



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>



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



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



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.

Agenda

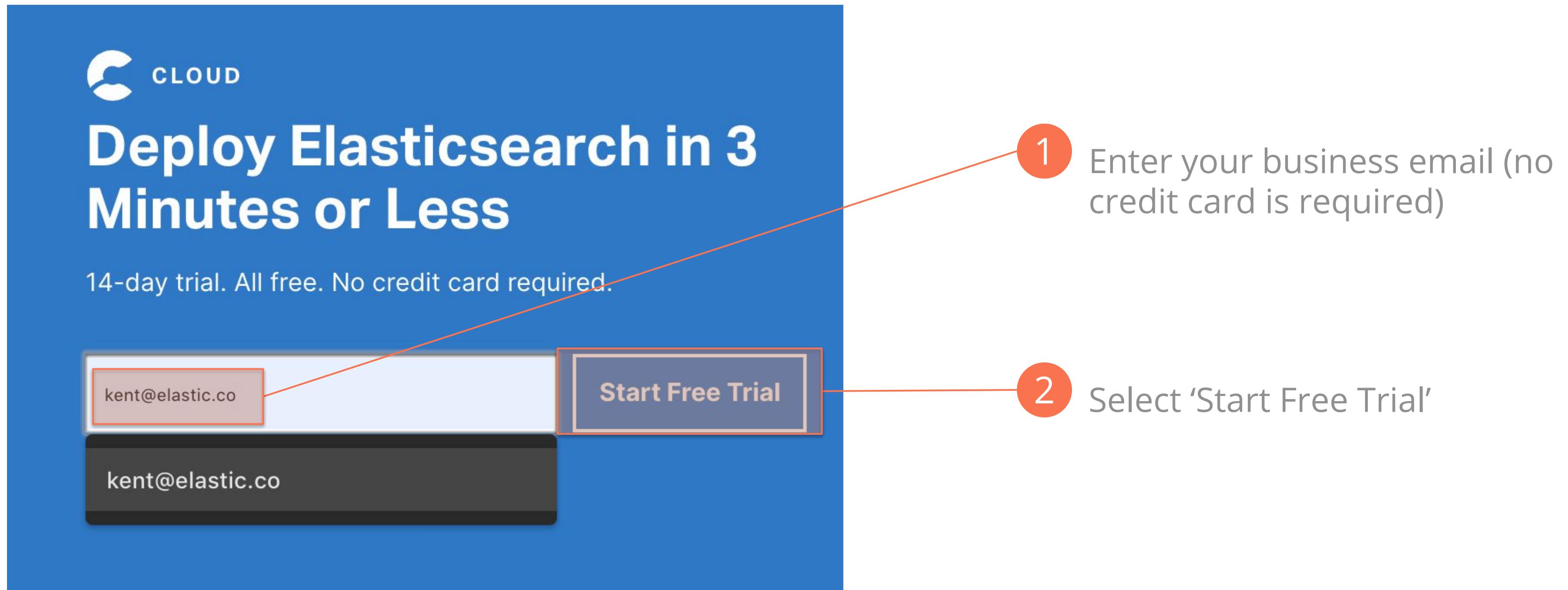
- 2:00 p.m. Welcome, Check-In, Setup your Elastic Lab Environment
Lab 1 - Create your Elastic Cloud Environment
- 2:30 p.m. Introductions & Opening Remarks
Elastic Stack Overview
- 3:00 p.m. MITRE ATT&CK™ Overview
Lab 2: Data Ingestion using Beats and MITRE ATT&CK
- 4:00 p.m. Threat Hunting leveraging 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

Lab 1

Elastic Cloud Setup

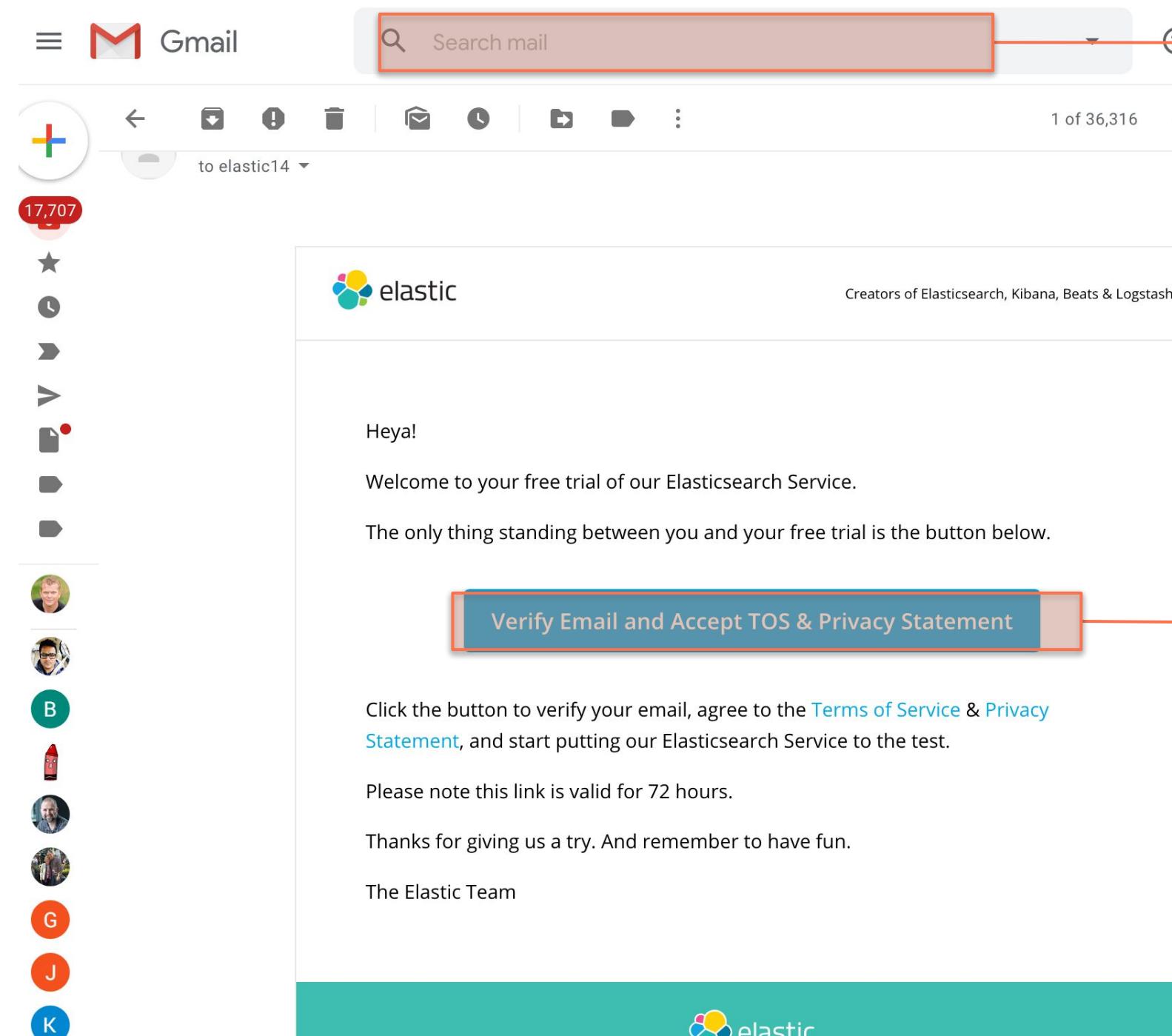
Sign up for the Elastic Cloud Trial

Go to <https://cloud.elastic.co>



Cloud account validation

Login to your business email

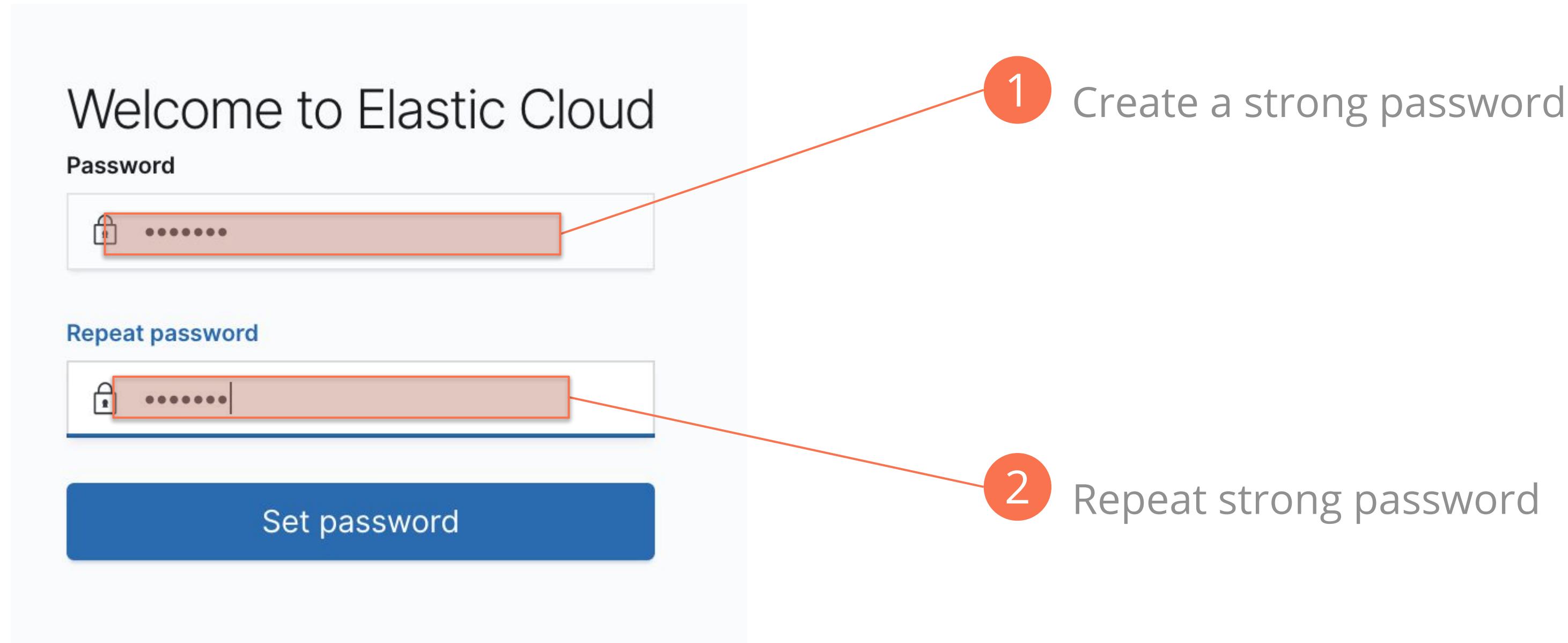


1 Find message with the Subject:
**'[Action Required] It Worked!
Your Elasticsearch Service
Trial Awaits.'**

2 Select the 'Verify Email...' link

Set password

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



Create new trial cluster

Kibana has multiple indices, select auditbeat

Welcome to your 14-day trial!

Enjoy your free deployment with the latest Elasticsearch and Kibana versions, security features, machine learning, and much more. It's all on us. If you enjoy Elastic Cloud, add a credit card to keep going for as long as you like.

Deployments



Create your first deployment

Deployments help you manage the Elasticsearch cluster and other Elastic products, like a Kibana or APM instance, in one place.

Spin up, scale, upgrade, and delete all from a deployment

Create deployment

1 Select 'Create deployment'

Create deployment

1 Name your deployment

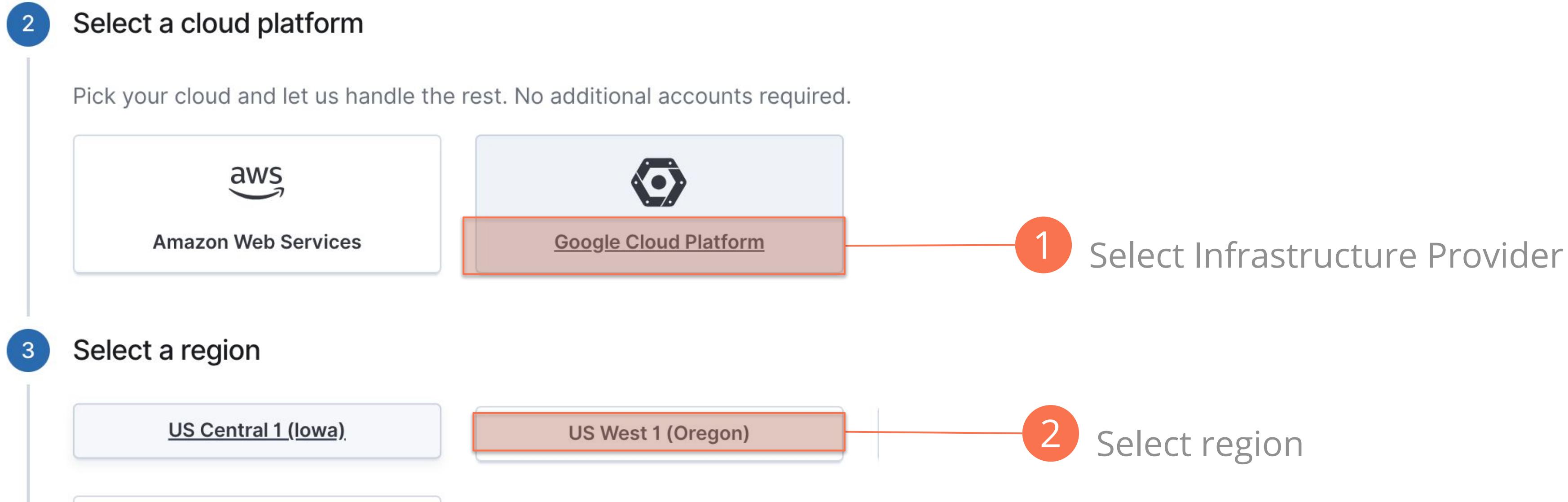
Give your deployment a name

workshop

2 Name the deployment 'workshop'

Deployment options

GCP in the US West region



Deployment options

Set deployment type and version

The screenshot shows the deployment setup interface with two main sections:

- Step 4: Set up your deployment**
 - Elastic Stack version:** 7.3.0 (highlighted with a red box)
 - Select a deployment to restore from its latest snapshot
 - Monitoring:**
 - Enable monitoring by shipping metrics to a deployment
- Step 5: Optimize your deployment**
 - I/O Optimized** (Recommended)
 - Use for search and general all-purpose workloads.
 - Includes a balance of compute, memory, and storage.
 - Default specs
 - Cloud icons: AWS, Azure, GCP, IBM
 - Compute**
 - Run CPU-intensive or run smart workloads
 - Cost-effective
 - Need less storage
 - Default specs
 - Cloud icon: AWS
- Deployment pricing**

Free! As part of your 14-day trial, you can try it out without card details or contact sales@elastic.co.

Three numbered callouts point to specific elements:

- 1 The version of the Elastic Stack to be deployed
- 2 Select 'I/O Optimized'
- 3 Select 'Customize Deployment'

Buttons at the bottom:

- Create deployment
- Customize deployment (highlighted with a red box)

Create deployment

Enable Machine Learning

The screenshot shows the Elasticsearch Machine Learning configuration interface. It includes a sidebar with a 'Machine Learning' icon and '1 configuration'. The main area displays a 'gcp.ml.1' instance with a 'Machine Learning' tab selected. The instance is described as 'An Elasticsearch machine learning instance.' A red box highlights the 'Enable' button. The 'Architecture' section shows 'Zone 1' with four nodes (yellow, pink, teal, red) and 'Zone 2' with one yellow node. A red box highlights the list of components: gcp.data.highio.1 (data), gcp.kibana.1 (kibana), gcp.ml.1 (ml), and gcp.apm.1 (apm). A red box also highlights the 'Create deployment' button at the bottom right.

- 1 Select 'Enable' in the Machine Learning configuration
- 2 Review 'Architecture summary'
- 3 Select 'Create deployment'

Cluster password

Save the password

workshop

Activity



Your deployment is being created

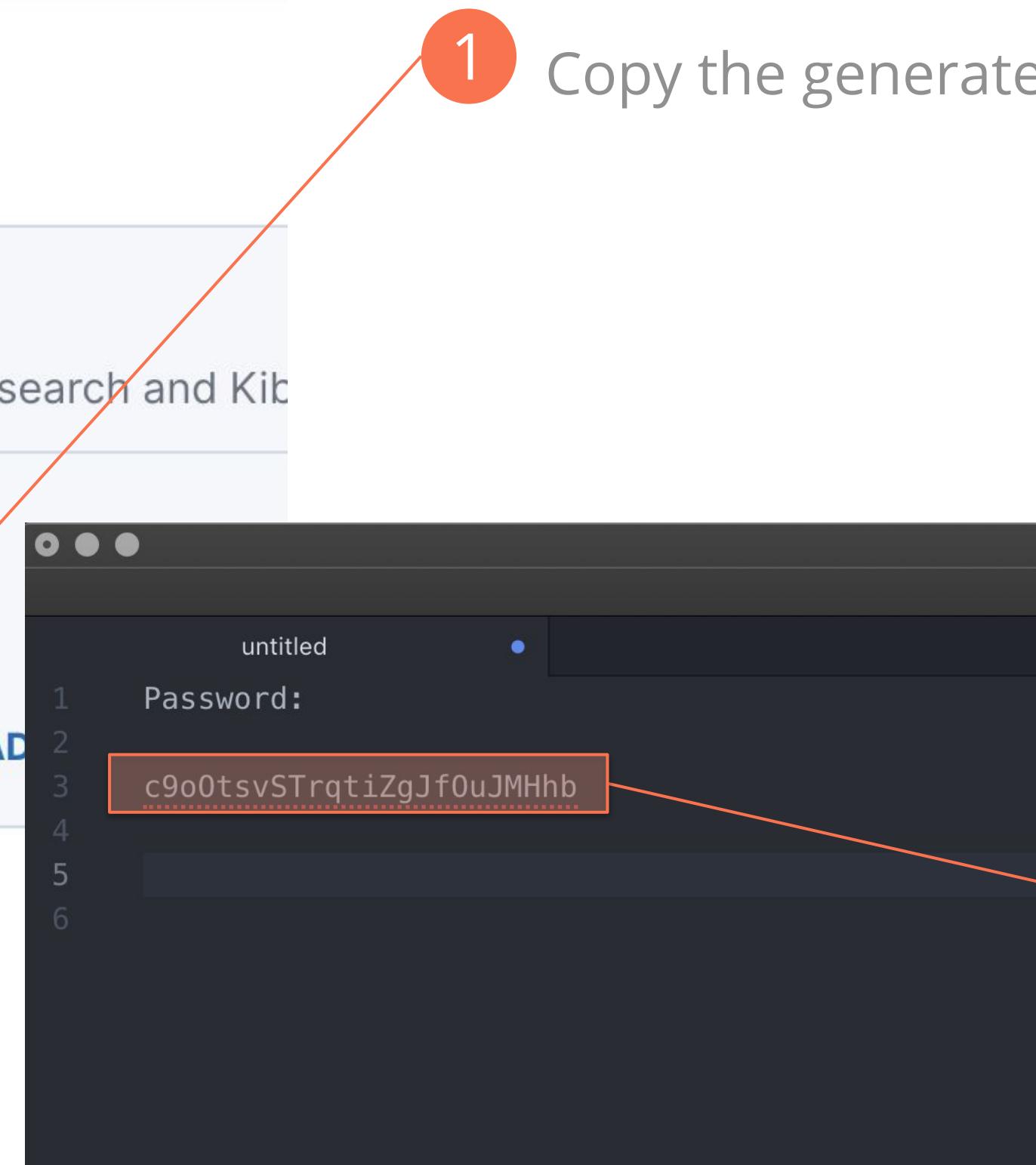
Estimated time is 3 minutes

Save your Elasticsearch and Kibana password

These credentials provide superuser access to Elasticsearch and Kib

Username	elastic
Password	c9o0tsvSTrqtizgJf0uJMhb

COPY **DOWNLOAD**



1

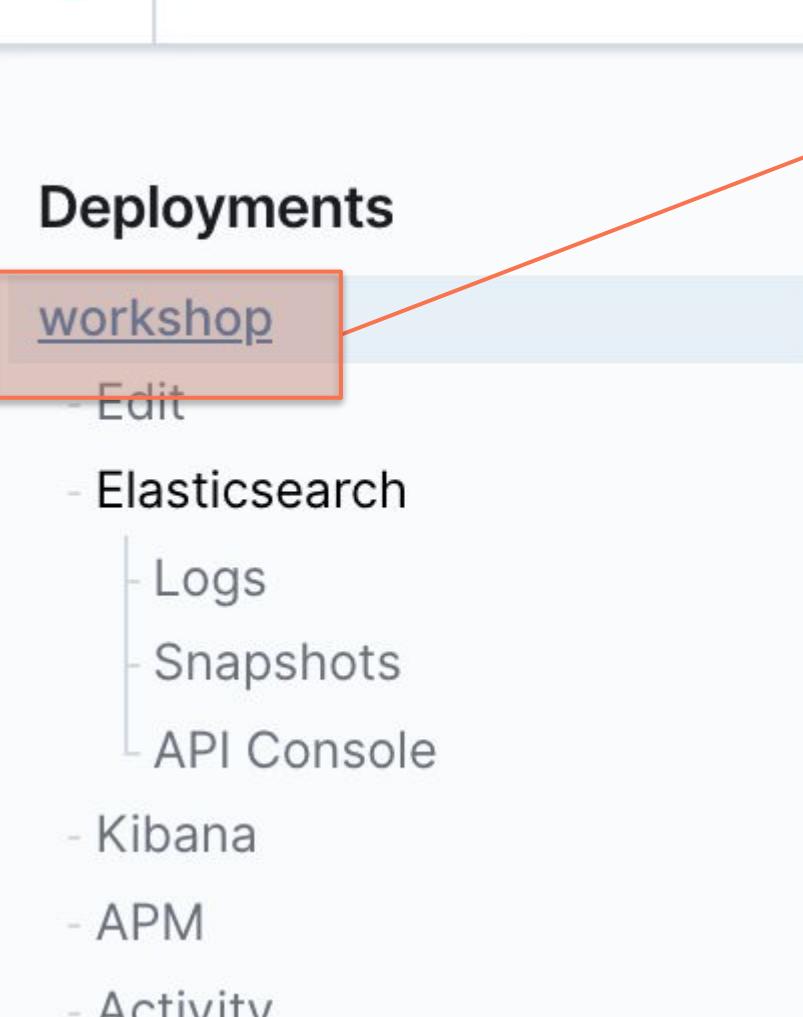
Copy the generated password

2

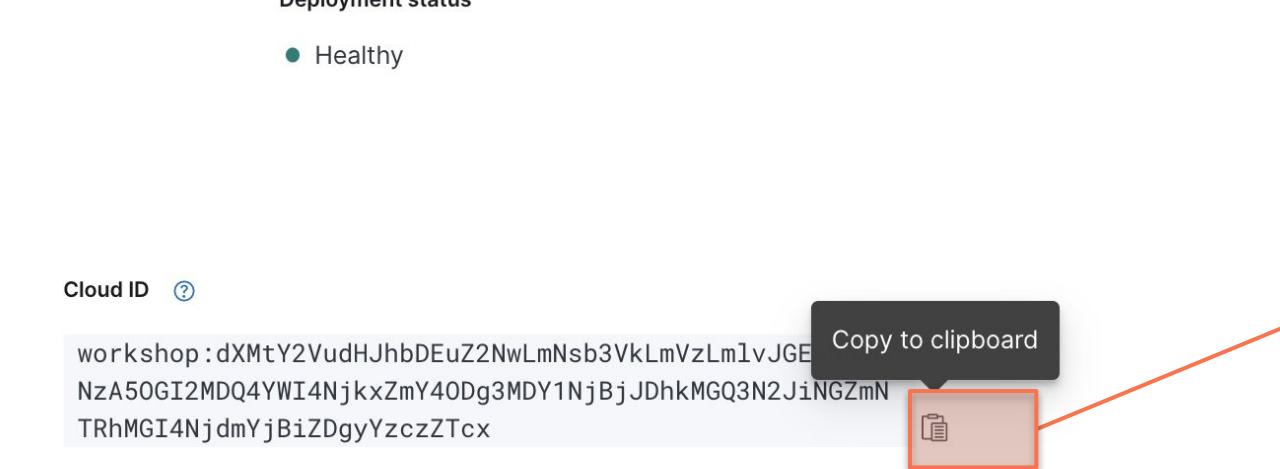
Paste the password in a local text editor

Cloud ID

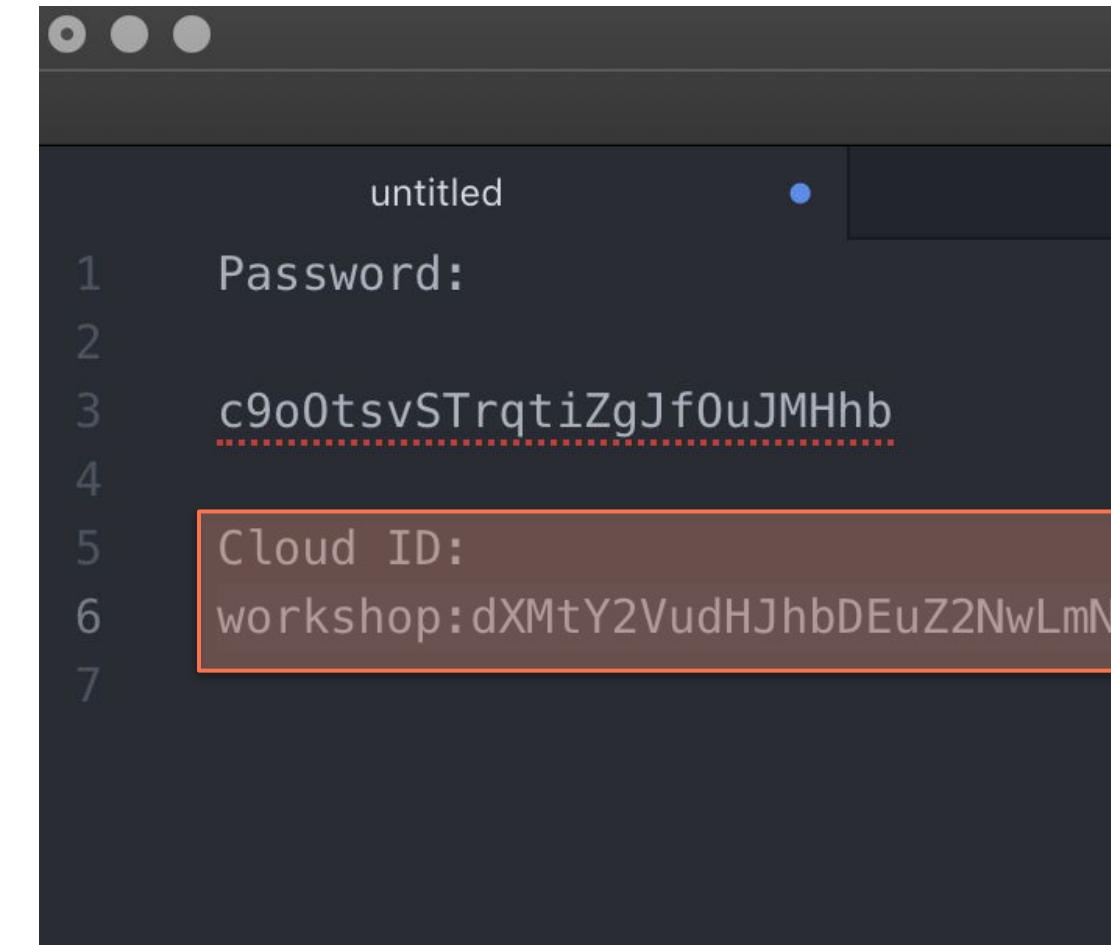
Save the Cloud ID



1 Select 'workshop' under deployments in the left navigation menu



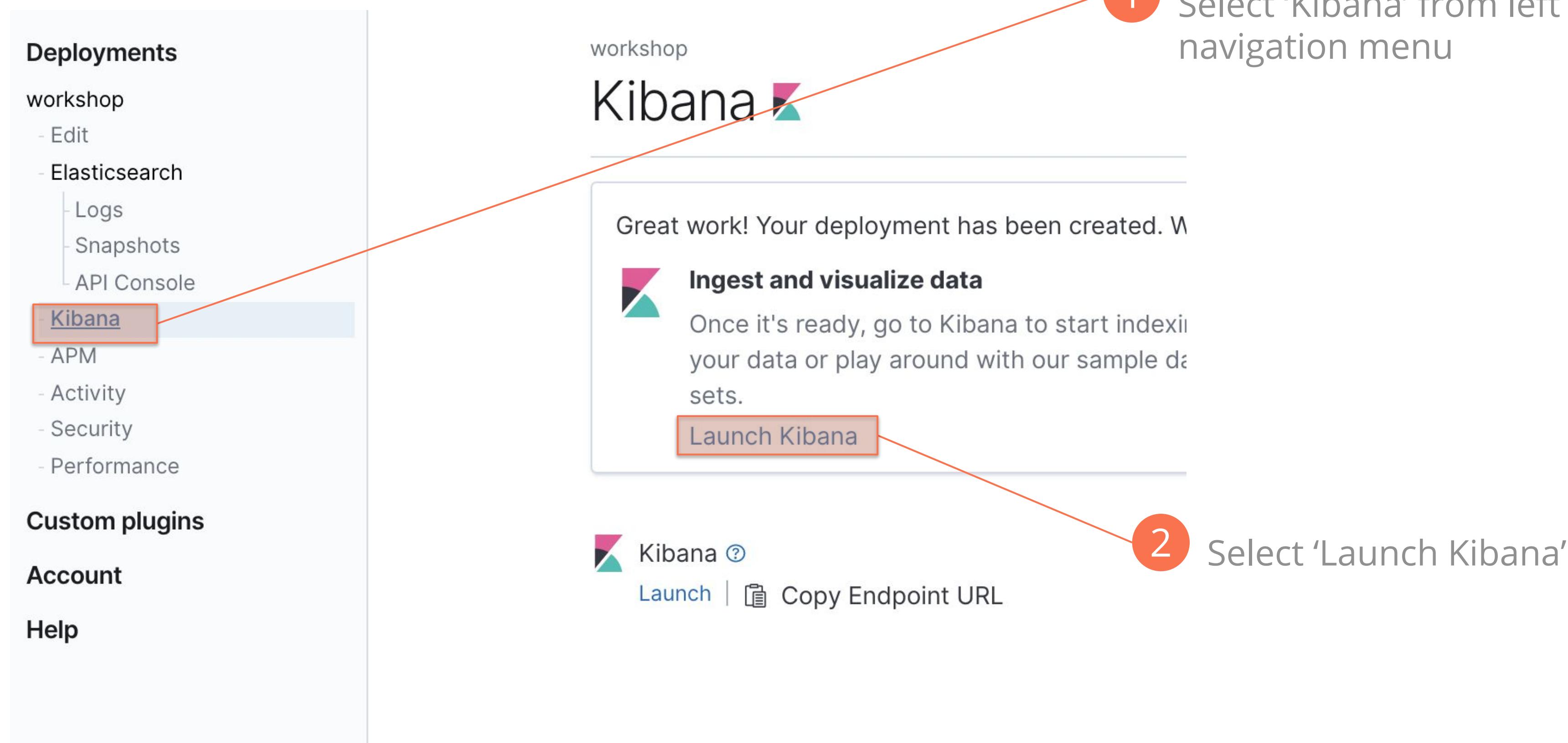
2 Copy the Cloud ID to the clipboard



3 Paste the Cloud ID into a local text editor

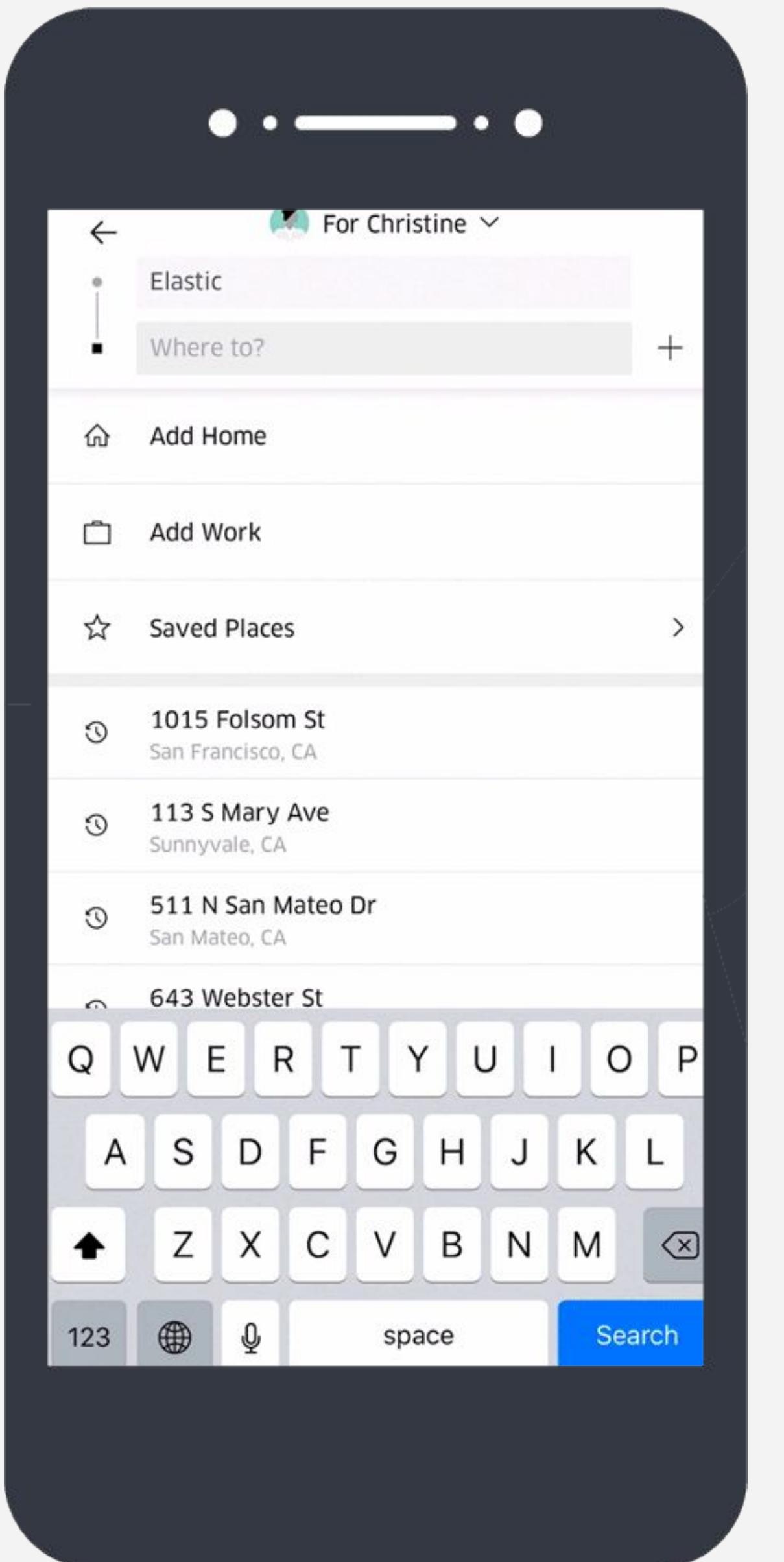
Launch Kibana

Setup complete, time to launch Kibana

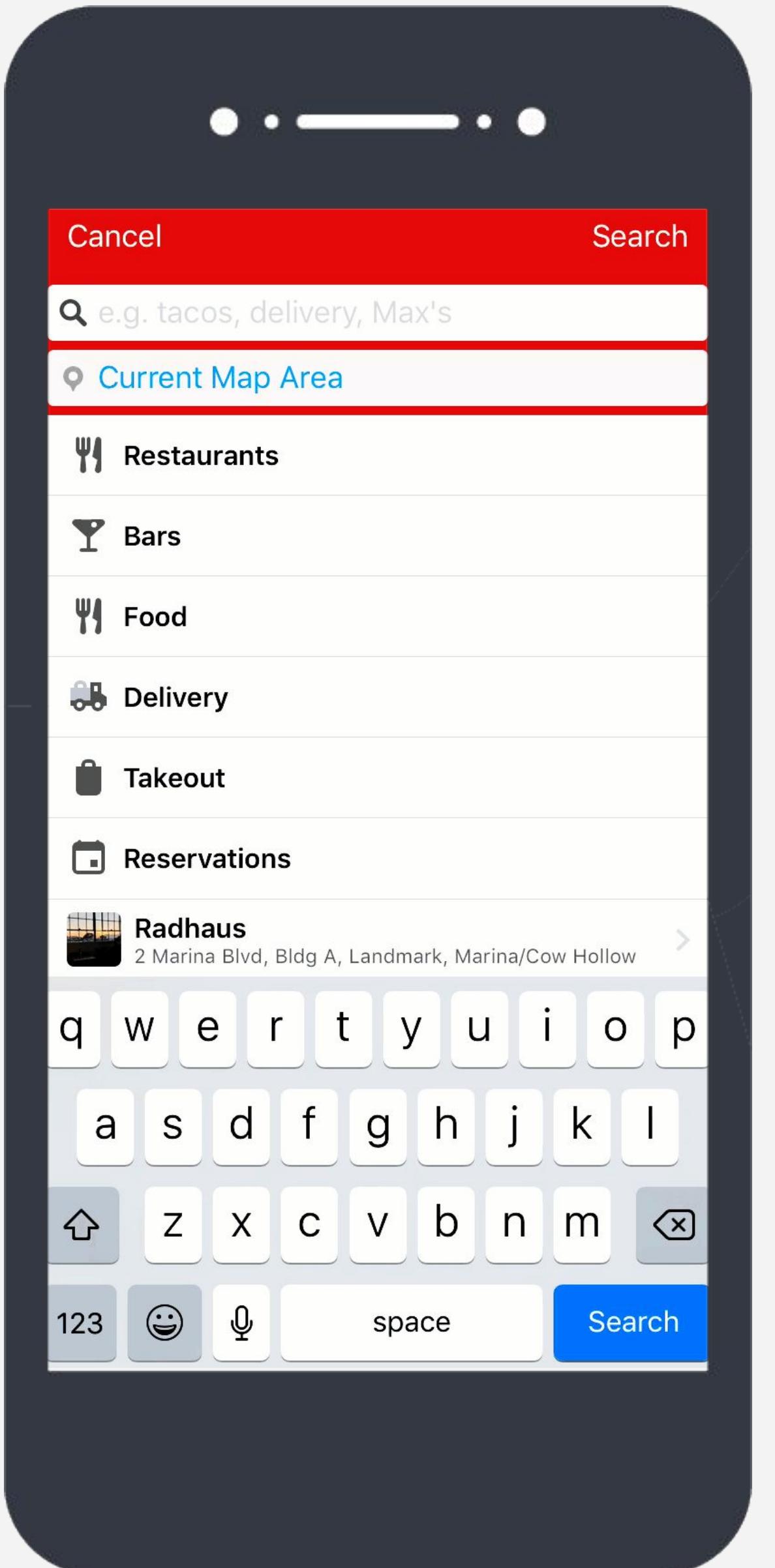


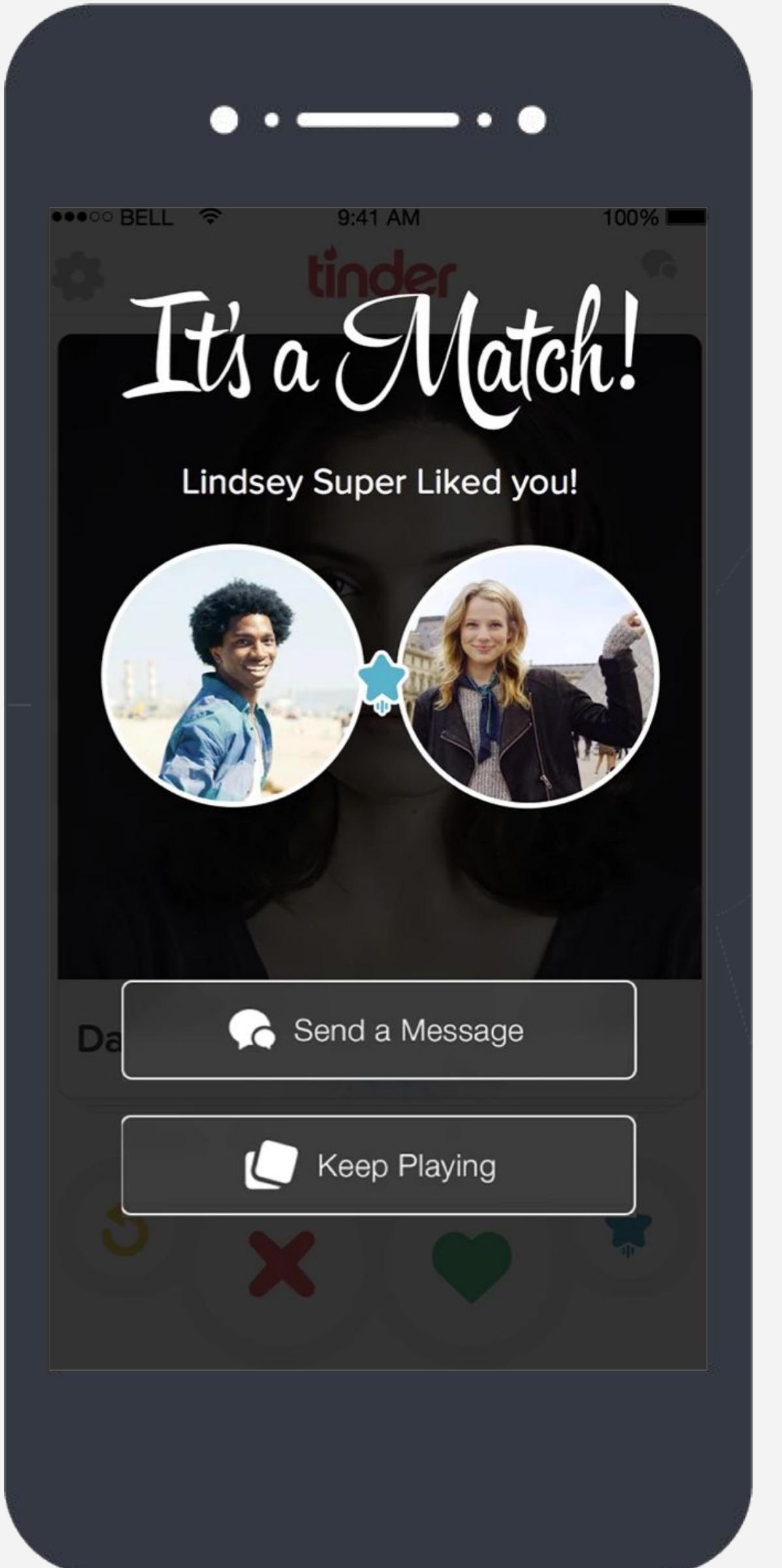
Elastic Stack Overview

Elastic is a search company
SIEM & security analytics
thrive on search



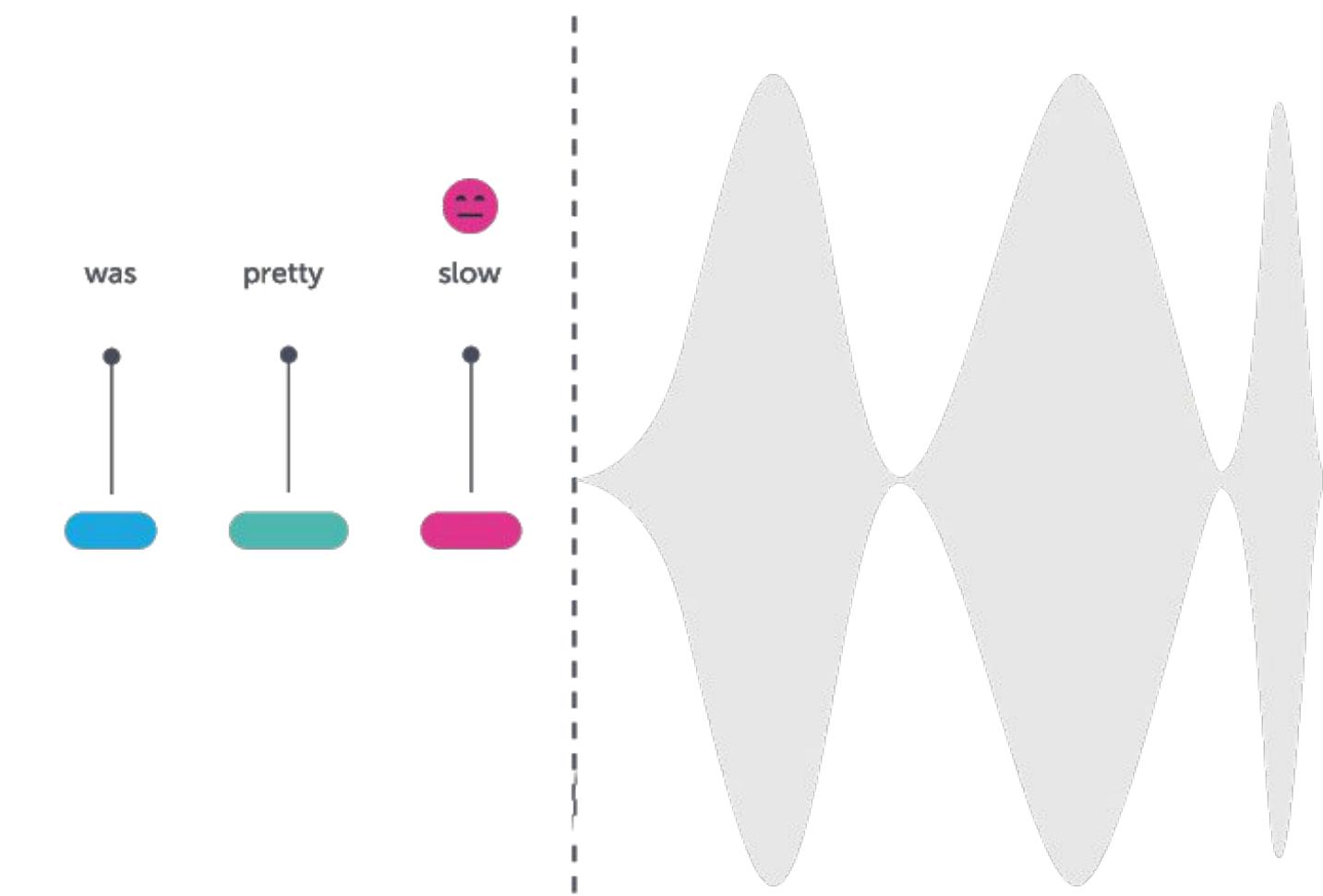
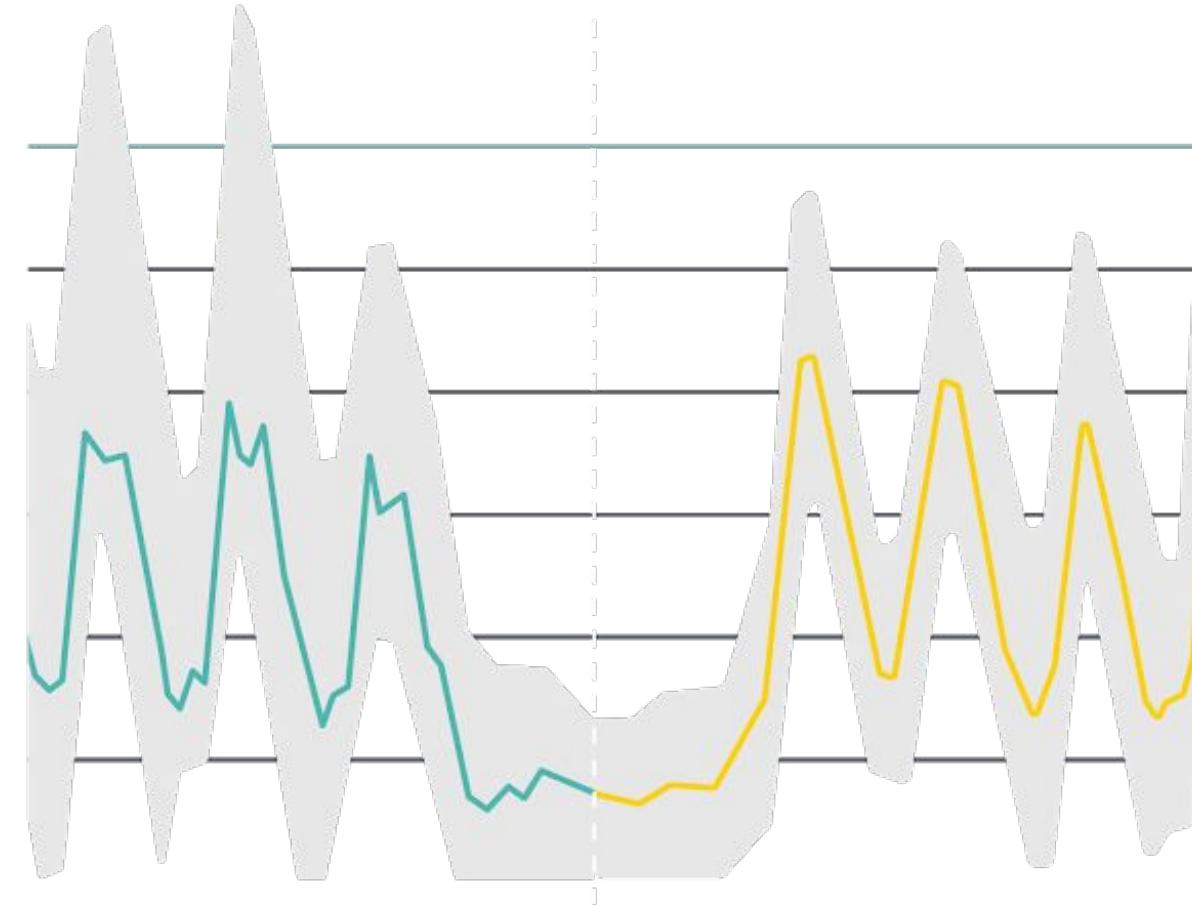
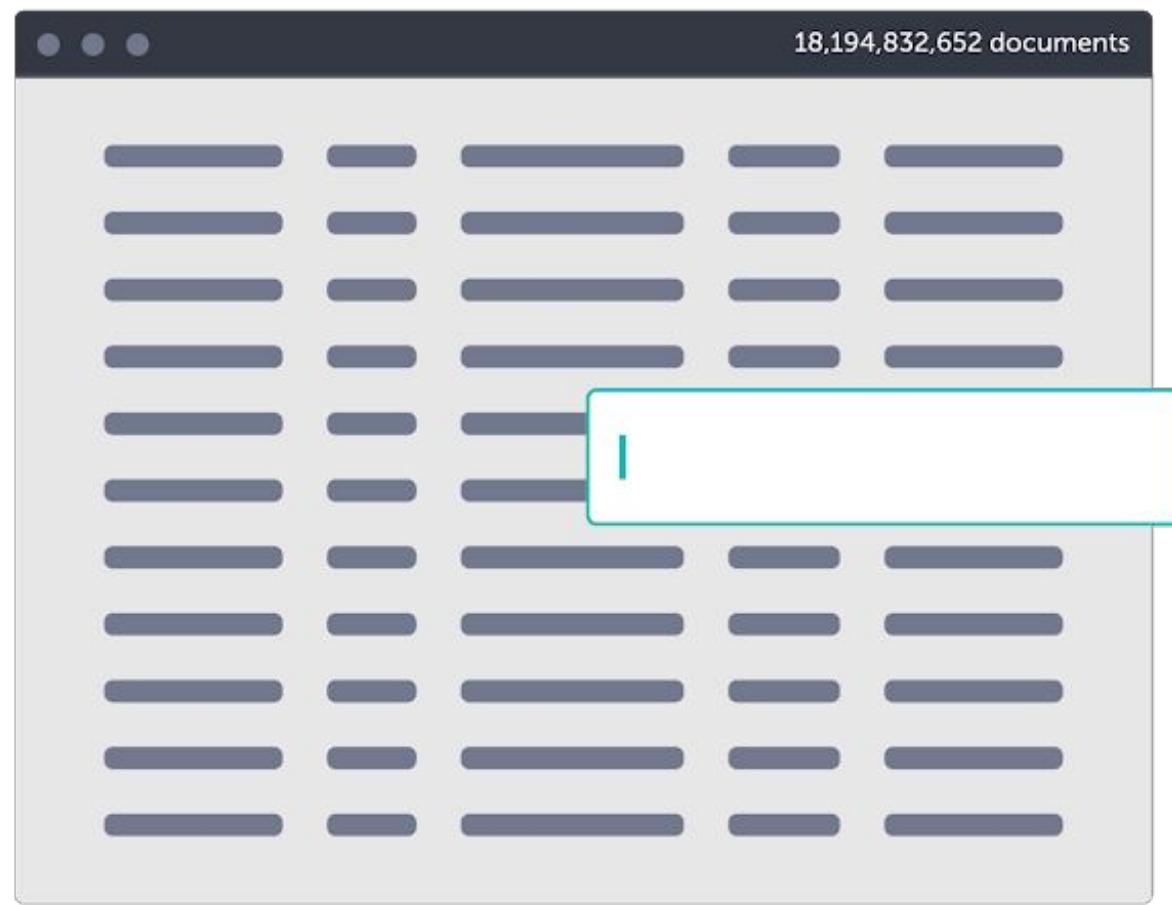
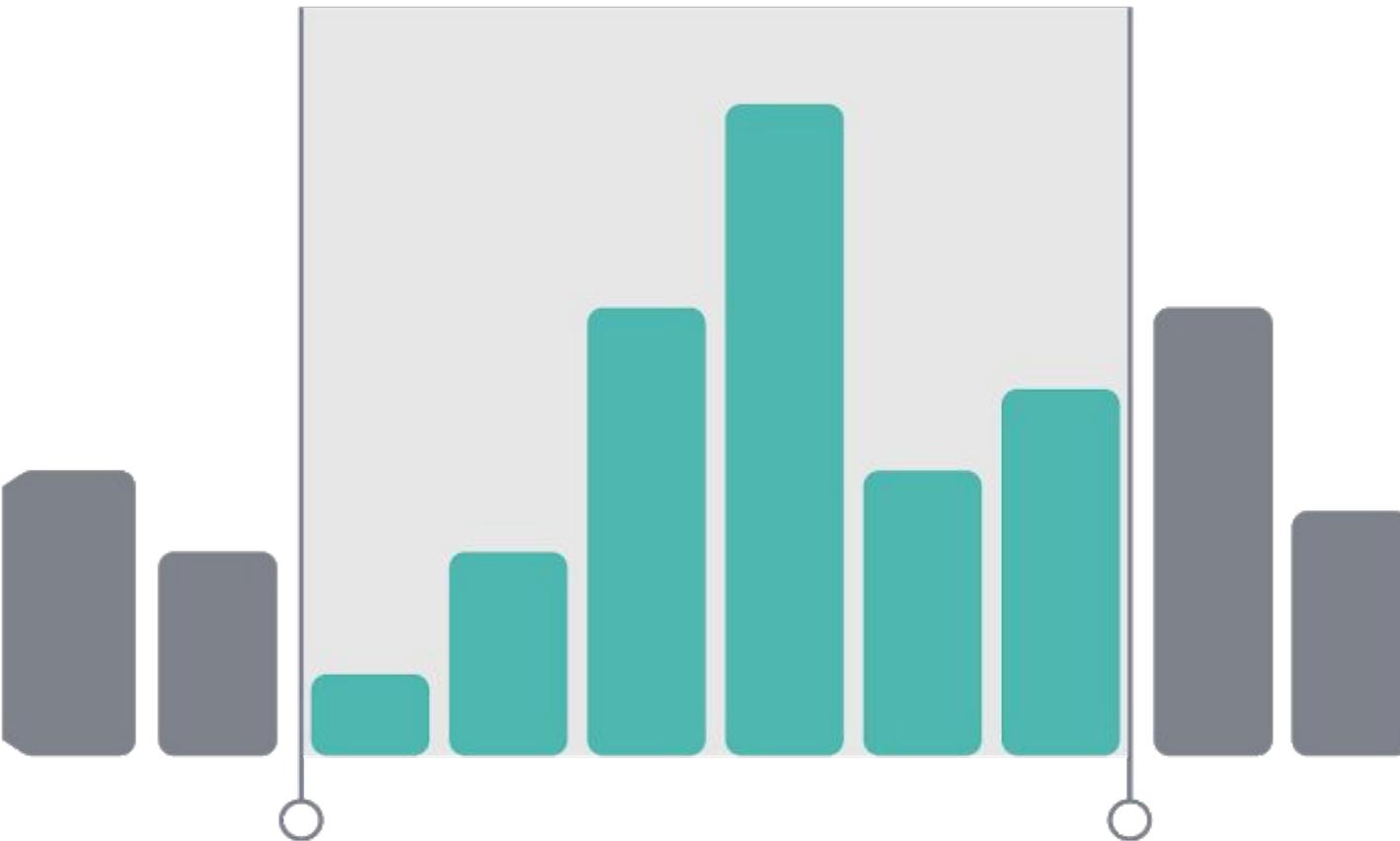
uber





tinder™

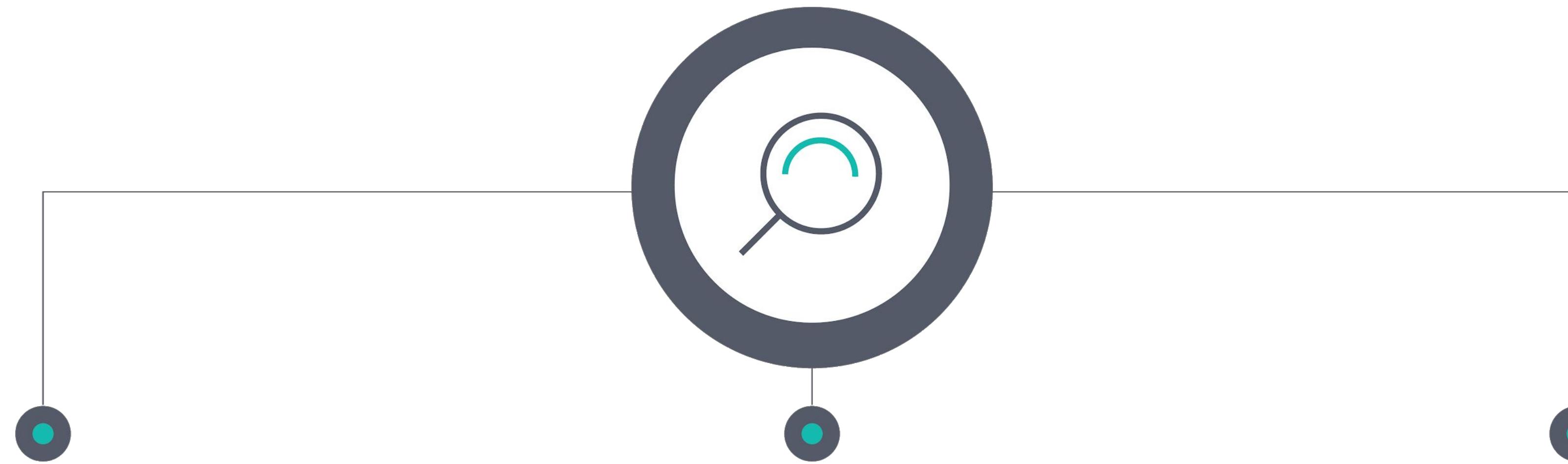
Search is a **constant/foundation**



Elastic's Heart: Elasticsearch



Technology **differentiation**



SCALE

Distributed by design

SPEED

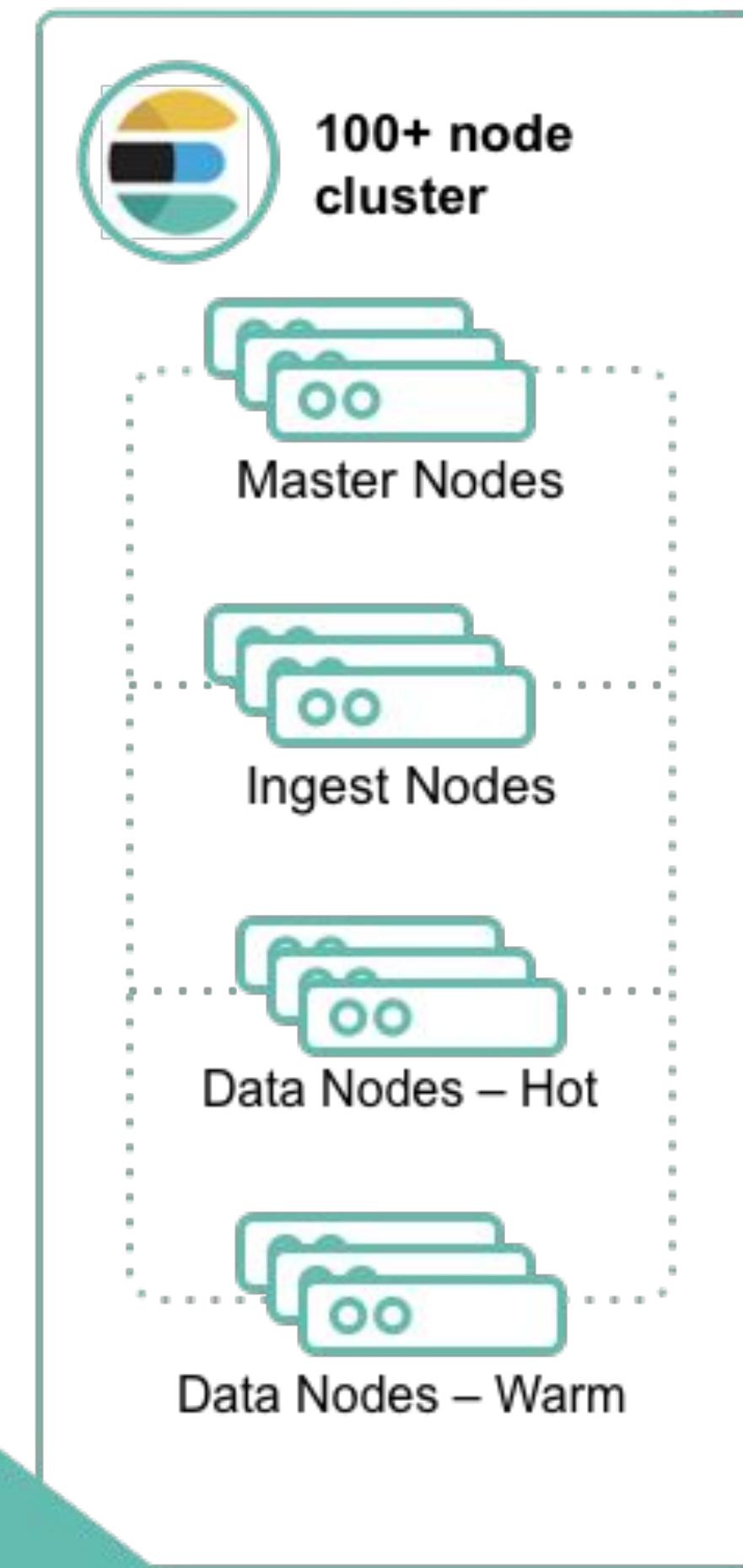
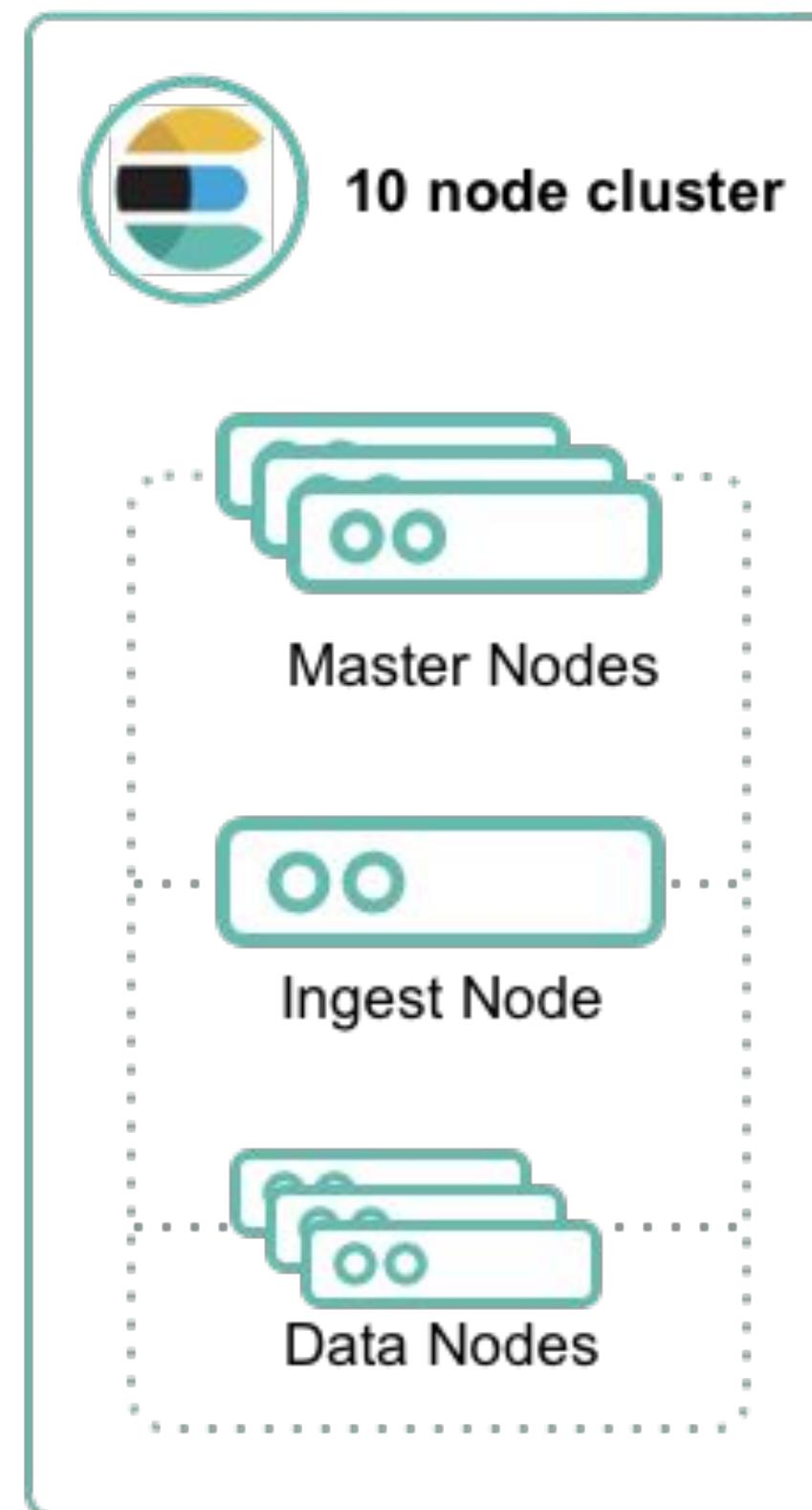
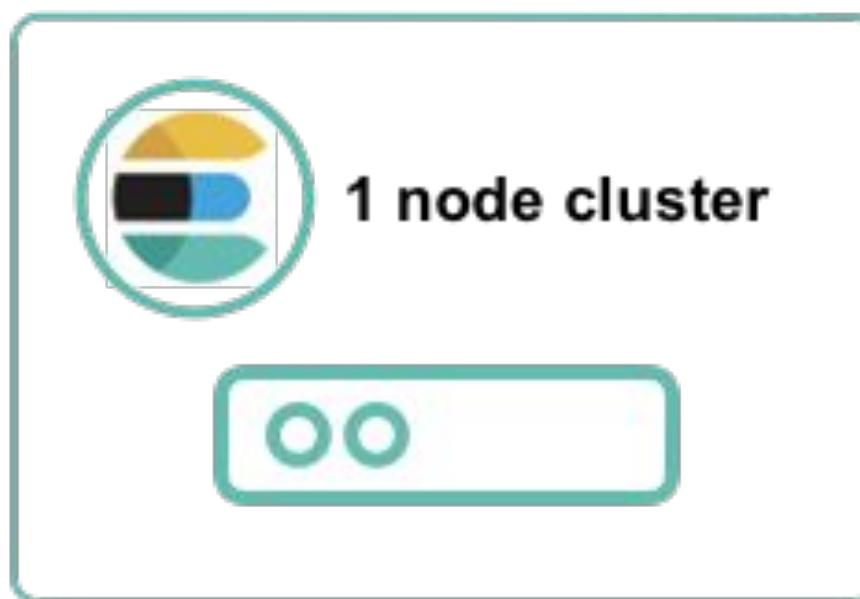
Find matches in milliseconds

RELEVANCE

Get highly relevant results

Elasticsearch

Distributed by design, scales horizontally



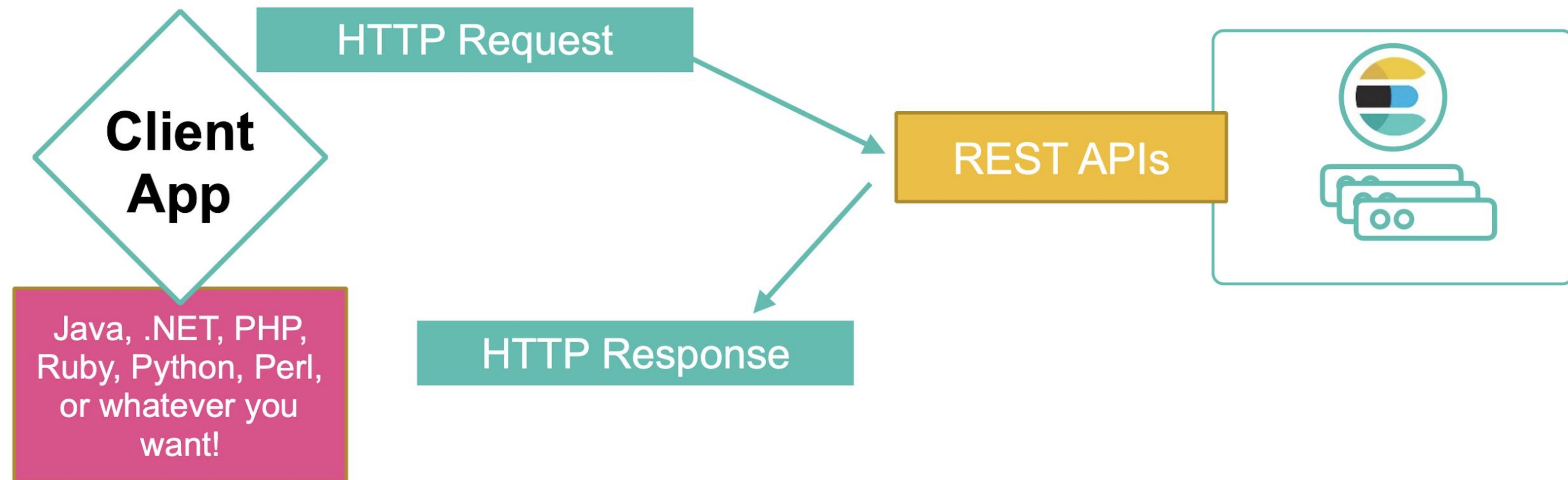
A **node** is an instance of Elasticsearch

A **cluster** is a collection of Elasticsearch nodes

Your cluster can grow as your needs grow

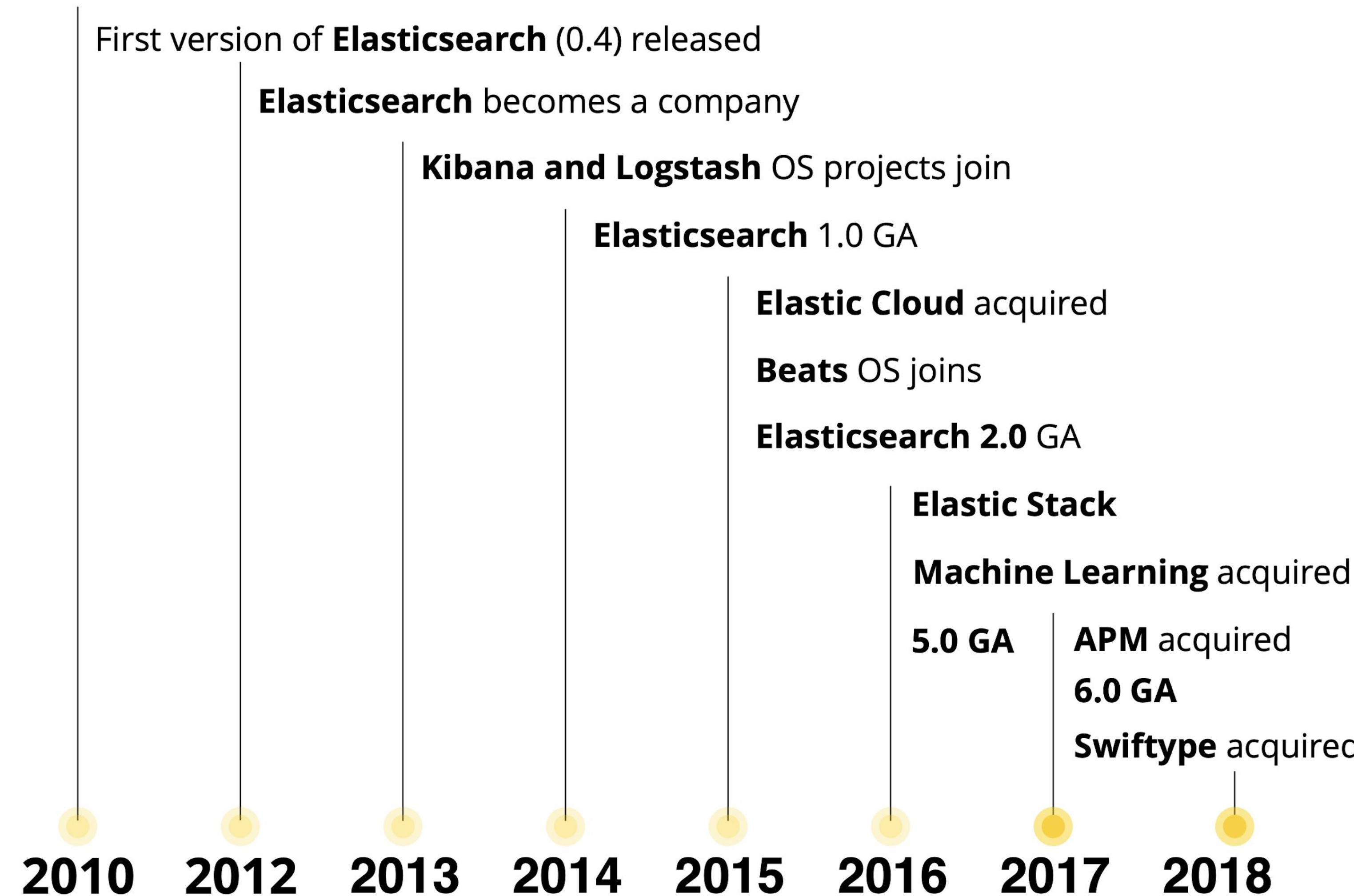
Elasticsearch is REST API First

Developer Friendly...but not everyone is a developer



The Evolution of Elasticsearch

How community has contributed to Elastic's direction





Logstash

ETL for Elasticsearch

Ingest data of all shapes, sizes,
and sources

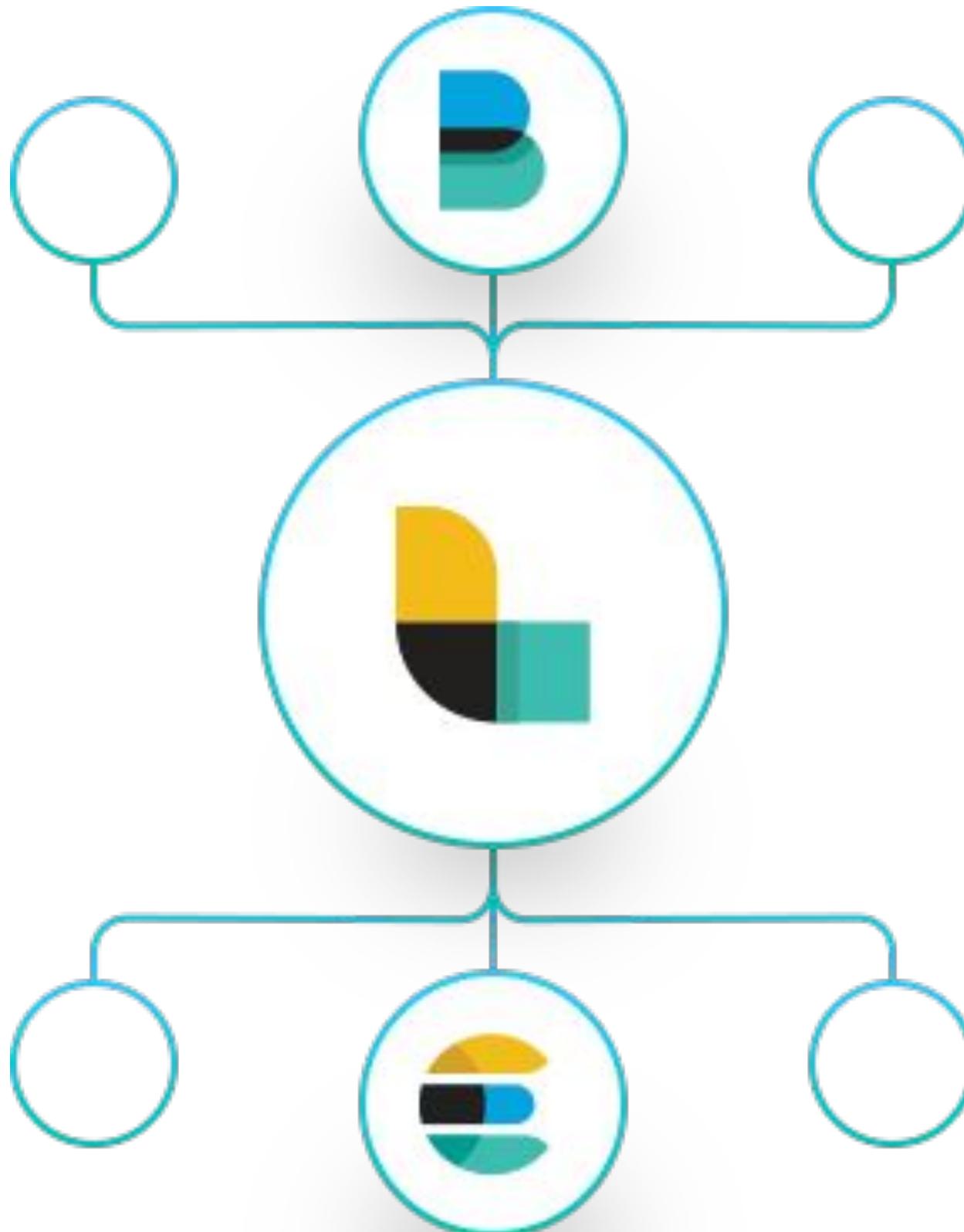
Secure and encrypt data
inputs

Parse and dynamically
transform data

Build your own pipelines

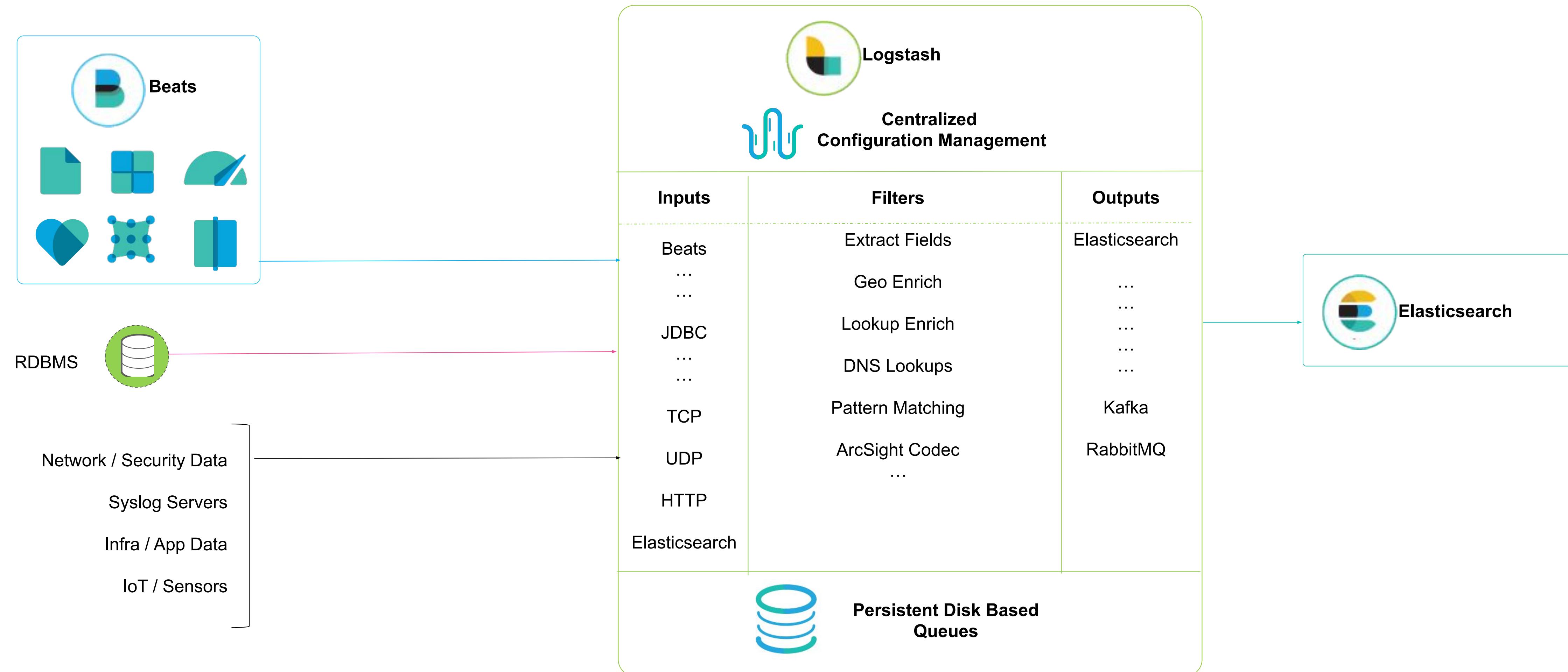
Transport data to any
output

Lots of plugins



Logstash Pipelines: Inputs + Filters + Outputs

Normalize and Enrich Data before Indexing



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

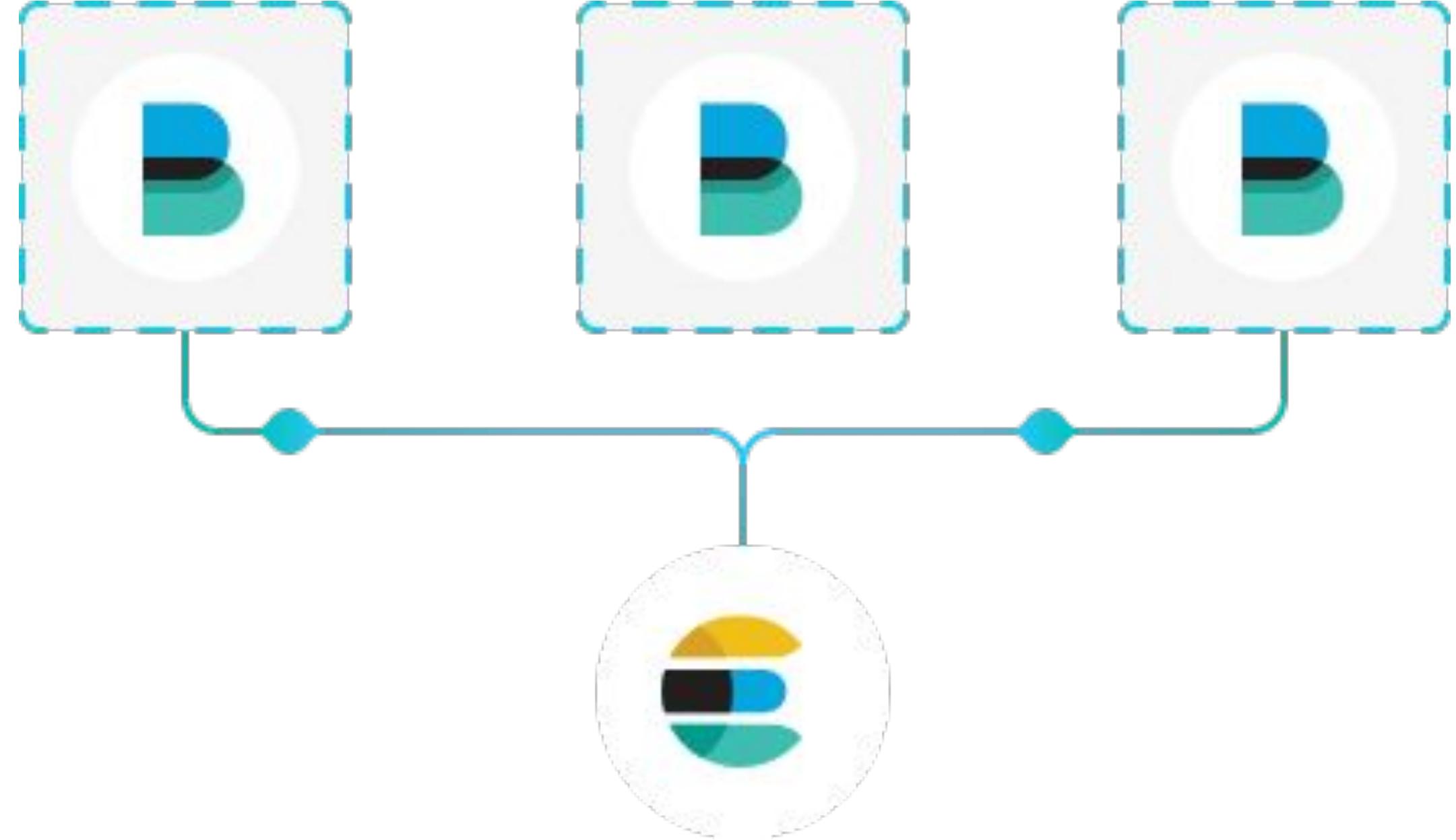
Destination fields describe details about the destination of a packet/event.

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



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



FileBeat
Log Files



MetricBeat
Metrics



PacketBeat
Network Data



WinLogBeat
Window Events



HeartBeat
Uptime Monitoring



AuditBeat
Audit Data

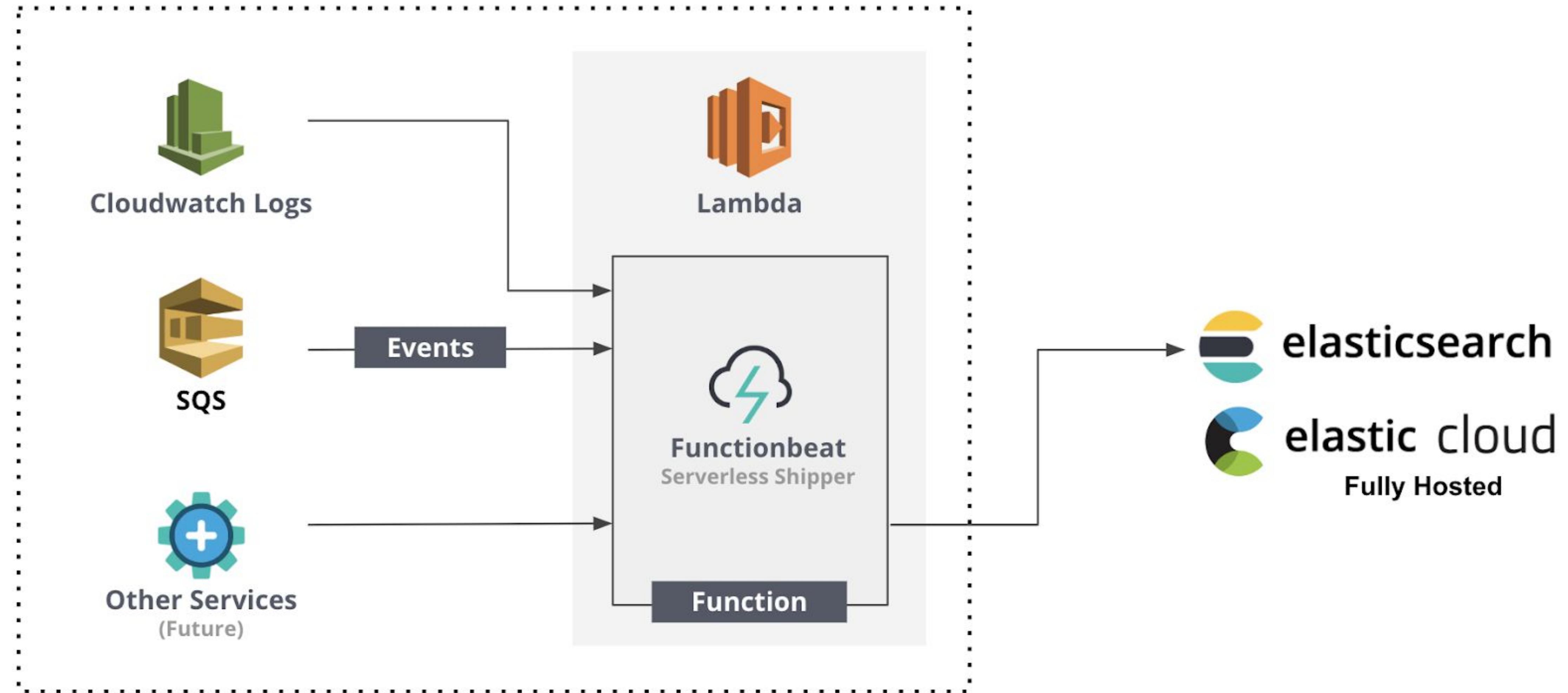


FunctionBeat
Serverless Shipper

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

FunctionBeat - Serverless shipper for Cloud Data

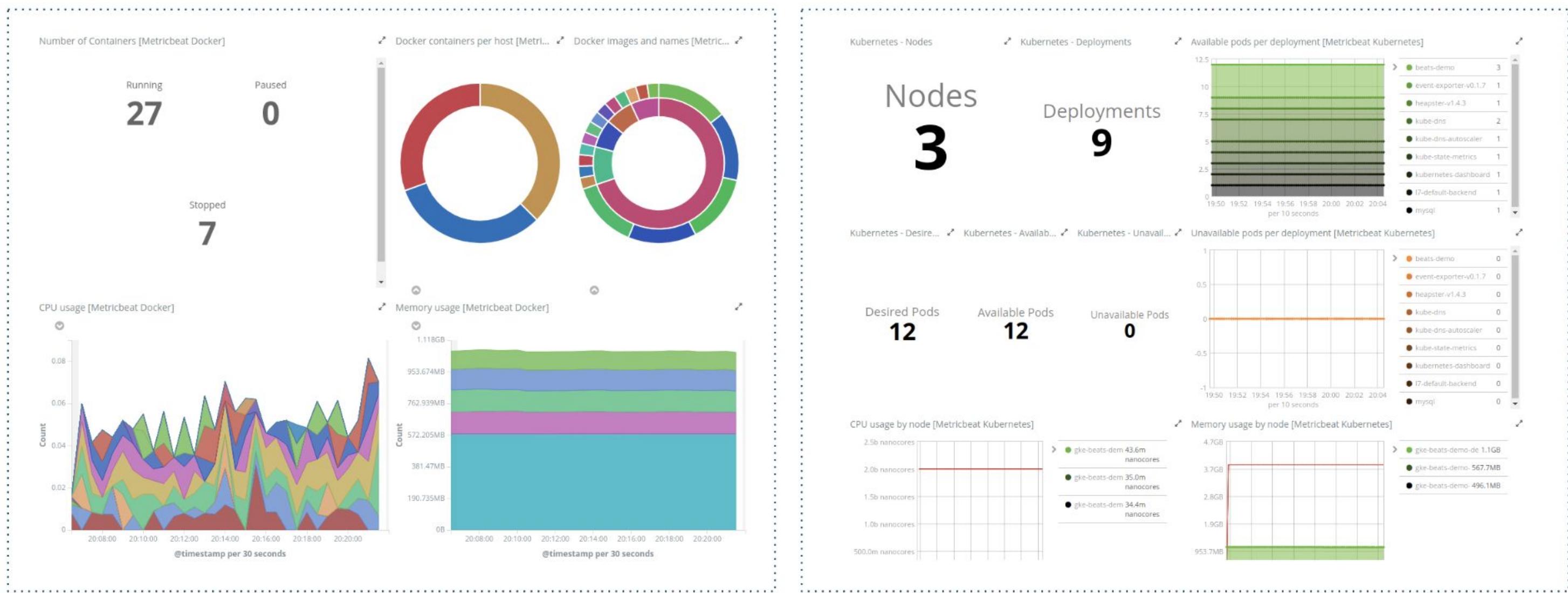
Ingest from CloudWatch Logs & Amazon SQS



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

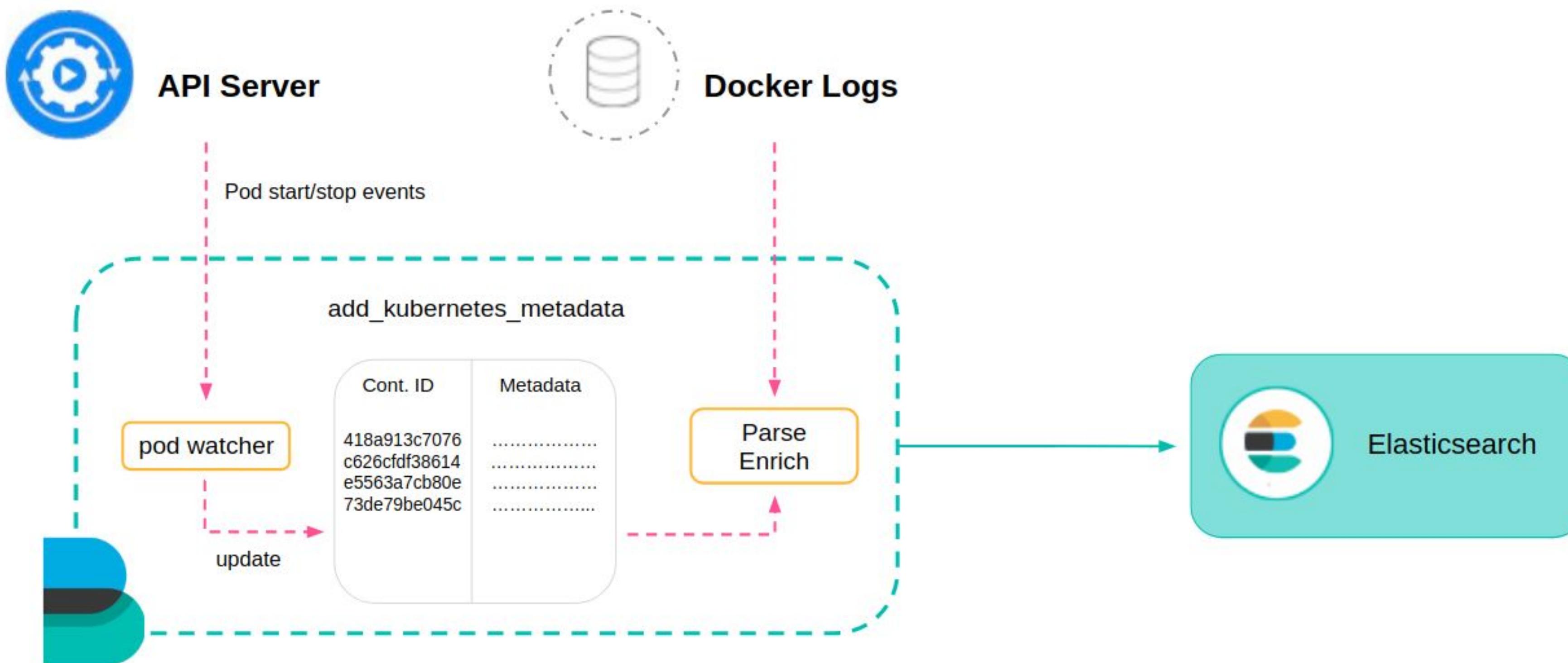


Modules



Kubernetes Log Collection with Filebeat

Fluentd is great, but Filebeat is even better!



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

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"  
    }  
  },  
}
```

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

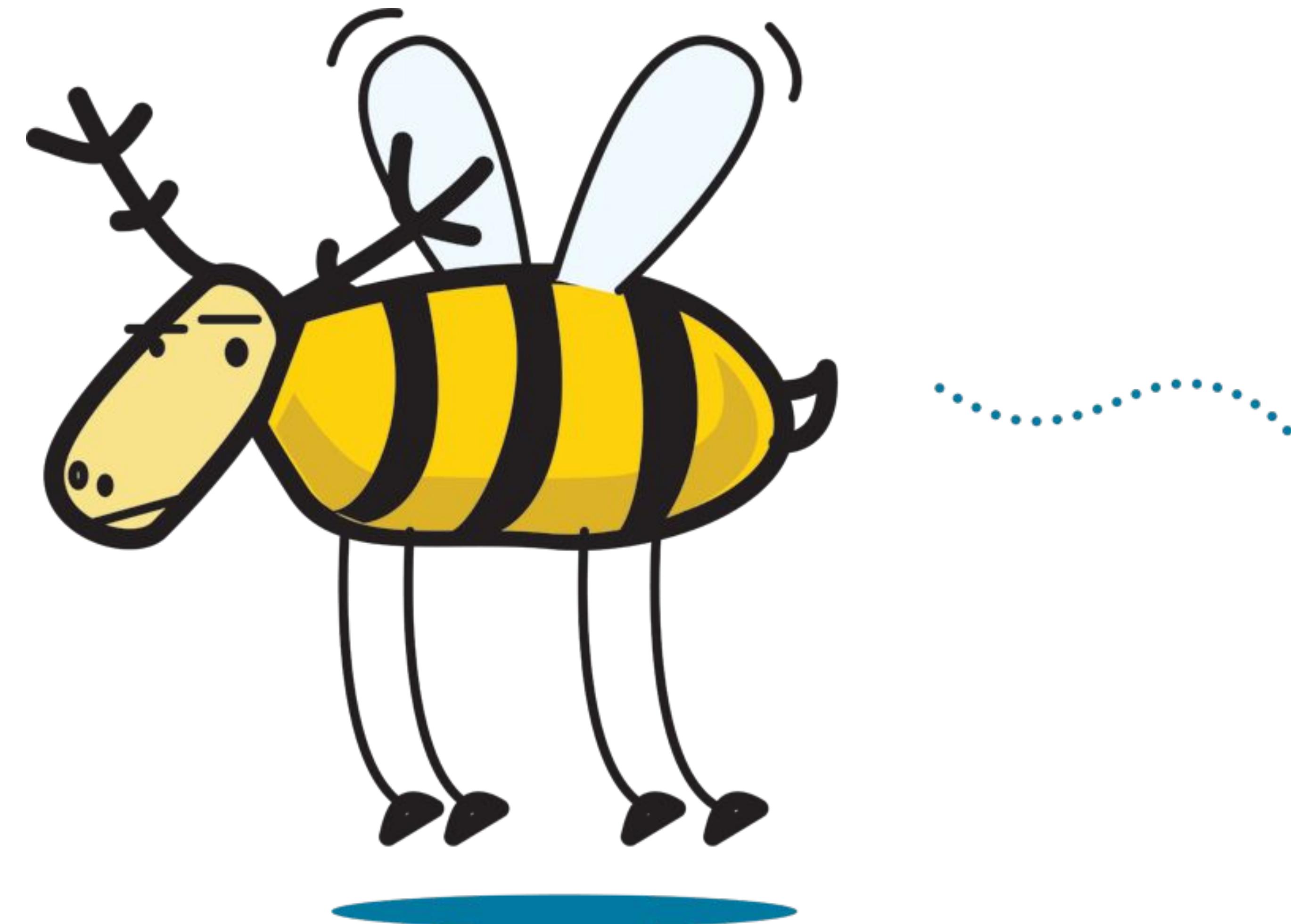
- The Metricbeat Prometheus module will query Prometheus exporters at the user-defined frequency.
- This method **does not require** Prometheus server to be in place, as the communication is directly between Metricbeat and Prometheus exporters.
- Support for TLS to ensure secure data transfer.

```
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.certificateAuthorities:  
  # - /var/run/secrets/kubernetes.io/serviceaccount/service-ca.crt
```

Say hello to the Elastic Stack



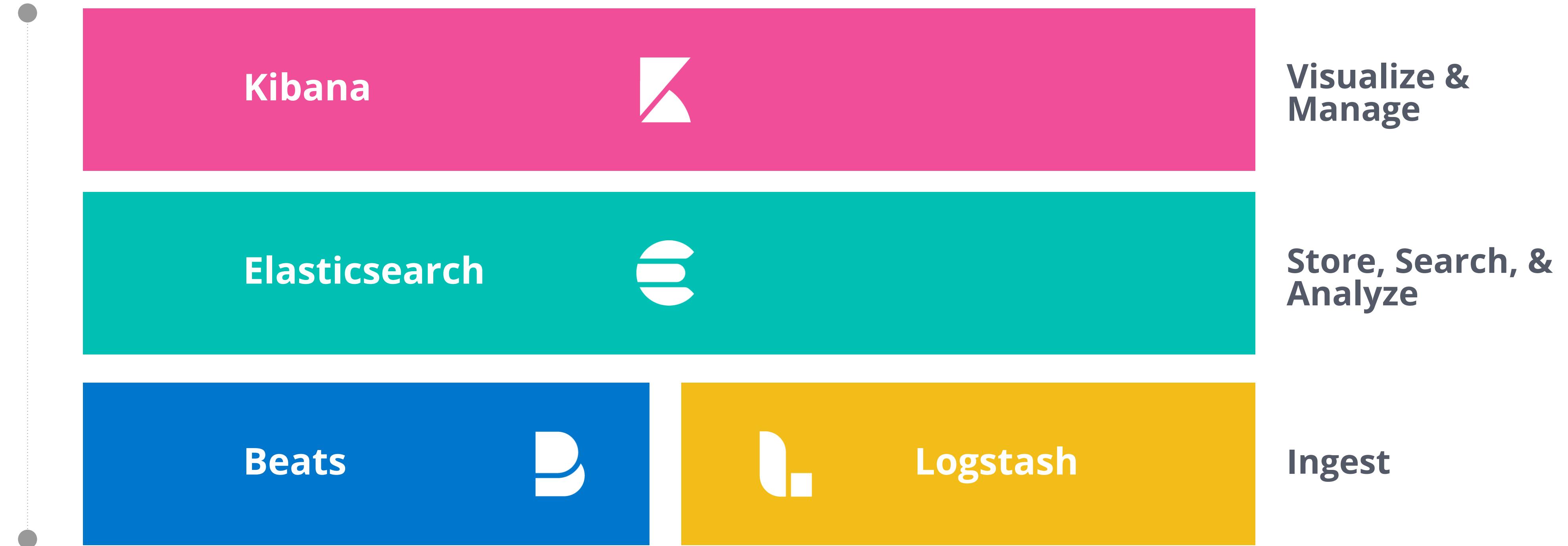
Say hello to (B)ELK!



Elastic Stack

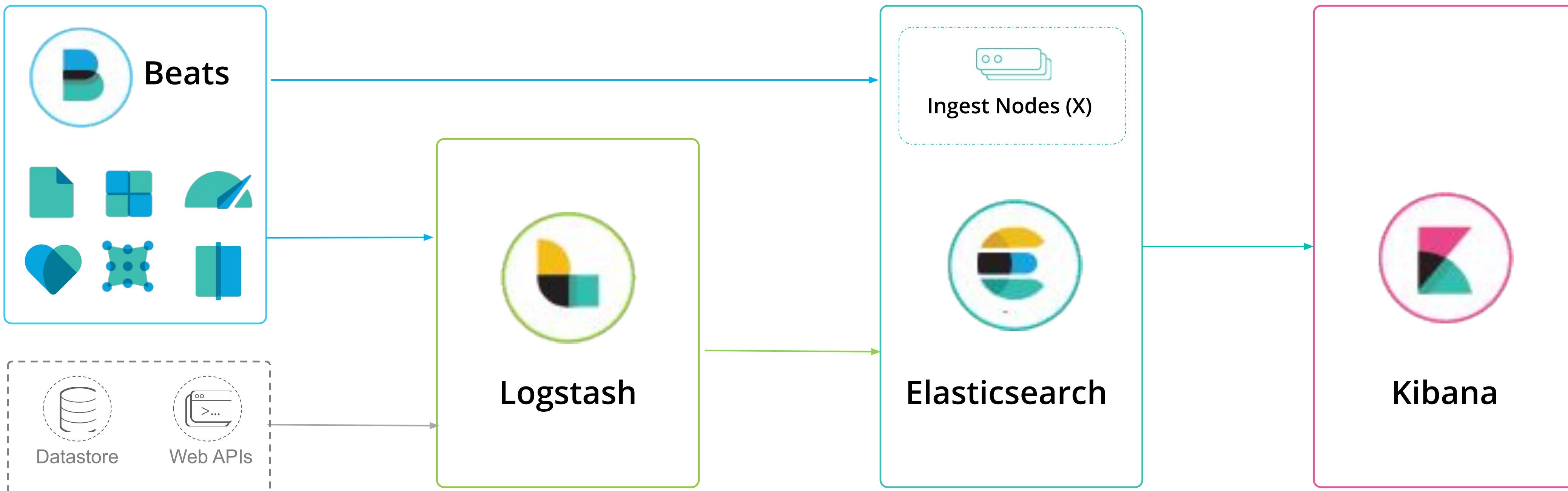


Elastic Stack



How Elastic Stack Components Work Together

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



Kibana Demo



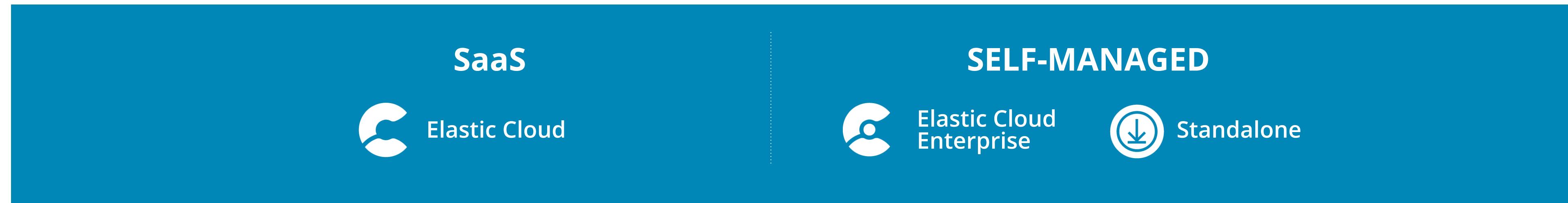
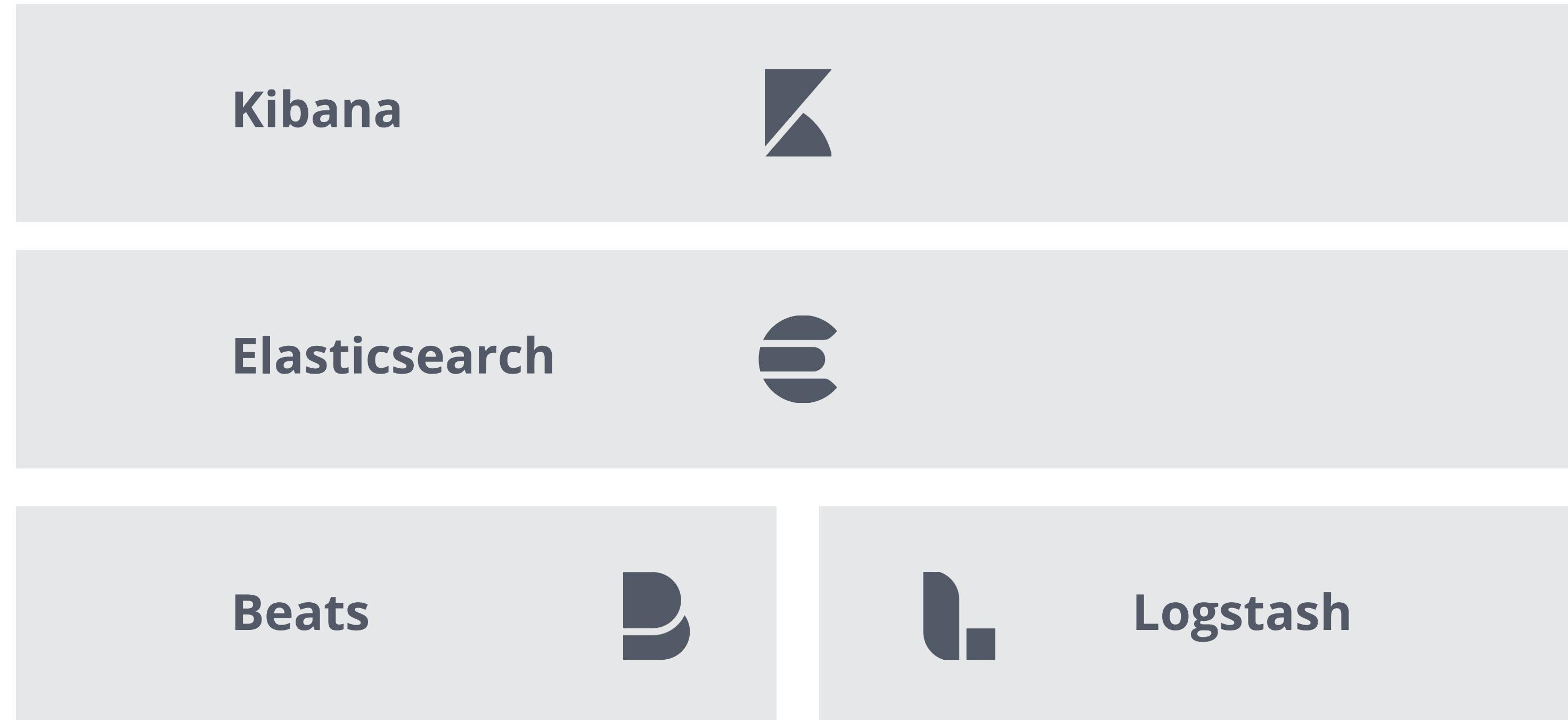
Elastic Stack Deployment Models

Deployment **options**

SOLUTIONS



Elastic Stack



Elastic Cloud

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



Deployments

Custom plugins

Account

Help

Create deployment

1 Name your deployment

Give your deployment a name



2 Select a cloud platform

Pick your cloud and let us handle the rest. No additional accounts required.



Amazon Web Services



[Google Cloud Platform](#)

3 Select a region

US Central 1 (Iowa)

US West 1 (Oregon)

[Europe West 1 \(Belgium\)](#)

Europe West 3 (Frankfurt)

Elastic Cloud Enterprise

Packaging years of SaaS experience into a product

[Deployments](#)

[Platform](#)

[Activity Feed](#)

Deployments

Filter by deployment name or id .

More filters ▾

Create deployment

Showing all 8 matching deployments

admin-console-
elasticsearch

e68992 v5.6.11

data.default

4 GB RAM, 1 node,
1 zone



app-prod-logging

2dc22b v6.4.0

data.default

4 GB RAM, 1 node,
1 zone

data.highstorage

4 GB RAM, 1 node,
1 zone

Kibana

Included



logging-and-metrics

7b14db v5.6.11

data.default

1 GB RAM, 1 node,
1 zone

Kibana

Included



rad-app-logging

999d16 v6.4.0

security-threat-hunting

f4fb8b v6.4.0

server-telemetry

1d3972 v6.4.0

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 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



Users Already Adopting the Elastic Stack for SIEM



Bell



Ψ



Security
Analytics
Customers



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

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

Lab 2

Data Ingestion using Beats and MITRE ATT&CK™

Setup Strigo

Your Training Environment

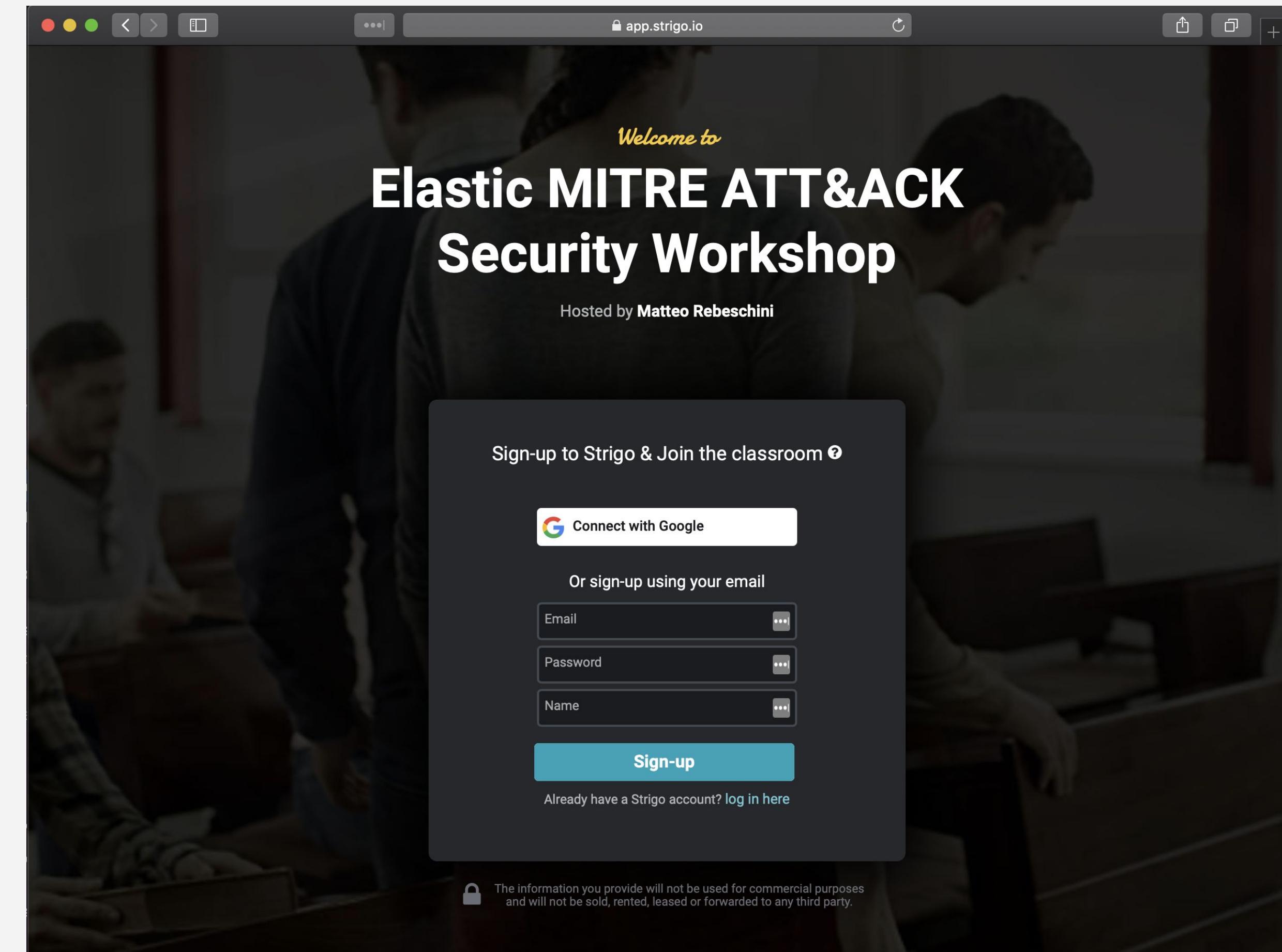
Class URL:

<https://bit.ly/BSidesLV2019>

Access Token:

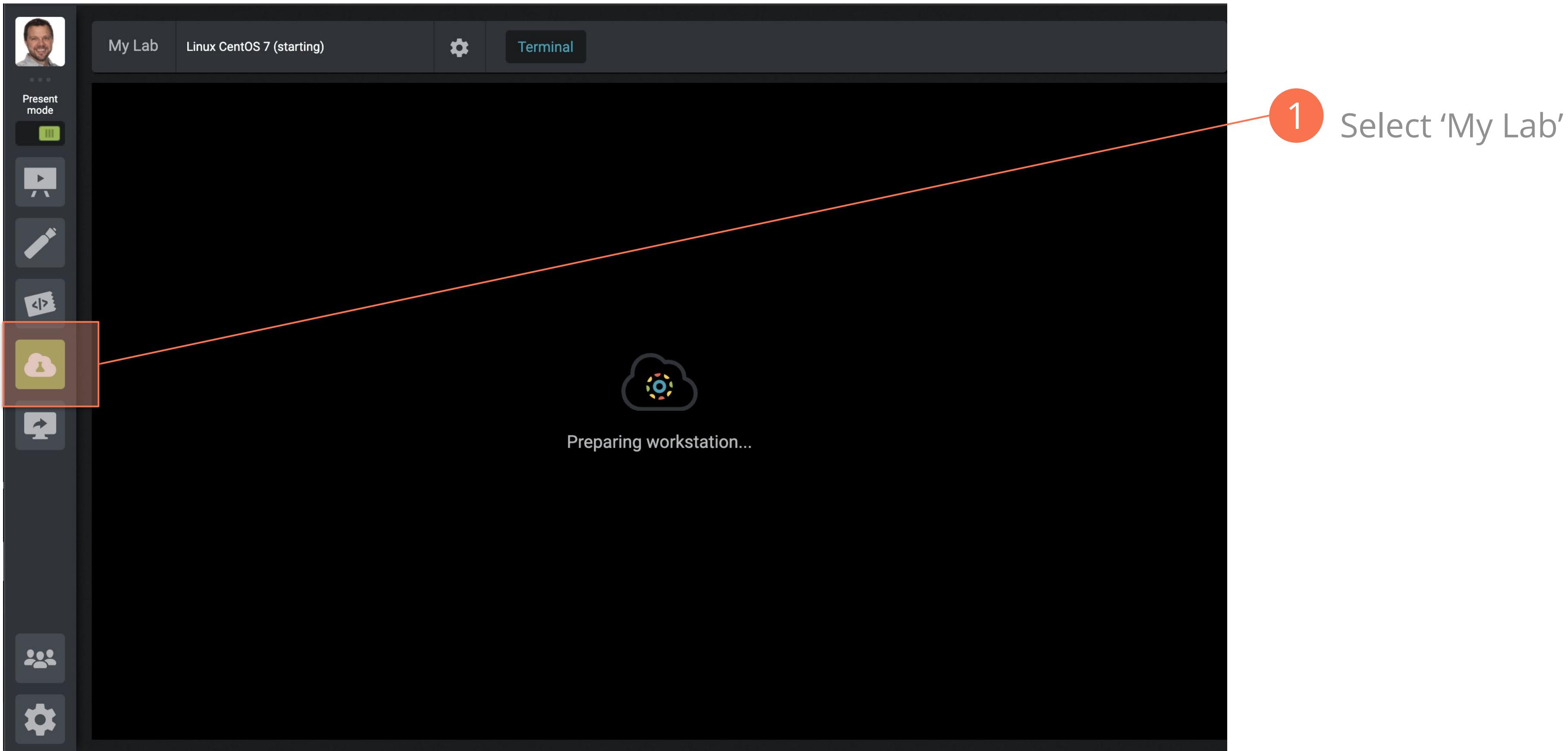
YK7M

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



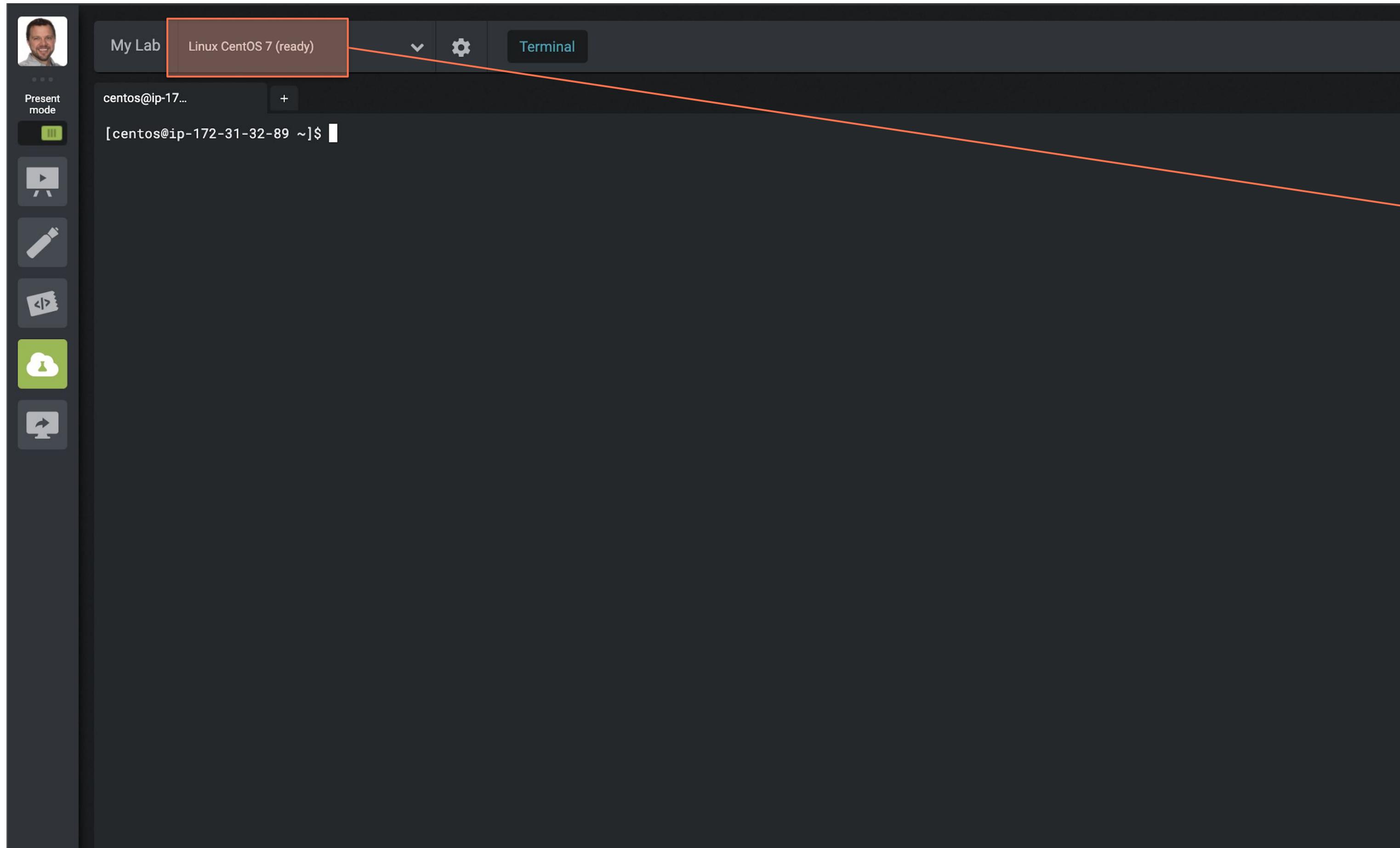
Linux Beats Scripted Install

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'

Linux Beats Scripted Install

Installation of MetricBeat, Filebeat, AuditBeat and PacketBeat

```
[centos@ip-172-31-32-89 ~]$ ./beats_install.sh
Enter your Elastic Cloud CLOUD_ID then press [ENTER]
bsides-test:dXMtd2VzdDEuZ2NwLmNs3VkLmVzLmlvJDFkZmI5NGN1N2JjZDQxNDA4NmYwZGM00GM5YjY0Y2QxJDdhMjk0ZjIzOTYzNzQ3ZTNhMzdiYjFmYmEzZGRhZTYz
Your CLOUD_ID is set to bsides-test:dXMtd2VzdDEuZ2NwLmNs3VkLmVzLmlvJDFkZmI5NGN1N2JjZDQxNDA4NmYwZGM00GM5YjY0Y2QxJDdhMjk0ZjIzOTYzNzQ3ZTNhMzdiYjFmYmEzZGRhZTYz

Enter you Elastic Cloud 'elastic' user password and then press [ENTER]
TunqACasd0ZAP7w4GMnu03PY
Your elastic password is set to TunqACasd0ZAP7w4GMnu03PY

Ready to Install? [y|n]
```

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

Windows Beats Scripted Install

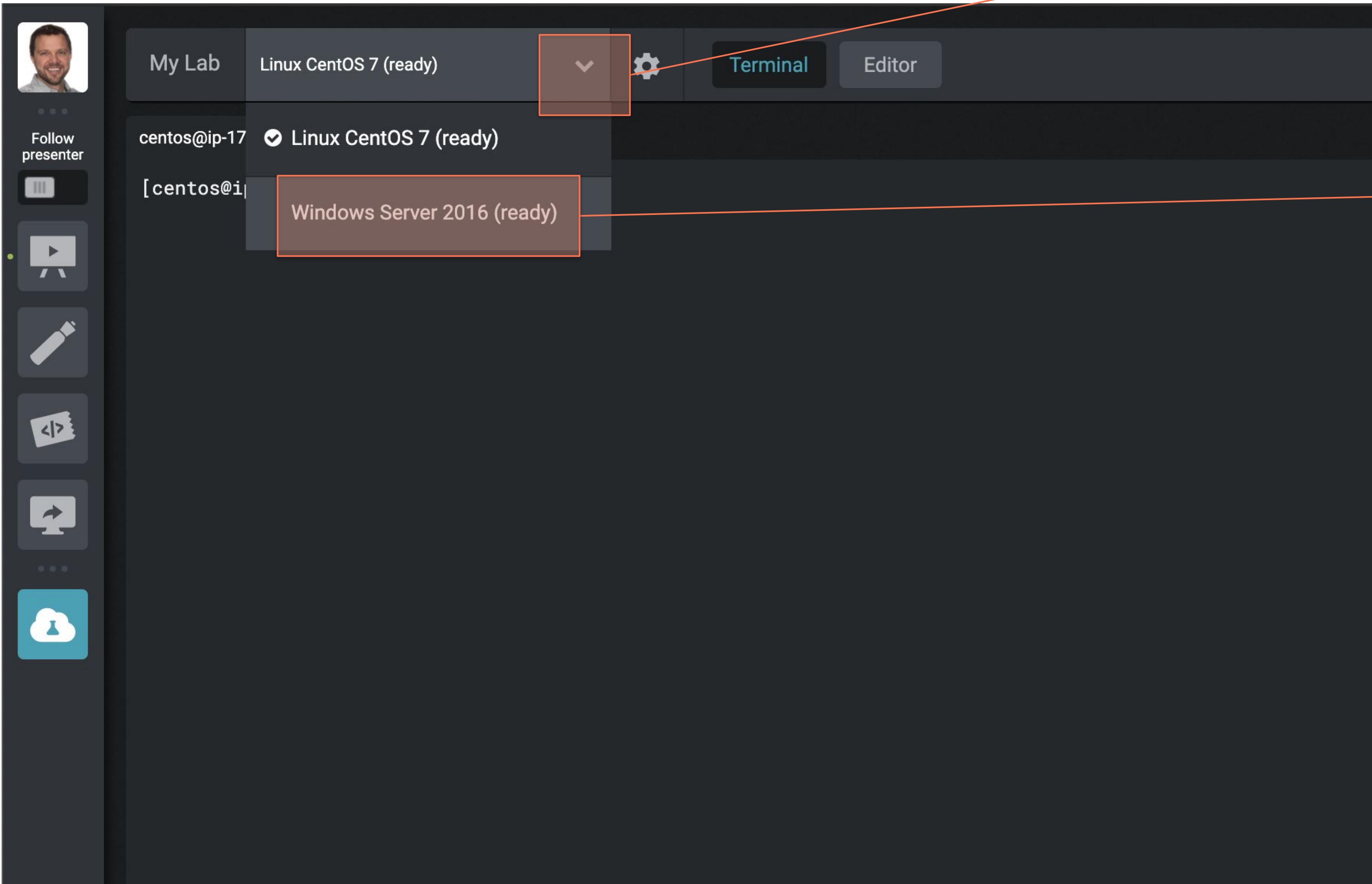
Access your Windows Server 2016 Instance

1

Select the arrow next to 'My Lab'

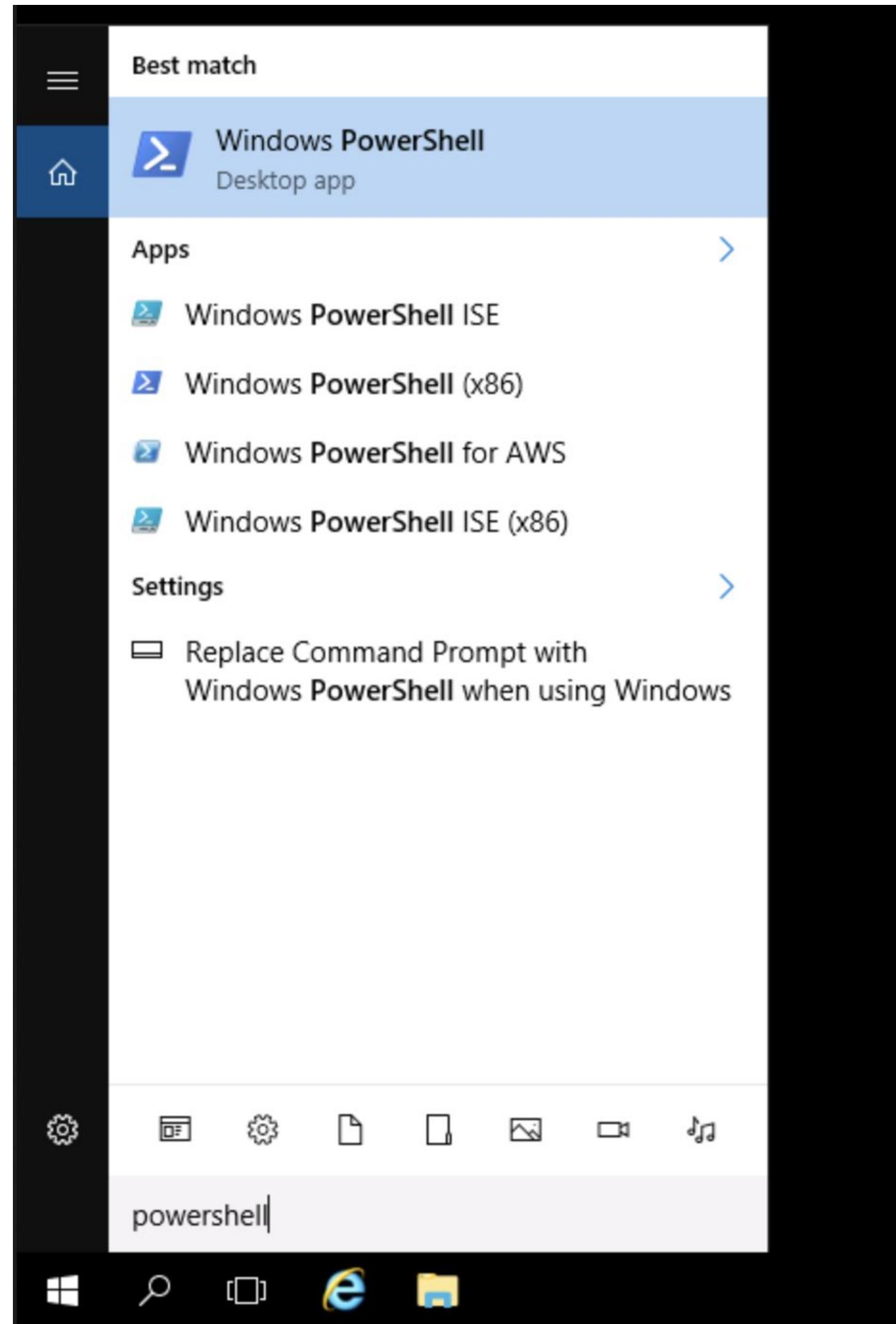
2

Select 'Windows Server 2016'



Windows Scripted Install

Install Sysmon with Custom Config Template



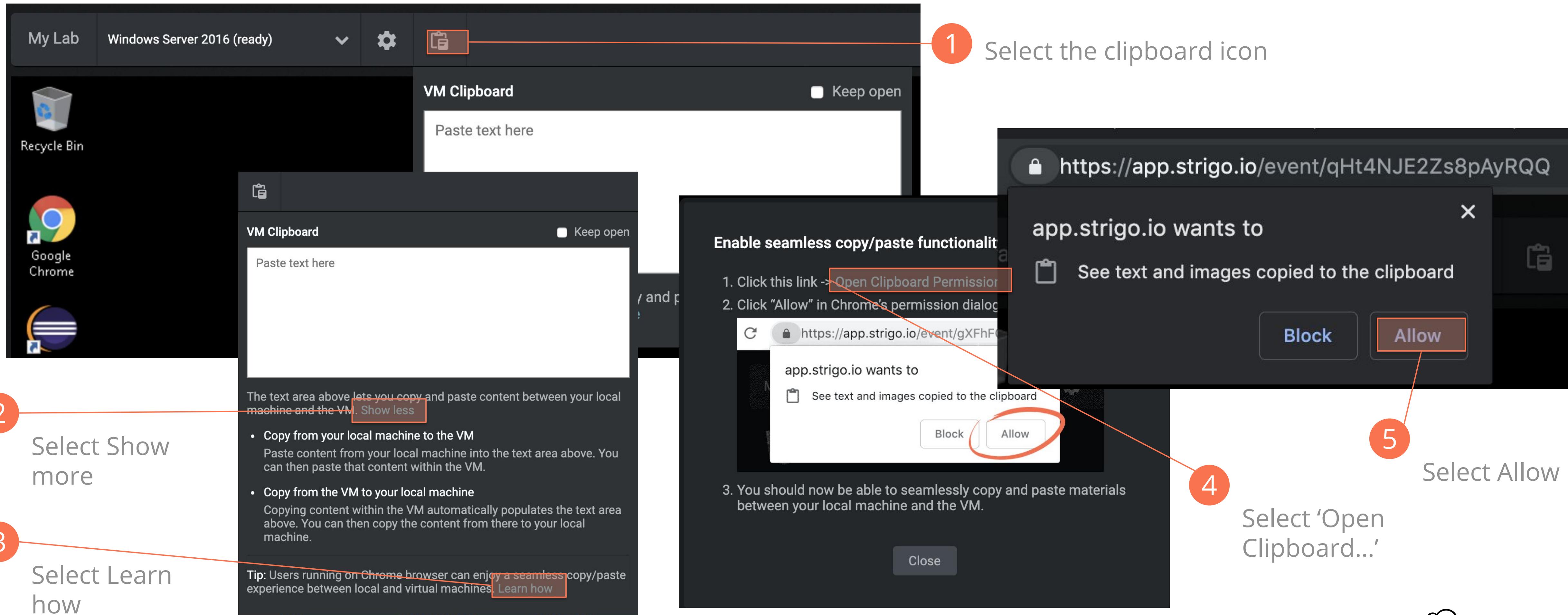
1 Type: cd ela <TAB> to autocomplete .\Elastic\
<RETURN/ENTER>

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

An Administrator PowerShell window titled "Administrator: Windows PowerShell". The command "cd ..\Elastic\" is typed and highlighted. The command ".\sysmon-install.ps1" is also typed and highlighted. The output shows "Installing Sysmon...". Below the command prompt, it says "Directory: C:\\" and lists a file "sysmon-temp" with mode "d----", last write time "8/2/2019 12:55 PM", and length "-----". The message "Installation Complete" is displayed. The PowerShell prompt PS C:\Users\Administrator\Elastic> is shown again at the bottom.

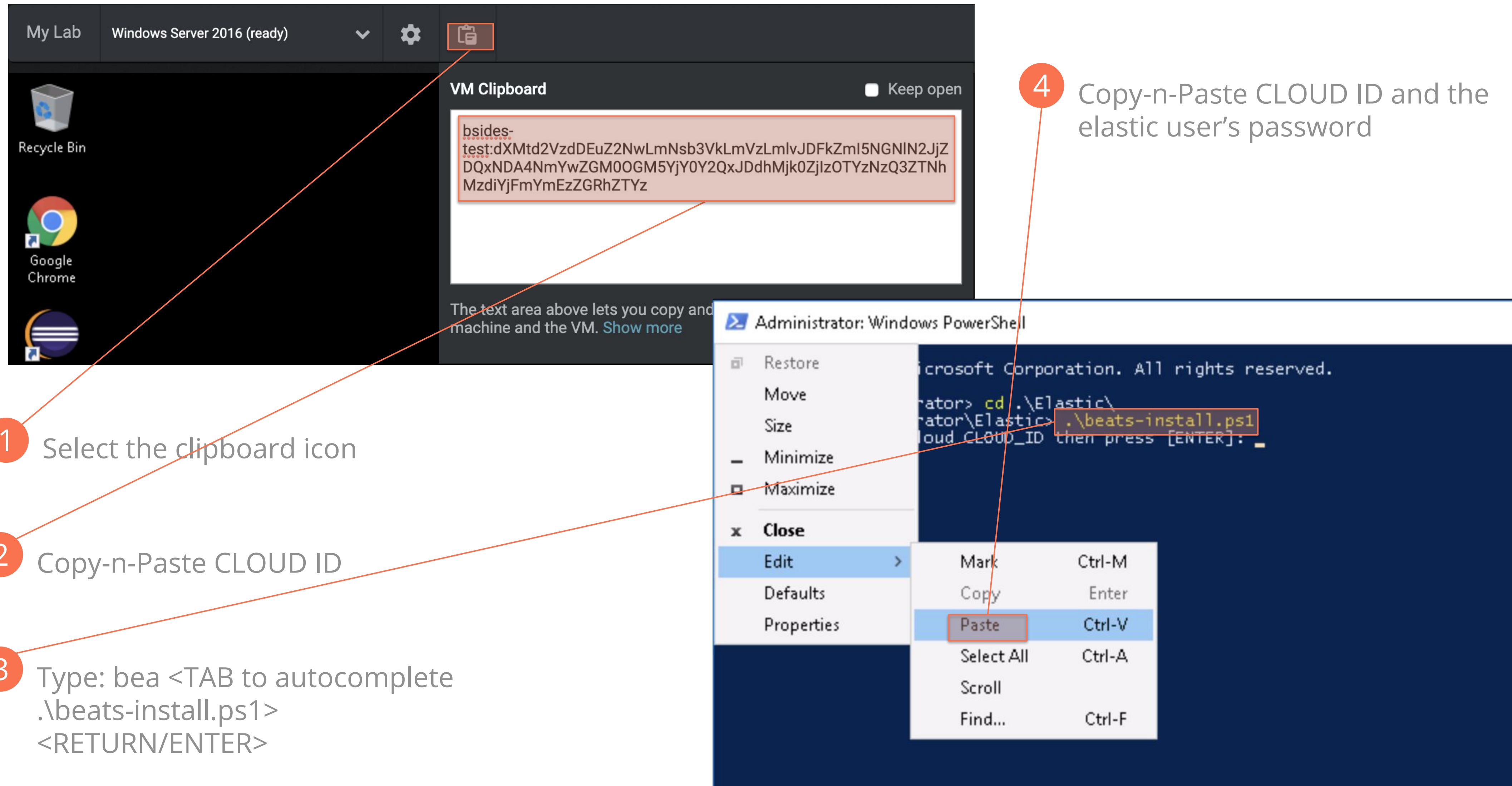
Windows Scripted Install

Seamless Clipboard Access using Google Chrome



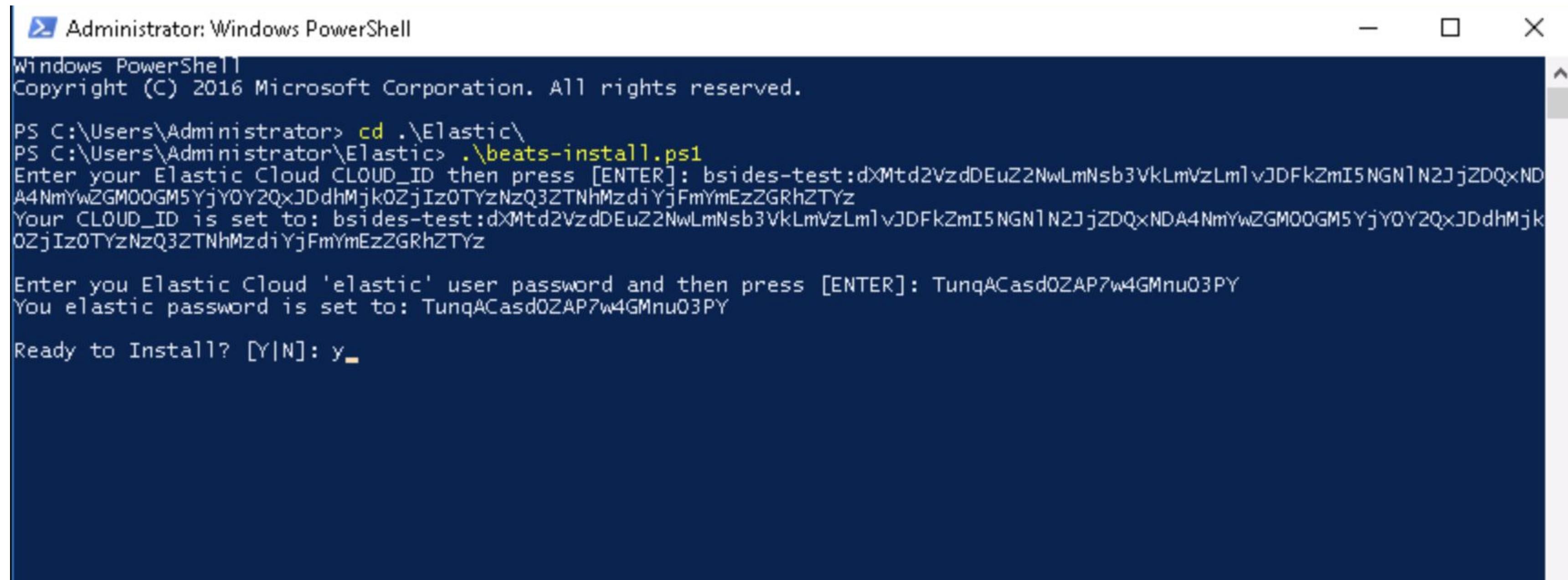
Windows Scripted Install

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



Windows Scripted Install

Winlogbeat & Metricbeat Installation



The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The window displays the following command-line session:

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

PS C:\Users\Administrator> cd .\Elastic\
PS C:\Users\Administrator\Elastic> .\beats-install.ps1
Enter your Elastic Cloud CLOUD_ID then press [ENTER]: bsides-test:dXMtD2VzdDEuZ2NwLmNsB3VkLmVzLm1vJDFkZmI5NGN1N20jZDQxND
A4NmYwZGM00GM5YjY0Y2QxDdhMjk0ZjIz0TYzNzQ3ZTNhMzdiYjFmYmEzZGRhZTYz
Your CLOUD_ID is set to: bsides-test:dXMtD2VzdDEuZ2NwLmNsB3VkLmVzLm1vJDFkZmI5NGN1N20jZDQxNDA4NmYwZGM00GM5YjY0Y2QxDdhMjk
0ZjIz0TYzNzQ3ZTNhMzdiYjFmYmEzZGRhZTYz

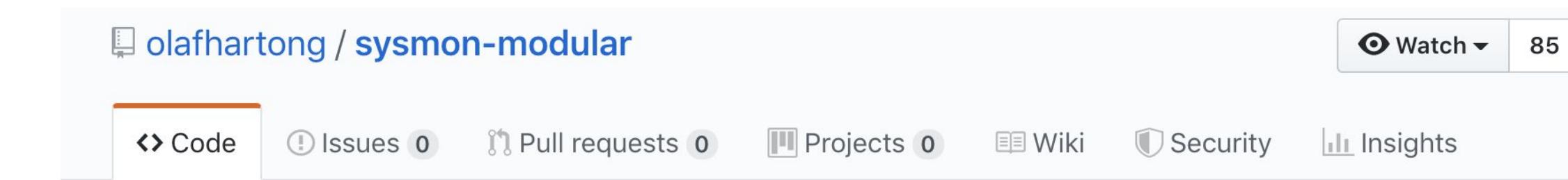
Enter your Elastic Cloud 'elastic' user password and then press [ENTER]: TunqACasd0ZAP7w4GMnu03PY
You elastic password is set to: TunqACasd0ZAP7w4GMnu03PY

Ready to Install? [Y|N]: y
```

ATT&CK™ Beats Community

ATT&CK™ configs Thanks to the community

- olafhartong / sysmon-modular



- bfuzzy / auditd-attack

A repository of sysmon configuration mappings

Branch: master ▾ New pull request

olafhartong several updates

- 10_process_access
- 11_file_create
- 12_13_14_registry_event
- 15_file_create_stream_hash
- 17_18_pipe_event
- 19_20_21_wmi_event
- 1_process_creation
- 2_file_create_time

bfuzzy auditd-attack

A Linux Auditd rule set mapped to MITRE's Attack Framework

Branch: master ▾ New pull request

olafhartong several updates

bfuzzy Commented out Ignoring SELinux IT IS bad practice

LICENSE Initial commit

README.md Update README.md

attack_map.png Updated ATT&CK Mappings

auditd-attack.rules Commented out Ignoring SELinux IT IS bad practice

base_config.rules base config

layer-2.json Updated ATT&CK Mapping

README.md

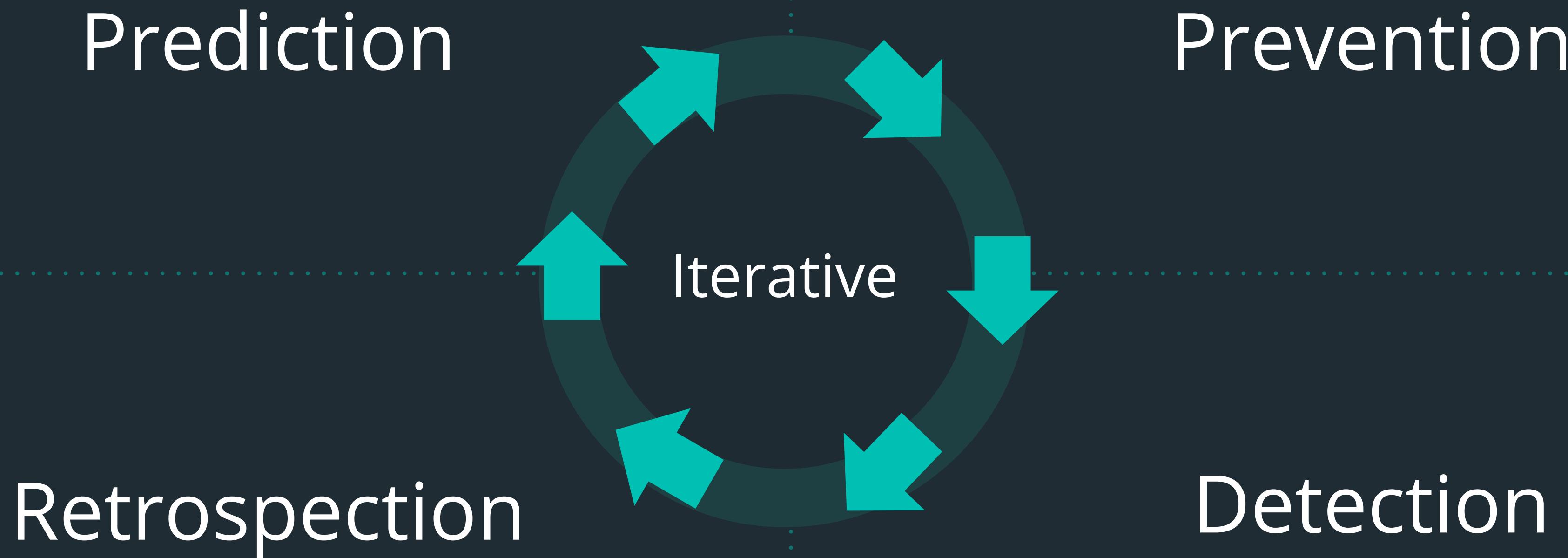
auditd-attack

A Linux Auditd rule set mapped to MITRE's Attack Framework

MITRE ATT&CK™

Overview

Prevention falls short



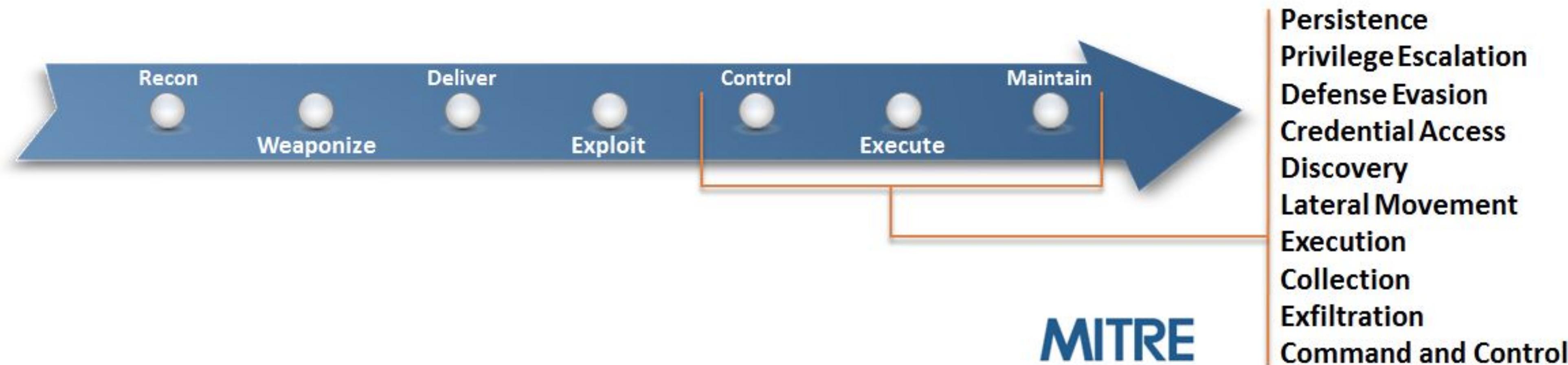
Focus on Detection



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.

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



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 perishes.

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	ApplInit 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	ApplInit 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

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

Contents [hide]

- 1 Windows
- 2 Mac and Linux
- 3 Examples
- 4 Mitigation
- 5 Detection
- 6 References

Windows

An example command that would obtain details on processes is "tasklist" using the [Tasklist](#) utility.

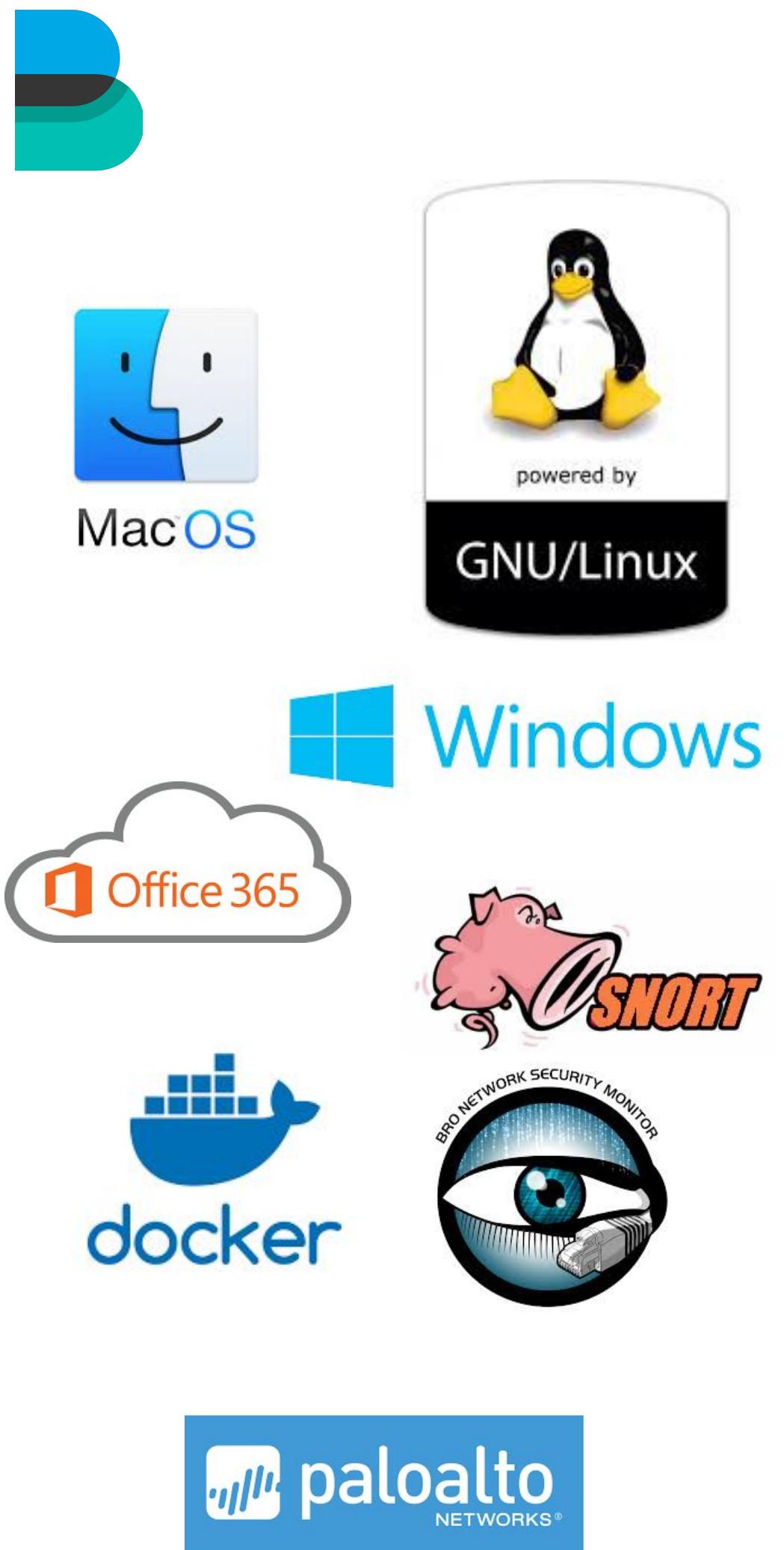
Mac and Linux

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

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

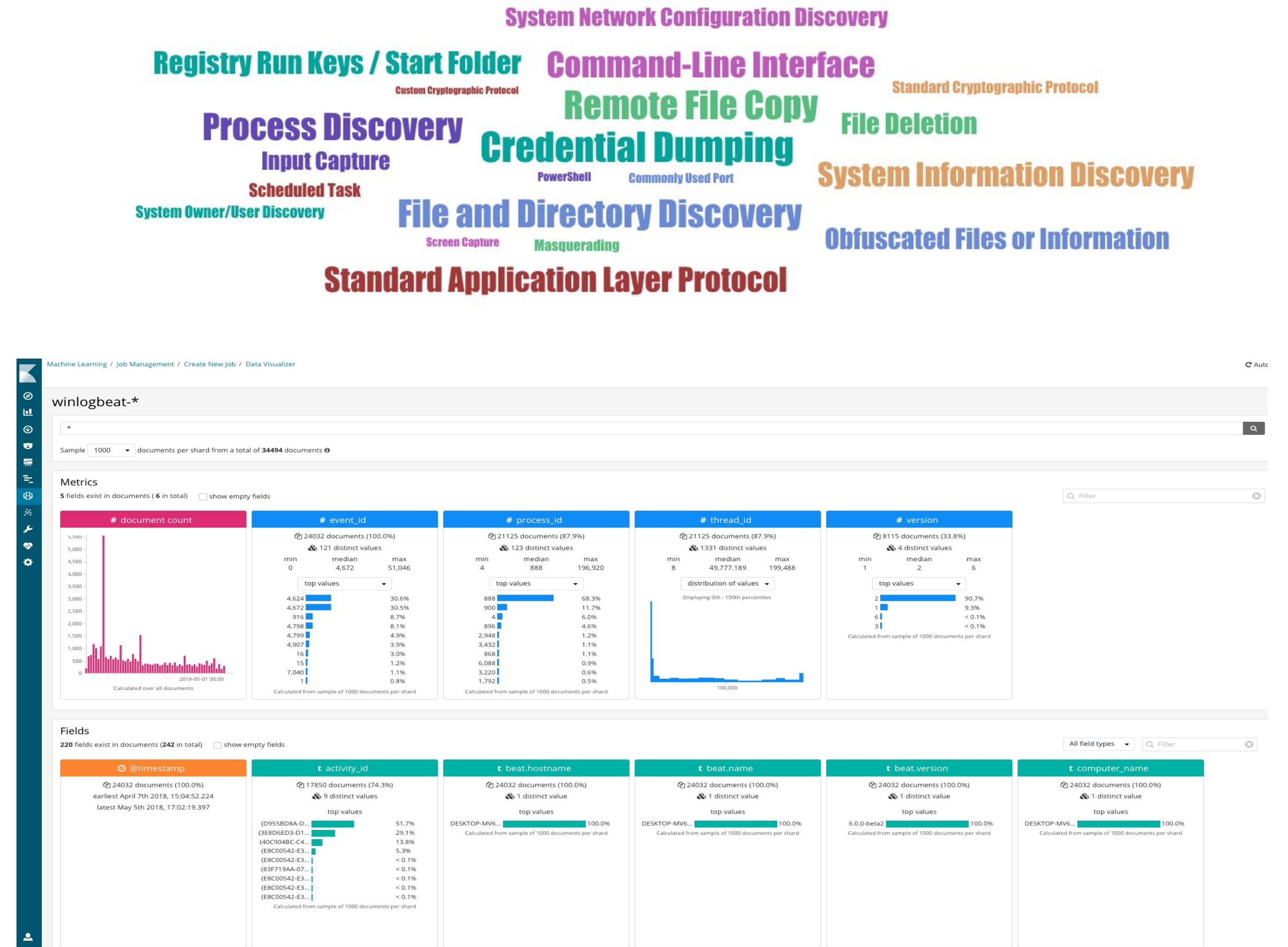
Data Quality

- 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?



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?



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

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

Lab 3

Finding MITRE ATT&CK™

TTPs

Launch Kibana from Cloud

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

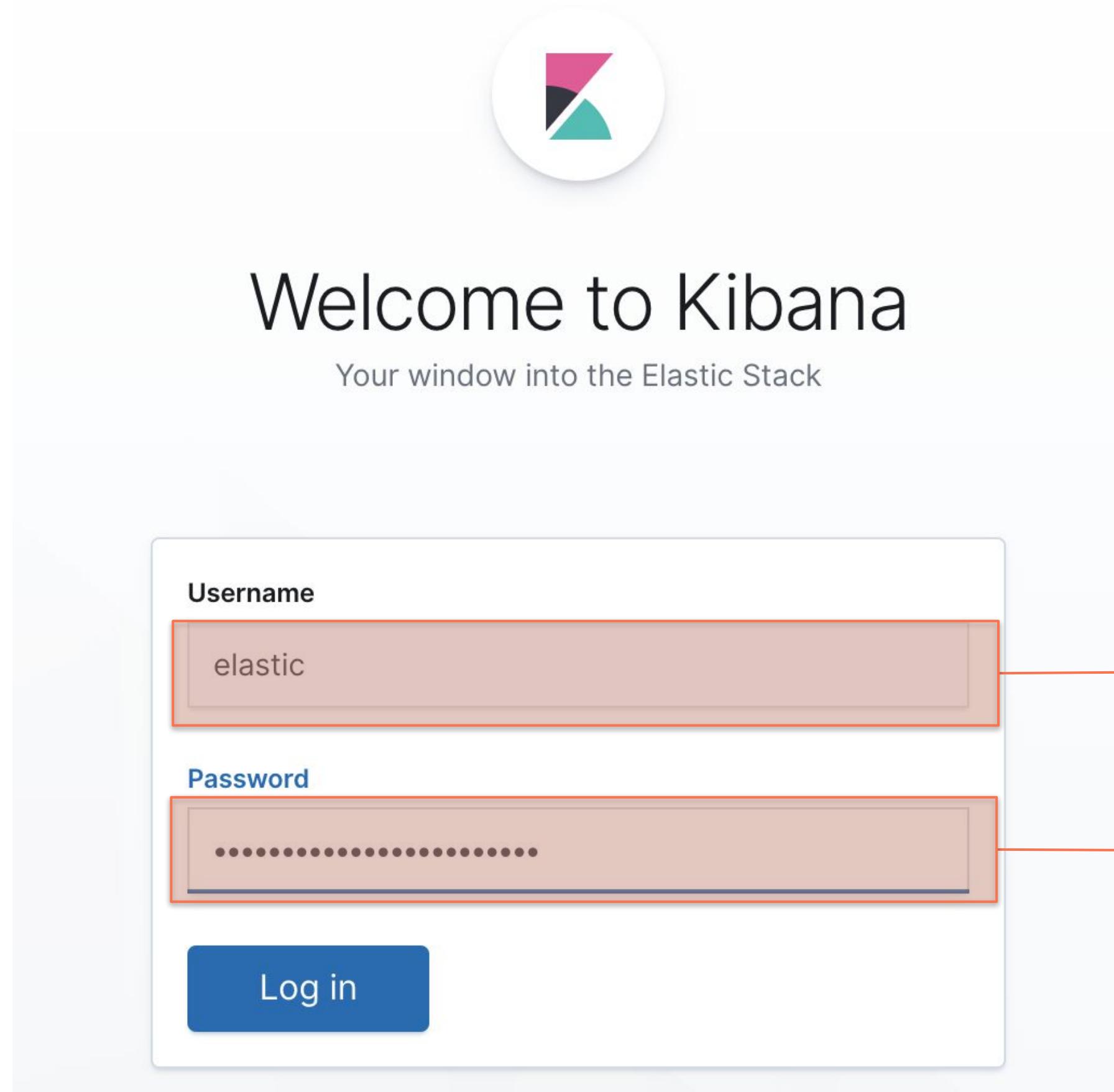
The screenshot shows the Elasticsearch Cloud interface. On the left, a sidebar lists 'Deployments', 'Custom plugins', 'Account', and 'Help'. Under 'Deployments', a 'workshop' deployment is listed with options: 'Edit', 'Elasticsearch' (with 'Logs', 'Snapshots', 'API Console'), 'Kibana' (which is highlighted with a red box), 'APM', 'Activity', 'Security', and 'Performance'. The main content area shows the 'workshop' deployment details. It includes a 'Kibana' section with the Kibana logo and the text: 'Great work! Your deployment has been created. What would like to do next?'. It offers two paths: 'Ingest and visualize data' (with a 'Launch Kibana' button) and 'Migrate existing data' (with a 'Reindex or Restore' button). At the bottom of the deployment card, there is a 'Kibana' section with a 'Launch' button and a 'Copy Endpoint URL' button, both highlighted with a red box.

1 Select Kibana under the newly created deployment.

2 Select Launch in the Kibana details.

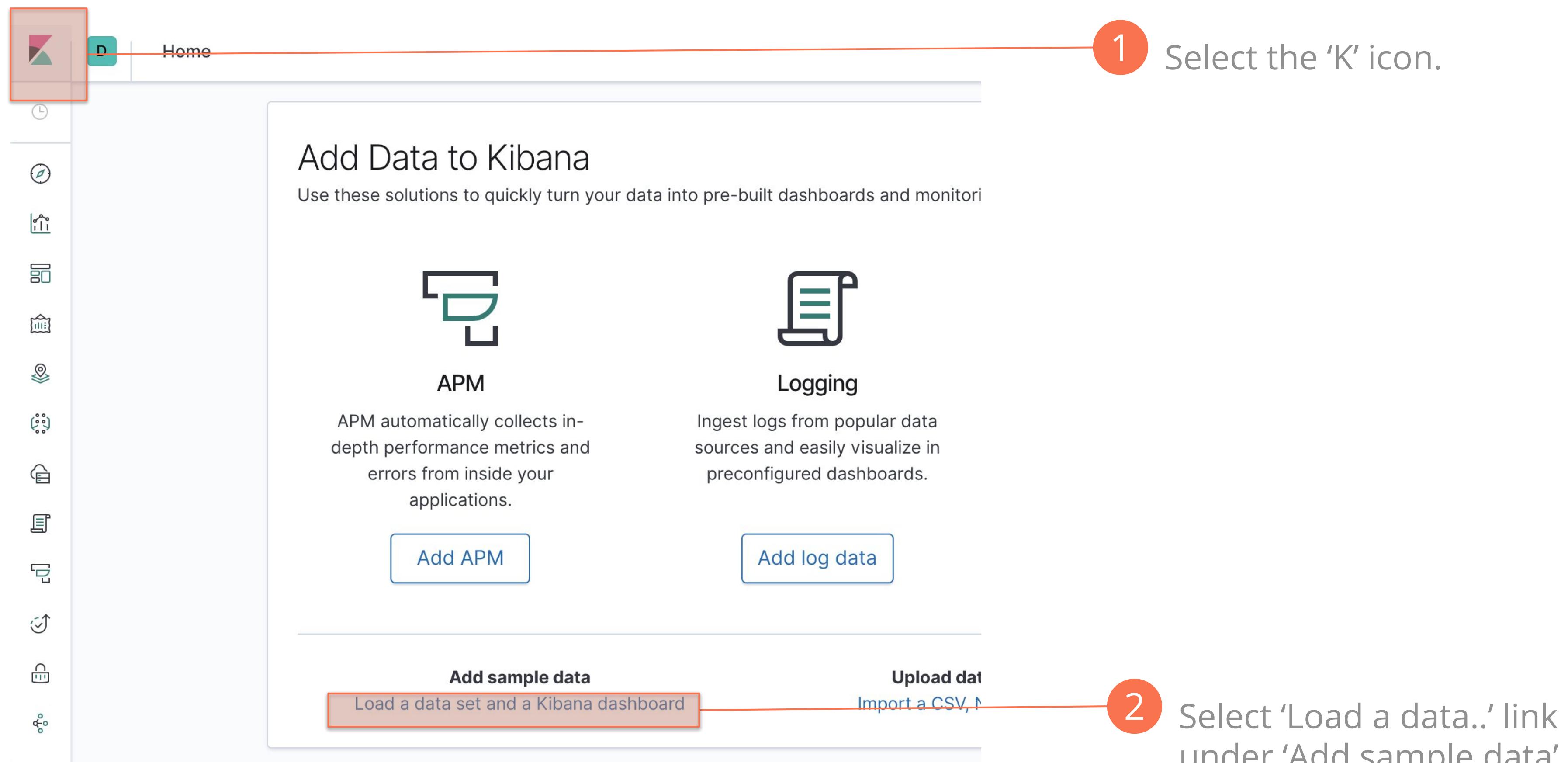
Log into Kibana

Setting Time Ranges



Load Sample Data in Kibana

Kibana load data page



Loading sample data into the Elastic Stack

Load all three data sets

Add Data to Kibana

All Logging Metrics SIEM **Sample data**

Sample eCommerce orders
Sample data, visualizations, and dashboards for tracking eCommerce orders.

Add data

Sample flight data
Sample data, visualizations, and dashboards for monitoring flight routes.

Add data

Sample web logs
Sample data, visualizations, and dashboards for monitoring web logs.

Add data

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

Navigate to Stack Monitoring

Second icon (heart) from the bottom left Navigation menu

The screenshot shows the Kibana interface for adding data. At the top, there are icons for Home and Add data. Below the Home icon is a blue square with a white heart symbol. The main area displays three sample dashboards:

- Sample eCommerce orders:** Shows a summary of sales with a gauge for "Trans / day" (139), a donut chart for "average spend" (\$75.23 per order), and a donut chart for "average items" (2.163 per order). It also includes a line chart for "Total Revenue" (\$77,638.33) and a bar chart for "Sales by Category".
- Sample flight data:** Shows a summary of flight routes with a donut chart for "origin city" (Kuala Lumpur 30%), a line chart for "Flight Count and Average Total Price" (\$596 Avg. Ticket Price), and a gauge for "Total Flights" (313). It also includes a bar chart for "Total Delays" (68) and a line chart for "Flight Delays".
- Sample web logs:** Shows a summary of web traffic with a gauge for "Unique Visitors" (801), a donut chart for "Article Type" (news 30%), and a line chart for "Response Codes over Time + Annotations". It also includes a bar chart for "Unique Pictures vs. Average Bytes" and a line chart for "File Type".

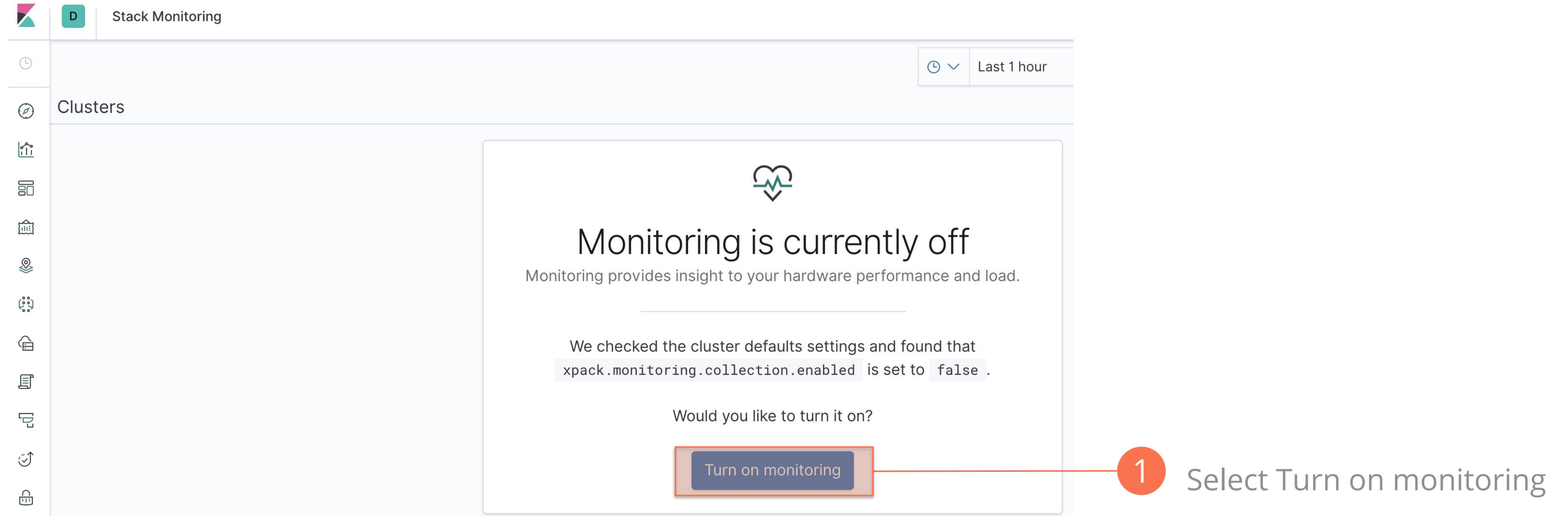
At the bottom, there is a navigation bar with icons for Home, Add data, Refresh, Settings, and a gear icon. The gear icon is highlighted with a red box. Next to it is the "Stack Monitoring" icon, which is also highlighted with a red box.

1

Select Stack Monitoring

Enable Stack Monitoring

Stack monitoring lets you understand Elastic Cloud cluster performance



Ensure your Beats agents are online

After a few minutes, you should see 6 beats enabled

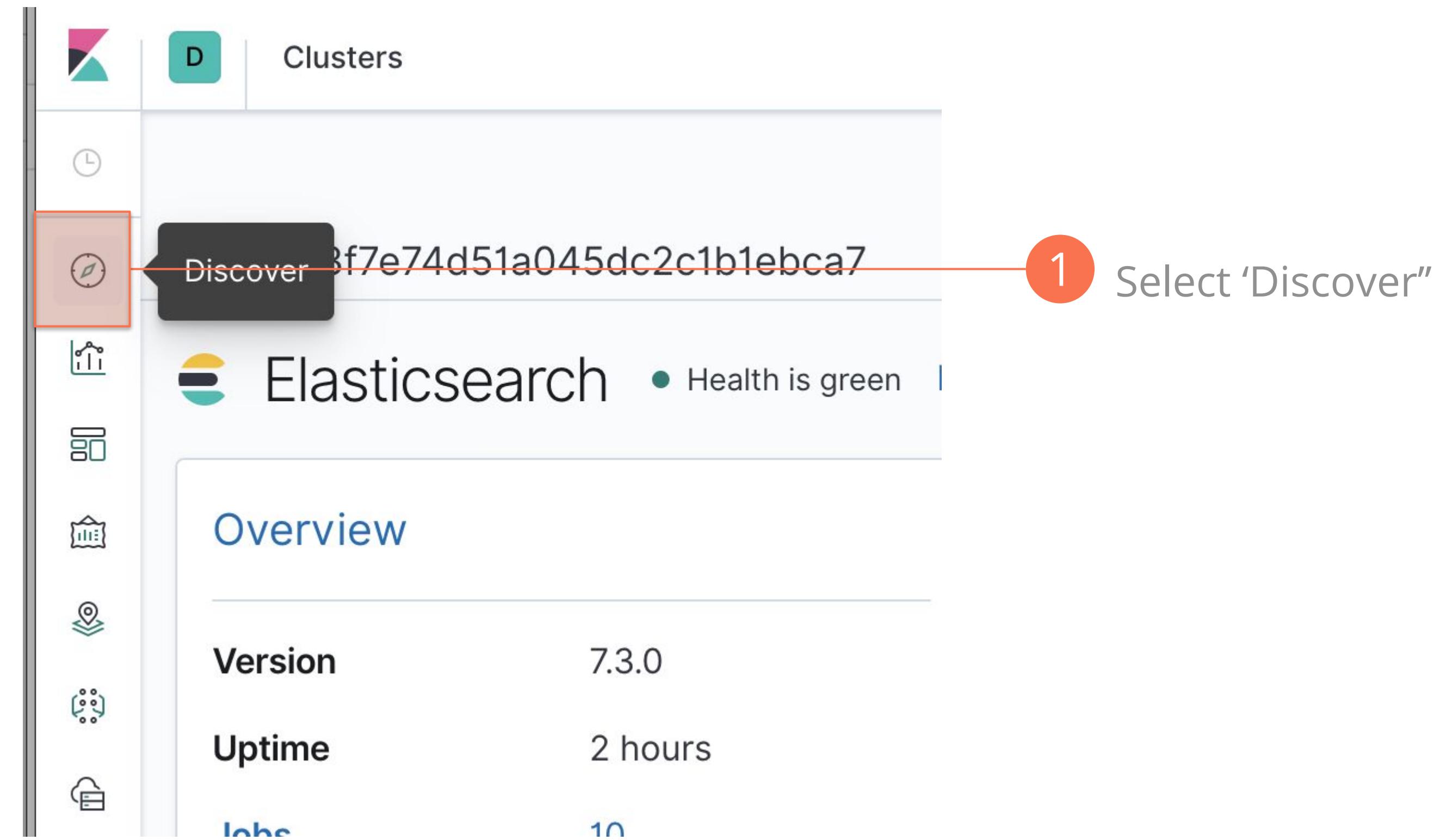
The screenshot shows the Elasticsearch dashboard with the following sections:

- Clusters**: Shows a single cluster with a green health status. Overview details: Version 7.3.0, Uptime 2 hours, Jobs 10. Node statistics: Disk Available 99.78% (243.5 GB / 244.0 GB), JVM Heap 31.47% (1.6 GB / 4.9 GB).
- Kibana**: Shows a green health status. Overview details: Requests 4, Max. Response Time 3 ms. Instance statistics: Connections 16, Memory Usage 37.10% (313.9 MB / 846.0 MB).
- Beats**: Shows a green health status. Overview details: Total Events 23.9k, Bytes Sent 49.5 MB. Beat instance statistics:
 - Beats: 6 (highlighted with a red box)
 - Metricbeat: 2
 - Filebeat: 1
 - Auditbeat: 1
 - Packetbeat: 1
 - Winlogbeat: 1
- APM**: Shows a green health status. Overview details: Processed Events 0, Last Event 1 seconds ago. APM Server statistics: APM Servers: 1, Memory Usage.

1 Six Beats should be enabled

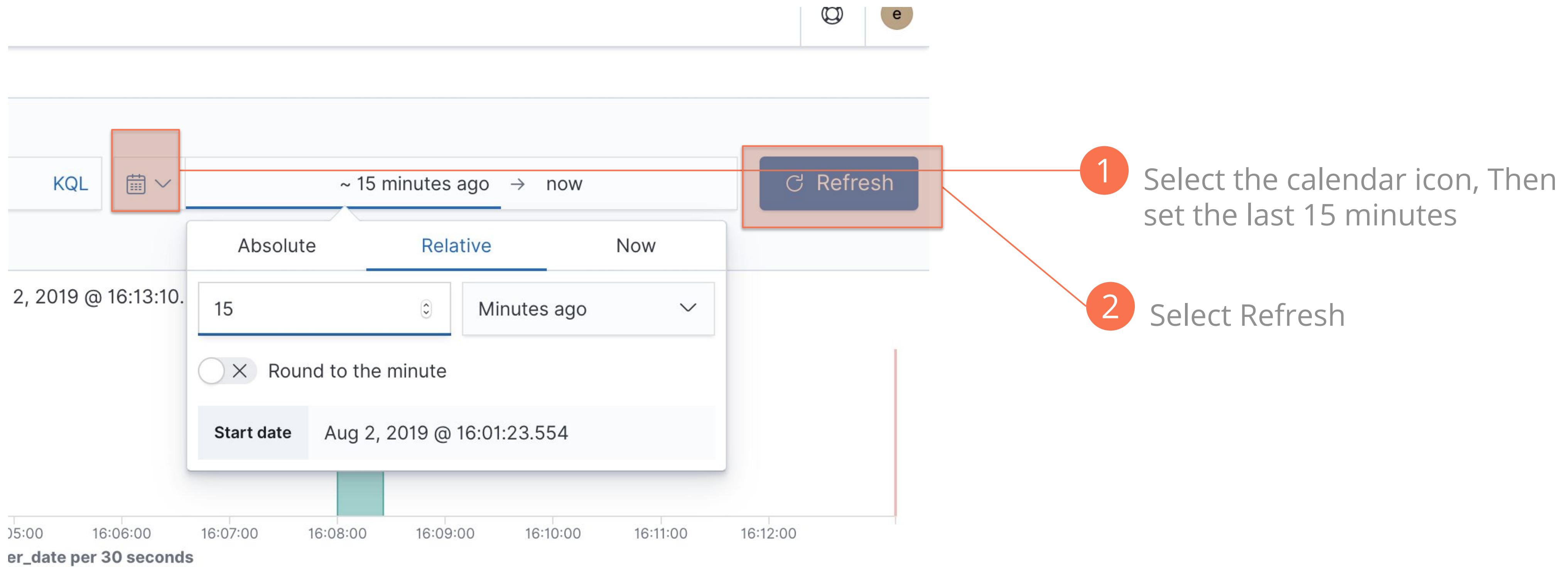
Move to the Discover app

Discovering what is in the data



Setting the time range

Ensure kibana is set to the last 15 minutes



Select the index

Kibana has multiple indices, select auditbeat

The screenshot shows the Kibana Discover App interface. On the left, there's a sidebar with icons for location, chart, file, and cloud. The main area shows two search results:

- Discover**: Shows 2 hits. The index dropdown menu is open, with the 'Selected fields' section highlighted by a red box. A red circle labeled '1' points to the 'Selected fields' section.
- Discover**: Shows 8 hits. The 'Selected fields' section is also highlighted by a red box. A red circle labeled '1' points to this section as well.

In the bottom right, there's a histogram with 'Count' on the y-axis (0, 1, 2, 3, 4) and a teal square icon.

Selected fields (highlighted by red box):

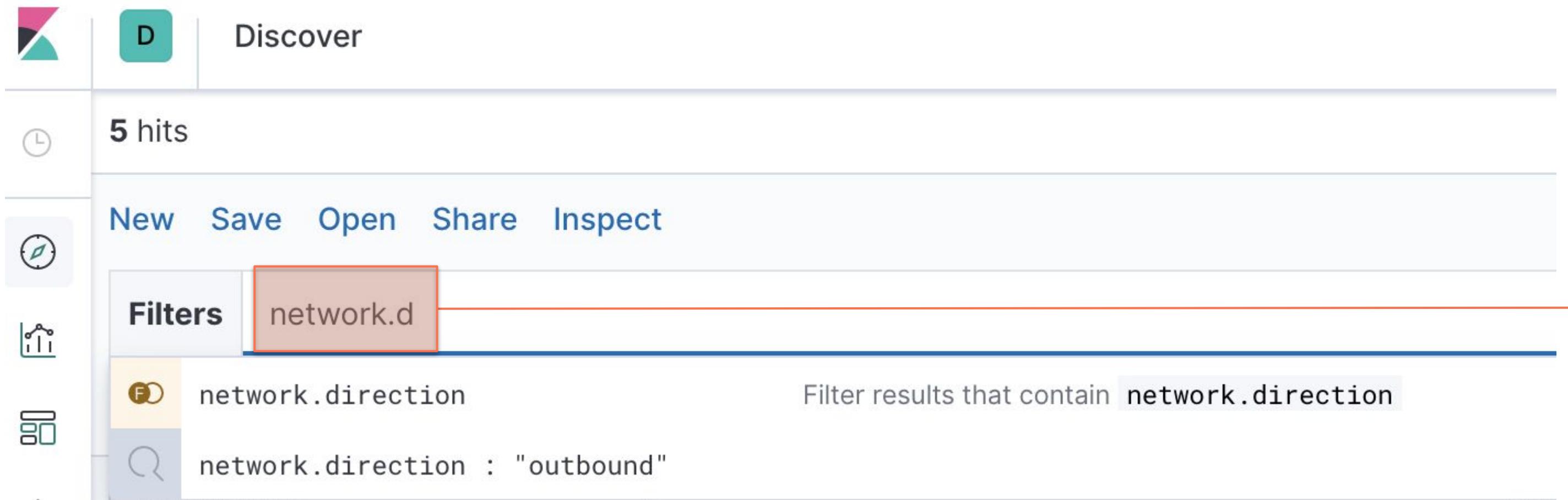
- ? _source
- auditbeat-*** (highlighted by red box)
- filebeat-*
- kibana_sample_data_ecommerce
- kibana_sample_data_flights

Select the Index drop down
menu under 'Filter' in the
Discovery App

Select 'auditbeat'

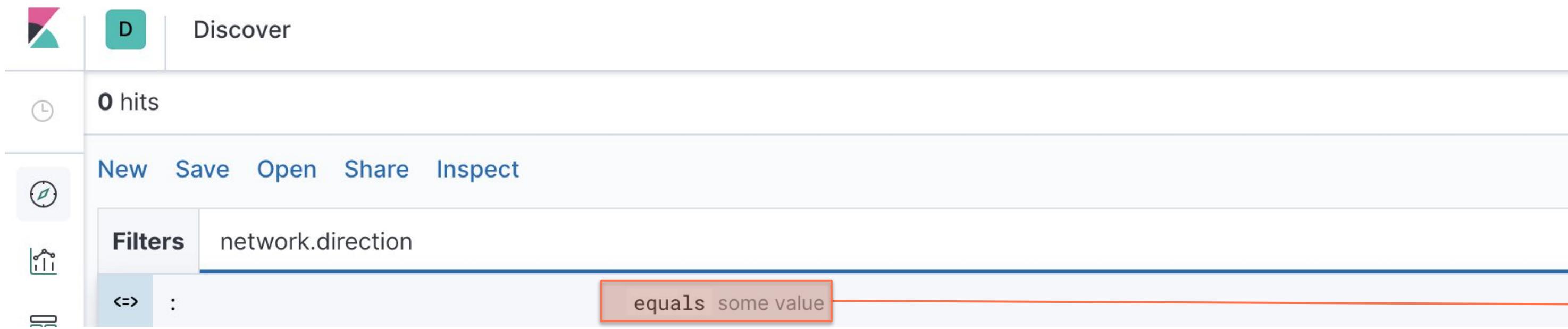
Search with KQL in Kibana

The default way to search



This screenshot shows the Kibana Discover interface. At the top, there's a navigation bar with a Kibana icon, a teal 'Discover' button, and a blue 'D' button. Below the navigation is a header with a clock icon and the text '5 hits'. Underneath is a toolbar with 'New', 'Save', 'Open', 'Share', and 'Inspect' buttons. On the far left is a sidebar with icons for 'Discover', 'Dashboard', 'Visualize', and 'Logs'. The main area is titled 'Filters' and contains a dropdown menu with 'network.d' selected. A tooltip below the dropdown says 'Filter results that contain network.direction'. Below the dropdown are two other filter options: 'network.direction' and 'network.direction : "outbound"'. The entire 'Filters' section is highlighted with a red box.

- 1 Type 'network.d' and select network.direction from the drop down menu



This screenshot shows the Kibana Discover interface again. The top navigation bar and sidebar are identical to the first screenshot. The main area is titled 'Filters' and contains a dropdown menu with 'network.direction' selected. Below the dropdown is a field with a colon ':'. A tooltip above the colon says 'equals some value'. The entire 'Filters' section is highlighted with a red box.

- 2 Select 'equals some value'

Search with KQL in Kibana

search with autocomplete

The screenshot shows two stacked Kibana Discover interfaces.

Top Interface:

- Header: Discover
- Search bar: network.direction :|
- Filters section:
 - "outbound"
 - "inbound"** (highlighted with a red box)
 - "listening"
- Result count: 0 hits

Bottom Interface:

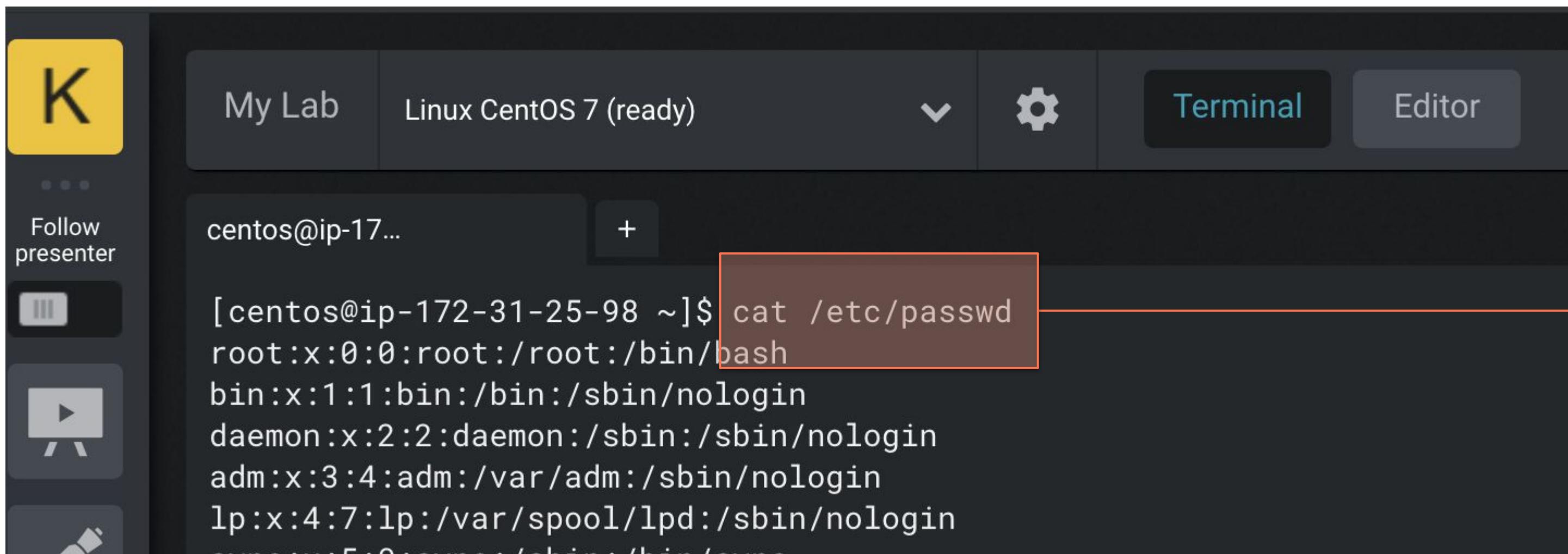
- Header: Discover
- Search bar: network.direction : "inbound" (highlighted with a red box)
- Filters section:
 - + Add filter
- Result count: 5 hits
- Selected fields: auditbeat-*
- Available fields: @timestamp
- Selected field details: _source
- Visualizations: A histogram showing Count vs. time, with a single bin at approximately 1.5.

Annotations:

- 1 Select 'inbound'
- 2 Results are filtered for inbound

ATT&CK Technique T1078 Valid Accounts

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



The screenshot shows a terminal window titled "My Lab" with the subtitle "Linux CentOS 7 (ready)". The terminal interface includes a sidebar with icons for "Follow presenter", "Screenshot", "Video", and "Note". The main terminal area displays the command "cat /etc/passwd" being run by a user named "centos". The output of the command is shown in a red box:

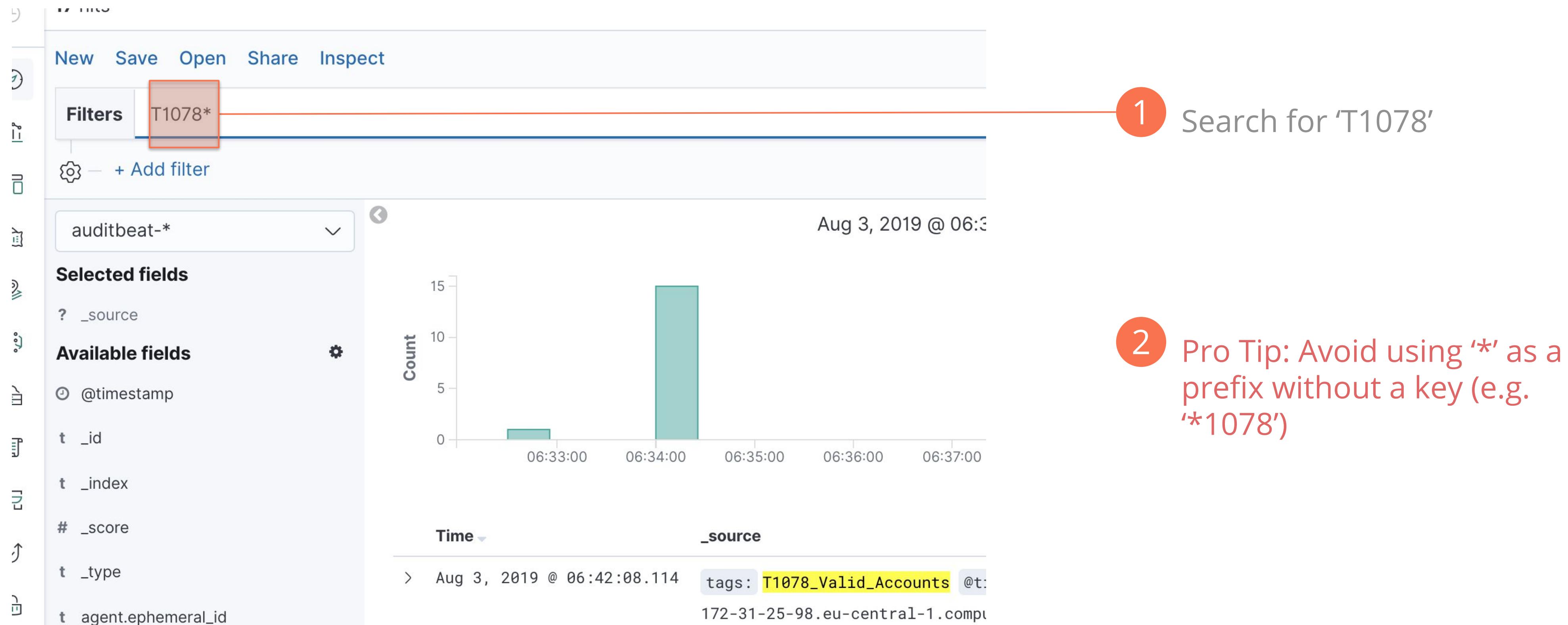
```
[centos@ip-172-31-25-98 ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin

```

- 1 Type 'cat /etc/passwd' in the terminal

Find T1078 events

Search using wildcards



Inspect an event

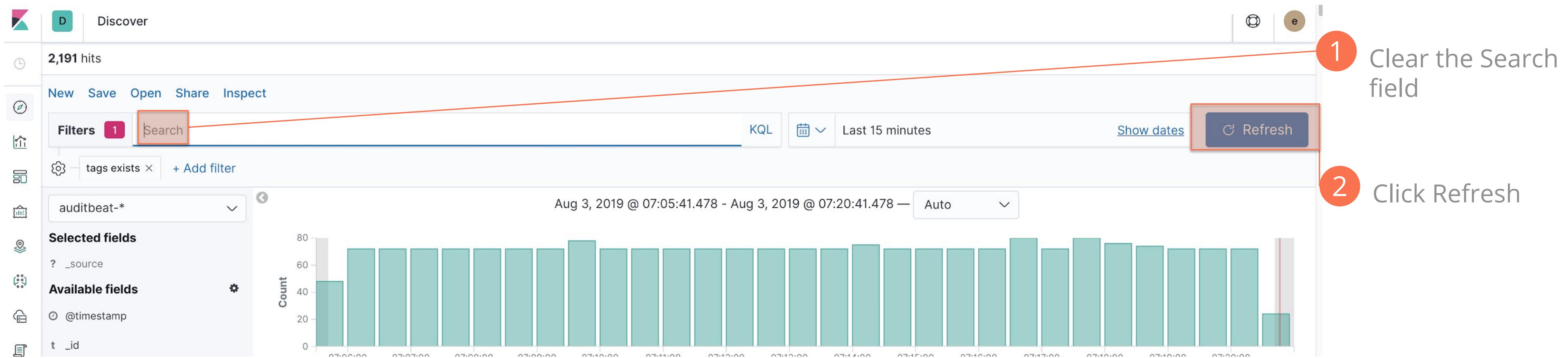
review the fields in an event, filter on 'contains tag'

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

- Select the star icon to filter for events that contain the 'tags' field

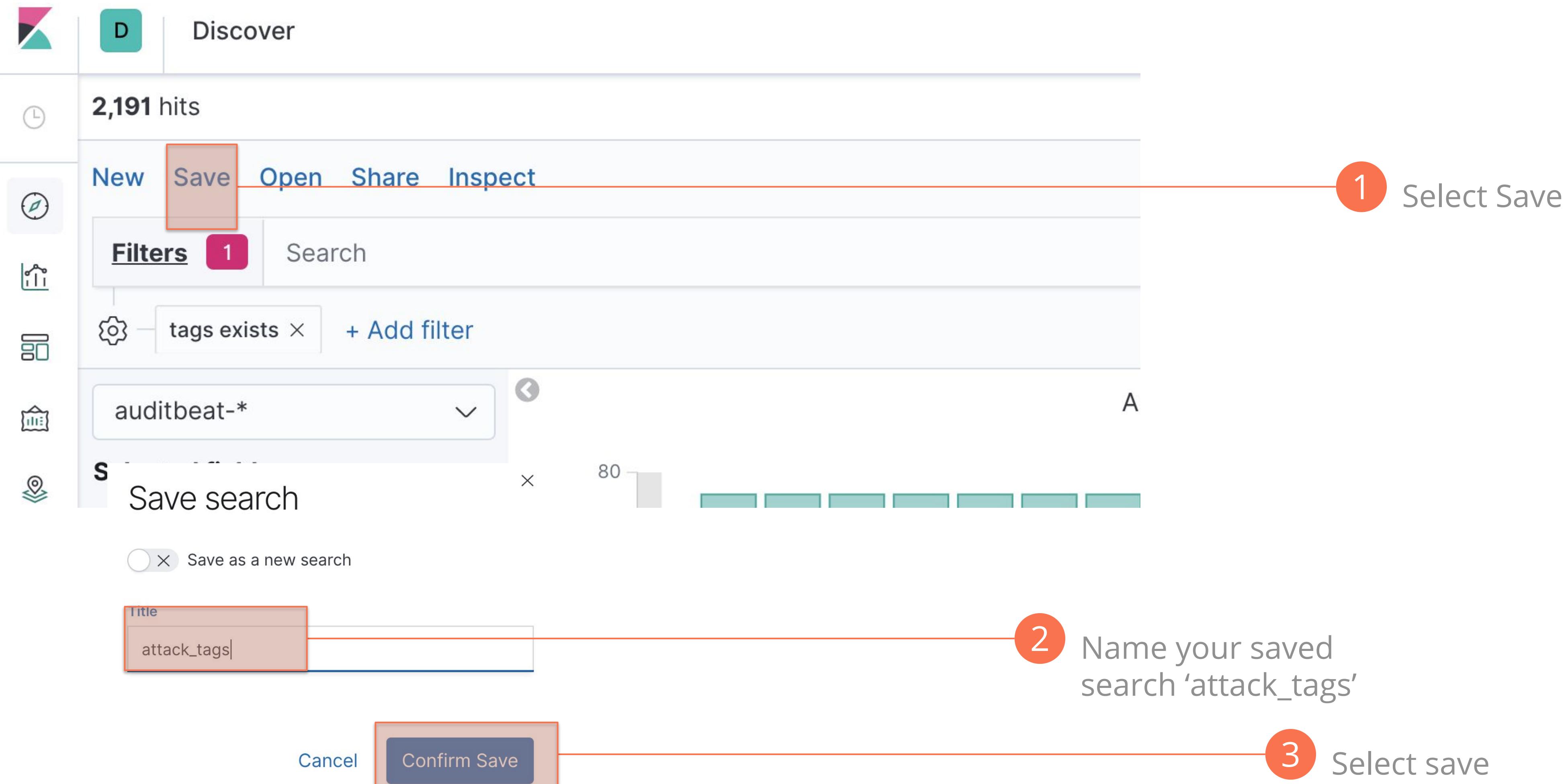
Apply tag exists filter

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



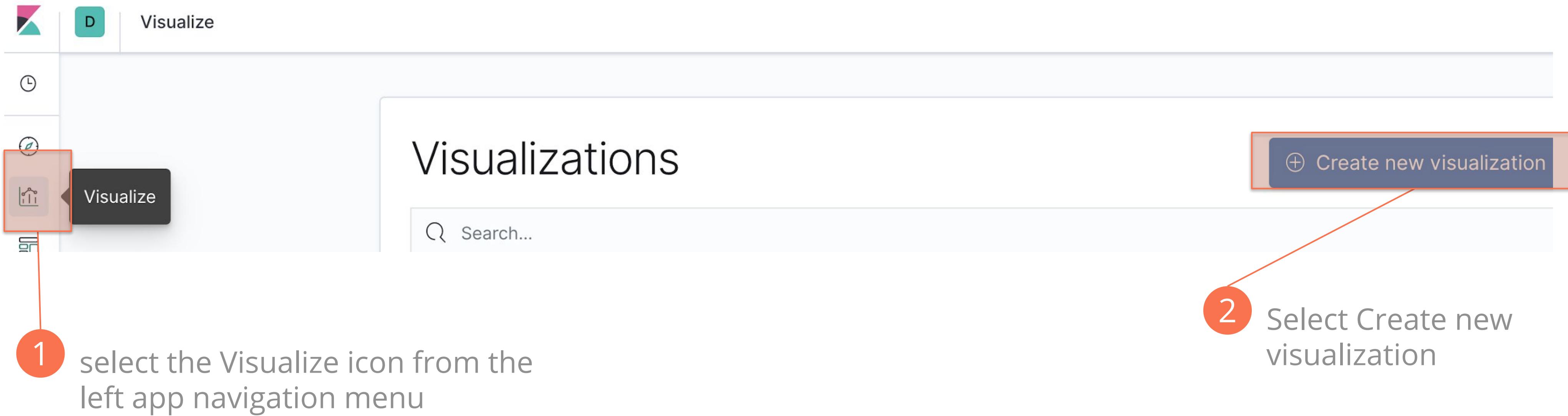
Create a saved search

save your tags filter for reuse



Start creating a new visualization

create a new visualization in the Visualize Kibana app



Create a new data table visualization

reuse your 'attack_tags' saved search

New Visualization

The screenshot shows the Kibana interface for creating a new visualization. At the top left is a filter bar with a magnifying glass icon and the word "Filter". Below it is a row of visualization icons: Area, Controls (selected), Coordinate Map, Data Table (highlighted with a red box), Gauge, Goal, Heat Map, and Horizontal Bar. To the right of these is a description of the selected "Data Table" visualization: "Display values in a table". A red line with a numbered callout "1" points from the "Data Table" icon to the text "Select the Data Table icon". Below this is a modal window titled "New Data Table / Choose a source". It contains a search bar with the text "attac" and a dropdown menu with the option "attack_tags" highlighted with a red box. A red line with a numbered callout "2" points from the "attack_tags" option to the text "Type 'attac' and select 'attack_tags'".

Filter

Data Table
Display values in a table

1 Select the Data Table icon

Area Controls Coordinate Map Data Table Gauge Goal Heat Map Horizontal Bar

2 Type 'attac' and select 'attack_tags'

New Data Table / Choose a source

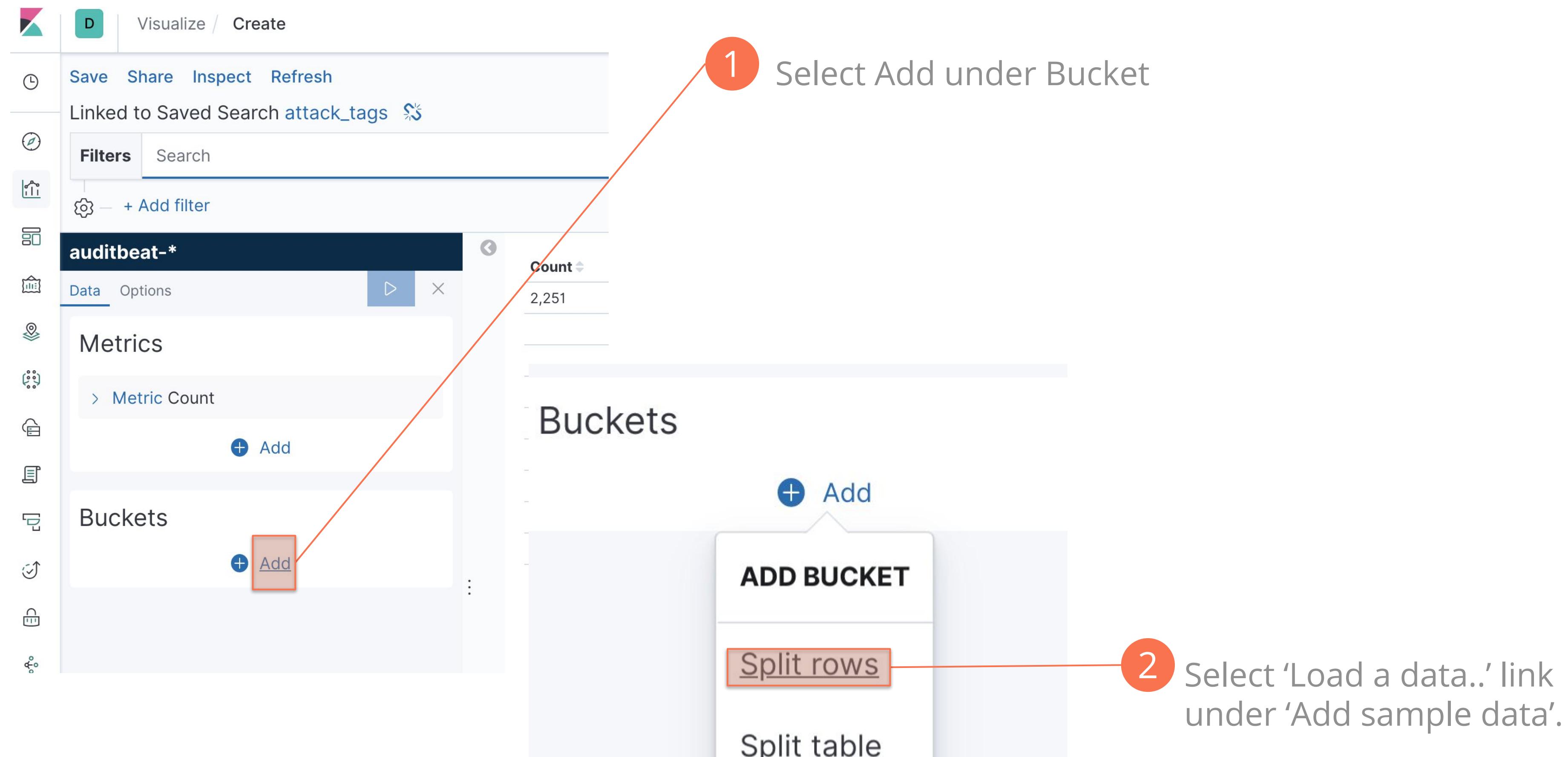
Sort ▾ Types 2 ▾

attac

attack_tags

Editing Data Table

split rows



Editing Data Table

use terms

The screenshot shows the 'Buckets' section of the Elasticsearch interface. Under 'Aggregation', a dropdown menu is open with the placeholder 'Select an aggregation'. Below the dropdown, a list of aggregation types is shown: Geohash, Geotile, Histogram, IPv4 Range, Range, Significant Terms, and Terms. The 'Terms' option is highlighted with a red box and has a red line pointing to it from the number 1.

1 Select the Terms Aggregation

This screenshot shows the 'Field' selection step. A search bar at the top contains the text 'tag'. Below the search bar, a list of fields is displayed: string, container.image.tag, and tags. The 'tags' option is highlighted with a red box and has a red line pointing to it from the number 2.

2 Type 'tags' and select it for Aggregation Field

This screenshot shows the 'Size' configuration step. It includes an 'Order' section with 'Descending' selected and a 'Size' input field set to '10'. The 'Size' input field is highlighted with a red box and has a red line pointing to it from the number 3.

3 Set the display Size to 10

See your updated data table visualization

apply you changes

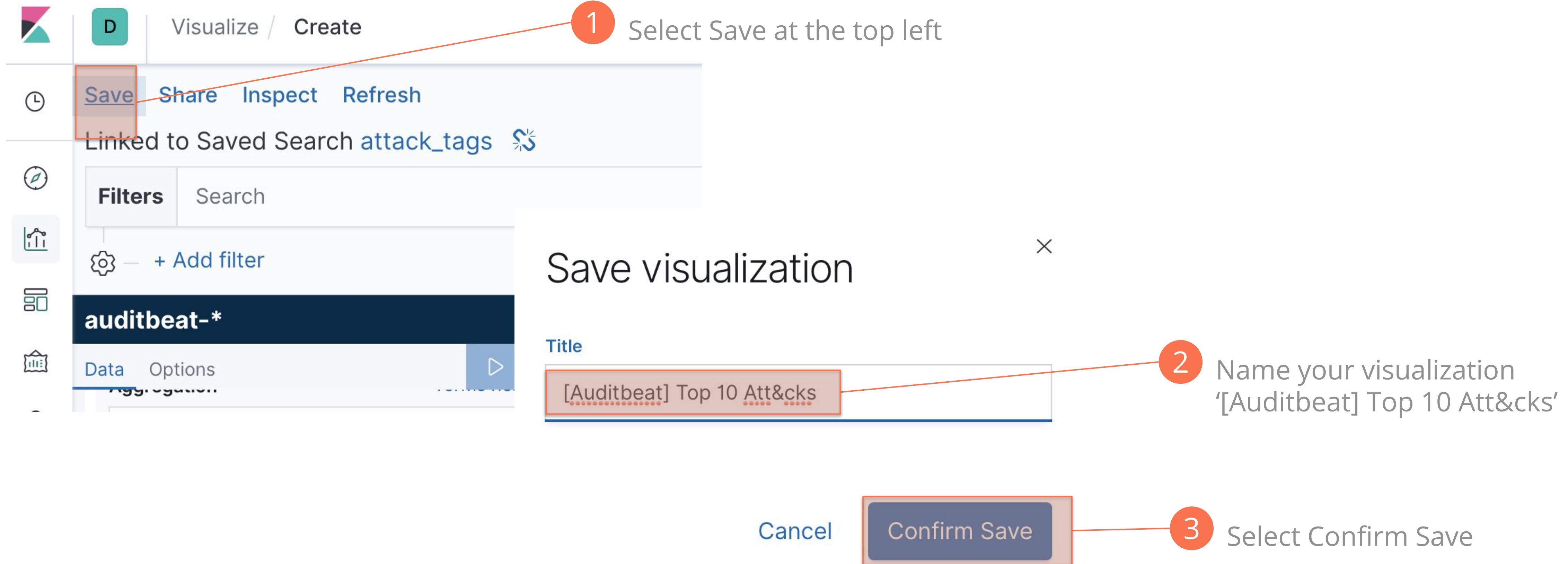
The screenshot shows the Kibana interface with a search bar at the top containing the query "auditbeat-*". Below the search bar, there are two tabs: "Data" (which is selected) and "Options". Under the "Data" tab, there are sections for "Terms", "Field", and "tags". The "tags" section has a dropdown menu with an "Apply changes" button, which is highlighted with a red box and circled with a red arrow labeled "1". To the right of this, there is a data table titled "tags: Descending". The table has a header row with "Count" and a descending arrow. The data rows are:

	Count
T1156_bash_profile_and_bashrc	1,434
T1043_Commonly_Used_Port	564
T1081_Credentials_In_Files	179
T1078_Valid_Accounts	33
T1016_System_Network_Configuration_Discovery	8
T1166_Seuuid_and_Setgid	7

A red arrow labeled "2" points from the "Count" column header to the first data row.

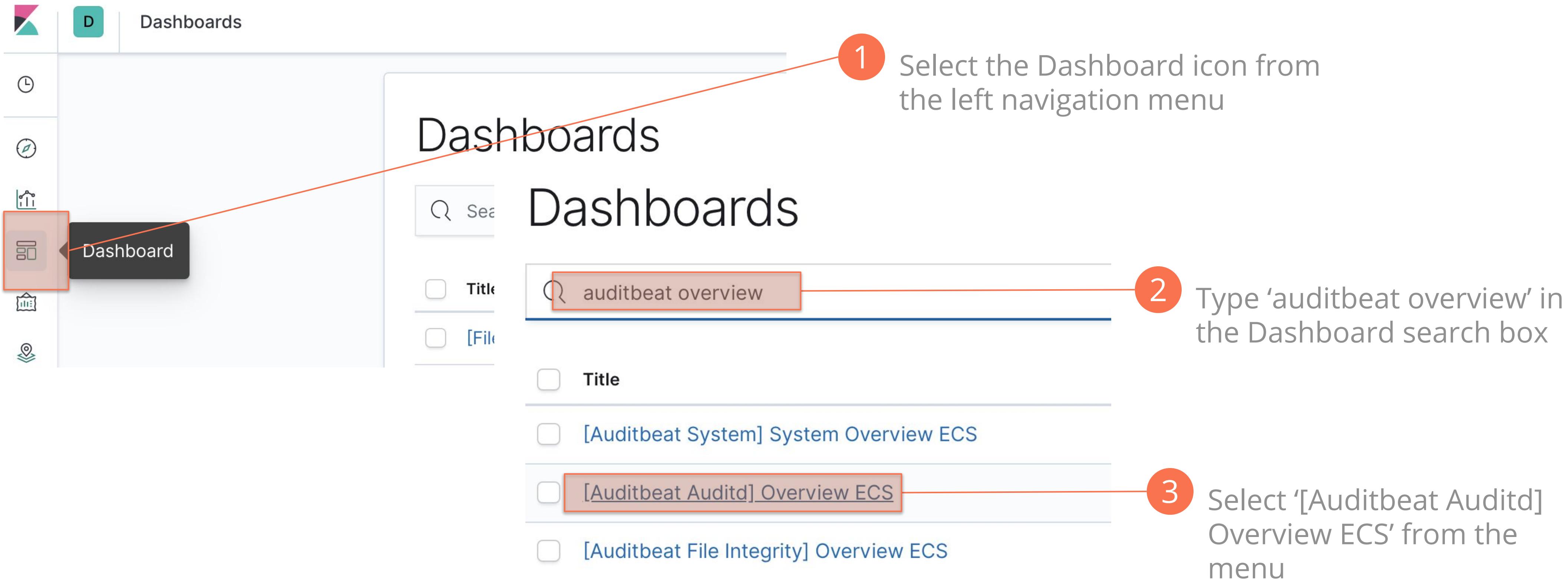
Save your visualization

Save your visualization for reuse



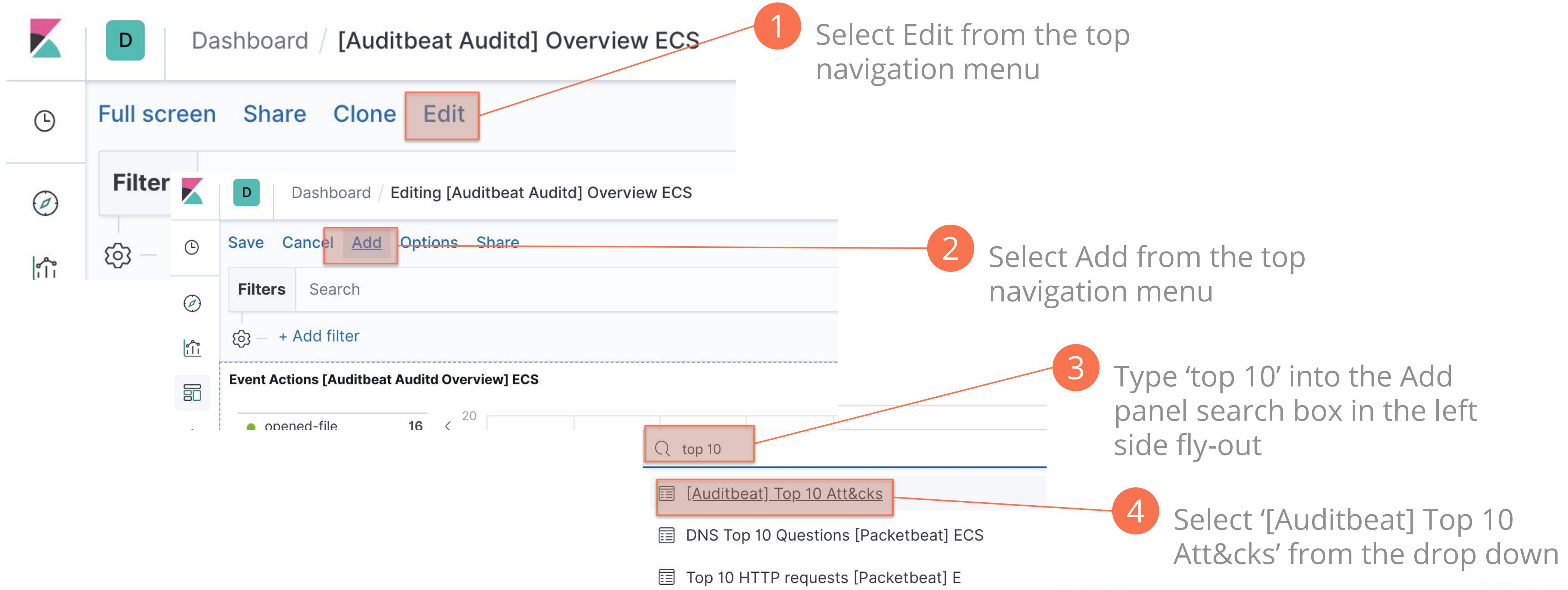
Add visualization to Auditbeat Overview

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



Add visualization to Auditbeat Overview dashboard

finish adding visualization



1 Select Edit from the top navigation menu

2 Select Add from the top navigation menu

3 Type 'top 10' into the Add panel search box in the left side fly-out

4 Select '[Auditbeat] Top 10 Att&cks' from the drop down

✓ [Auditbeat] Top 10 Att&cks (Data Table) was added to your dashboard

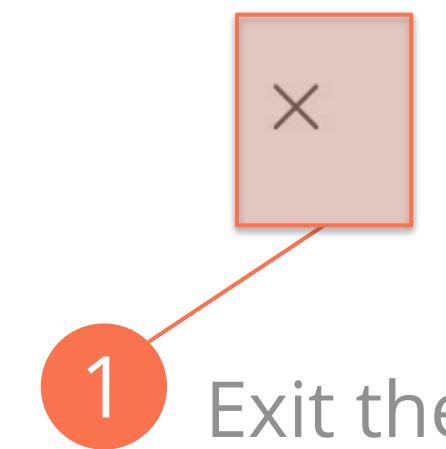
Load Sample Data in Kibana

Kibana load data page

Add panels

The screenshot shows the Kibana Load Data page. On the left, there is a sidebar with various icons for file operations like upload, download, and search. The main area displays a table of audit log entries. The first three rows show log entries from Aug 3, 2019, at 08:40:14.364, 08:40:14.363, and 08:40:14.363 respectively. The fourth row is highlighted with a red border and contains the title "[Auditbeat] Top 10 Att&cks". This row is part of a fly-out panel that includes a title bar with a close button and a table showing the top 10 attack types with their counts. The table data is as follows:

tags: Descending	Count
T1156_bash_profile_and_bashrc	1,442
T1043_Commonly_Used_Port	554
T1081_Credentials_In_Files	180
T1078_Valid_Accounts	15
T1099_Timestamp	3
T1166_Setuid_and_Setgid	1



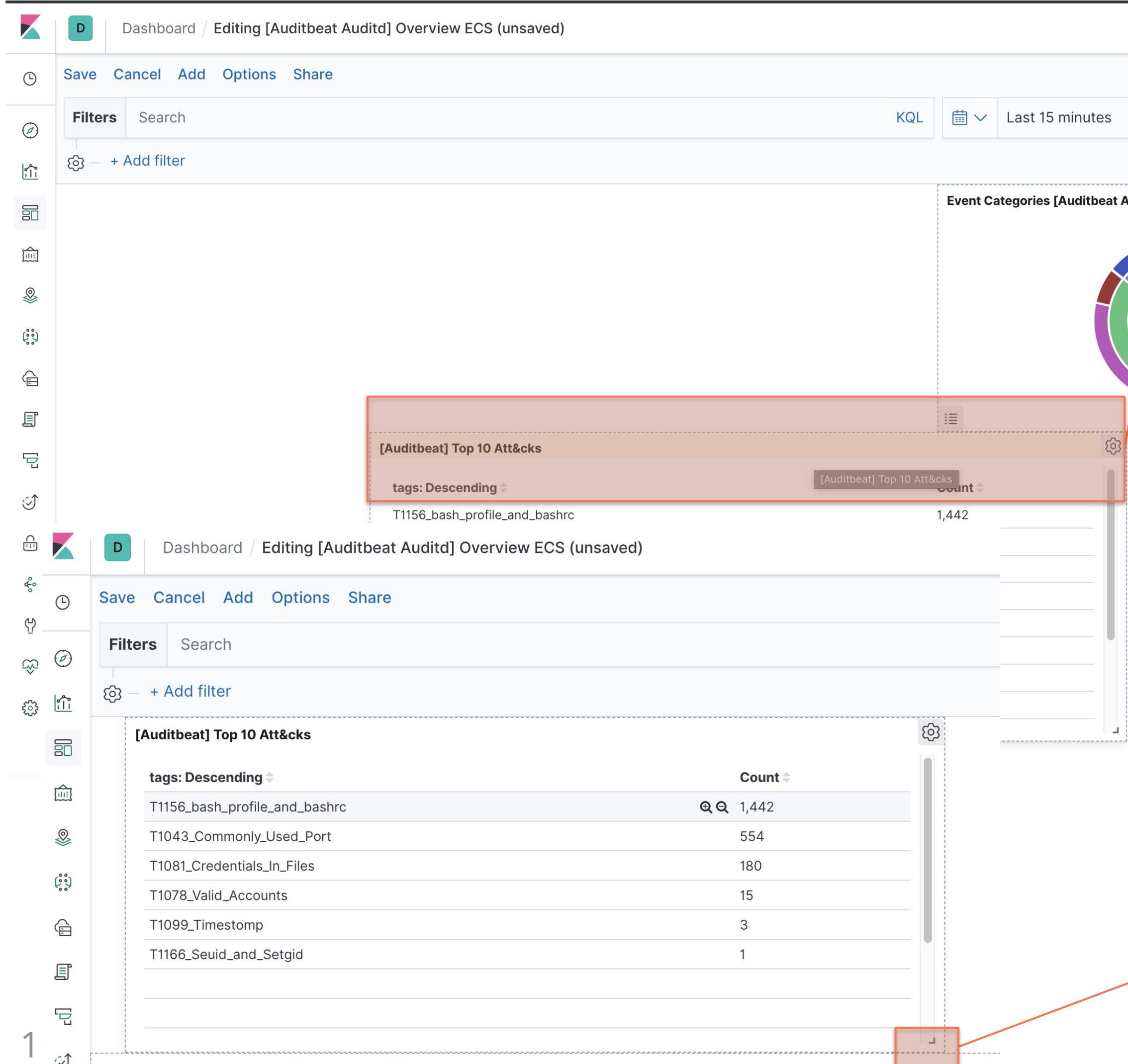
1 Exit the Add Panel fly-out



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

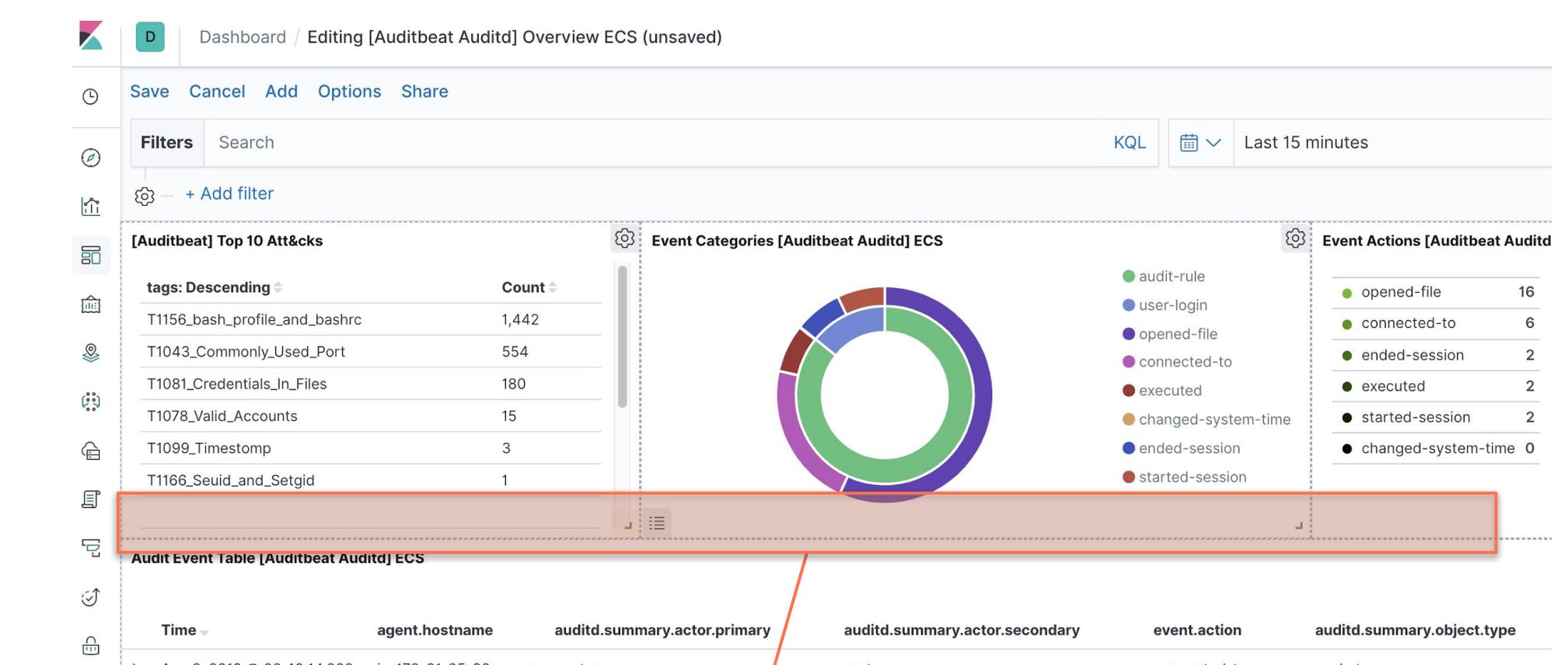
Reshaping the dashboard

changing the layout of a dashboard



1

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



3

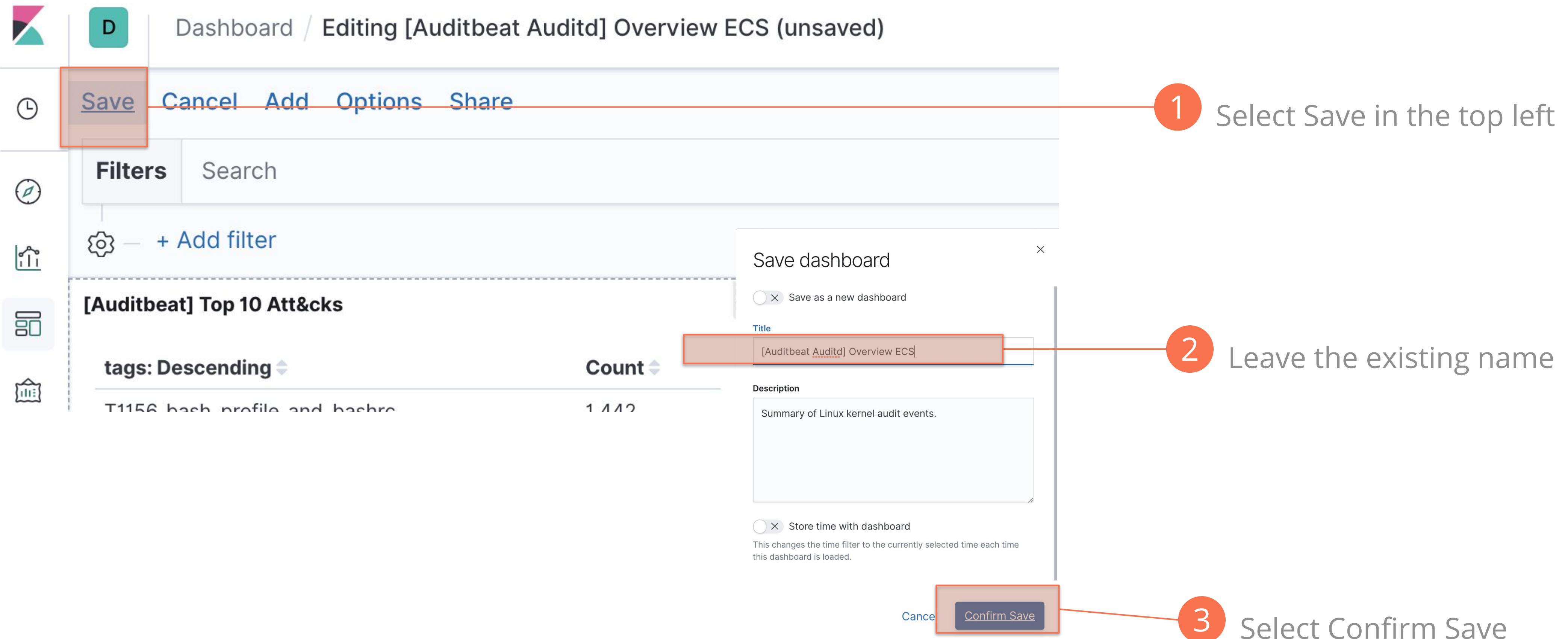
Resize other visualizations to better fit the screen

2

Resize the panel using the lower right resize arrow

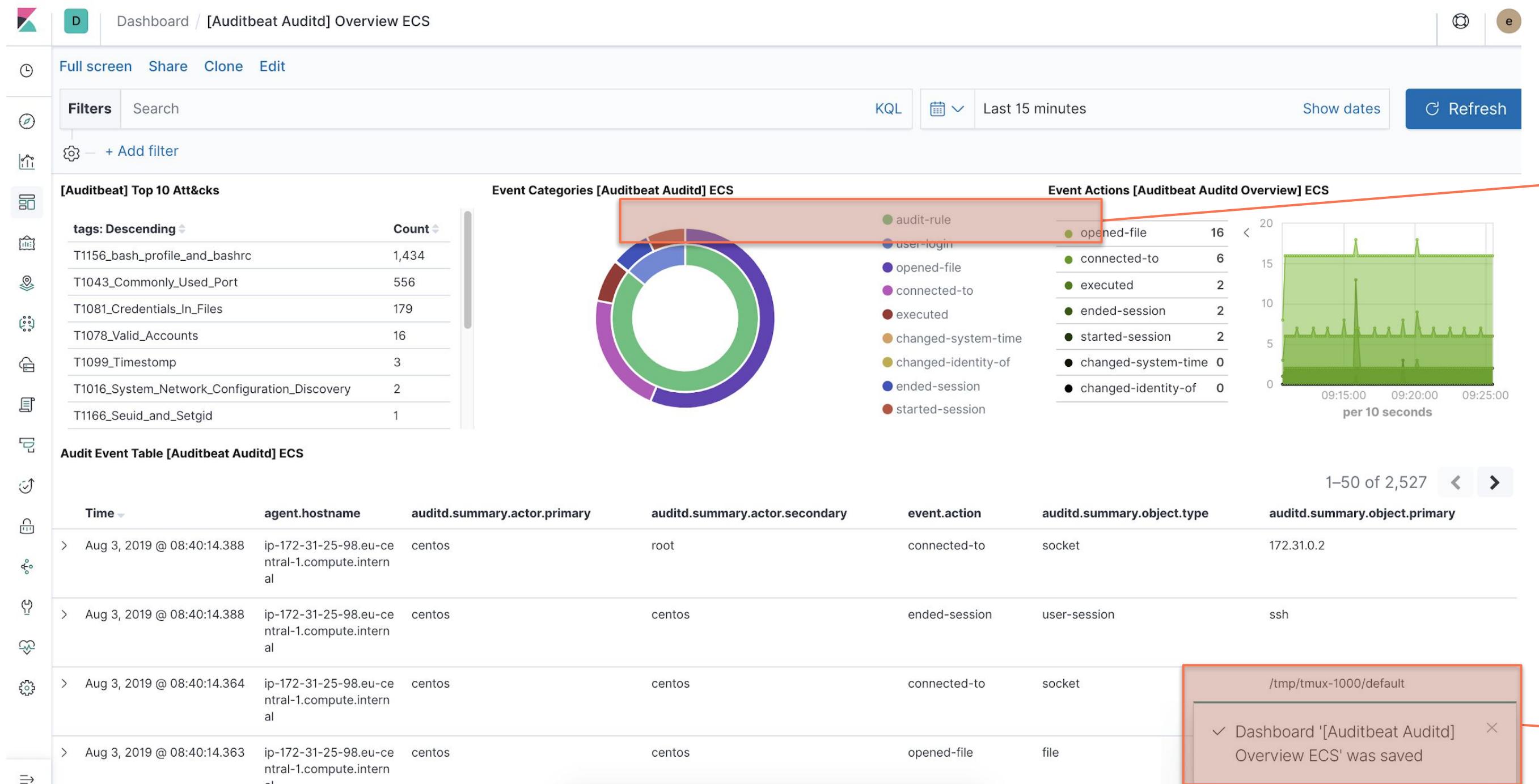
Save your updated dashboard

Top 10 attacks added to Auditbeat Overview



Play time

click around with '+' to filter data instantly

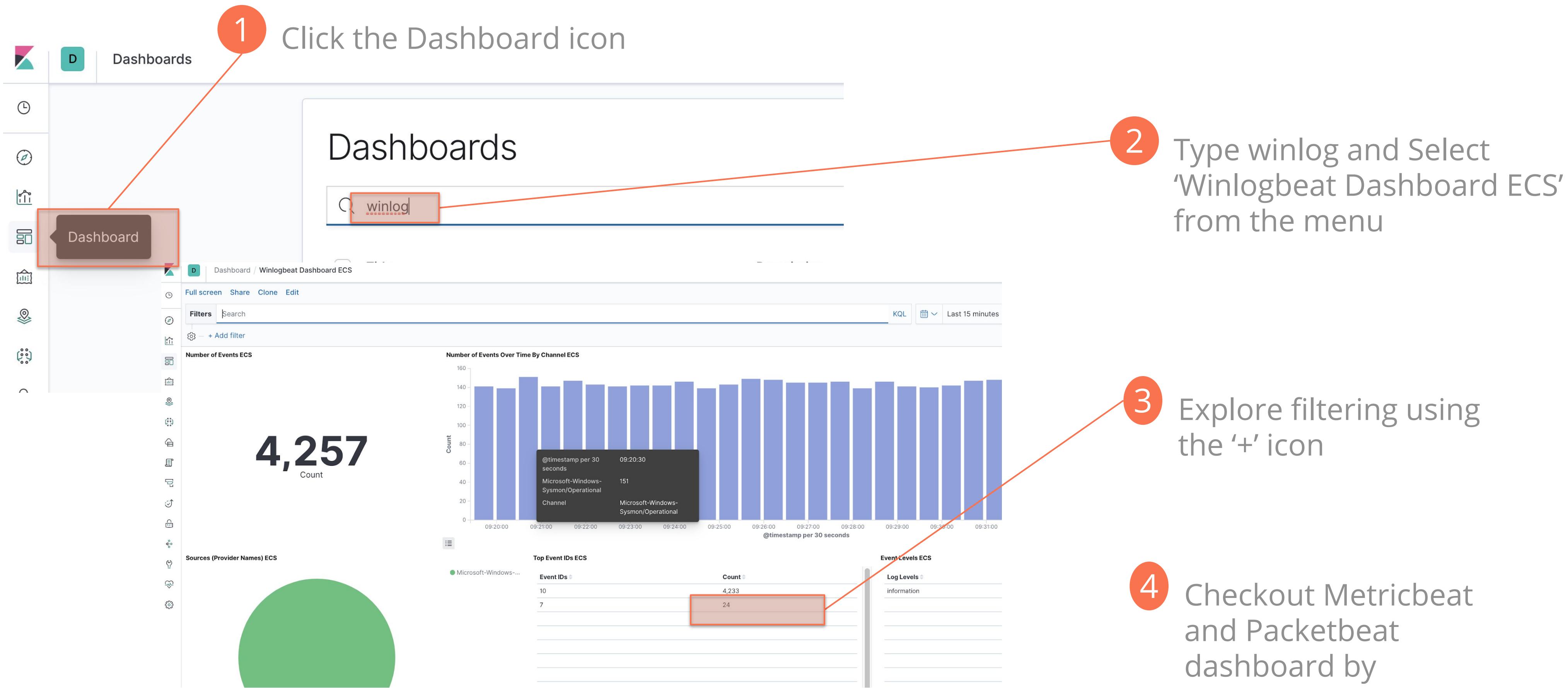


2 Select the '+' icon to create filters automatically

1 A saved tool tip should appear

Other Dashboards

click around with '+' to filter data instantly



ML Demo



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

Introducing Elastic SIEM

The screenshot shows the Elastic SIEM interface. At the top, there's a navigation bar with icons for Overview, Hosts (which is selected), Network, and Timelines. Below the navigation is a search bar and some date range controls. The main area is titled "Hosts" and displays three cards: "Hosts 904", "Hosts 10,633 Success / 33 Fail", and "Hosts 1,165 Source / 985 Destination". A modal window is open in the center, titled "Untitled Timeline". It contains an OR query builder with the condition "host.name: 'siem-es'". Below it is a search bar with the query "event.action:'config_change' and event.dataset:'file'". At the bottom of the modal, there's a table with fields: @timestamp, event.severity, event.category, event.action, and host.name. A specific event is highlighted: "Jun 3, 2019 @ 19:40:15.160" with fields audit-rule, executed, and siem-es. The event details show: Session # unset, user root, host siem-es, command executed, route is table local type local scope host dev eth0 proto 66 with result success.

SIEM App Targets SOC Analysts, Investigators



SOC Analyst

Don't spend days looking at alerts created by rules when only a few alerts matter



SOC Investigator

Metron enables massive amounts of data to identify and triage anomalies



SOC Manager

Automatically create incidents/cases with integrated workflow systems



Forensic Investigator

"Just in time evidence collection response" transforms data in real-time



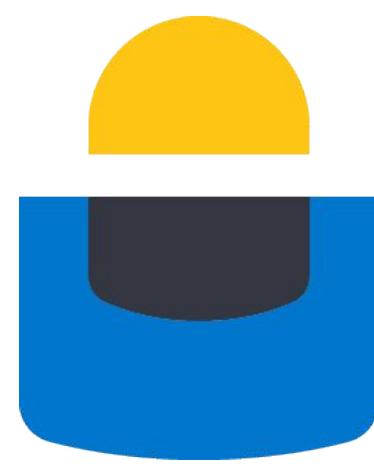
Security Platform Engineer

Single platform to manage and operate the ingestion, processing of cyber data



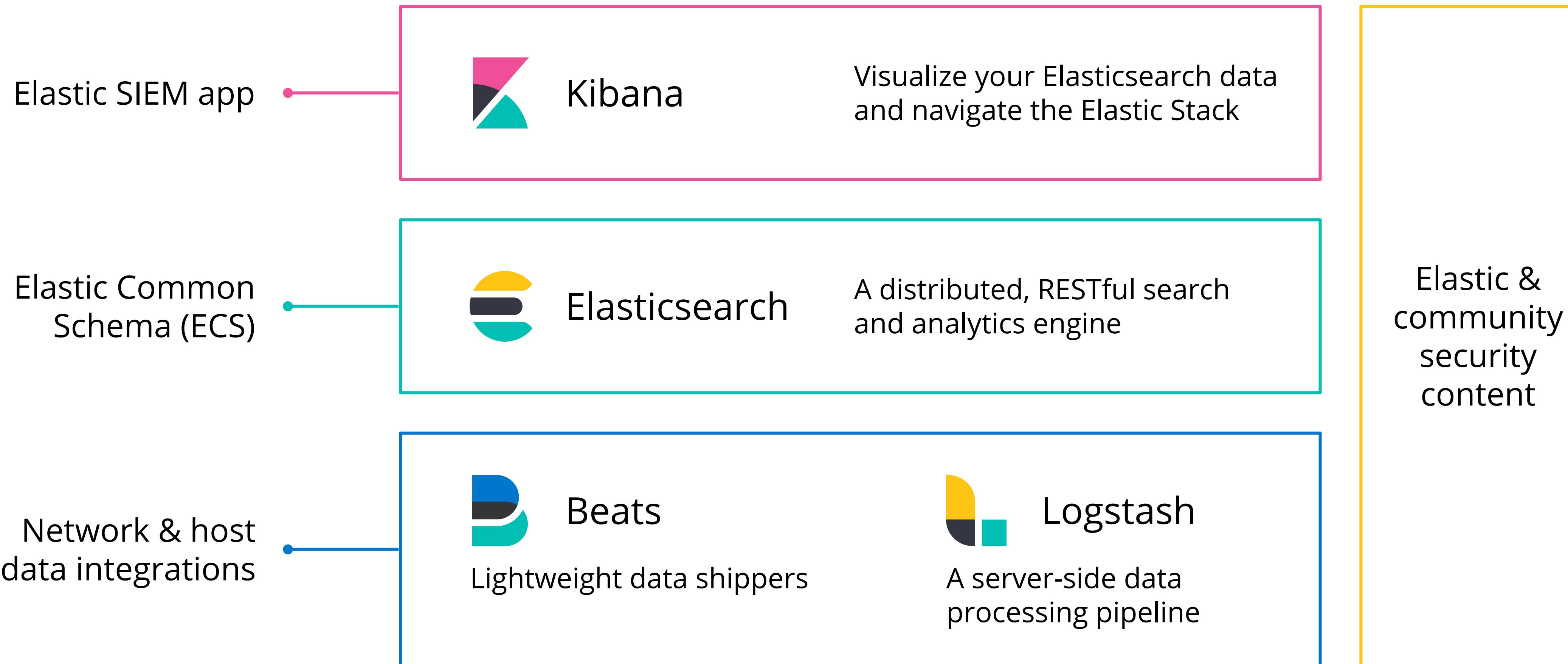
Security Data Scientist

Perform data science lifecycle activities, train, evaluate and score analytical models

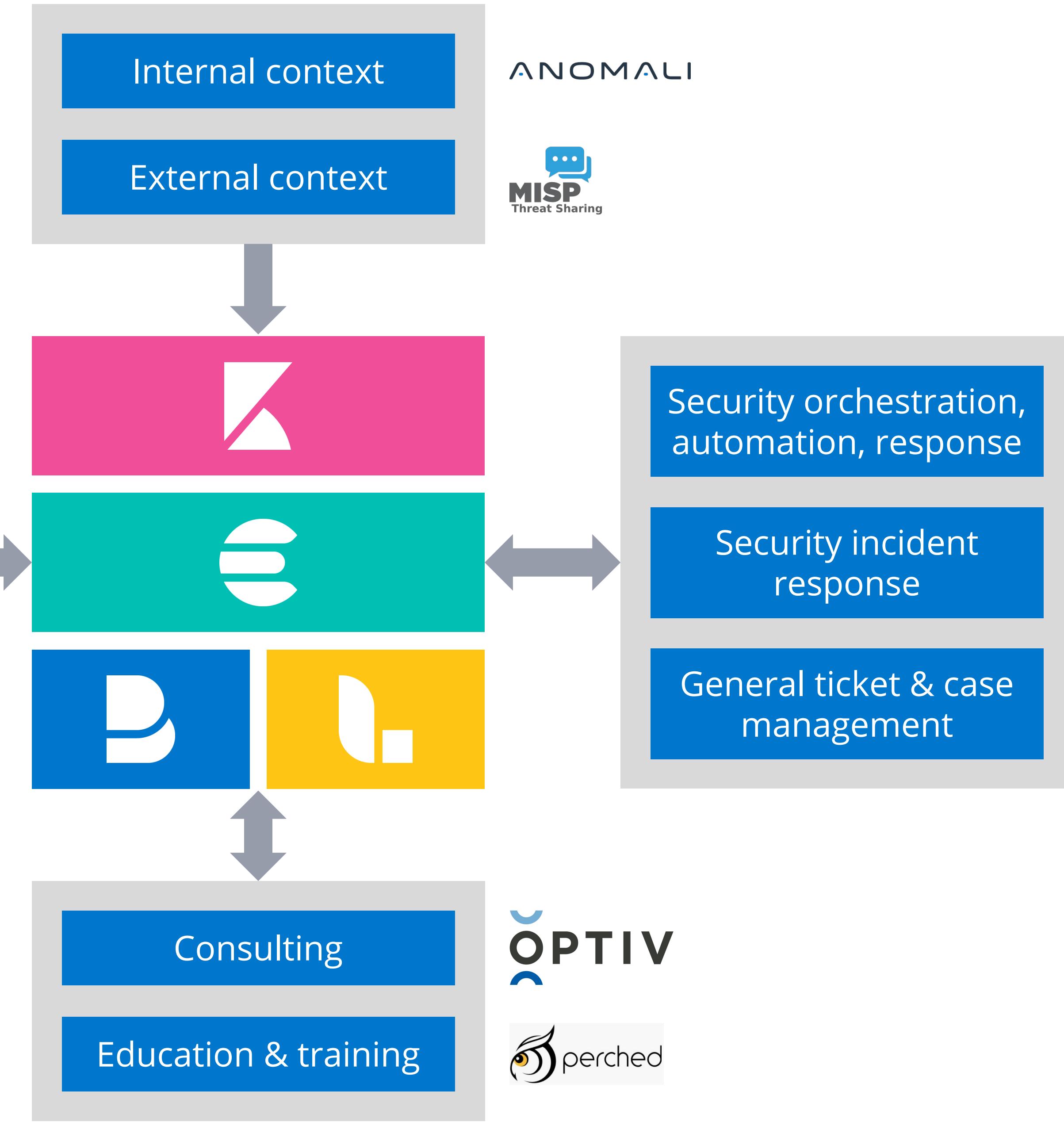


Elastic SIEM

A SIEM for Elastic Stack users everywhere



Elastic SIEM Ecosystem



Elastic SIEM Roadmap



Elastic Security Analytics Journey

BETA

Threat Intelligence Integration, User Analysis

SIEM Detection Rules, More Data Sources

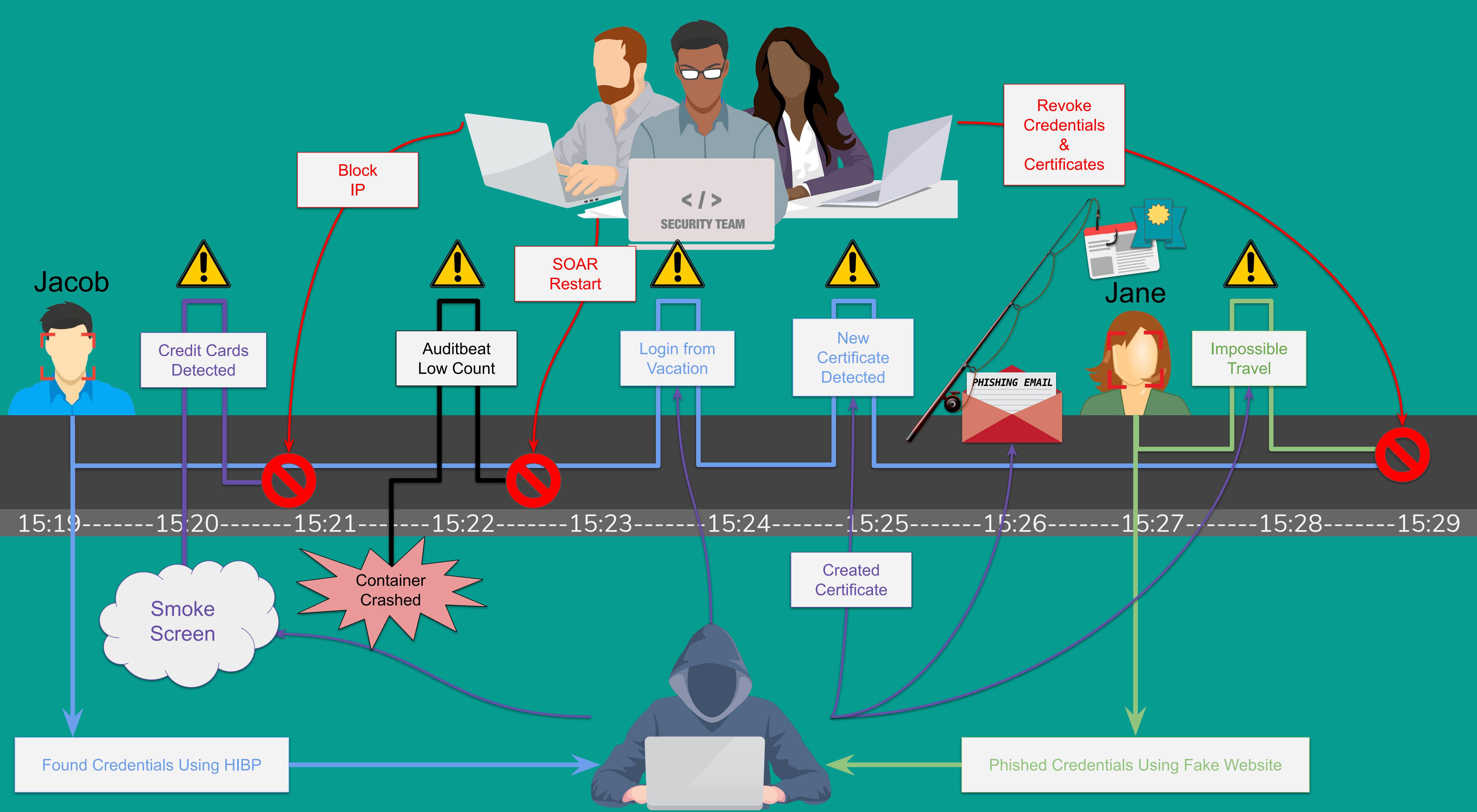
Dedicated SIEM App, SOC Workflow

Security Event Collection, Visualization, Dashboards

Elastic Common Schema (ECS)

YOU
ARE
HERE

Security Analytics Demo



Lab 4

Interacting with the Elastic SIEM App

Try it @ home

Elastic Cloud Trial
Available
for 2 Weeks

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





www.elastic.co