Home Network Monitoring Setup

ElasticStack SIEM
Presented By: Noah Goldberg
Demonstrations By: Lucas Hartford
SlideDeck By: Tony Florian

Table of Contents

This presentation contains the following chapters

01

Intro to ElasticStack

02

Registration & Deployment

03

Live Demonstrations

04

Dashboards

05

Reference Material

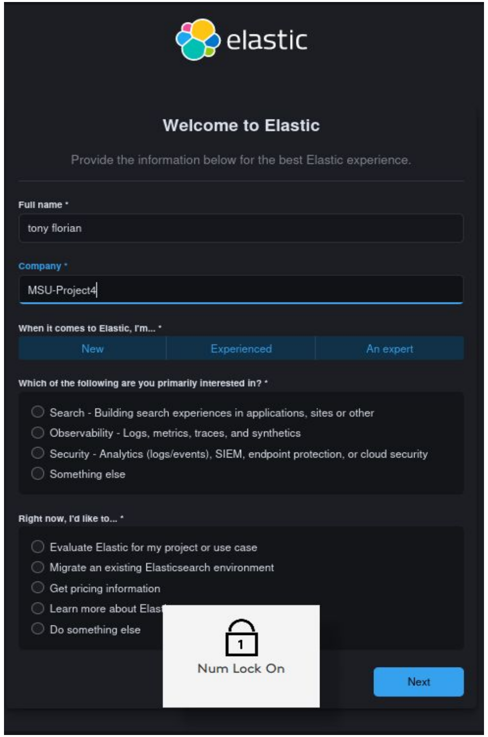
ElasticStack

What is ElasticStack and Why Use It?

- A data analytics platform designed to provide visibility into many kinds of datasets
- It can be configured as a SIEM solution at a bargain compared to big name SIEM vendors such as Splunk
- It provides great support for security monitoring, including pre-made rules and dashboards to provide mitigate common vulnerabilities and attack methods
- It also provides integrations with common platforms such as Azure, AWS, and CISCO products
- As you will see in our demonstrations, Elastic can provide nearly all of the same functionality that a dedicated SIEM platform would
- Elastic’s low cost to feature ratio makes it well-suited for low budget organizations looking to launch a security monitoring environment from scratch

Registration
&
Deployment

Initial Registration



Welcome to Elastic

Provide the information below for the best Elastic experience.

Full name *

tony florian

Company *

MSU-Project4

When it comes to Elastic, I'm... *

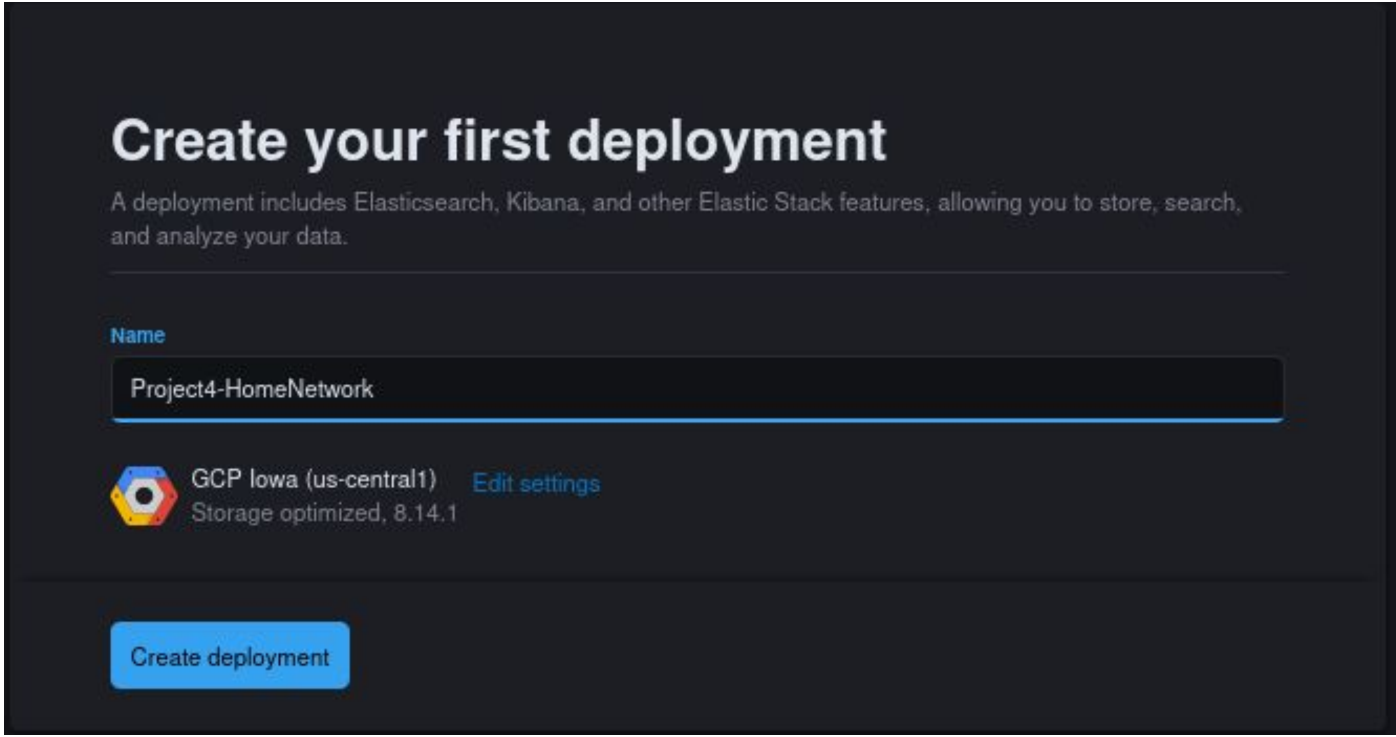
New | Experienced | An expert

Which of the following are you primarily interested in? *

○ Search - Building search experiences in applications, sites or other
○ Observability - Logs, metrics, traces, and synthetics
○ Security - Analytics (logs/events), SIEM, endpoint protection, or cloud security
○ Something else

Right now, I'd like to... *

○ Evaluate Elastic for my project or use case
○ Migrate an existing Elasticsearch environment
○ Get pricing information
○ Learn more about Elas
○ Do something else



Create your first deployment

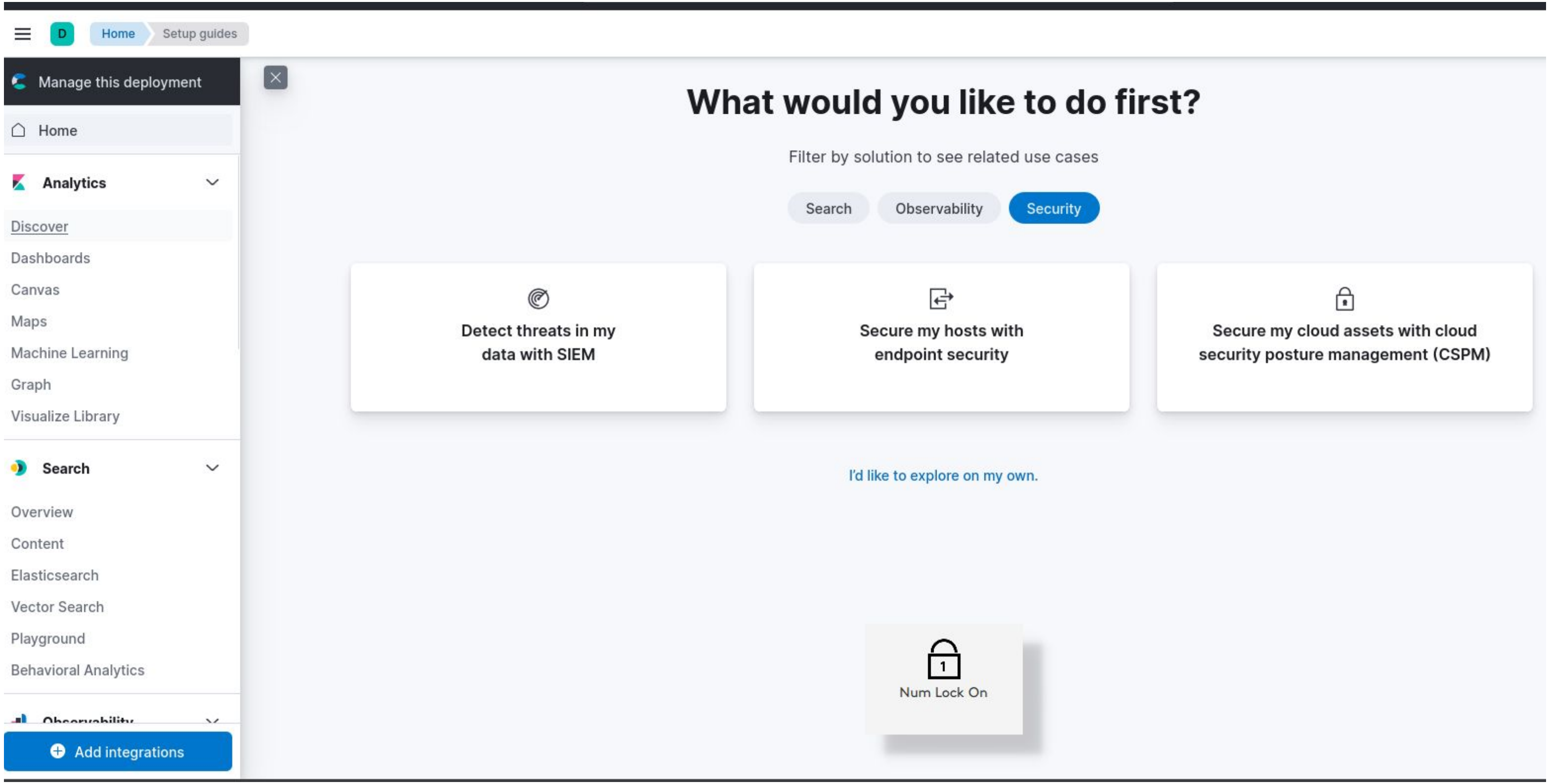
A deployment includes Elasticsearch, Kibana, and other Elastic Stack features, allowing you to store, search, and analyze your data.

Name

Project4-HomeNetwork

GCP Iowa (us-central1)
Storage optimized, 8.14.1

Post Deployment HomePage



What would you like to do first?

Filter by solution to see related use cases

Detect threats in my data with SIEM

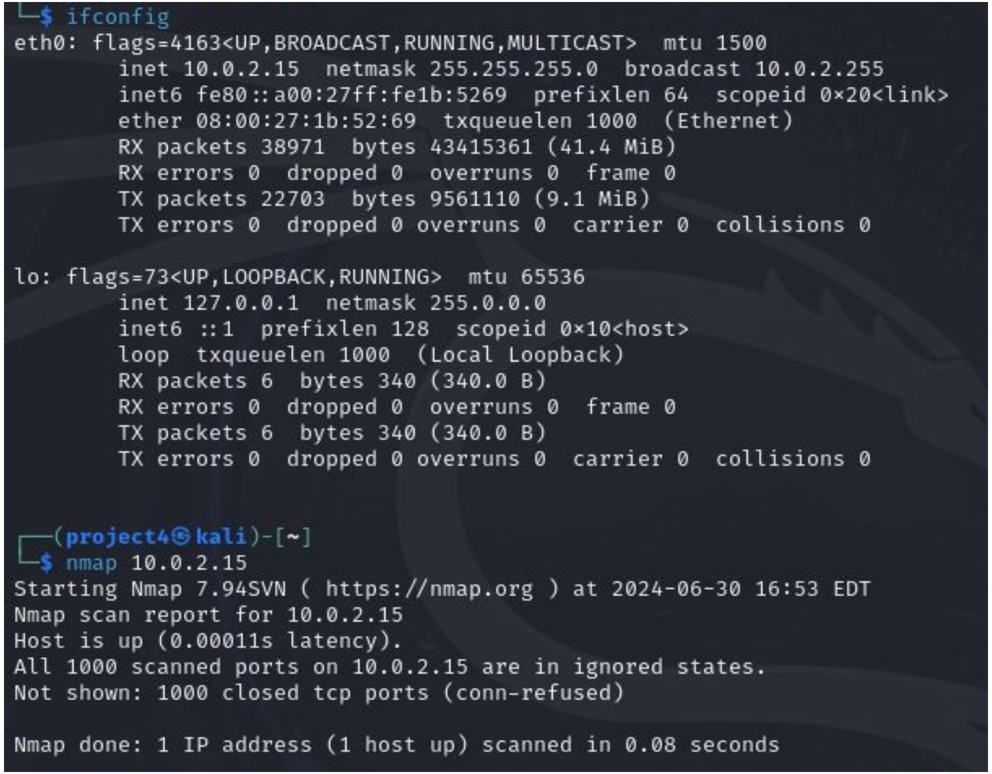
Secure my hosts with endpoint security

Secure my cloud assets with cloud security posture management (CSPM)

I'd like to explore on my own.

Live Demos

Simulated Attack



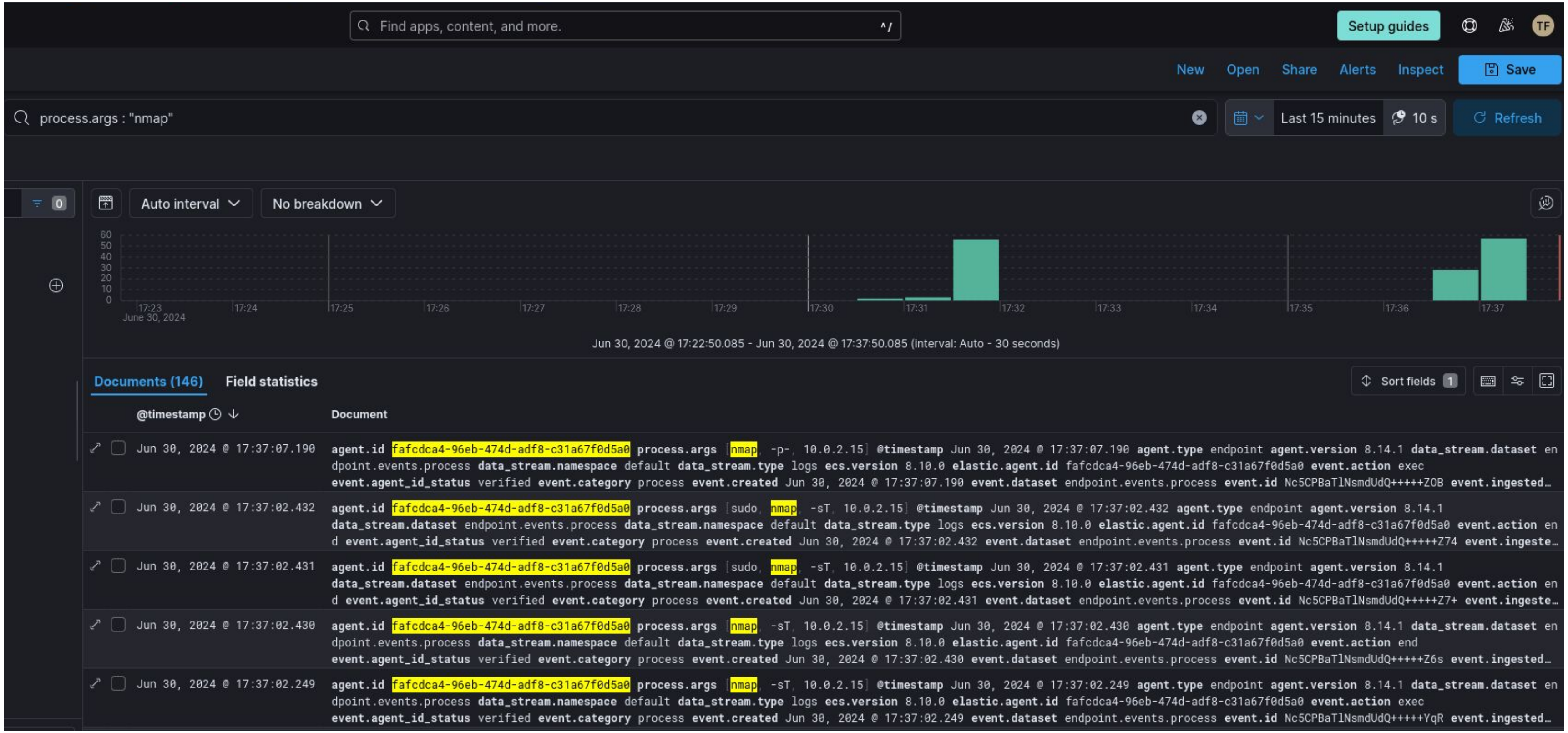
```
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe1b:5269  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:1b:52:69  txqueuelen 1000  (Ethernet)
        RX packets 38971  bytes 43415361 (41.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22703  bytes 9561110 (9.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 6  bytes 340 (340.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6  bytes 340 (340.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(project4㉿kali)-[~]
└─$ nmap 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-30 16:53 EDT
Nmap scan report for 10.0.2.15
Host is up (0.00011s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

Simulated attack Logs



process.args : "nmap"

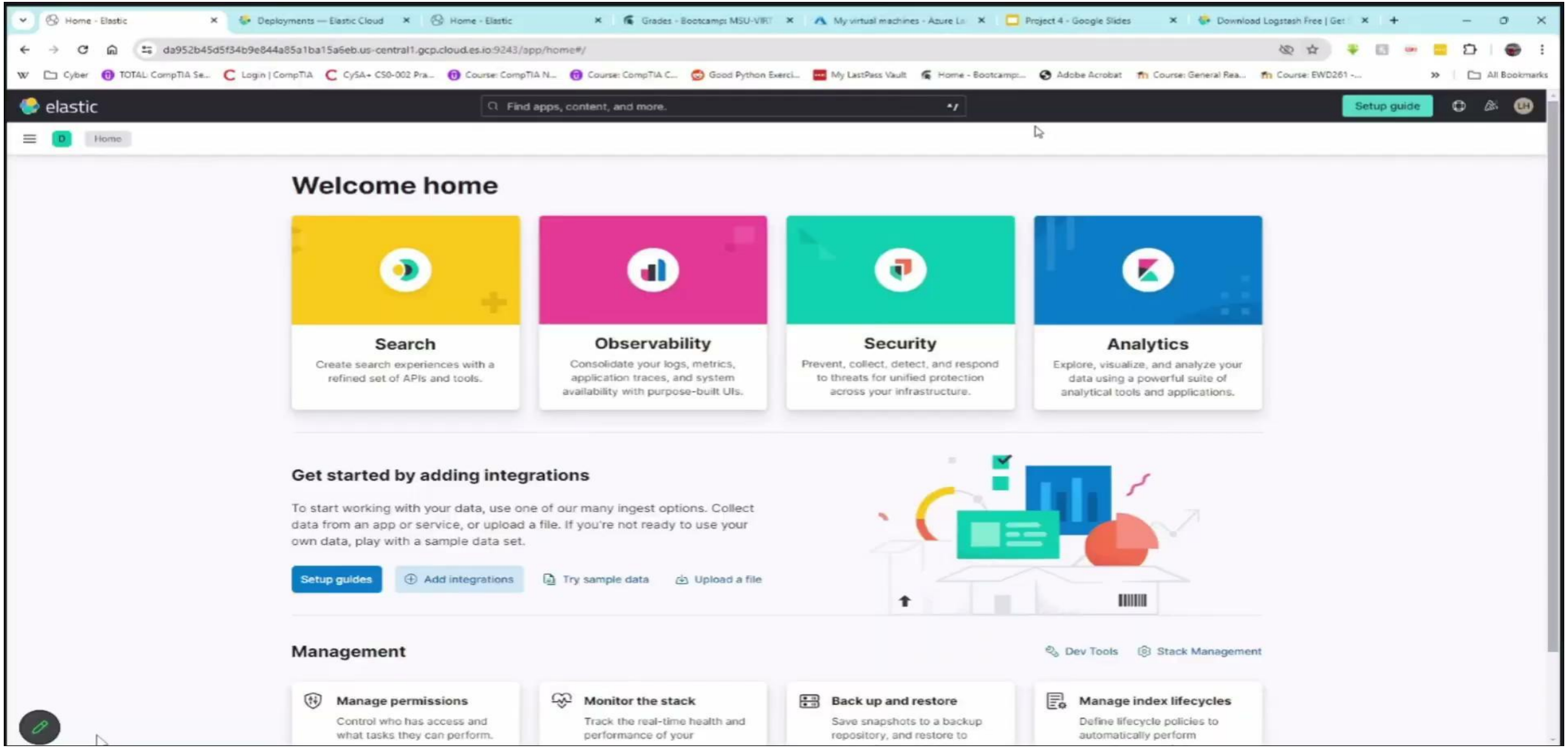
Jun 30, 2024 @ 17:22:50.085 - Jun 30, 2024 @ 17:37:50.085 (interval: Auto - 30 seconds)

Documents (146)

```
@timestamp                  Document
Jun 30, 2024 @ 17:37:07.190 agent.id fafcdca4-96eb-474d-adf8-c31a67f0d5a0 process.args [nmap, -p-, 10.0.2.15] @timestamp Jun 30, 2024 @ 17:37:07.190 agent.type endpoint agent.version 8.14.1 data_stream.dataset en
                            dpoint.events.process data_stream.namespace default data_stream.type logs ecs.version 8.10.0 elastic.agent.id fafcdca4-96eb-474d-adf8-c31a67f0d5a0 event.action exec
                            event.agent_id_status verified event.category process event.created Jun 30, 2024 @ 17:37:07.190 event.dataset endpoint.events.process event.id Nc5CPBaTlNsmdUdQ+++++ZOB event.ingested…
Jun 30, 2024 @ 17:37:02.432 agent.id fafcdca4-96eb-474d-adf8-c31a67f0d5a0 process.args [sudo, nmap, -sT, 10.0.2.15] @timestamp Jun 30, 2024 @ 17:37:02.432 agent.type endpoint agent.version 8.14.1
                            data_stream.dataset endpoint.events.process data_stream.namespace default data_stream.type logs ecs.version 8.10.0 elastic.agent.id fafcdca4-96eb-474d-adf8-c31a67f0d5a0 event.action en
                            d event.agent_id_status verified event.category process event.created Jun 30, 2024 @ 17:37:02.432 event.dataset endpoint.events.process event.id Nc5CPBaTlNsmdUdQ+++++Z74 event.ingeste…
Jun 30, 2024 @ 17:37:02.431 agent.id fafcdca4-96eb-474d-adf8-c31a67f0d5a0 process.args [sudo, nmap, -sT, 10.0.2.15] @timestamp Jun 30, 2024 @ 17:37:02.431 agent.type endpoint agent.version 8.14.1
                            data_stream.dataset endpoint.events.process data_stream.namespace default data_stream.type logs ecs.version 8.10.0 elastic.agent.id fafcdca4-96eb-474d-adf8-c31a67f0d5a0 event.action en
                            d event.agent_id_status verified event.category process event.created Jun 30, 2024 @ 17:37:02.431 event.dataset endpoint.events.process event.id Nc5CPBaTlNsmdUdQ+++++Z7+ event.ingeste…
Jun 30, 2024 @ 17:37:02.430 agent.id fafcdca4-96eb-474d-adf8-c31a67f0d5a0 process.args [nmap, -sT, 10.0.2.15] @timestamp Jun 30, 2024 @ 17:37:02.430 agent.type endpoint agent.version 8.14.1 data_stream.dataset en
                            dpoint.events.process data_stream.namespace default data_stream.type logs ecs.version 8.10.0 elastic.agent.id fafcdca4-96eb-474d-adf8-c31a67f0d5a0 event.action end
                            event.agent_id_status verified event.category process event.created Jun 30, 2024 @ 17:37:02.430 event.dataset endpoint.events.process event.id Nc5CPBaTlNsmdUdQ+++++Z6s event.ingested…
Jun 30, 2024 @ 17:37:02.249 agent.id fafcdca4-96eb-474d-adf8-c31a67f0d5a0 process.args [nmap, -sT, 10.0.2.15] @timestamp Jun 30, 2024 @ 17:37:02.249 agent.type endpoint agent.version 8.14.1 data_stream.dataset en
                            dpoint.events.process data_stream.namespace default data_stream.type logs ecs.version 8.10.0 elastic.agent.id fafcdca4-96eb-474d-adf8-c31a67f0d5a0 event.action exec
                            event.agent_id_status verified event.category process event.created Jun 30, 2024 @ 17:37:02.249 event.dataset endpoint.events.process event.id Nc5CPBaTlNsmdUdQ+++++YqR event.ingested…
```

Live Demo (Adding Agent)

Live Demo (Alerts)



Welcome home

Search
Create search experiences with a refined set of APIs and tools.

Observability
Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.

Security
Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.

Analytics
Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

Get started by adding integrations

To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to use your own data, play with a sample data set.

Setup guides | Add integrations | Try sample data | Upload a file

Management

Dev Tools | Stack Management

Manage permissions
Control who has access and what tasks they can perform.

Monitor the stack
Track the real-time health and performance of your

Back up and restore
Save snapshots to a backup repository, and restore to

Manage index lifecycles
Define lifecycle policies to automatically perform

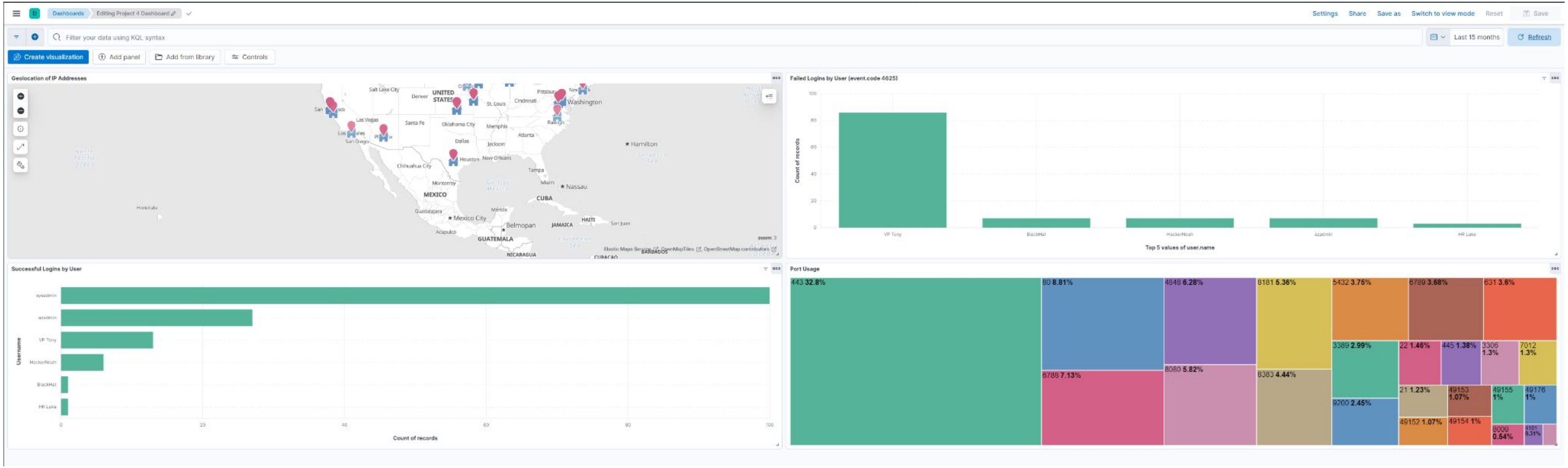
Live Demo (DashBoards)

Demonstration Summary

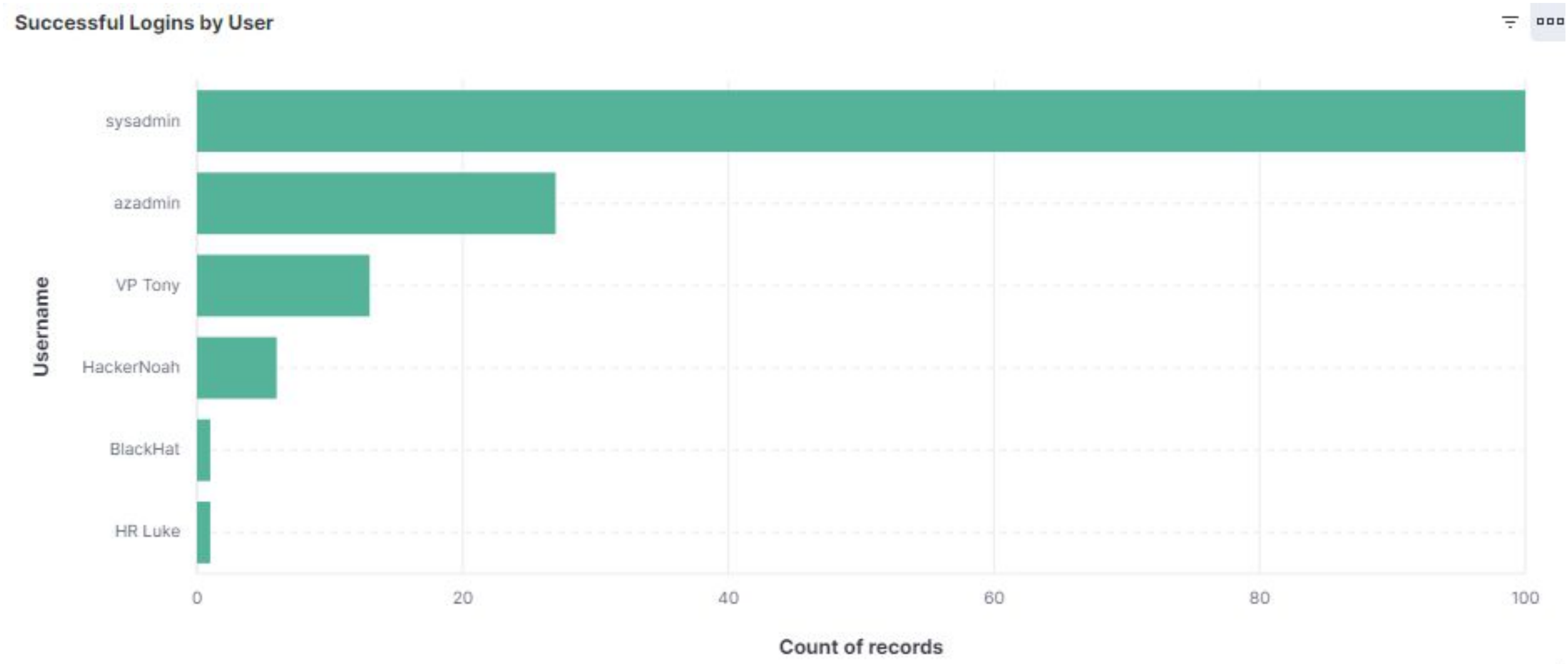
- Adding Agents
    - Connecting Streams of data between HOST and Elastic-Deployment
    - This allows for multiple assets to be monitored in and outside of the network
- Creating Alerts
    - Customized alerts can generate reports/emails that are sent to the SOC team/administrators based on the thresholds set.
- Visualized Dashboards
    - Used to correlate information from the data stream using graphs/maps

Dashboards

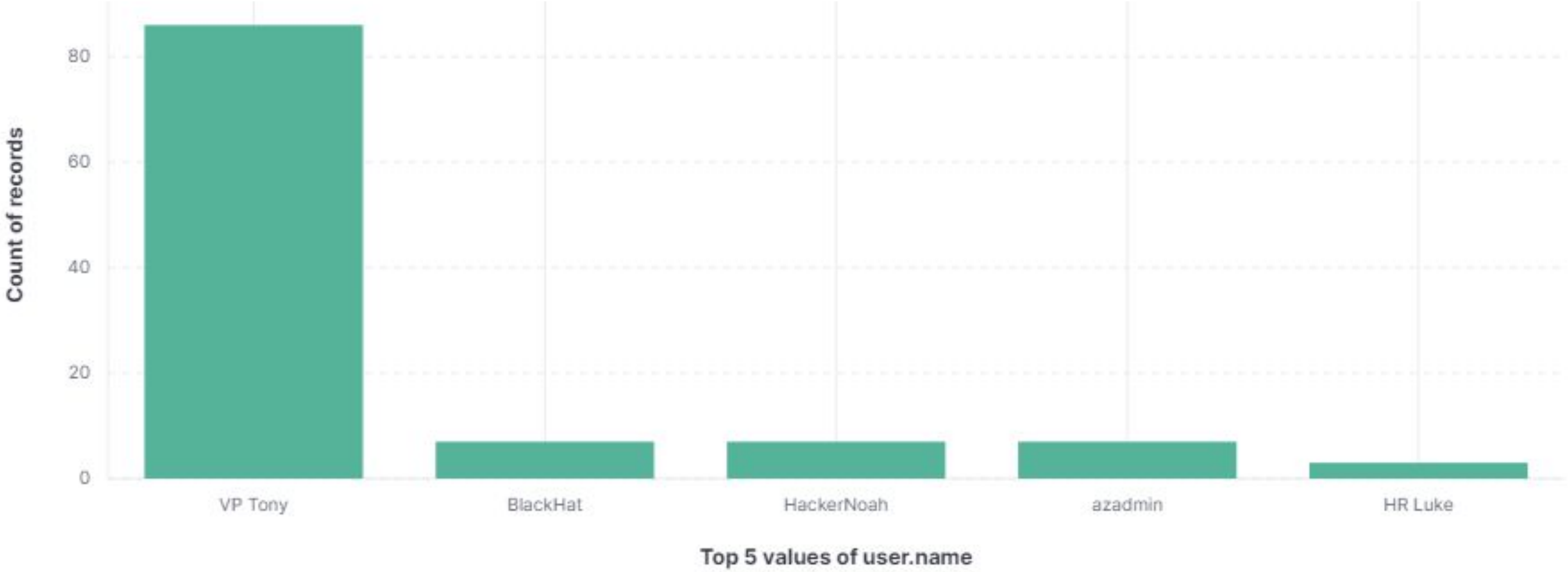
Example of a ElasticSearch Dashboard



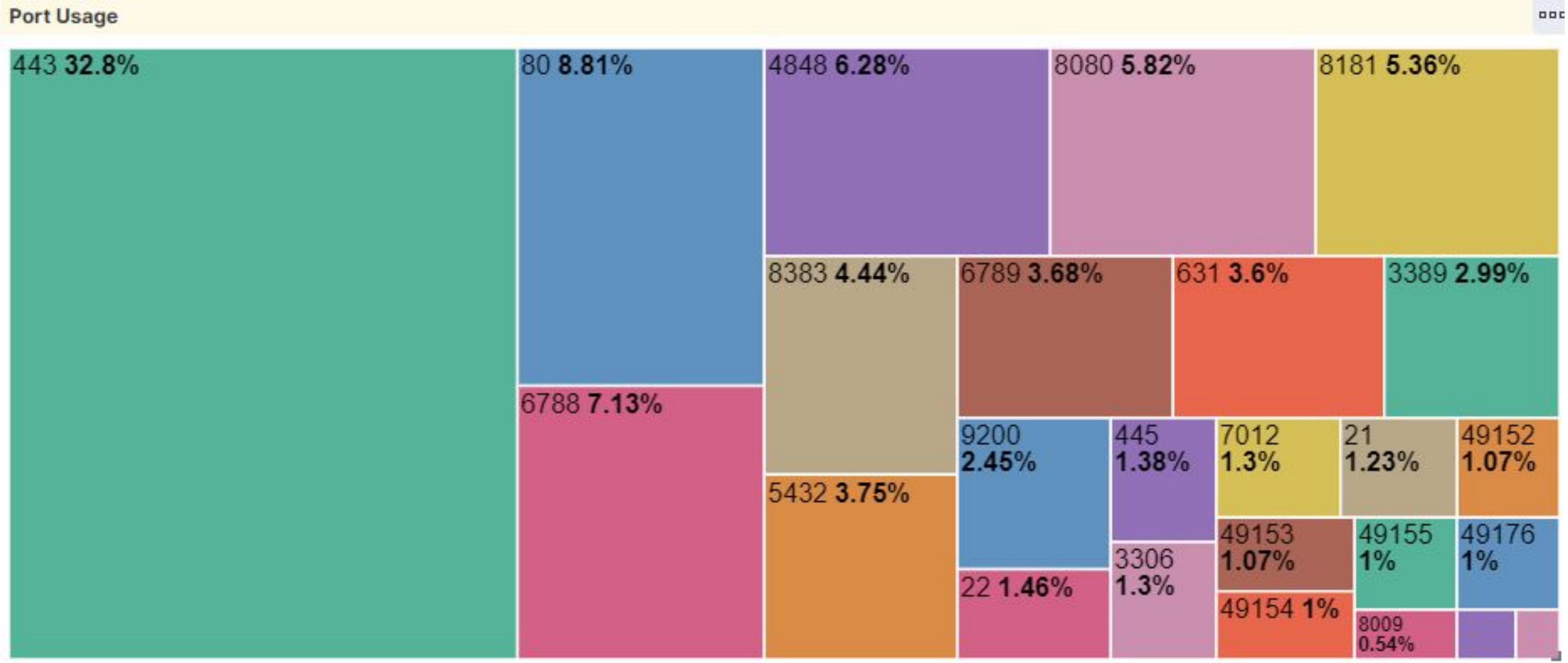
Successful Logins By User Bar Graph



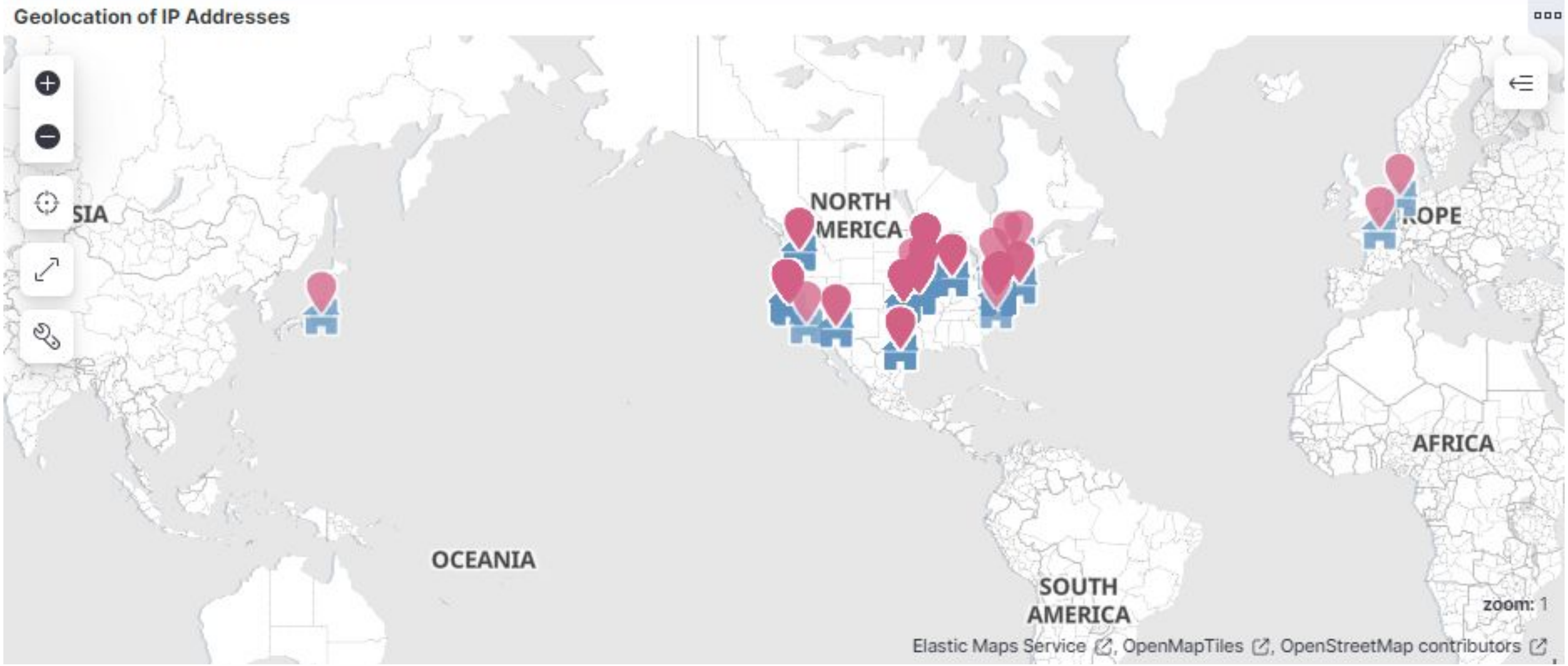
Failed Logins By User Column Chart



Port Usage TreeMap



IP Address Geolocations



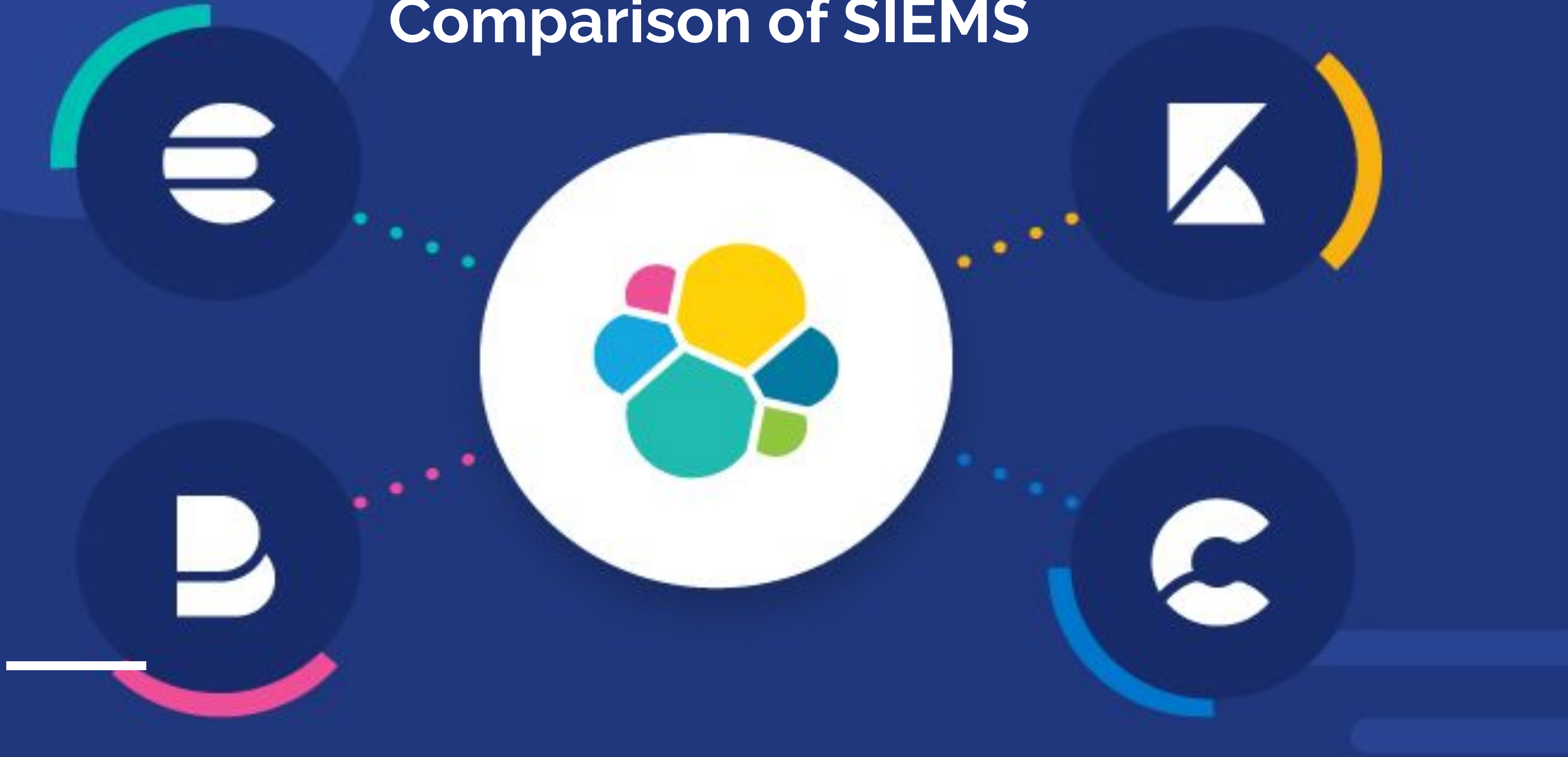
Geolocation of IP Addresses
SIA
NORTH AMERICA
ROPE
AFRICA
OCEANIA
SOUTH AMERICA
zoom: 1
Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors

Reference

Reference Material

- For more Information Regarding ELK (ElastickStack)
  - https://www.elastic.co/docs
- Learn more about different SIEMs
  - https://www.exabeam.com/explainers/siem-tools/siem-solutions/
- ElasticStack in the real world
  - https://www.elastic.co/customers/tamus

Comparison of SIEMS



Pricing Comparison

ElasticSearch pricing depends on the size of the deployment. With 45 GB of available data storage, our cost would be $97.82/month or $1,173.84 per year. If we wanted 720 GB of storage instead, and scaled the rest of our deployment accordingly, the cost is around $2190 per month.

For comparison, a ballpark estimate for a small organizations Splunk deployment is $150 per GB of ingested data. At that price, a comparable Splunk environment to the one we created in the ElasticStack would cost about $6750 per year, roughly 6x the price.