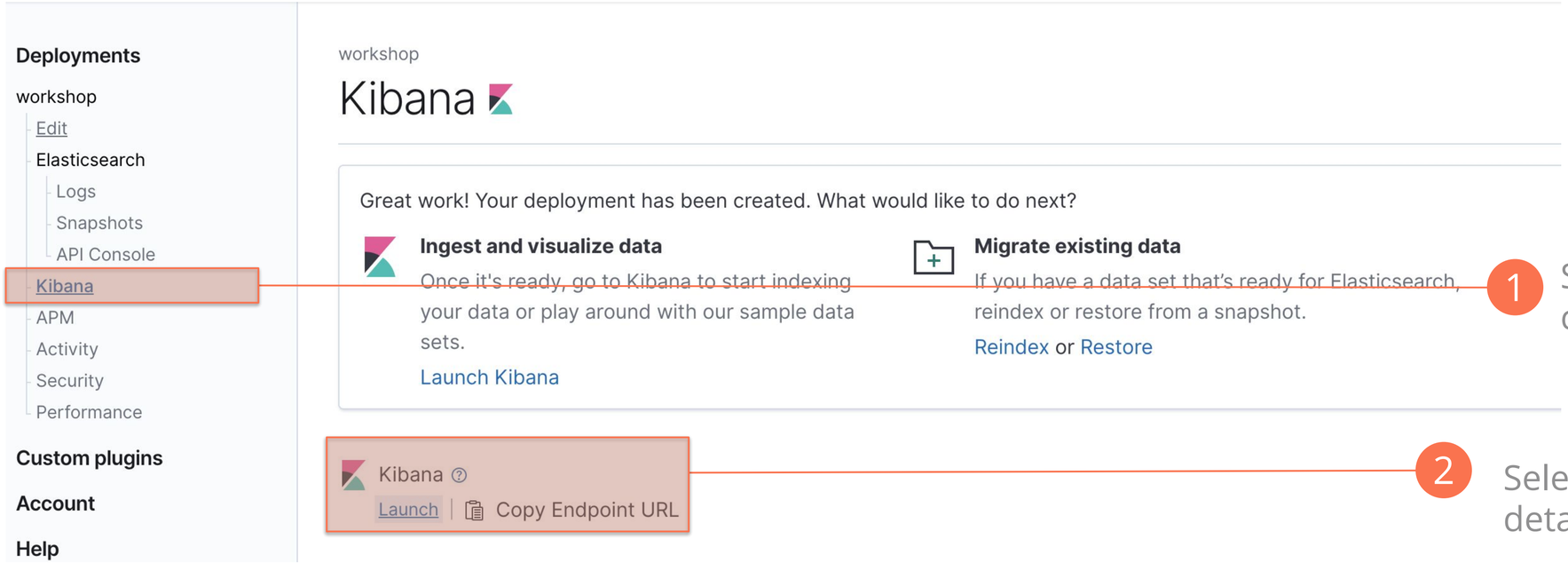
Lab 3

Finding MITRE ATT&CK™ TTPs

elastic

Launch Kibana from Cloud

Login to cloud.elastic.co account created in lab #1



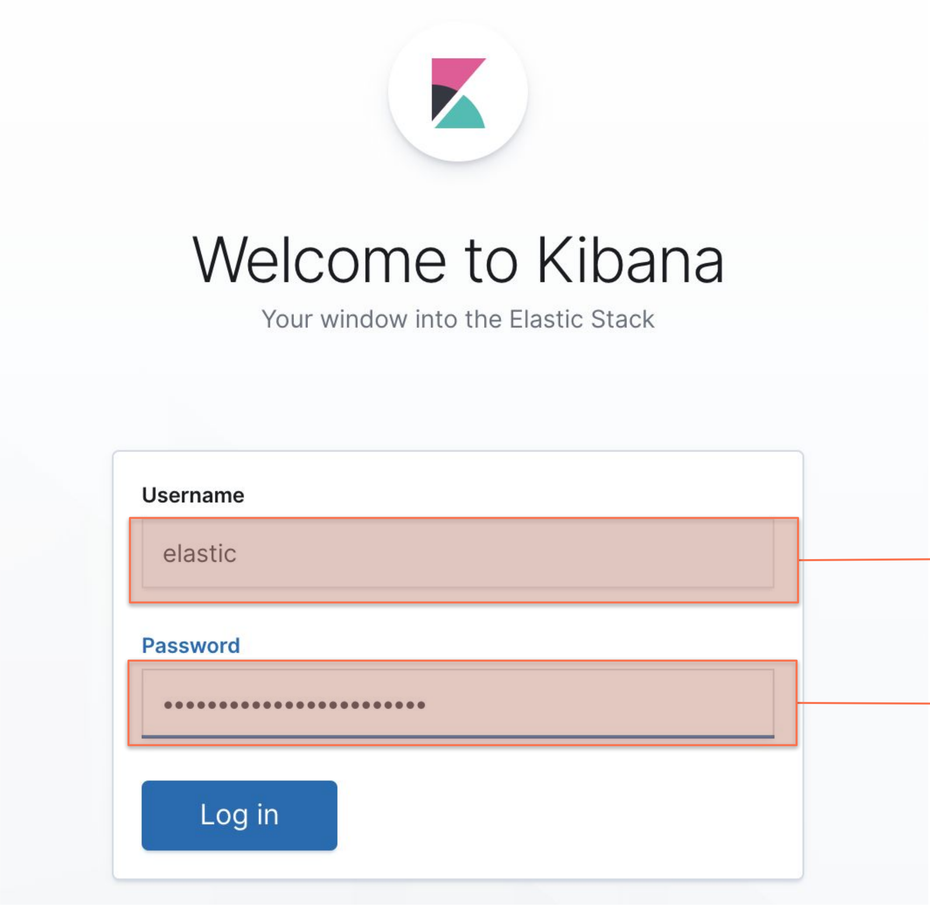
1 Select Kibana under the newly created deployment.

2 Select Launch in the Kibana details.

elastic

Log into Kibana

Setting Time Ranges

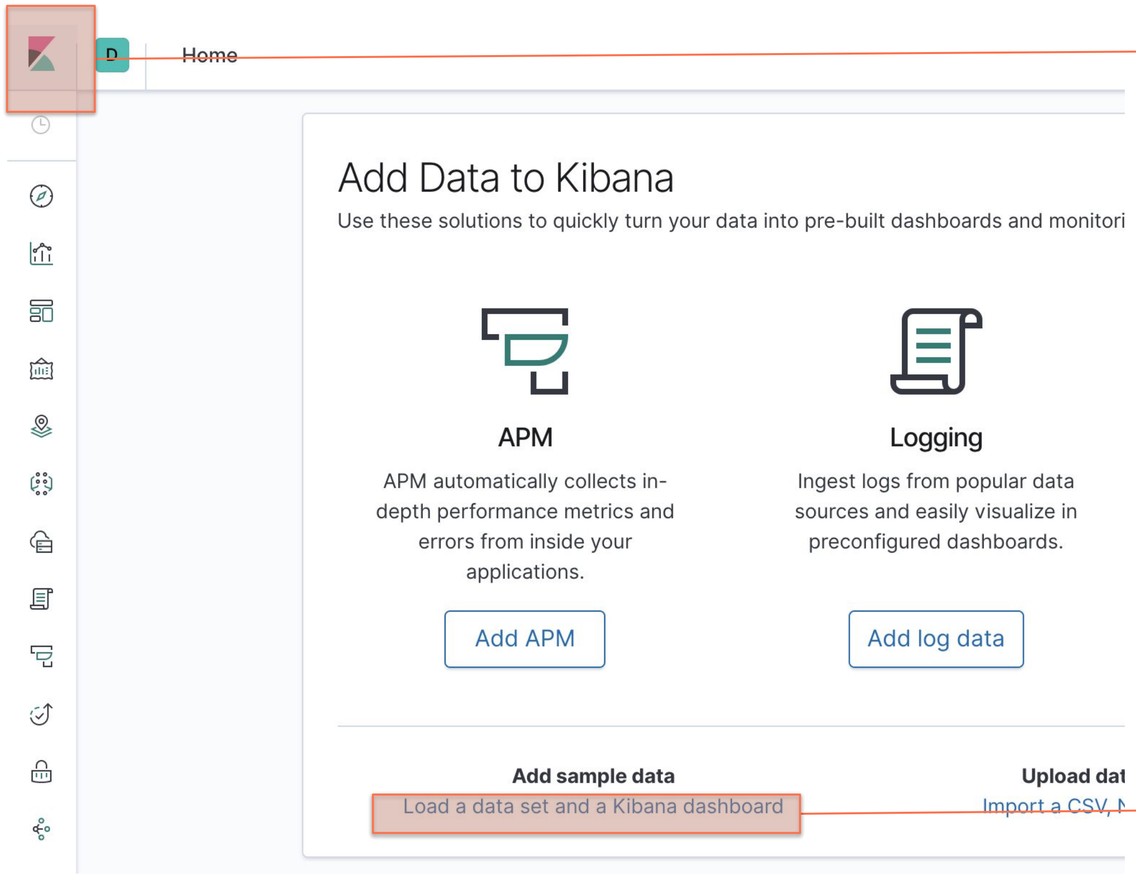


1. Username is: elastic
2. Copy-n-Paste the Cloud elastic user password saved in Lab #1.

elastic

Load Sample Data in Kibana

Kibana load data page



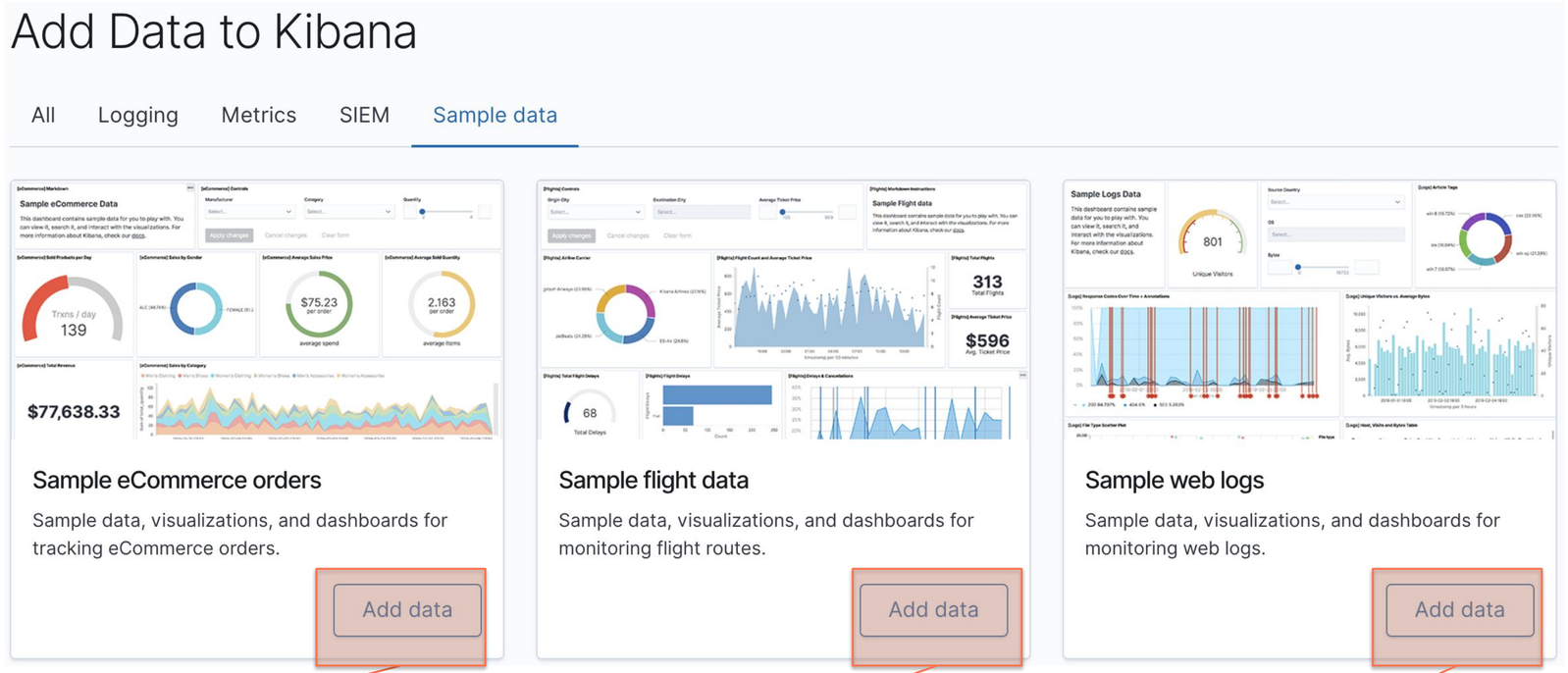
1 Select the ‘K’ icon.

2 Select ‘Load a data..’ link under ‘Add sample data’.

elastic

Loading sample data into the Elastic Stack

Load all three data sets

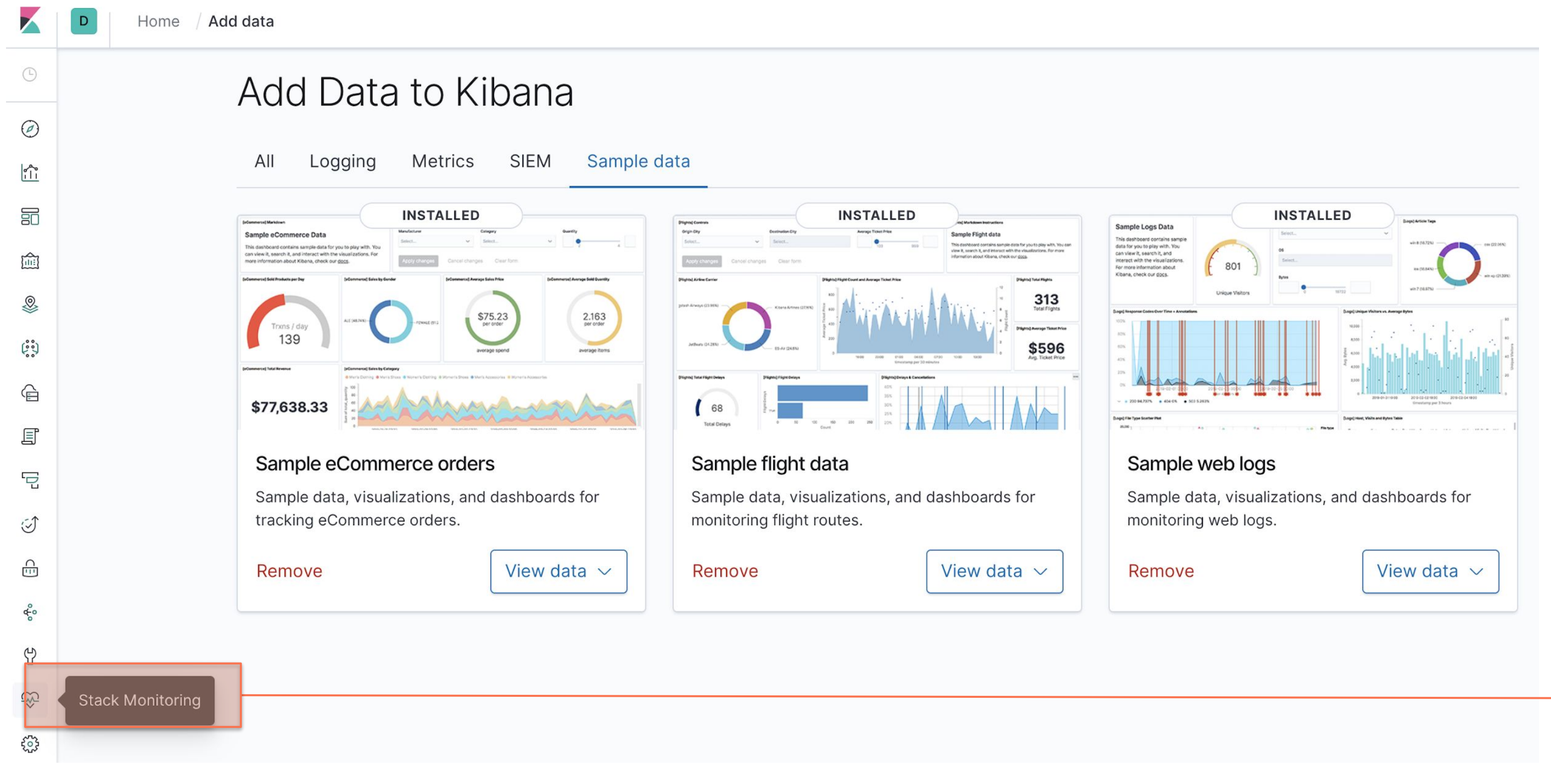


1. Add Sample eCommerce orders
2. Add Sample flight data
3. Add Sample web logs

elastic

Navigate to Stack Monitoring

Second icon (heart) from the bottom left Navigation menu

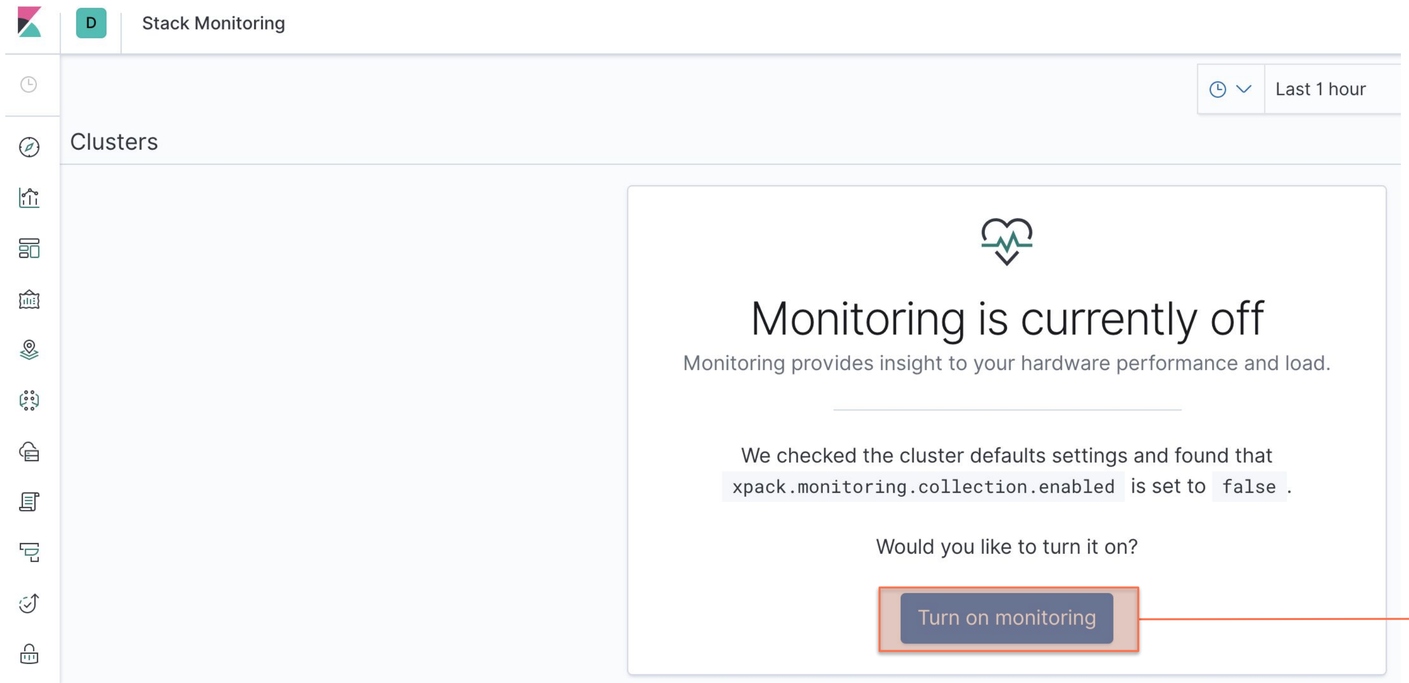


1 Select Stack Monitoring

elastic

Enable Stack Monitoring

Stack monitoring lets you understand Elastic Cloud cluster perfomance

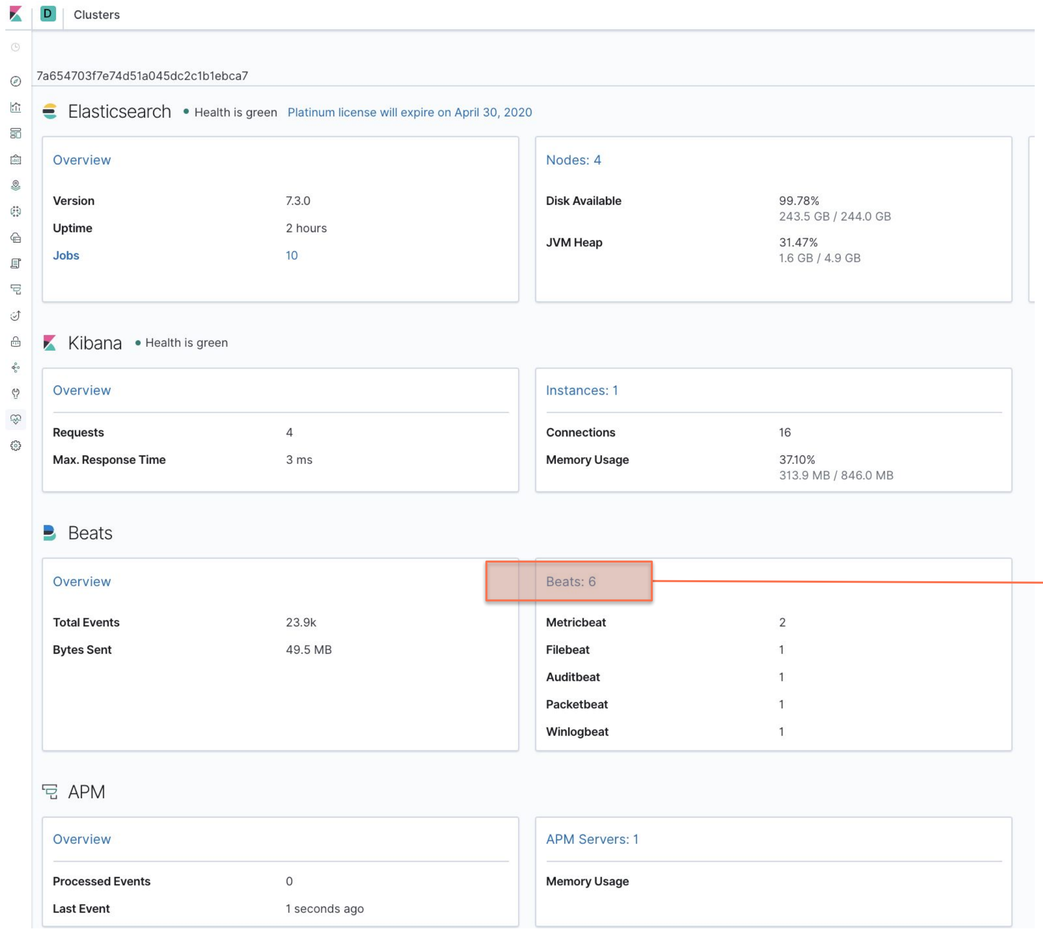


1 Select Turn on monitoring

elastic

Ensure your Beats agents are online

After a few minutes, you should see 6 beats enabled

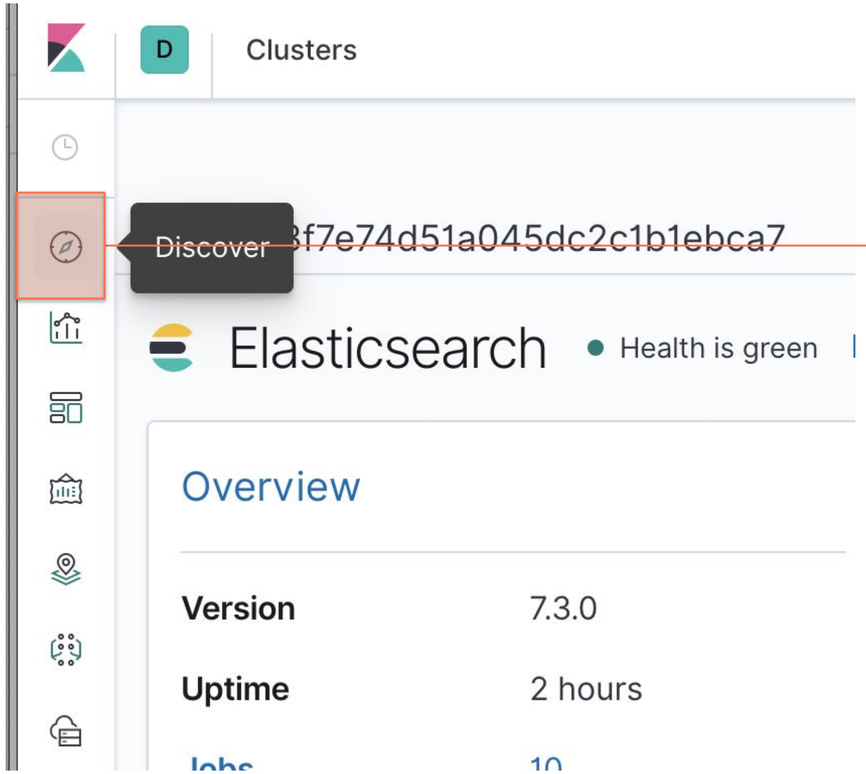


1 Six Beats should be enabled

elastic

Move to the Discover app

Discovering what is in the data

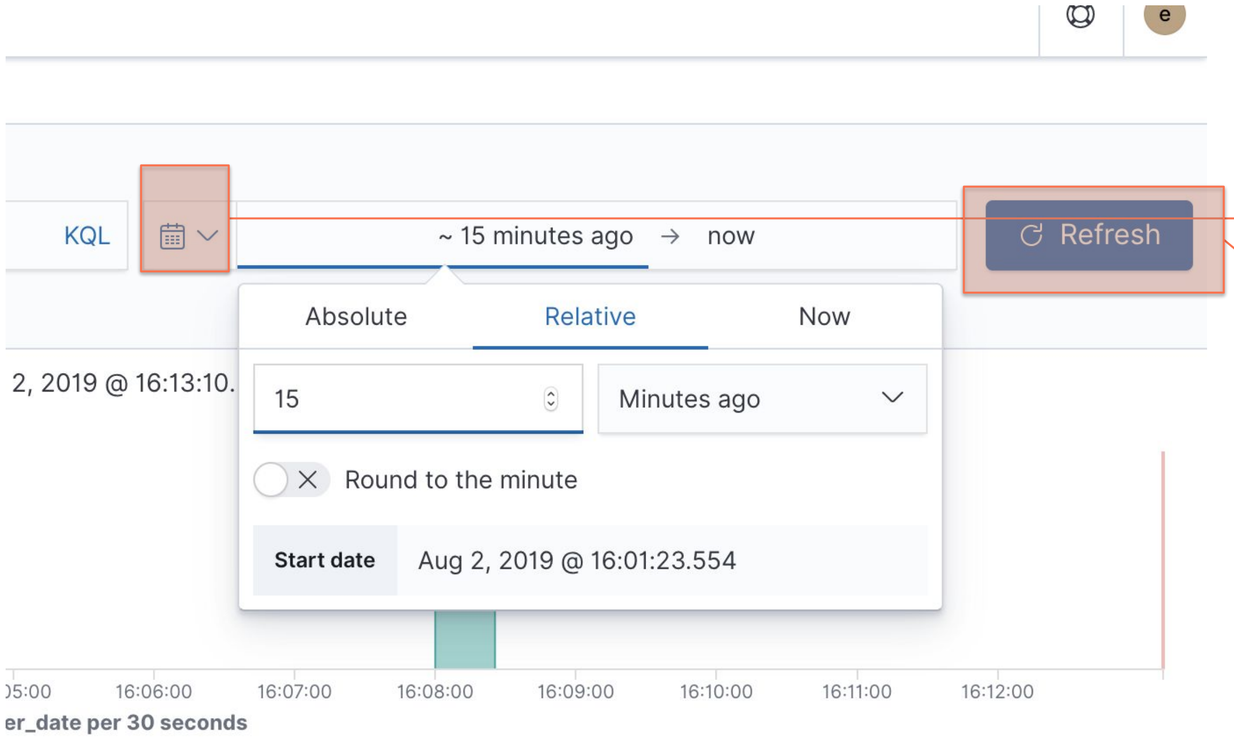


1 Select ‘Discover”

elastic

Setting the time range

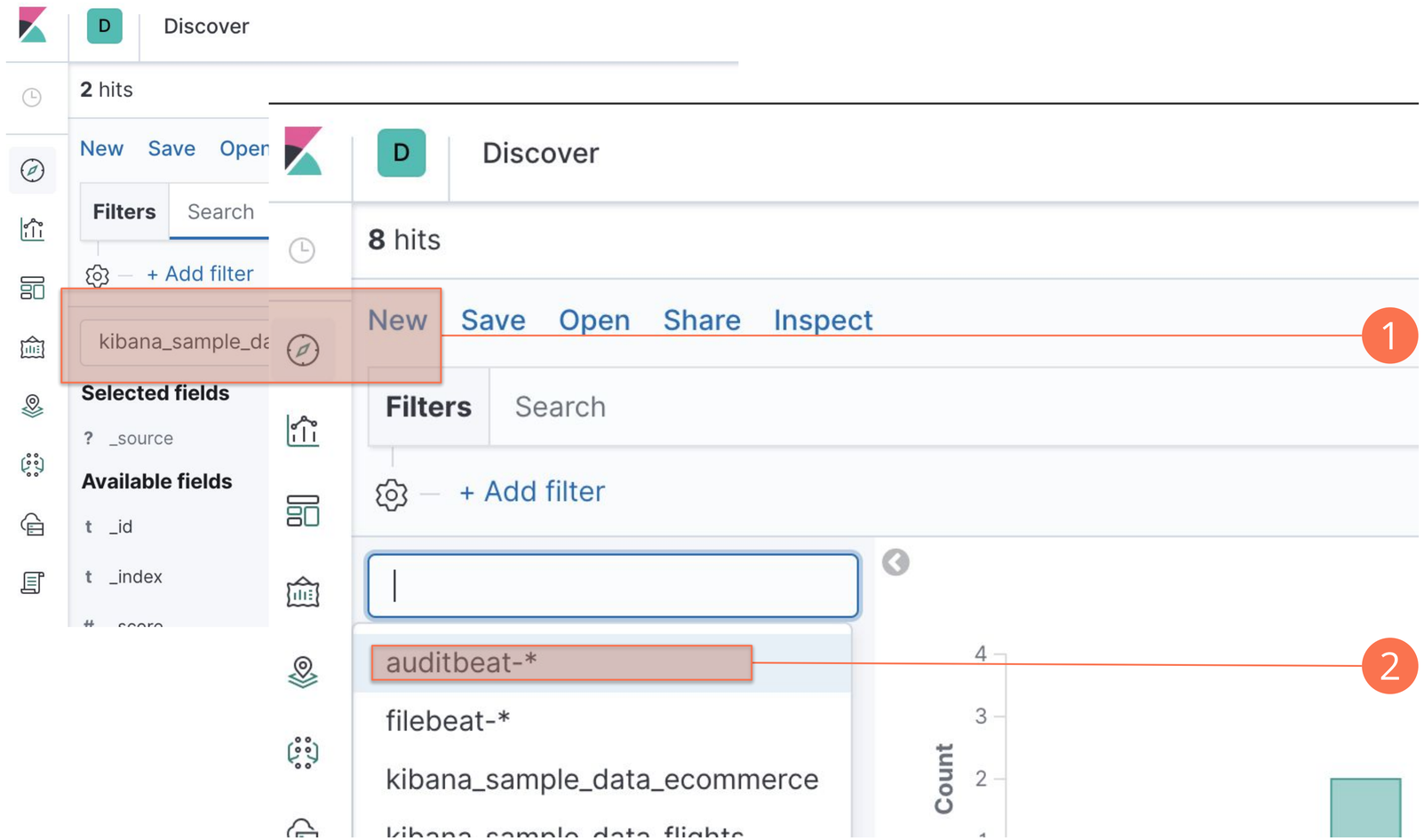
Ensure kibana is set to the last 15 minutes



1. Select the calendar icon, Then set the last 15 minutes
2. Select Refresh

Select the index

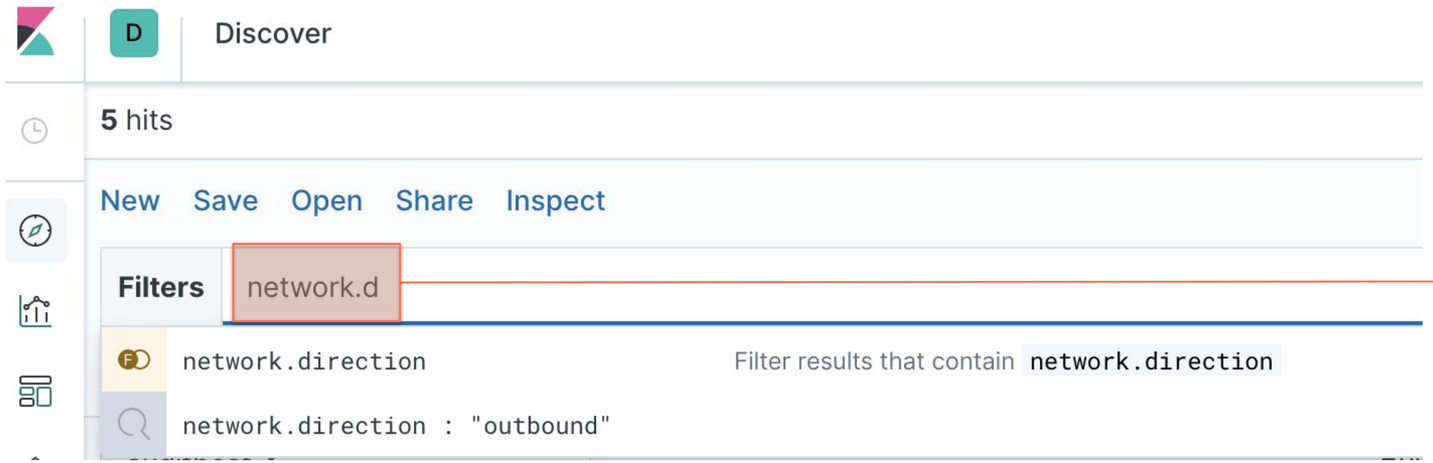
Kibana has multiple indices, select auditbeat



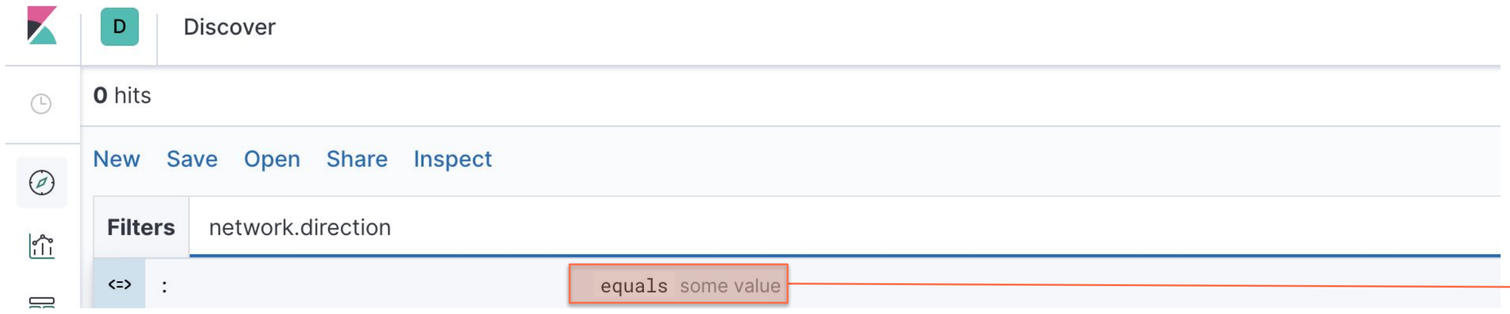
elastic

Search with KQL in Kibana

The default way to search



1 Type ‘network.d’ and select network.direction from the drop down menu

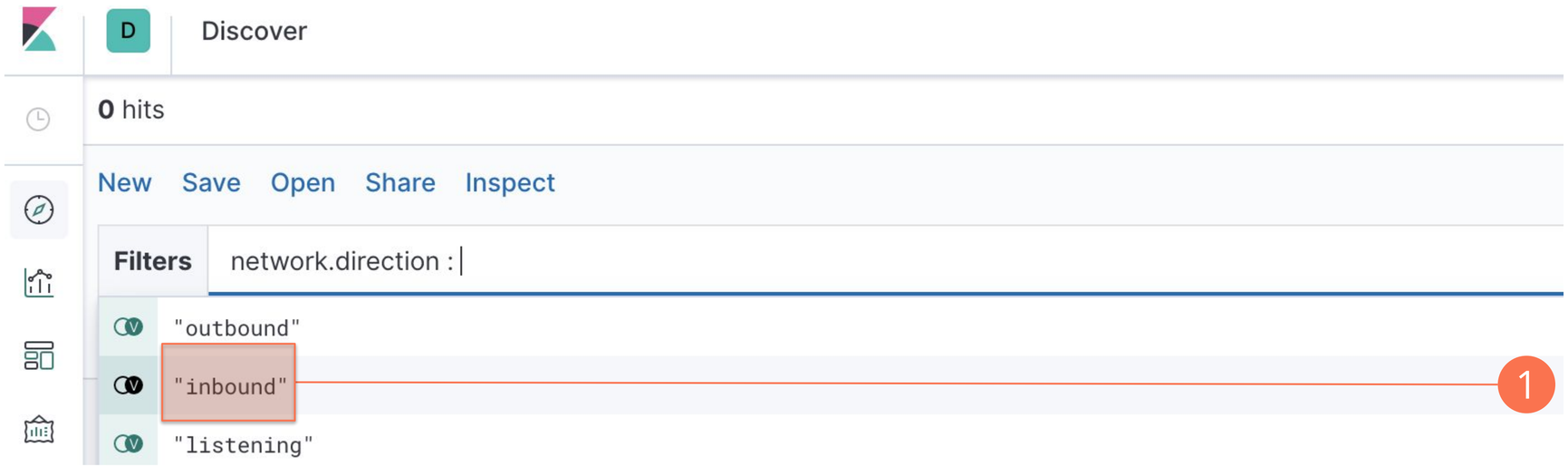


2 Select ‘equals some value’

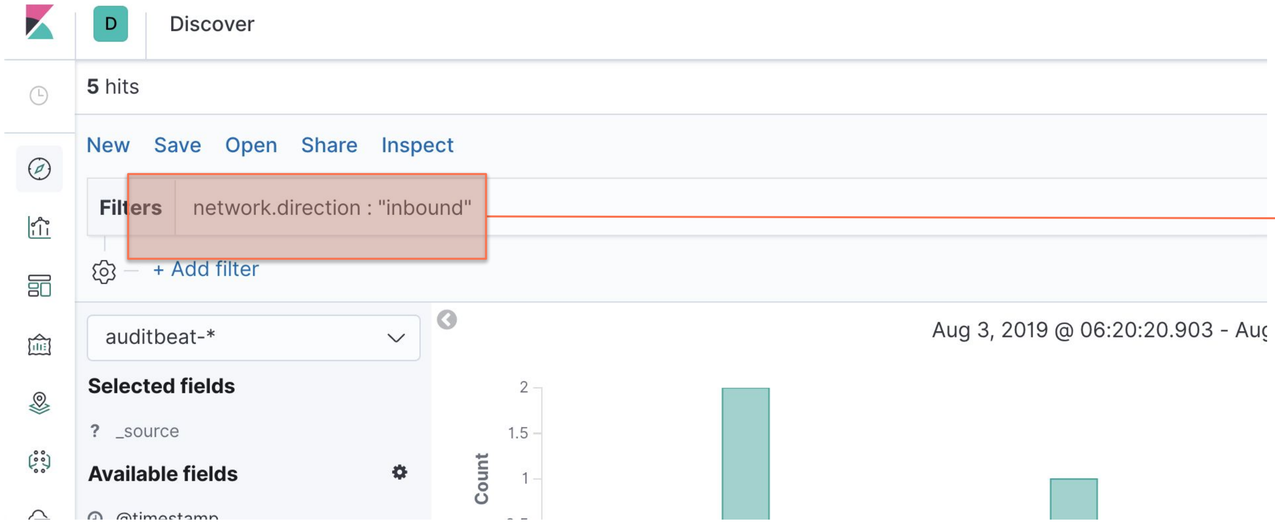
elastic

Search with KQL in Kibana

search with autocomplete



1 Select ‘ inbound’

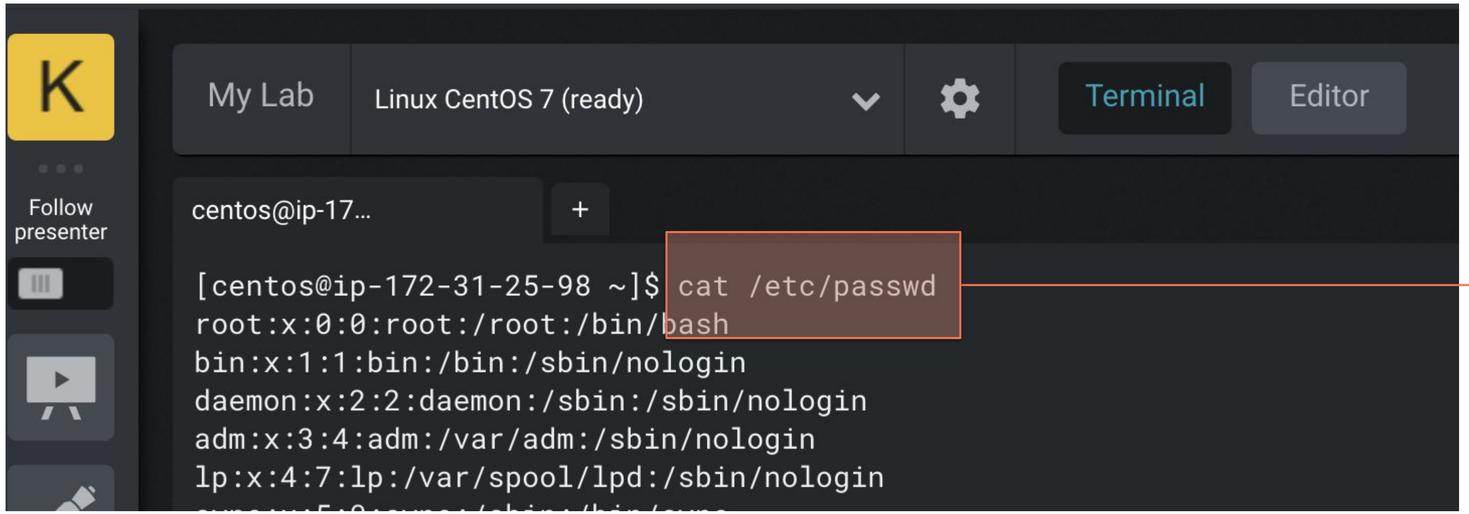


2 Results are filtered for inbound

elastic

ATT&CK Technique T1078 Valid Accounts

in strigo’s Linux lab terminal: cat /etc/passwd

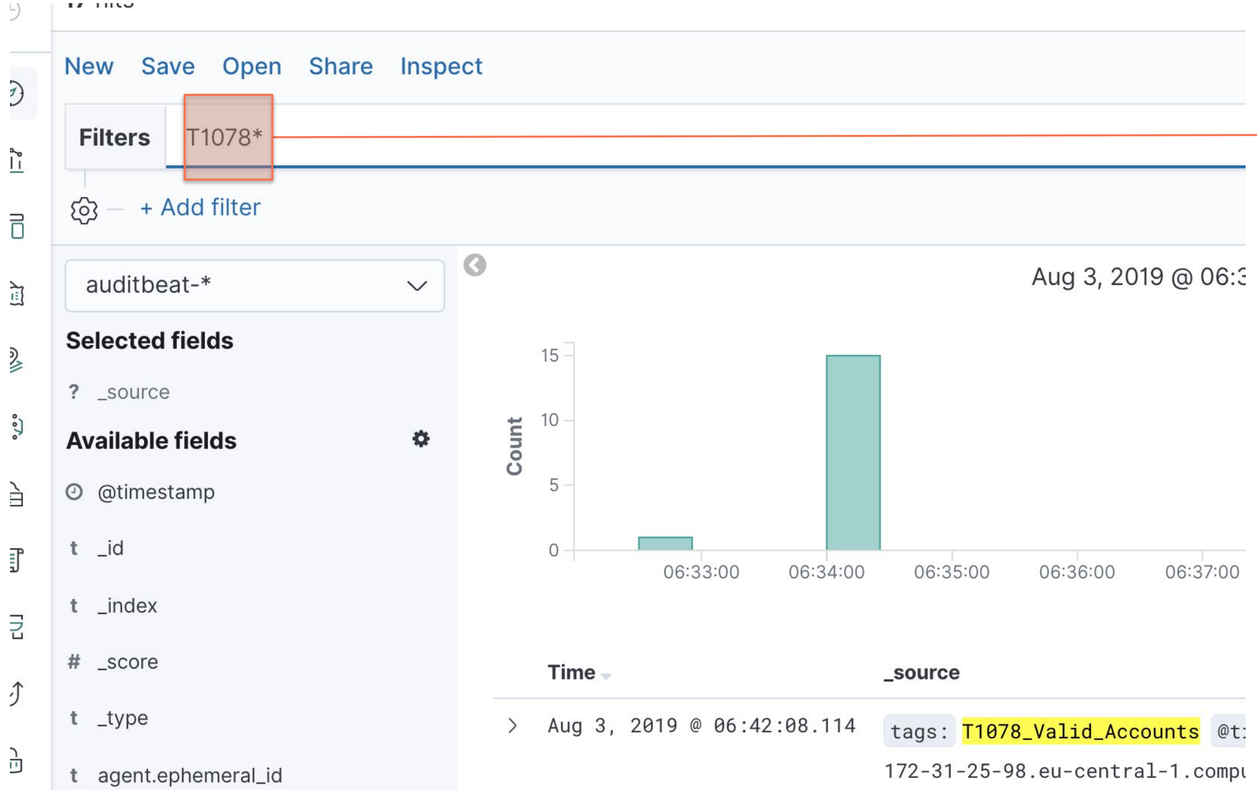


1 Type ‘cat /etc/passwd’ in the terminal

elastic

Find T1078 events

Search using wildcards



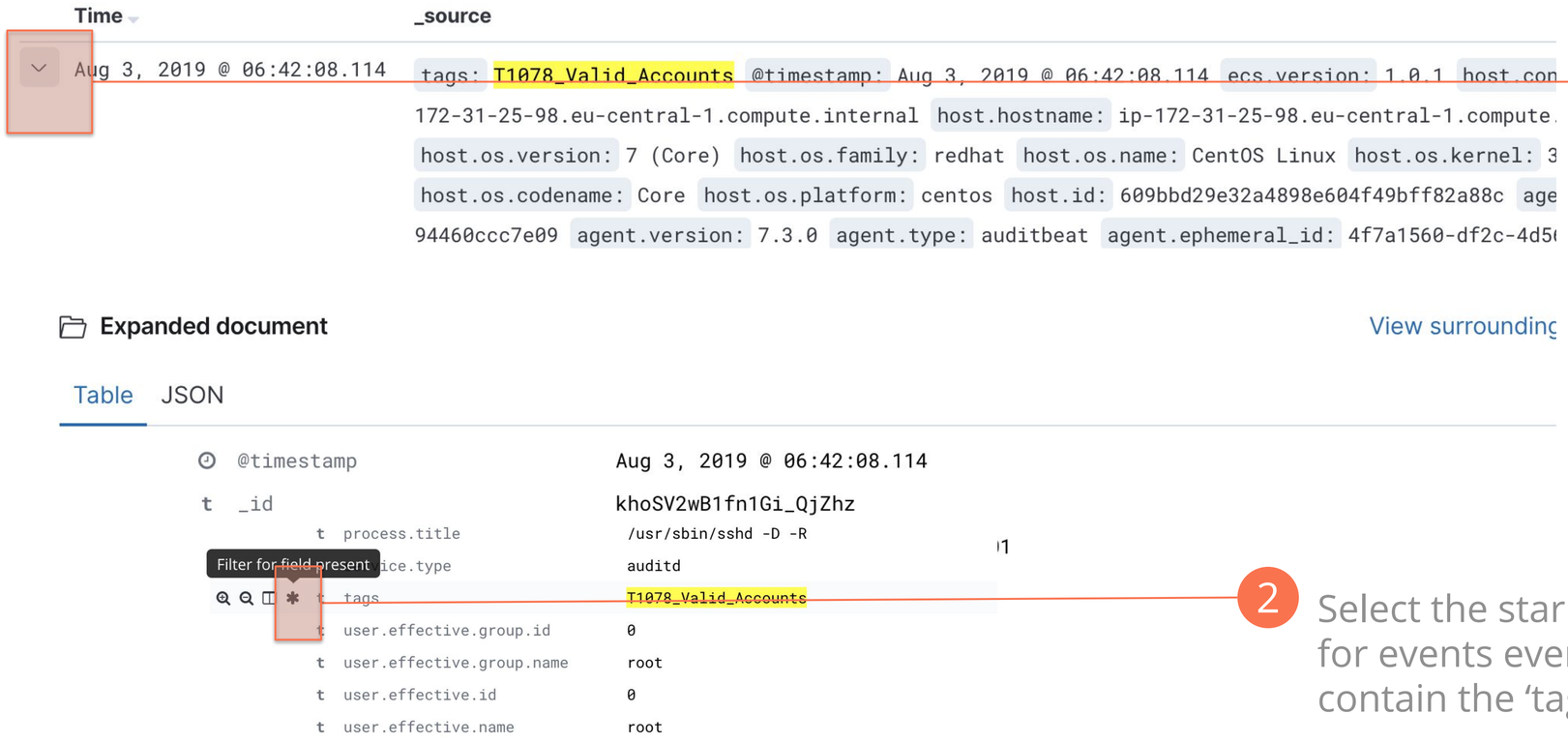
1 Search for ‘T1078’

2 Pro Tip: Avoid using ‘*’ as a prefix without a key (e.g. ‘*1078’)

elastic

Inspect an event

review the fields in an event, filter on ‘contains tag’



1 Select the drop down arrow icon next to a matching event.

2 Select the star icon to filter for events events that contain the ‘tags’ field

elastic

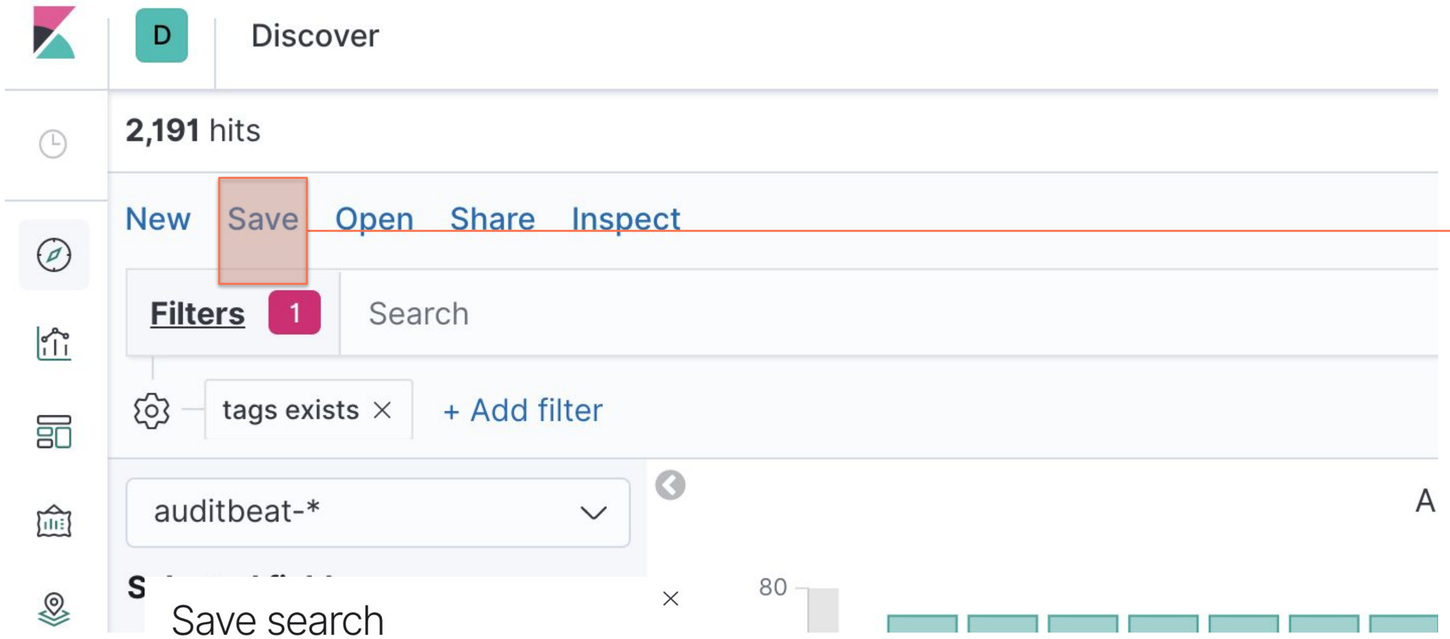
Apply tag exists filter

clear the search box and refresh to see only results that contain ‘tag’

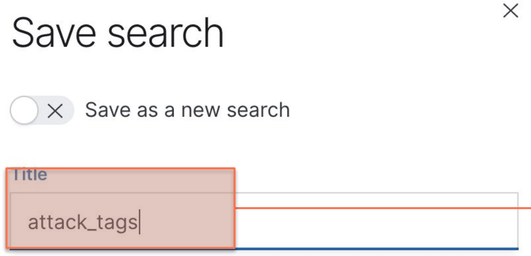
elastic

Create a saved search

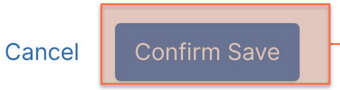
save your tags filter for reuse



1 Select Save



2 Name your saved search ‘attack_tags’

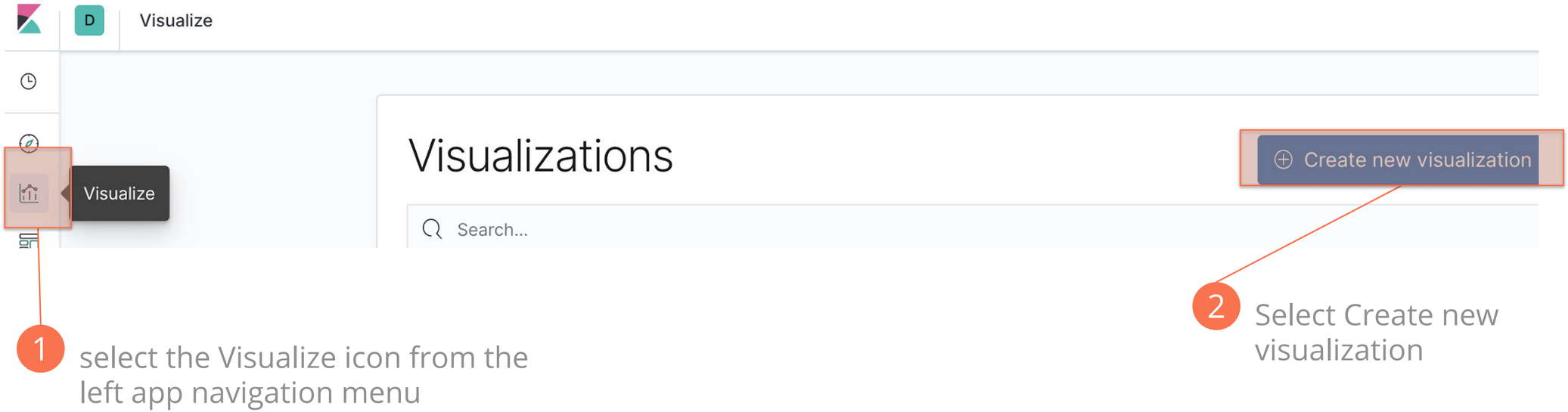


3 Select save

elastic

Start creating a new visualization

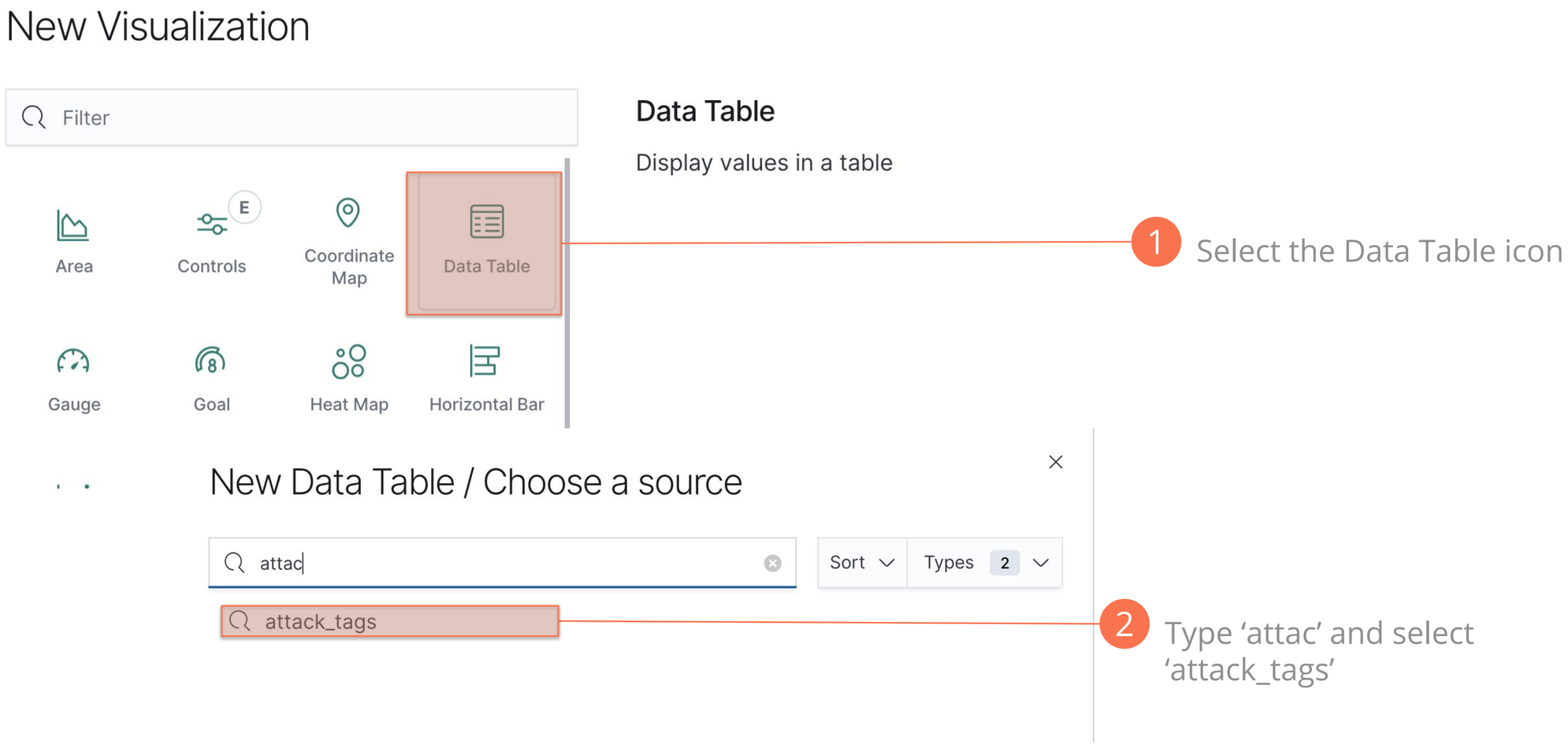
create a new visualization in the Visualize Kibana app



elastic

Create a new data table visualization

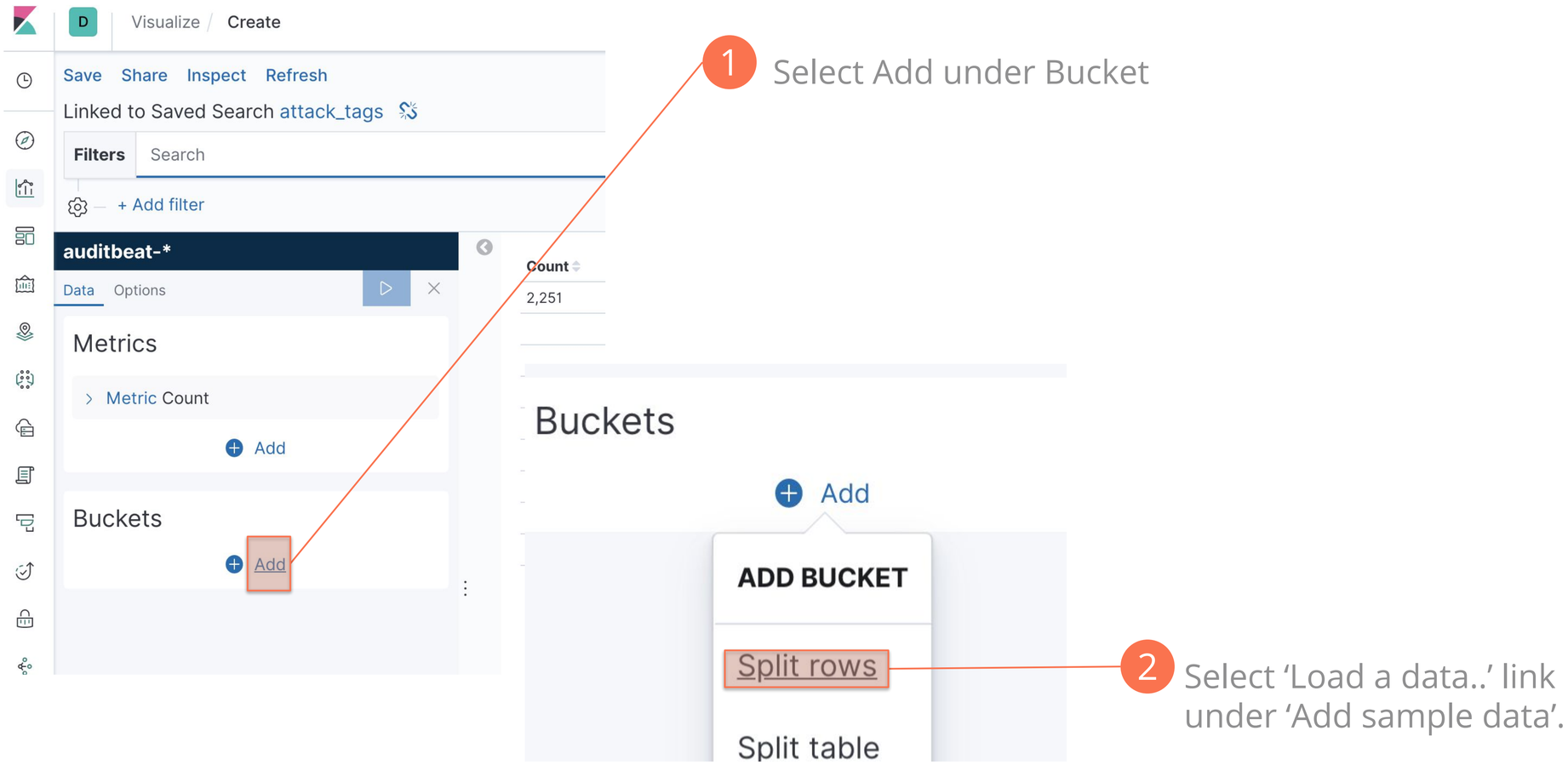
reuse your ‘attack_tags’ saved search



elastic

Editing Data Table

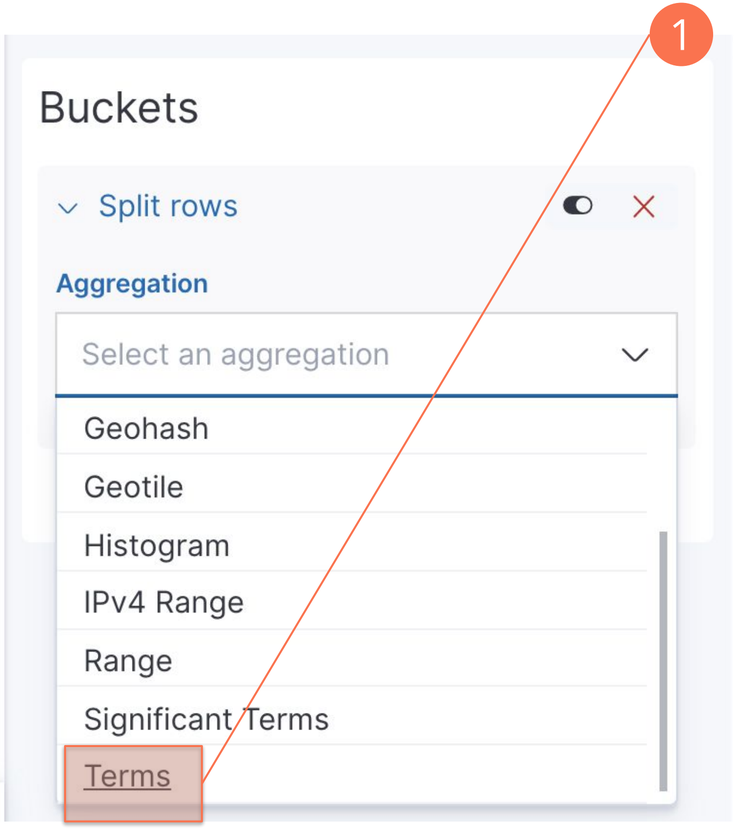
split rows



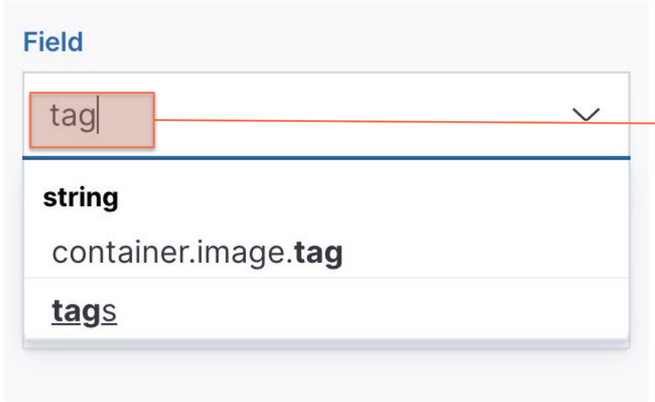
elastic

Editing Data Table

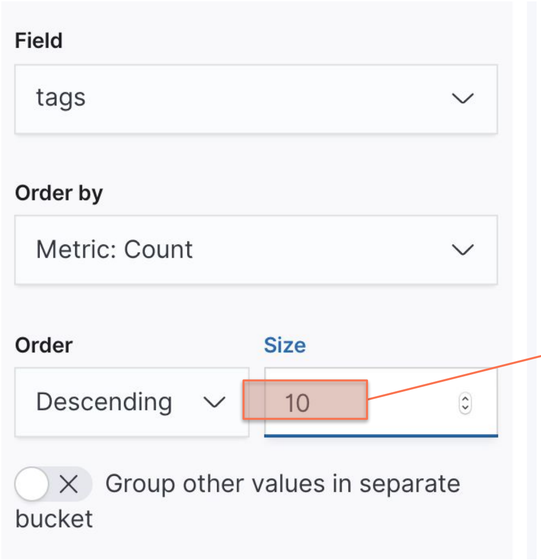
use terms



1 Select the Terms Aggregation



2 Type ‘tags’ and select it for Aggregation Field

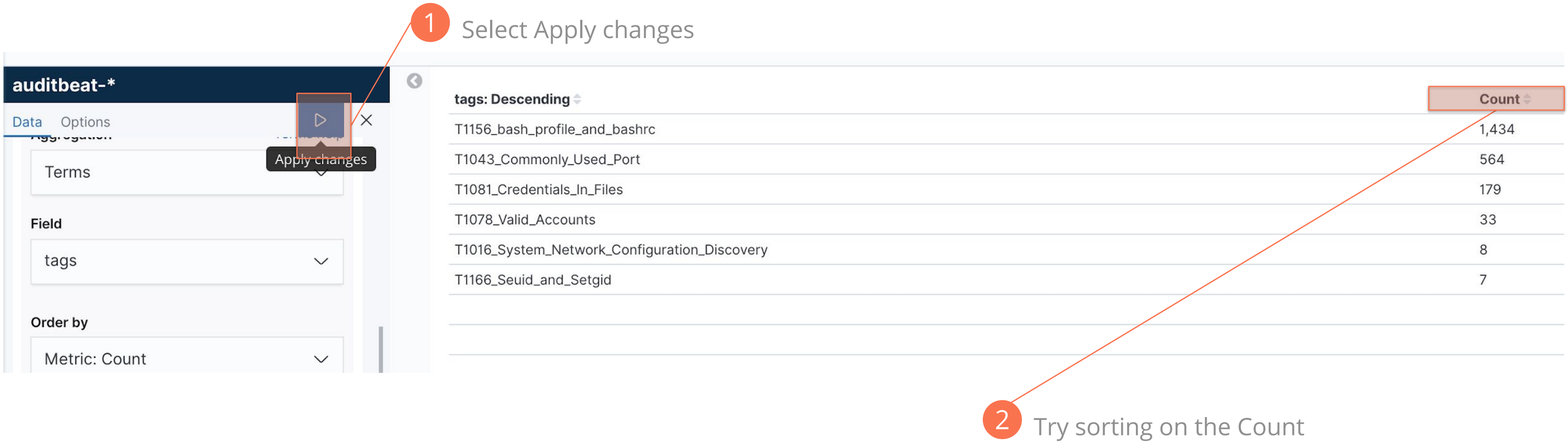


3 Set the display Size to 10

elastic

See your updated data table visualization

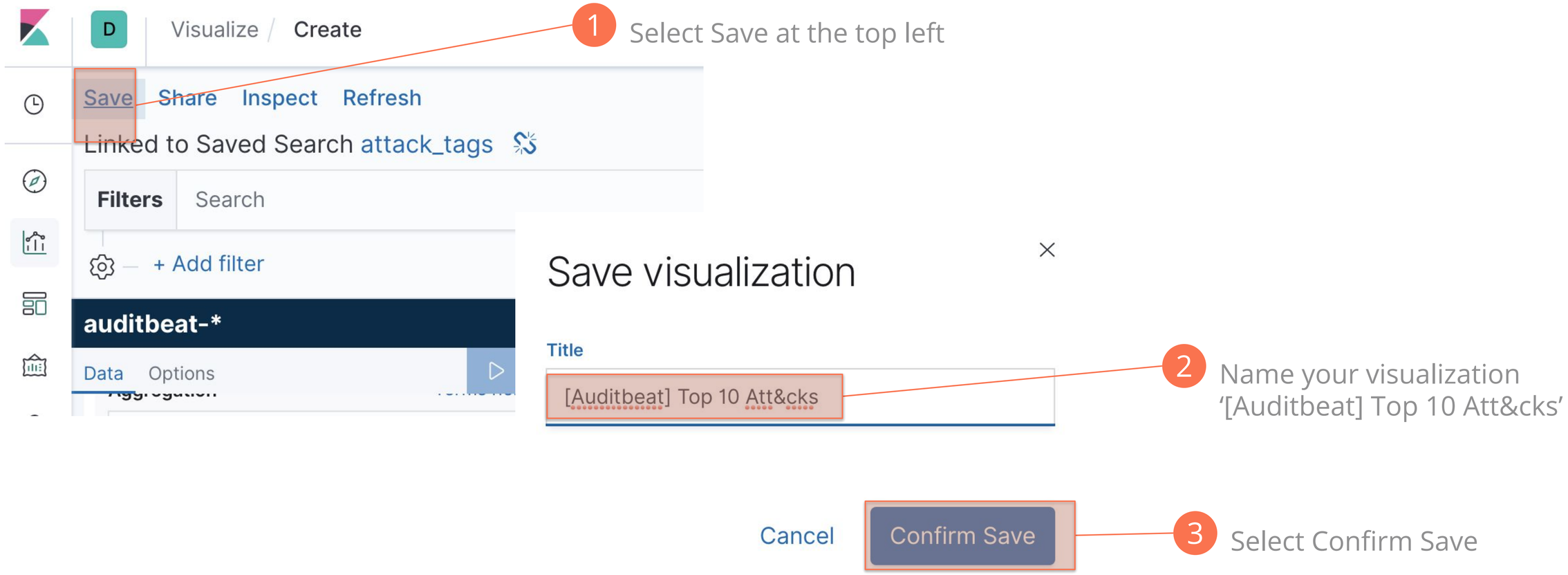
apply you changes



elastic

Save your visualization

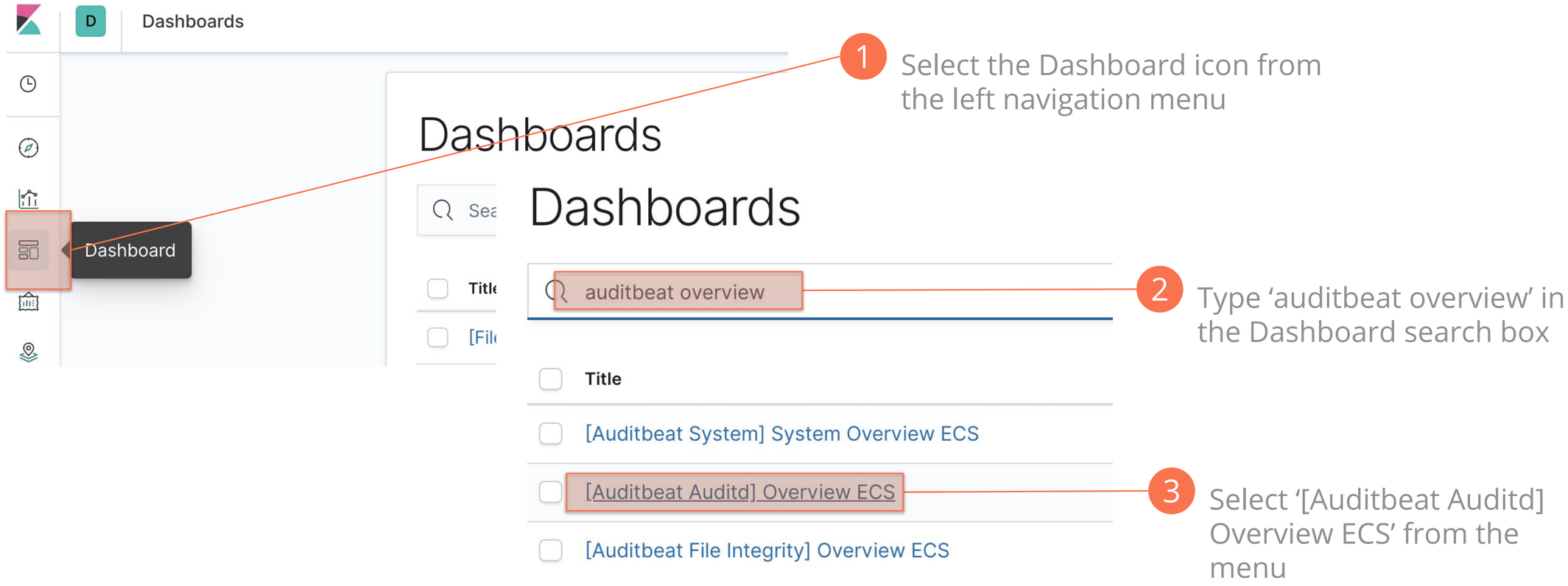
Save your visualization for reuse



elastic

Add visualization to Auditbeat Overview

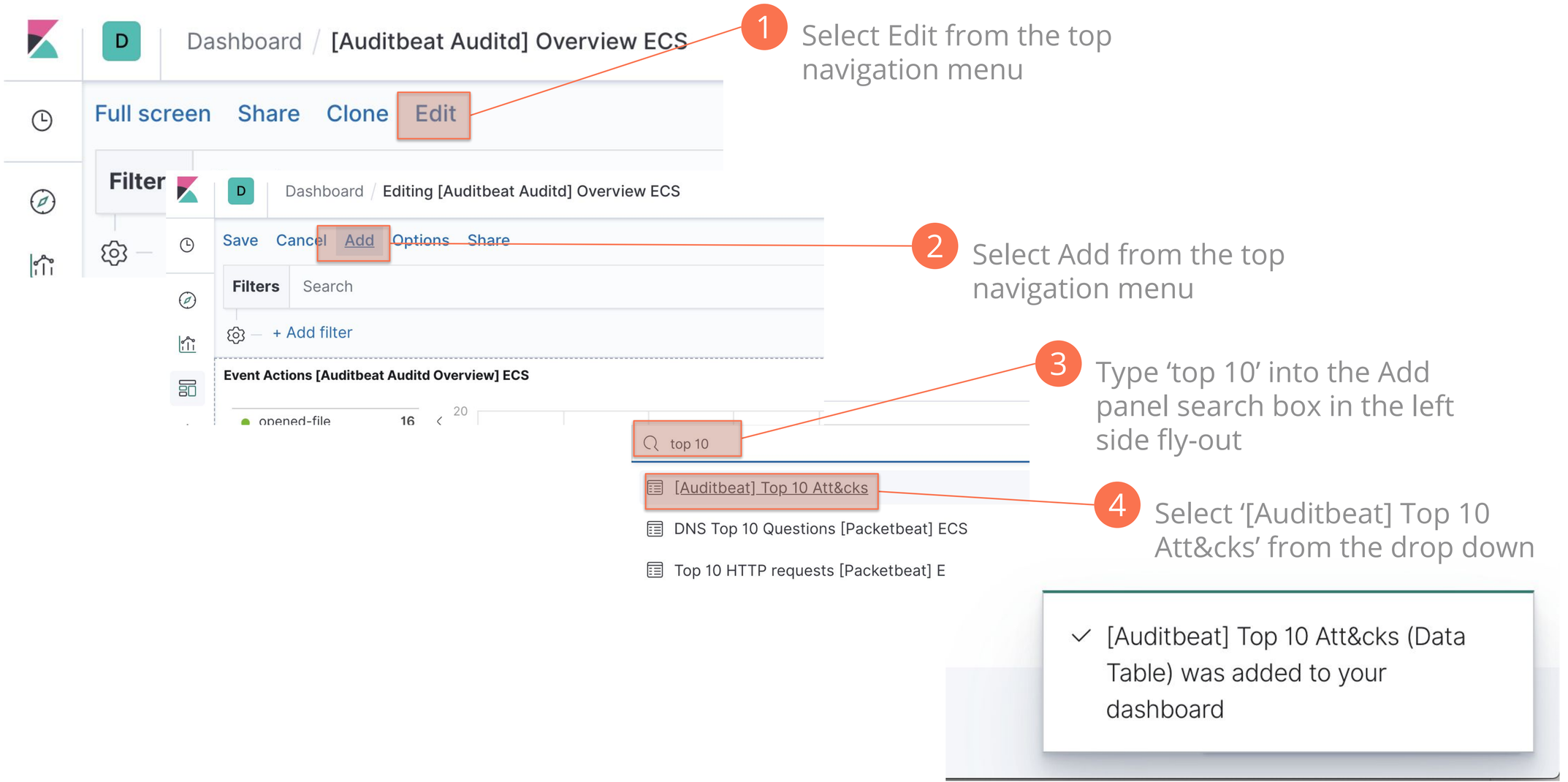
navigate to the '[Auditbeat Auditd] Overview ECS' dashboard



elastic

Add visualization to Auditbeat Overview dashboard

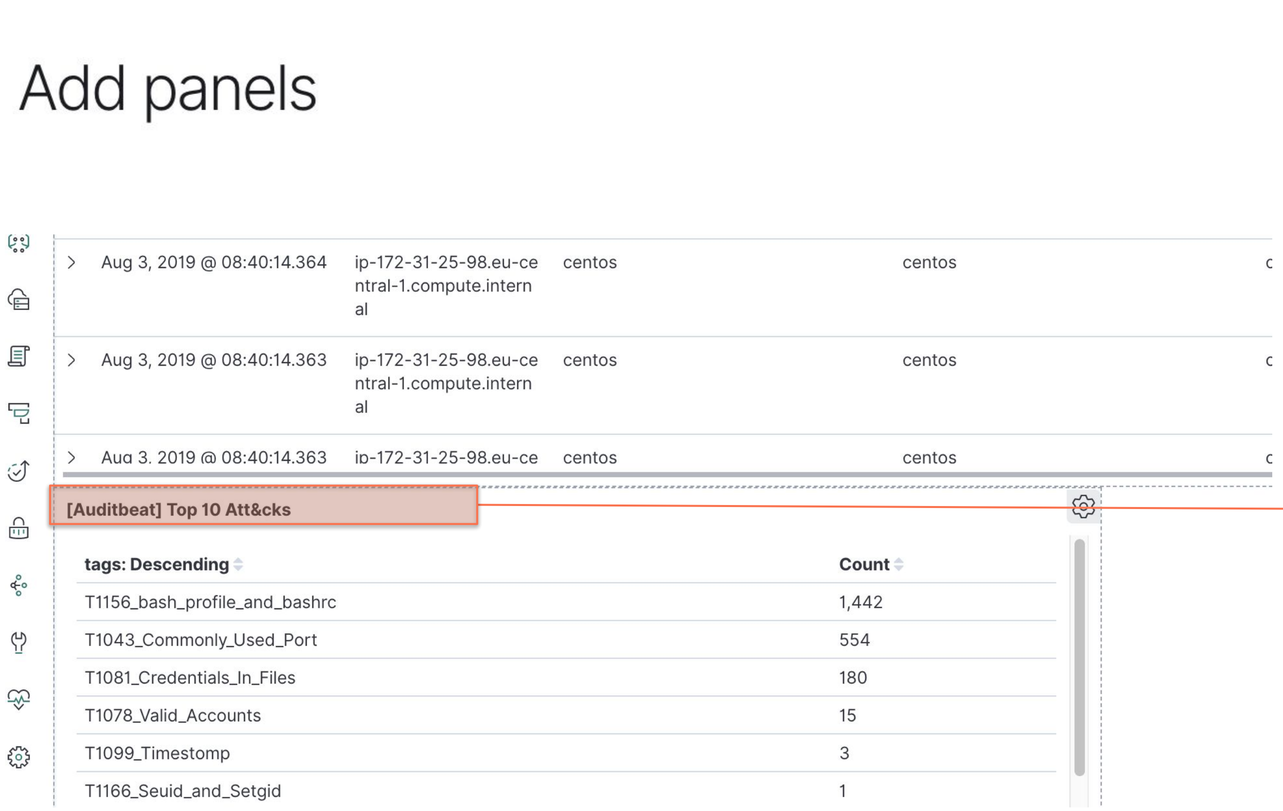
finish adding visualization



elastic

Load Sample Data in Kibana

Kibana load data page



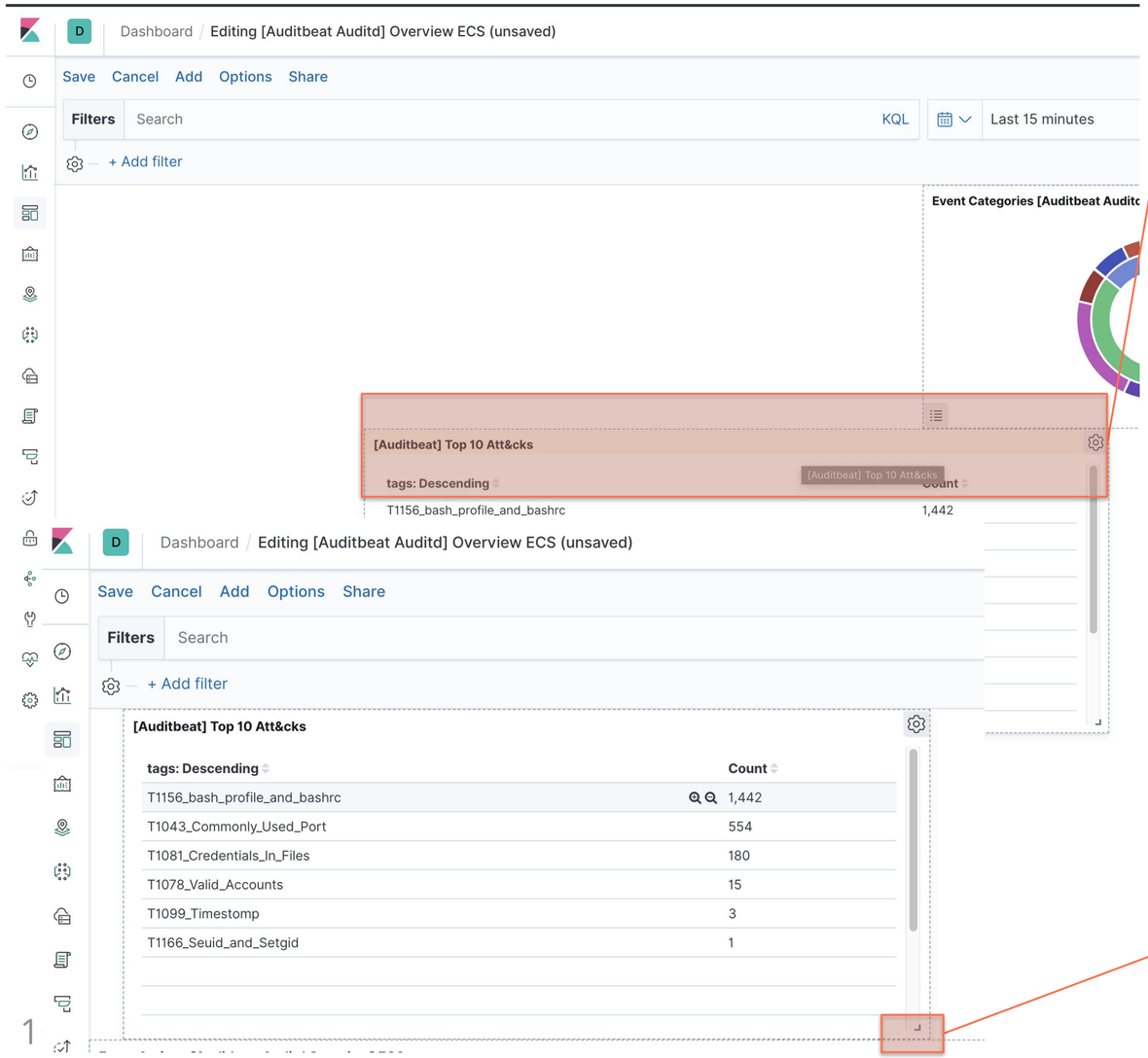
1 Exit the Add Panel fly-out

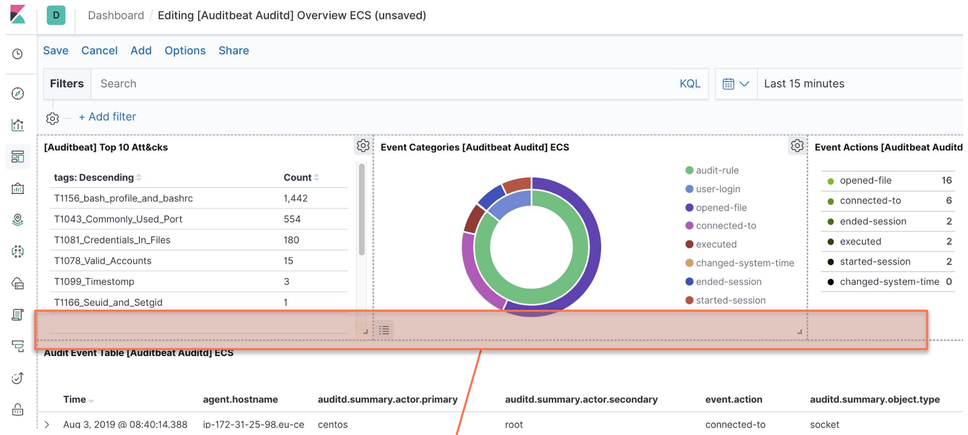
2 Scroll down to the very bottom of the dashboard to find your visualization

Reshaping the dashboard

changing the layout of a dashboard

1 Drag the visualization to the top by dragging while holding the left click button down.



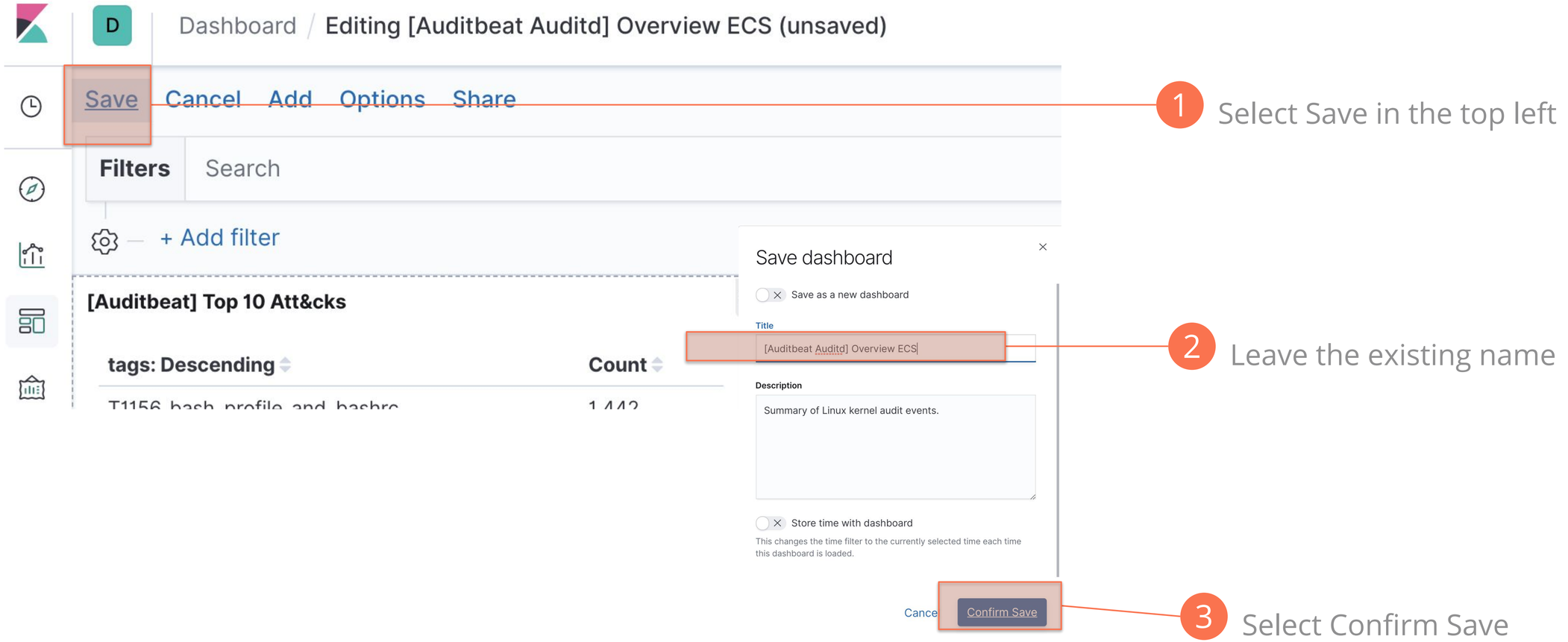


3 Resize other visualizations to better fit the screen

2 Resize the panel using the lower right resize arrow

Save your updated dashboard

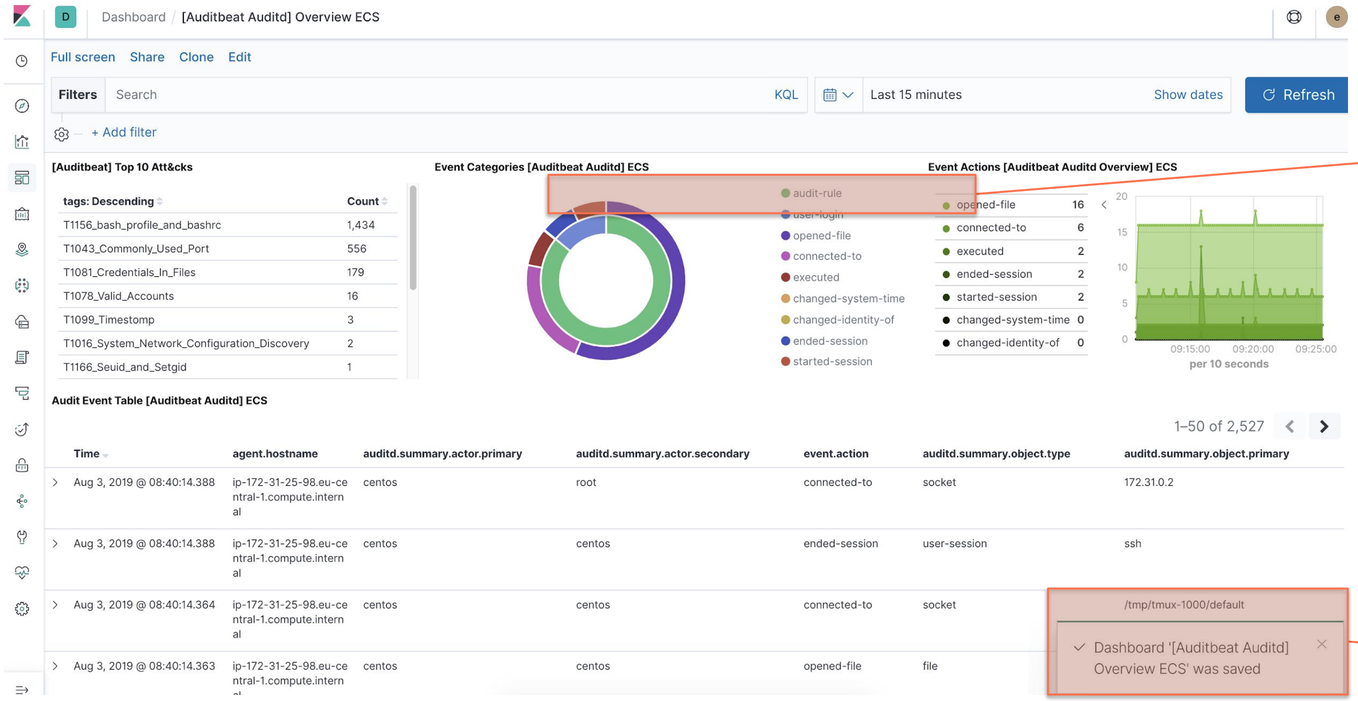
Top 10 attacks added to Auditbeat Overview



elastic

Play time

click around with ‘+’ to filter data instantly

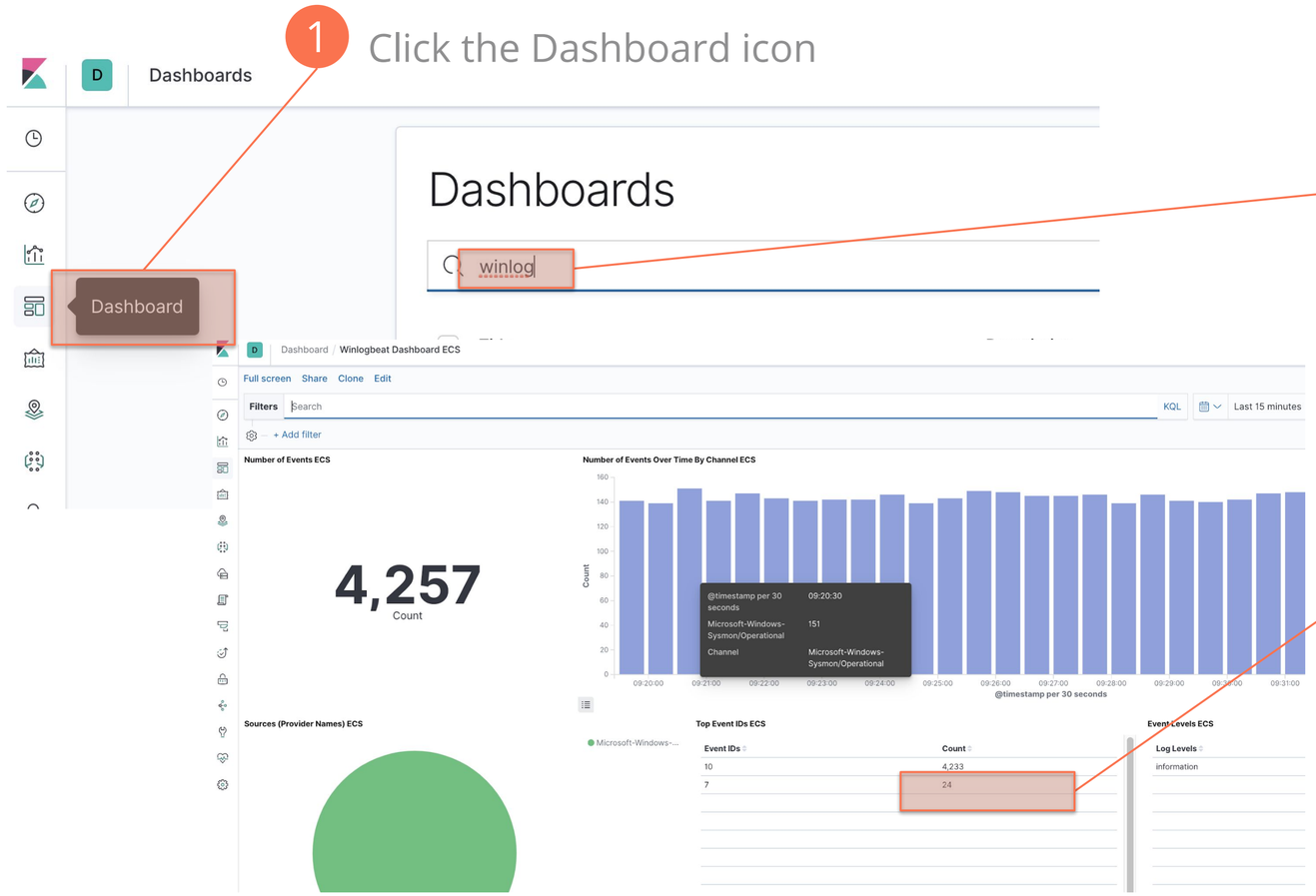


2 Select the ‘+’ icon to create filters automatically

1 A saved tool tip should appear

Other Dashboards

click around with ‘+’ to filter data instantly



elastic

ML Demo

elastic

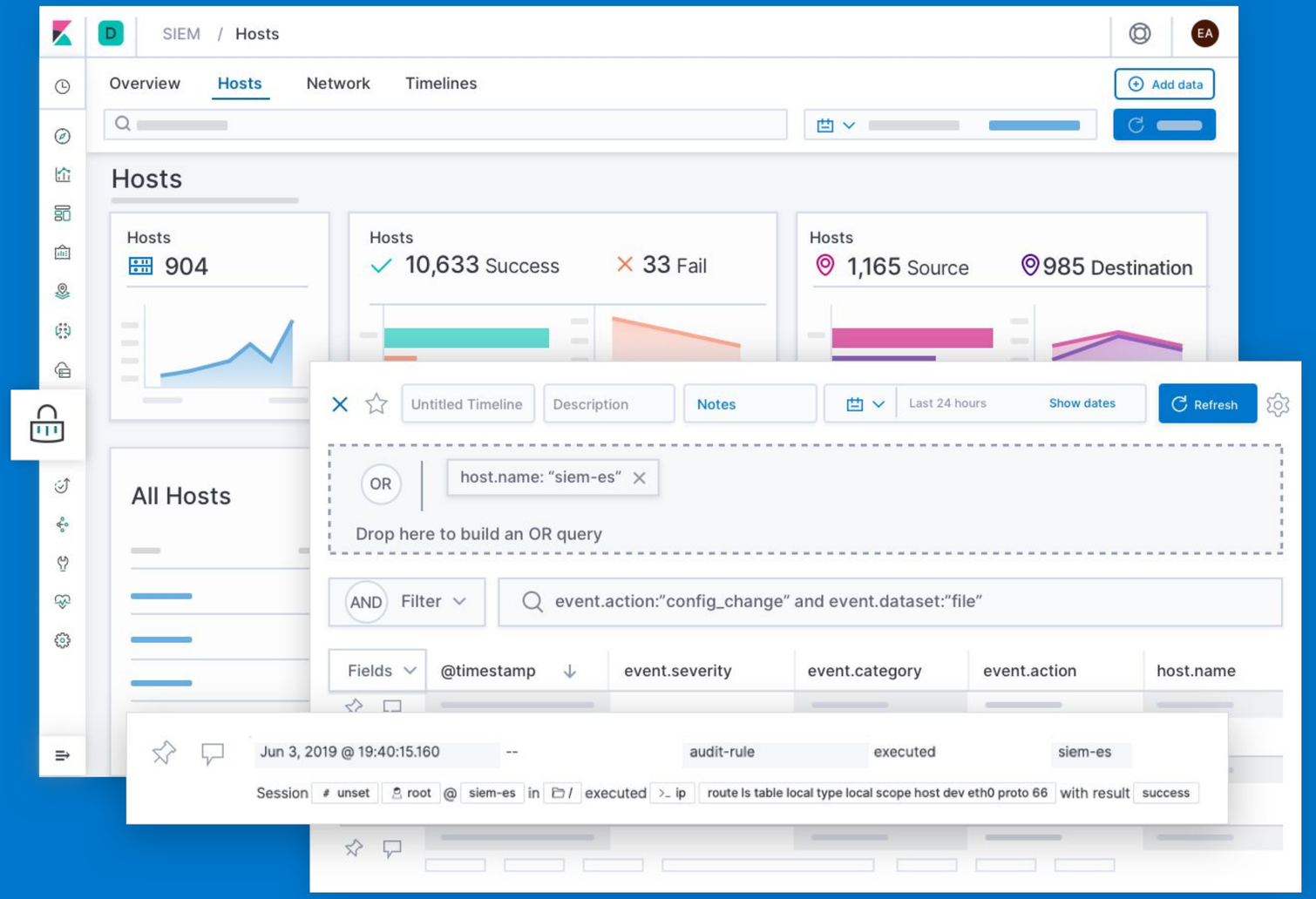
Agenda

2:00 p.m.	Welcome, Check-In, Setup your Elastic Lab Environment
	Lab 1 - Create your Elastic Cloud Environment
2:30 p.m.	Introductions & Opening Remarks
	Elastic Stack Overview
3:00 p.m.	MITRE ATT&CK™ Overview
	Lab 2: Data Ingestion using Beats and MITRE ATT&CK
4:00 p.m.	Threat Hunting leveraging MITRE ATT&CK™ Host-level TTPs
	Lab 3: Finding Host-level TTPs using Kibana
4:30 p.m.	Introducing Elastic SIEM
	Lab 4: Interacting with the Elastic SIEM App
5:00 p.m.	Q&A Session & Group Discussions
5:30 p.m.	Workshop Concludes

elastic

Introducing

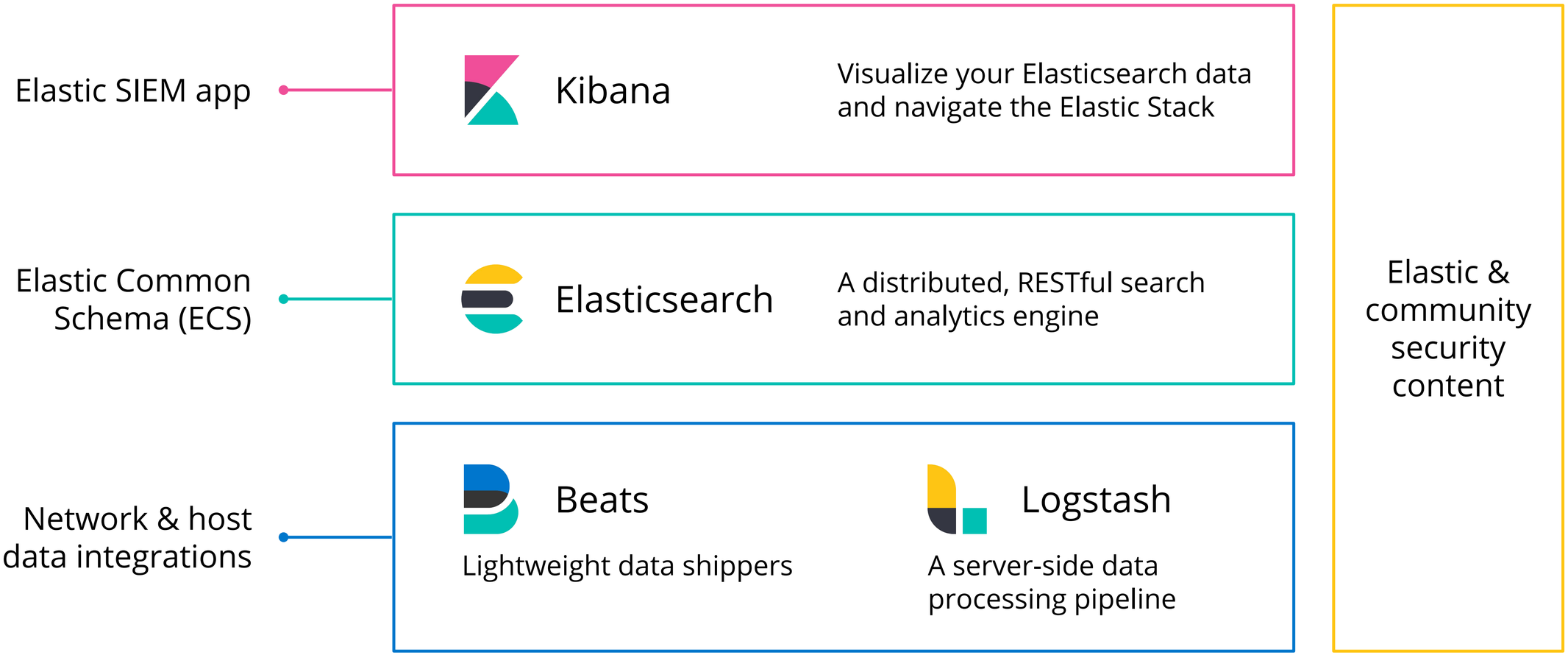
Elastic SIEM



SIEM App Targets SOC Analysts, Investigators

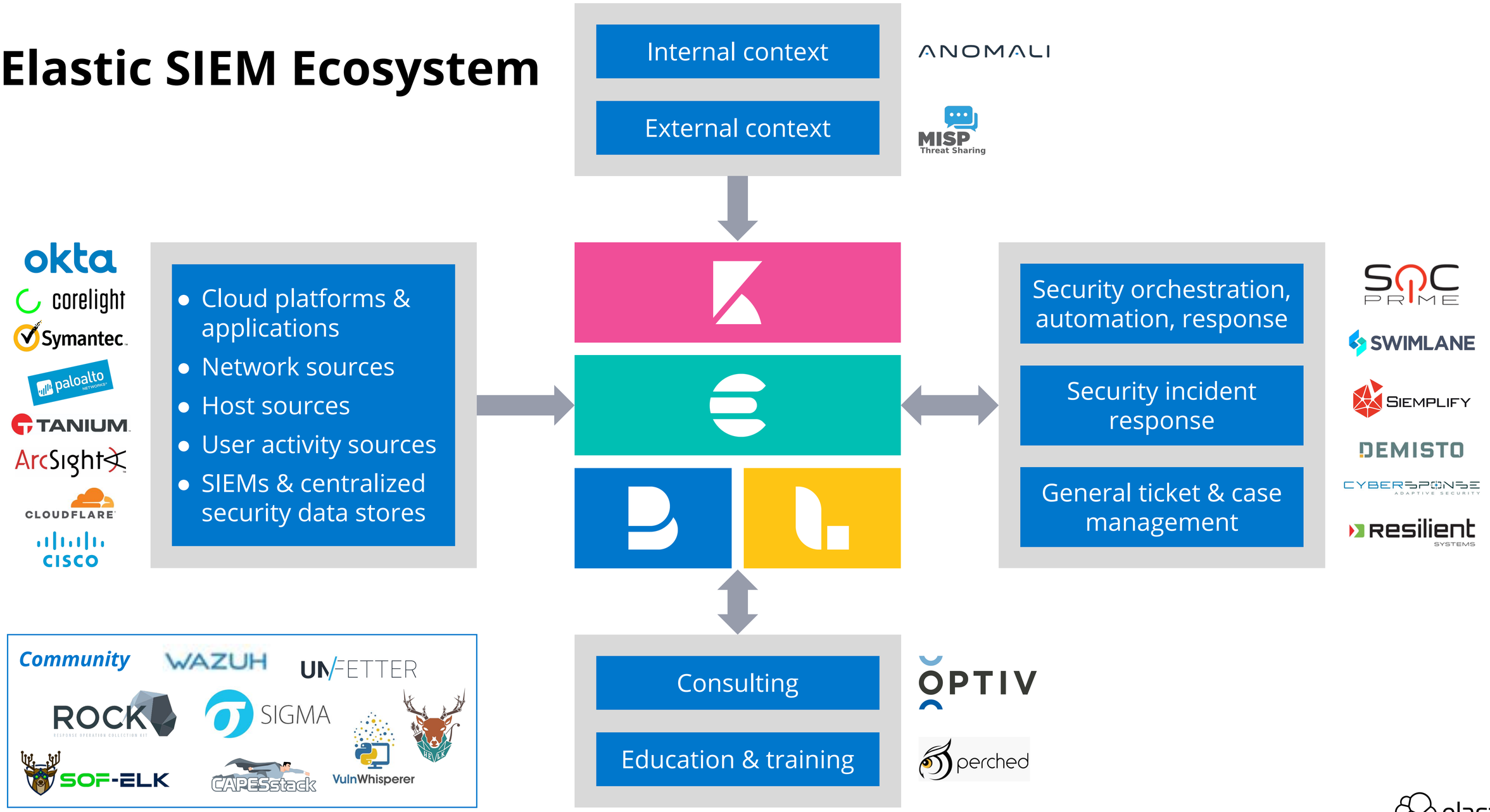
Elastic SIEM

A SIEM for Elastic Stack users everywhere



elastic

Elastic SIEM Ecosystem



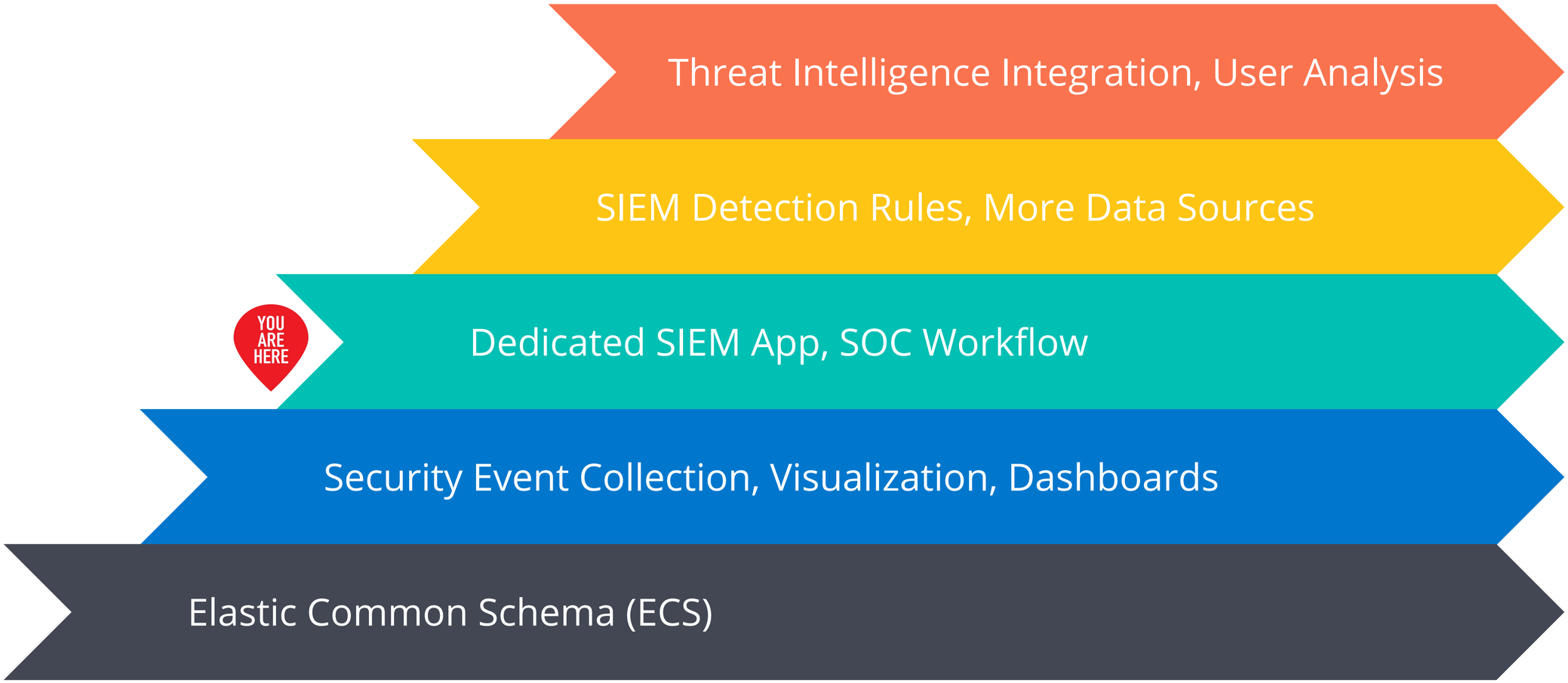
elastic

Elastic SIEM

Roadmap

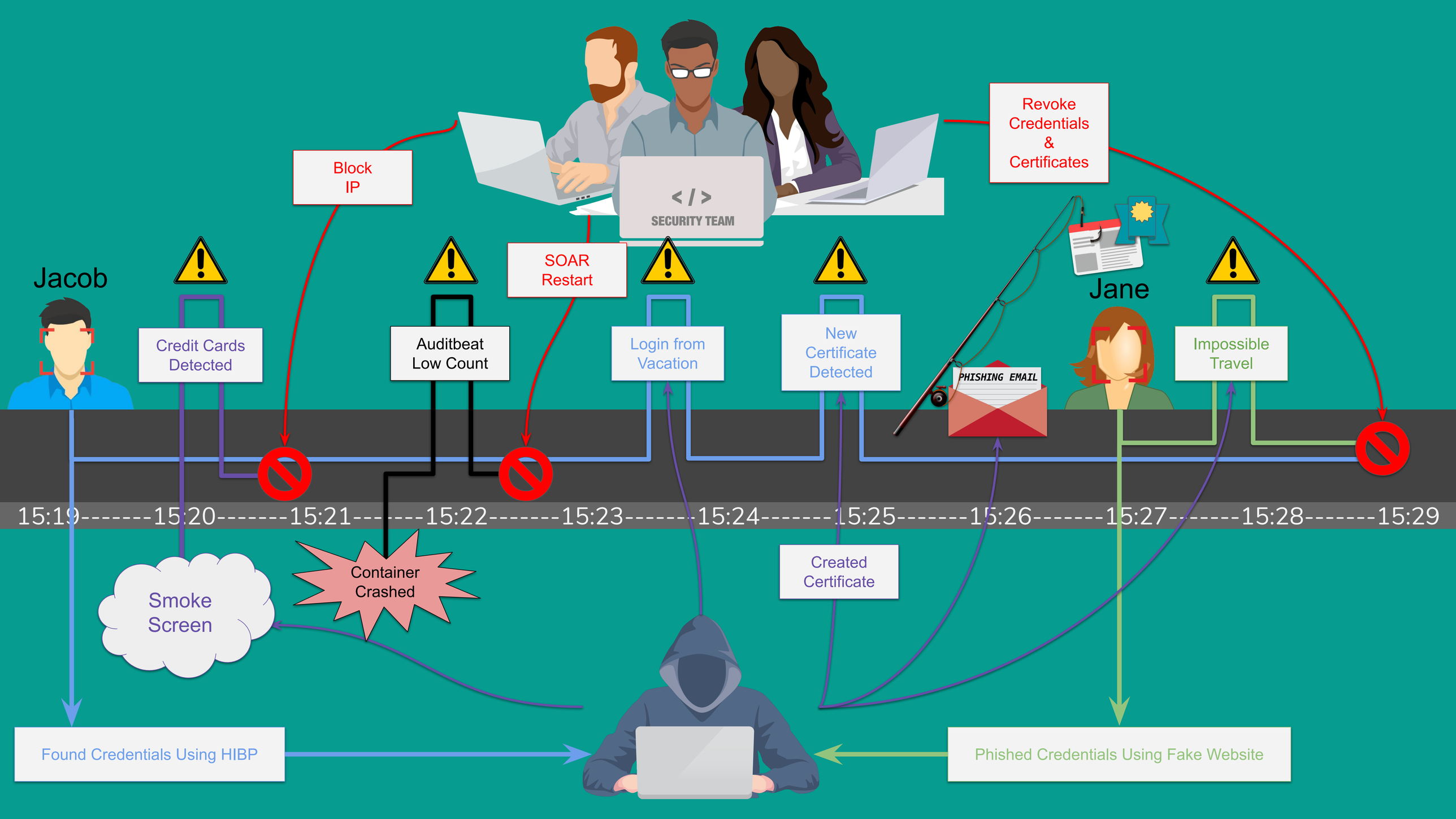
elastic

Elastic Security Analytics Journey



Security Analytics Demo

elastic


Block IP
SECURITY TEAM
Revoke Credentials & Certificates
SOAR Restart
Jacob
Jane
Credit Cards Detected
Auditbeat Low Count
Login from Vacation
New Certificate Detected
PHISHING EMAIL
Impossible Travel
15:19------15:20------15:21------15:22------15:23------15:24------15:25------15:26------15:27------15:28------15:29
Smoke Screen
Container Crashed
Created Certificate
Found Credentials Using HIBP
Phished Credentials Using Fake Website

Lab 4

Interacting with the Elastic SIEM App

elastic

Try it @ home

Elastic Cloud Trial
Available
for 2 Weeks

https://github.com/mrebeschini/2019BSidesLV

elastic

www.elastic.co