Empower your Security Analysts with the Elastic Stack

Thorben Jändling – Solutions Architect @Elastic

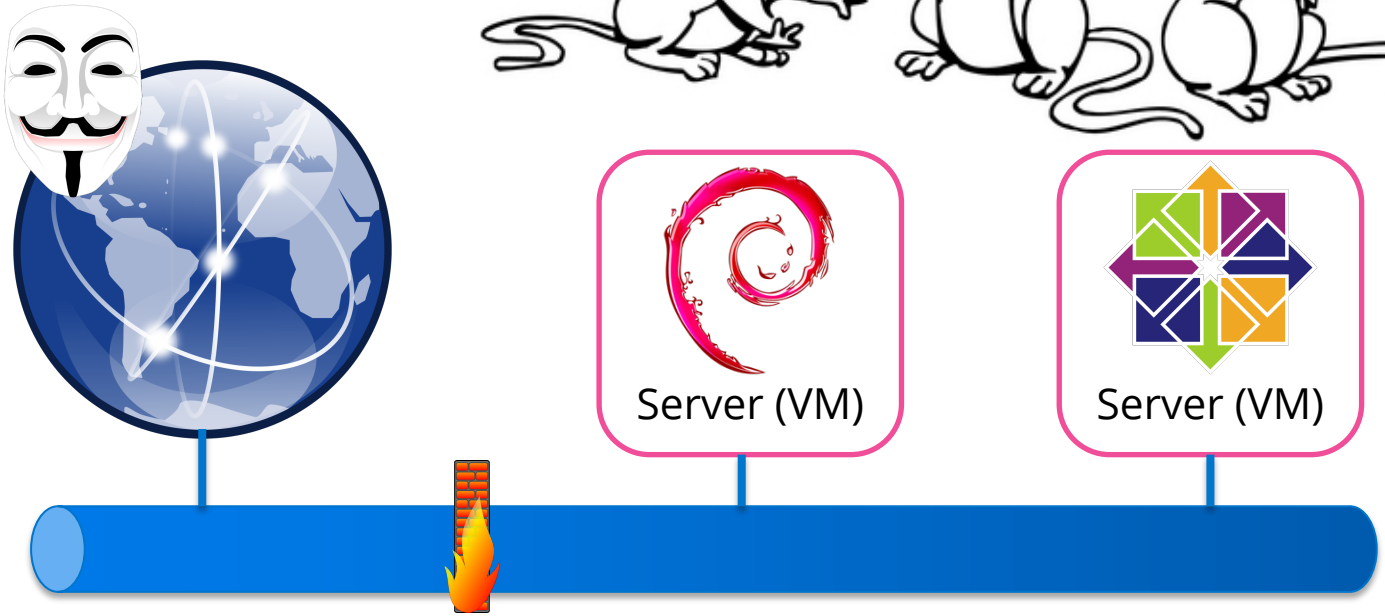
An Out-of-the-Box Elastic Stack experience (ES-OOTB)

From Zero to Security Analyst in 30min.

elastic

What ICT Security can feel like

But, also our initial demo setup



https://ela.st/es-ootb

elastic

I just followed the documentation

Follow along at home: **https://ela.st/es-ootb**

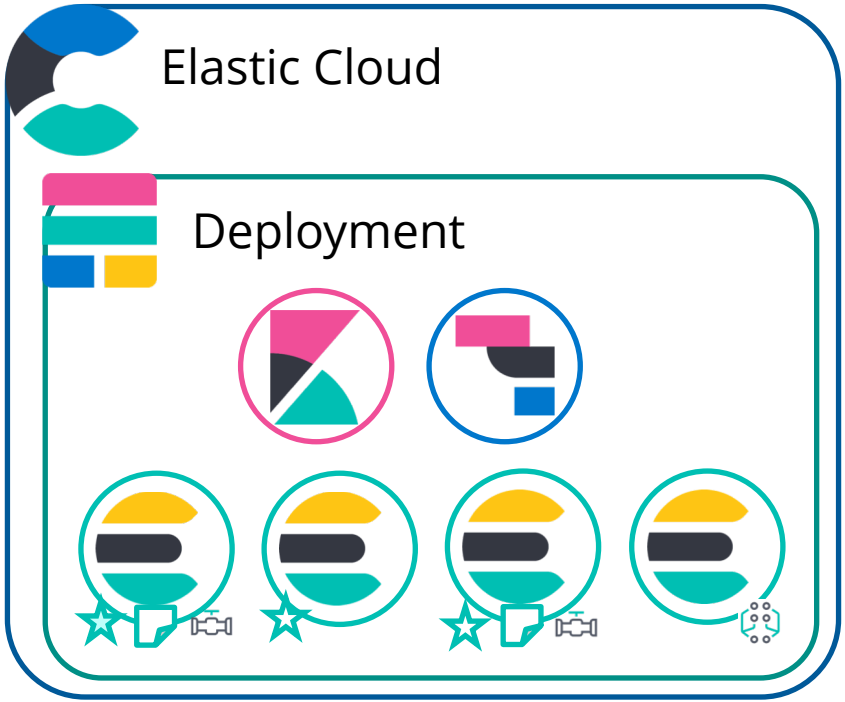
- The entire setup is created by a few small bash scripts,
  (saves time as this talk is only 30min. long)
- These scripts are available here: **https://ela.st/es-ootb**
- The script is annotated with links to the documentation for each step therein

- *You can get an Elastic Cloud trail and a VM (or two) to recreate everything you see here today!*

These slides are mostly intended for offline reading, and most will be skipped in favour of the live demo

Phase 1: Deploy Elasticsearch, Kibana & APM server

Follow along at home: **https://ela.st/es-ootb**



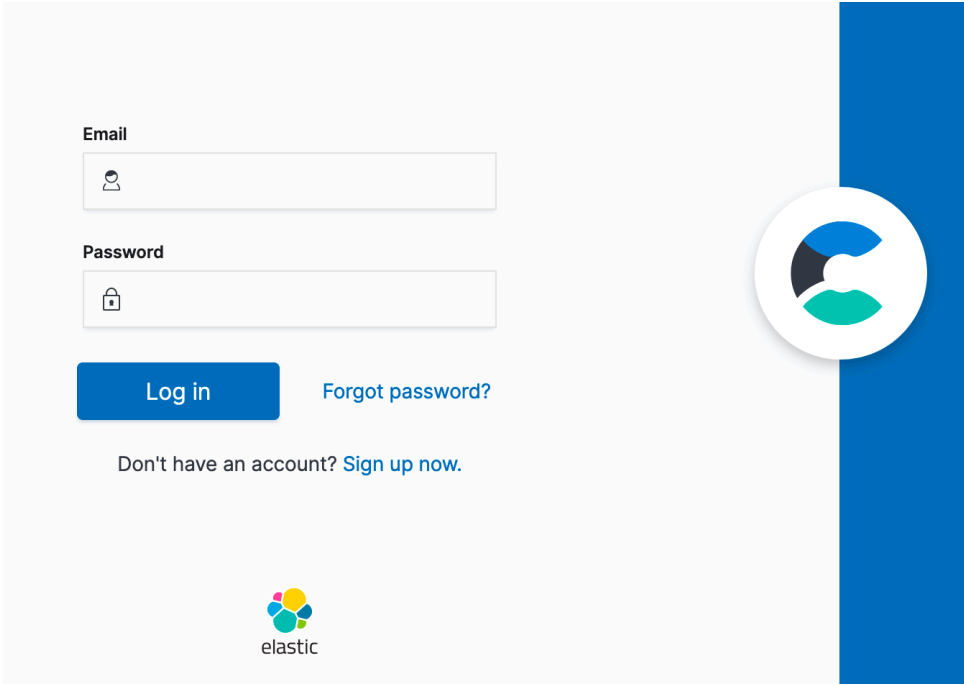
https://ela.st/es-ootb

elastic

Goto Elastic Cloud

Phase 1 – Step 1

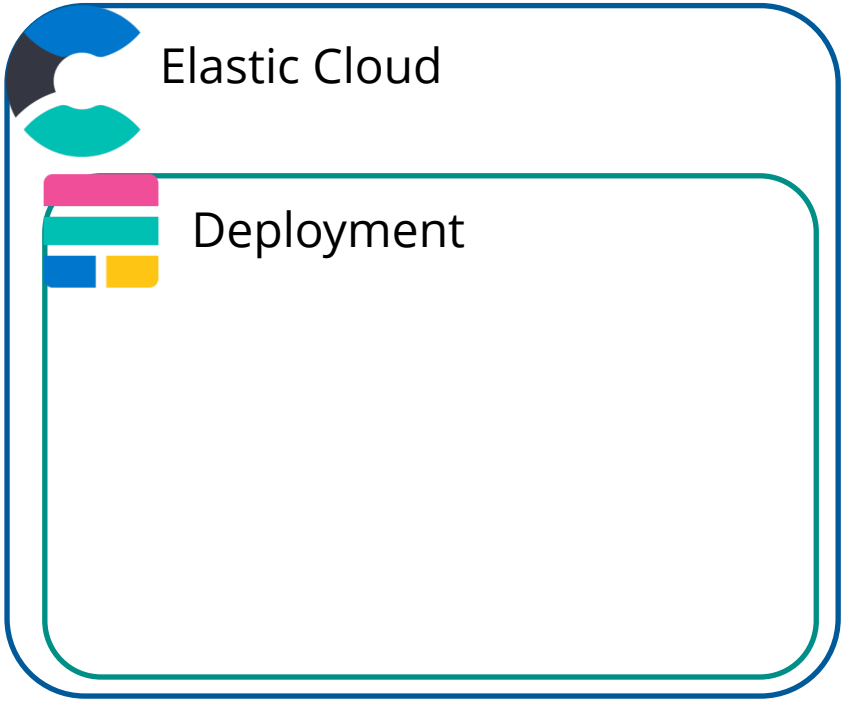
Elastic Cloud



https://ela.st/es-ootb

Create Deployment

Phase 1 – Step 2A



Create deployment

Spin up your deployment to start configuring your Elastic Stack, either with templates or customize

1 **Name your deployment**

Give your deployment a name

elasticon

2 **Select a cloud platform**

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

aws
Amazon Web Services

Google Cloud Platform

3 **Select a region**

US Central 1 (Iowa)

US West 1 (Oregon)

Europe W

Asia Pacific (Tokyo)

Asia Pacific (Sydney)

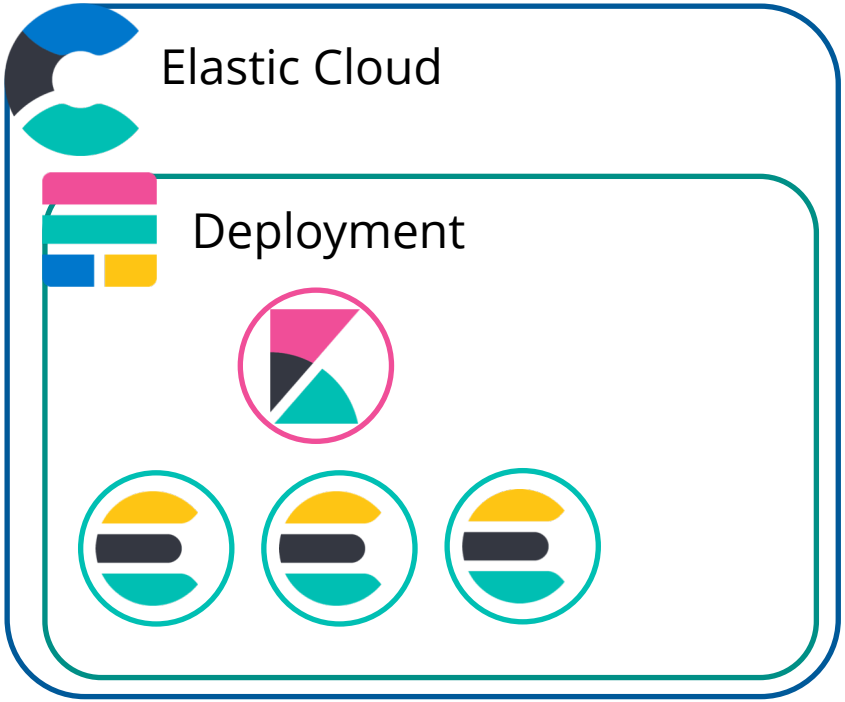
4 **Set up your deployment**

Elastic Stack version

7.4.0 Edit

Customise Deployment

Phase 1 – Step 2B



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

Compute Optimized

Run CPU-intensive workloads or run smaller workloads cost-effectively when you need less memory and storage.

Default specs

Me

Perforr oper includ frequ

Cross Cluster Search

Use to search data across one or more associated deployments

Default specs

Elastic Cloud supports many more options to cater to your specific use case such as hot· setup optimized for analytics etc. Learn more

Deployment pricing

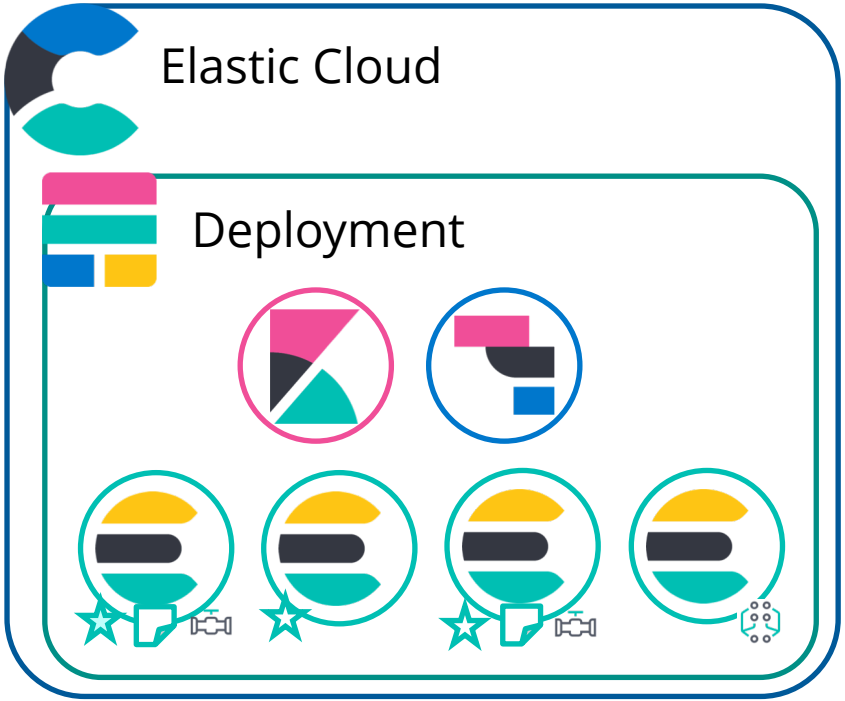
Hourly rate $0.5696

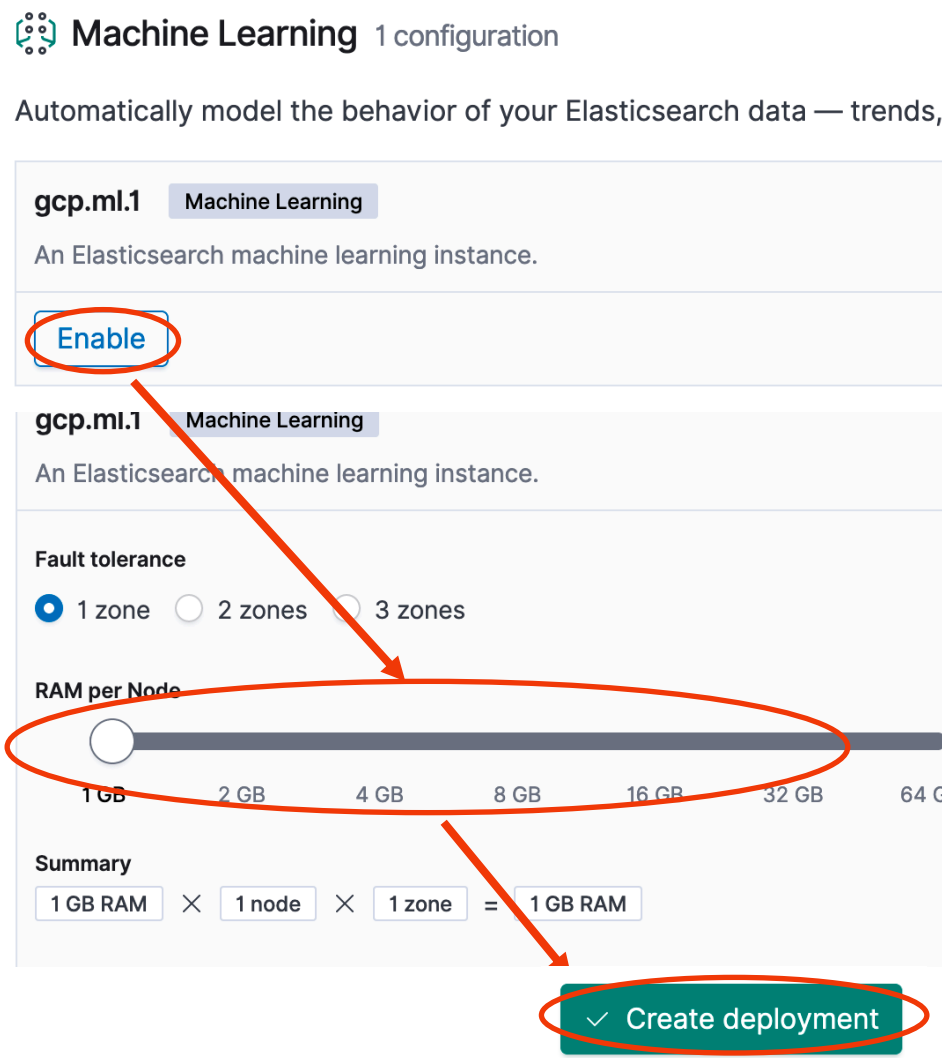
Creat eployment

Customize deployment

Enable APM + Machine Learning

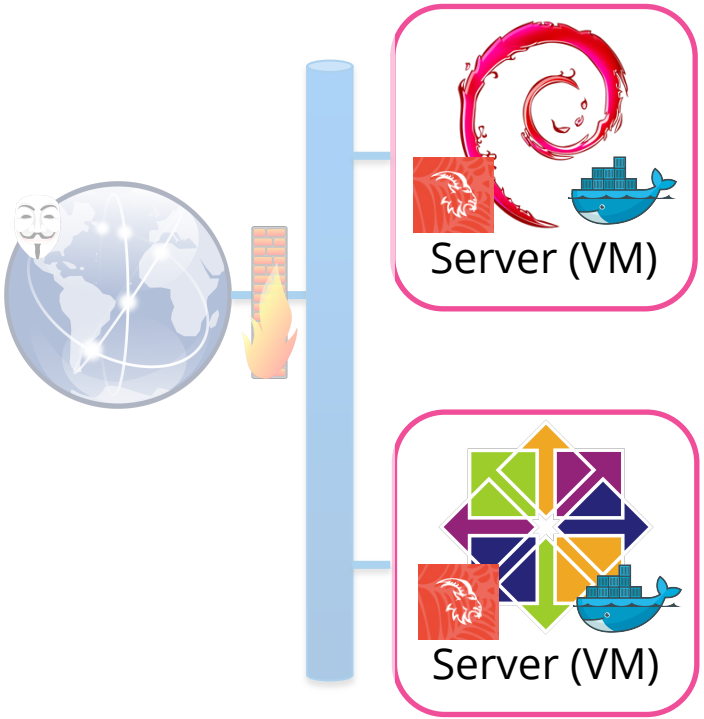
Phase 1 – Step 2C

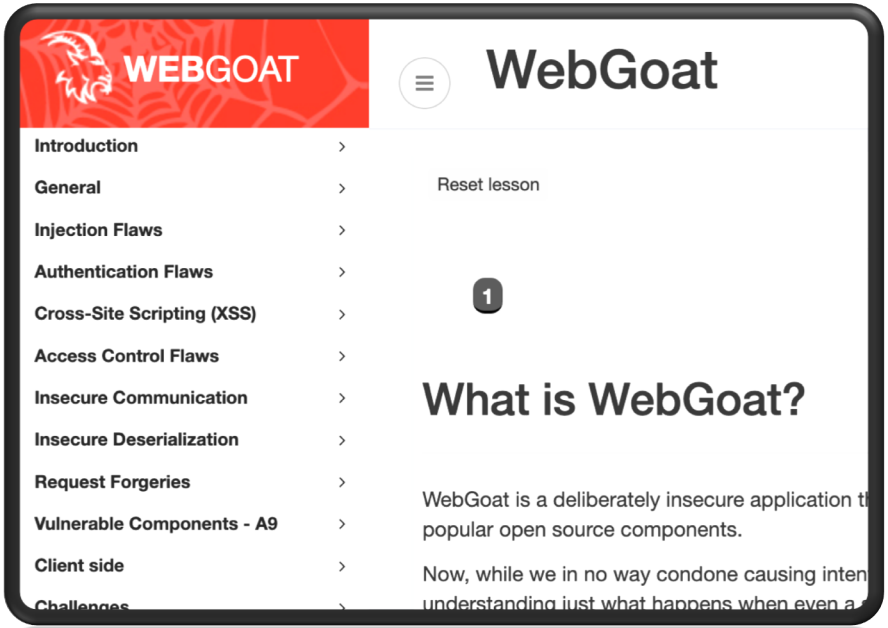




Phase 2: Deploy our web services

Follow along at home: **https://ela.st/es-ootb**





https://ela.st/es-ootb elastic

Deploy WebGoat on Docker

Phase 2 – Step 1

```
~ $ screen -dR
```

In screen **1**:

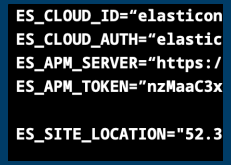
```
~ $ git clone
https://github.com/ThorbenJ/el
astic-ootb.git


~ $ cd elastic-ootb/scripts/


~/elastic-ootb/scripts
$ bash webgoat_on_docker.sh up
```

webgoat_on_docker.sh will:

- Install Docker CE & docker-compose
- Give the current user permissions to operate docker
  - Possibly require the user to login again
- Fetch WebGoat's docker-compose description file
- Execute docker-compose on webgoat's file with the arguments given to the script
- Read the annotation in the script before usage

(Recommend using screen or tmux, to run in the background)

https://ela.st/es-ootb elastic



WARNING

WARNING

- In this demonstration we have been configuring our agents to use the ‘elastic’ superuser.
- This user has full admin access over your elasticsearch deployment.
- **Do not use the ‘elastic’ account for agent deployment**

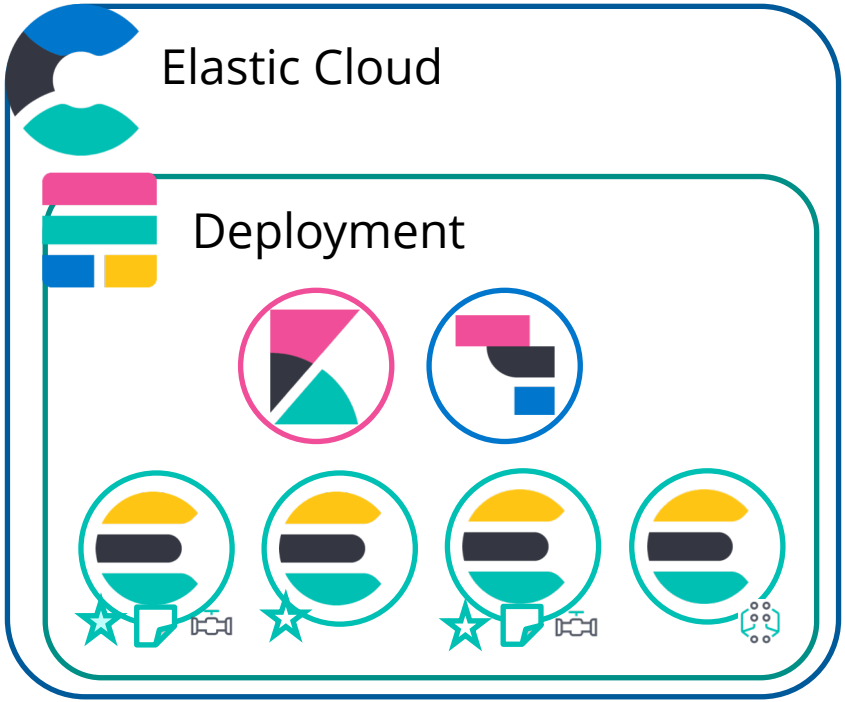
With more time and effort, you can create dedicated users for your agents to use (this step was skipped in this demo).

Only one of each beat type & version needs a user privileged enough to run the ‘setup’ command.

elastic

Grab you cloud deployment details

Phases 3 & 4 preparation



https://ela.st/es-ootb

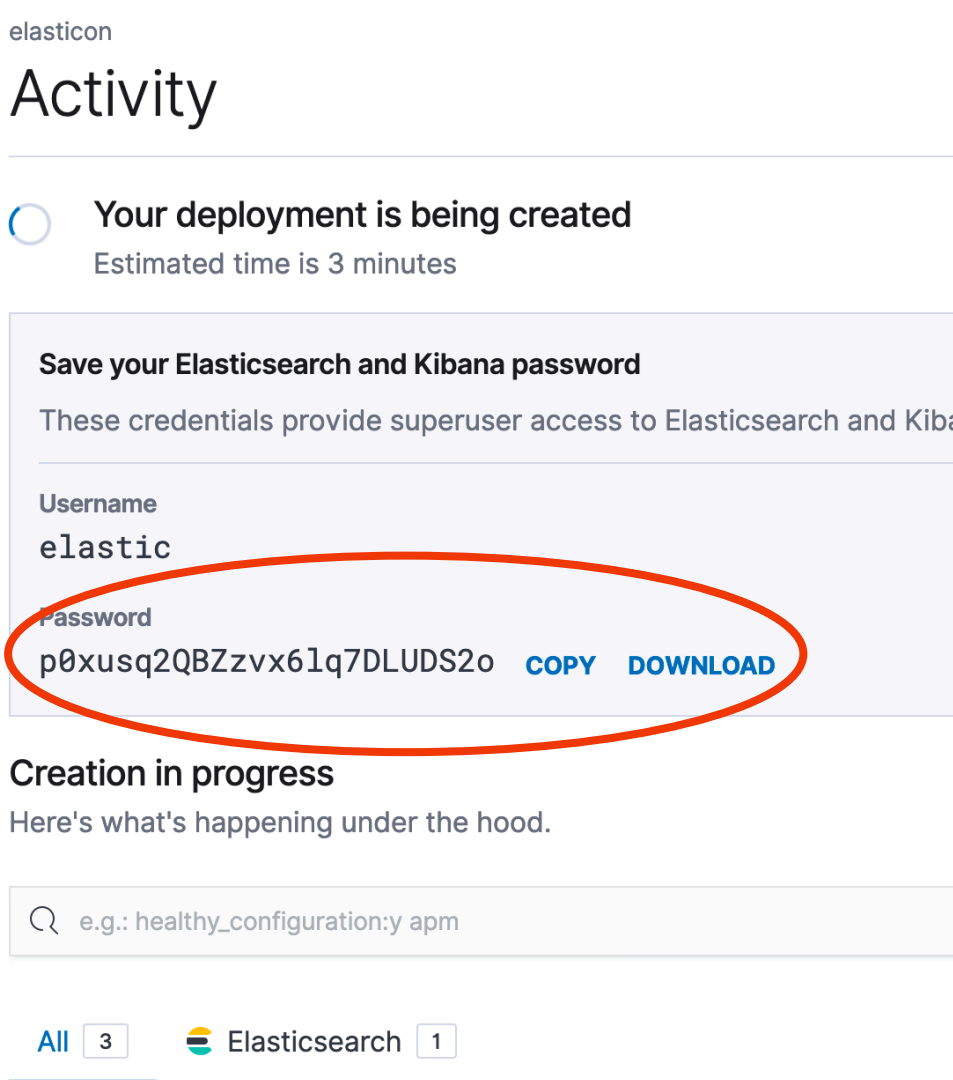
elastic

Your first & last chance to grab your password

Phases 3 & 4 preparation – Step 1

In “es-ootb.conf”:

```
ES_CLOUD_ID=
ES_CLOUD_AUTH=“elastic:p0xusq2QBZ
ES_APM_SERVER=
ES_APM_TOKEN=
```

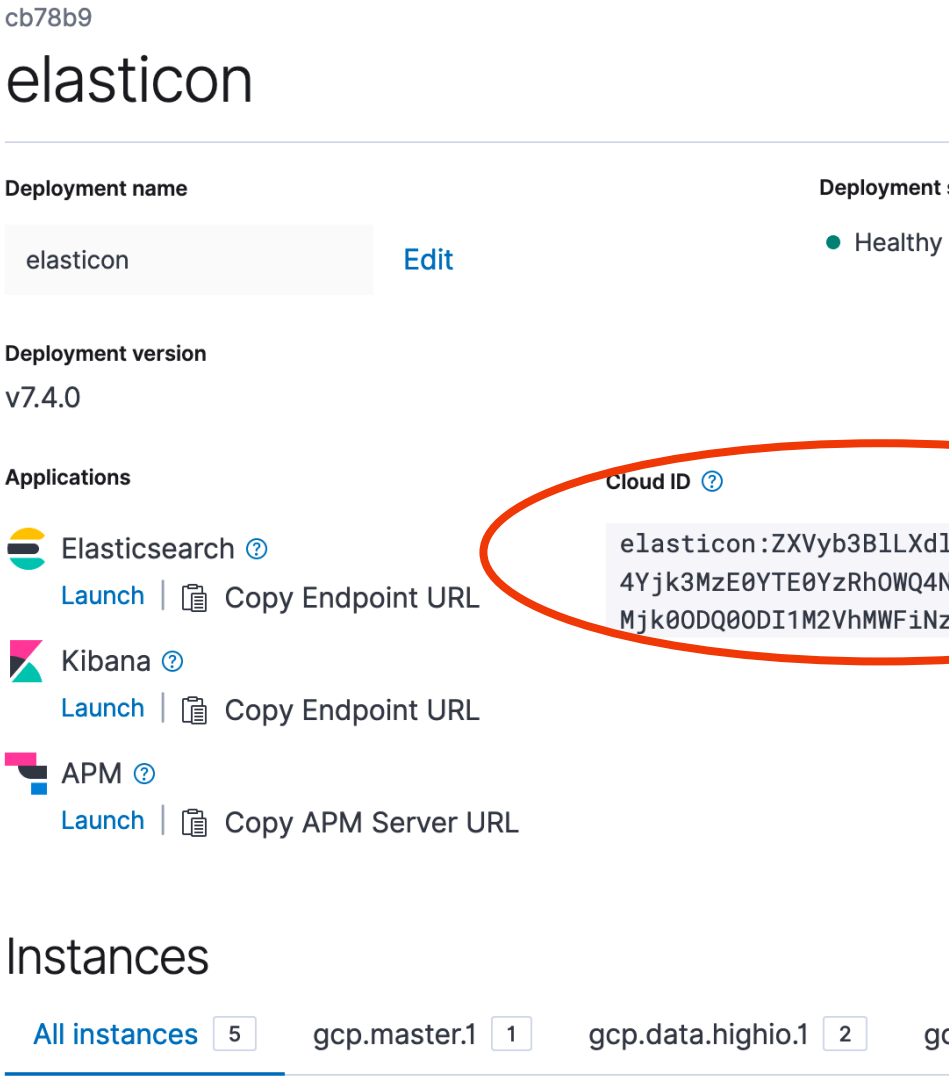


Grab your Cloud ID

Phases 3 & 4 preparation – Step 2

In “es-ootb.conf”:

```
ES_CLOUD_ID=“elasticon:ZXVyb3BlLX
ES_CLOUD_AUTH=“elastic:p0xusq2QBZ
ES_APM_SERVER=
ES_APM_TOKEN=
```

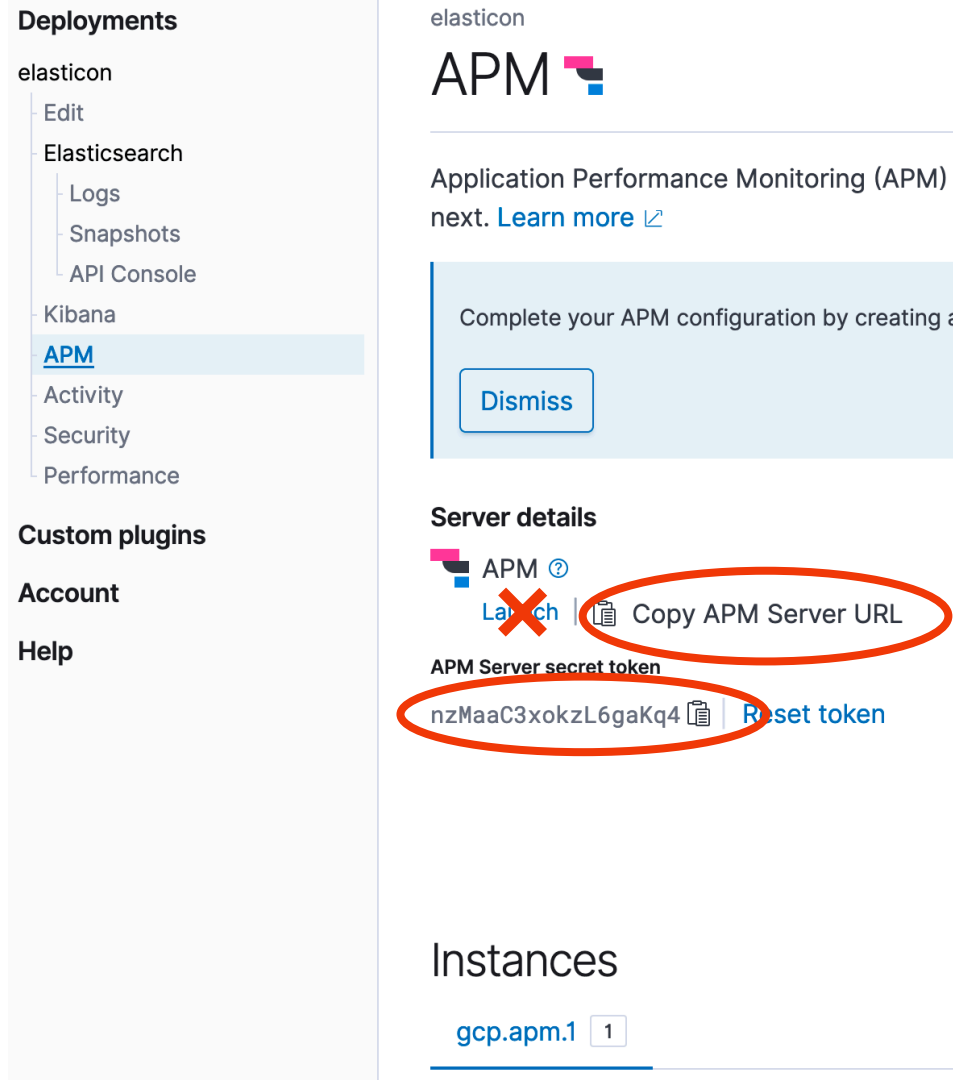


Grab your APM server credentials

Phases 3 & 4 preparation – Step 3

In “es-ootb.conf”:

```
ES_CLOUD_ID=“elasticon:ZXVyb3BlLX
ES_CLOUD_AUTH=“elastic:p0xusq2QBZ
ES_APM_SERVER=“https://8d74c7195c
ES_APM_TOKEN=”nzMaaC3xokzL6gaKq4”
```

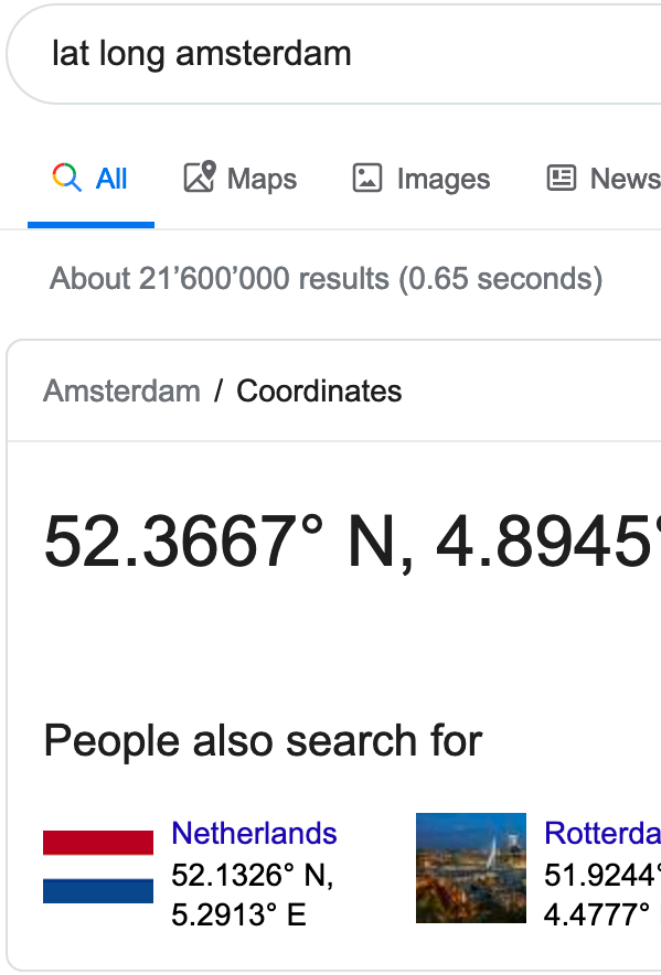


Give your datacenter's private IPs a location

Phases 3 & 4 preparation – Step 4 **OPTIONAL**

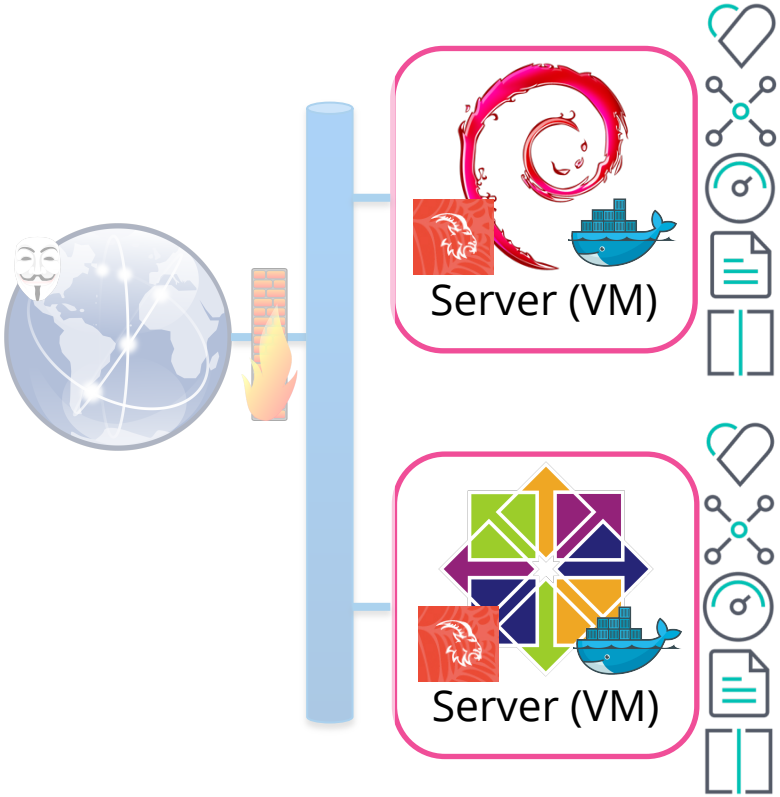
In "es-ootb.conf":

```
ES_CLOUD_ID="elasticon:ZXVyb3BlLX
ES_CLOUD_AUTH="elastic:p0xusq2QBZ
ES_APM_SERVER="https://8d74c7195c
ES_APM_TOKEN="nzMaaC3xokzL6gaKq4"

ES_SITE_LOCATION="52.3667:4.8945"
```



Phase 3: Deploy the Beats

Follow along at home: **https://ela.st/es-ootb**



Heartbeat

Packetbeat

Metricbeat

Filebeat

Auditbeat

Deploy our Beats agents

Phase 3 – Step 1

In screen **0**:

```
~ $ cd elastic-ootb/scripts/


~/elastic-ootb/scripts
$ cat > es-ootb.conf
 <<paste content>>
ctrl+d


~/elastic-ootb/scripts
$ bash beats-ootb.sh setup
```

beats-ootb.sh will:

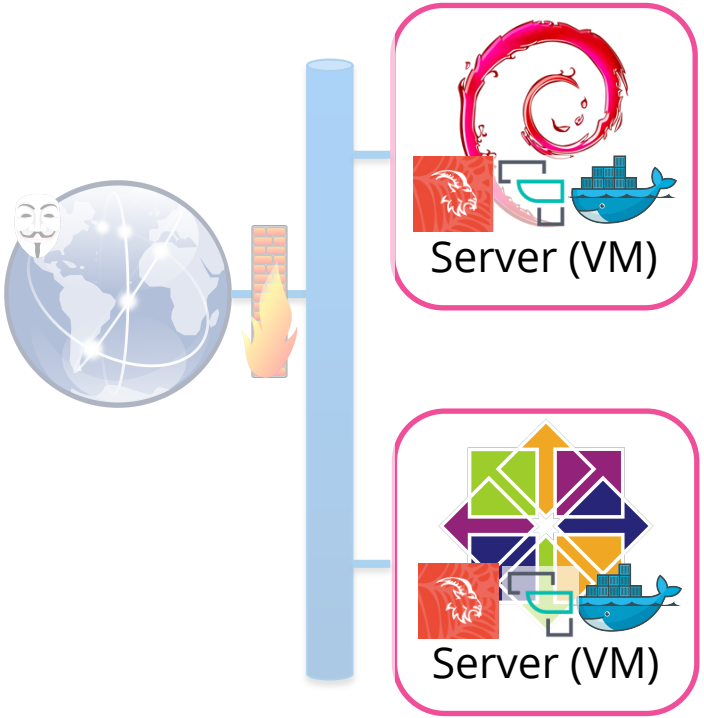
- Install each beat
- Configure each beat, including:
  - Data collection inputs/modules/etc.
  - Data processors (e.g. add host information)
  - Data output to an Elastic Cloud deployment
- If the 'setup' argument is given:
  - Ingest pipelines will be created in Elasticsearch for each beat type
    - e.g. Add Geo-information to IP addresses
  - Have each beat configure their ootb setup on elasticsearch & kibana
    - ILM, Dashboards, ML, Mapping templates…
- Launch each beat

Please read the annotation at the top; then skip the functions and start following the script at the bottom.

https://ela.st/es-ootb

Phase 4: Setup APM agents

Follow along at home: **https://ela.st/es-ootb**



Java APM Agent

Deploy Standalone Java Agent

Phase 4 – Step 1

In screen **2**:

```
~ $ cd elastic-ootb/scripts/


<<Assume es-ootb.conf was
created as in previous step>>


~/elastic-ootb/scripts
$ bash apm-ootb.sh
```

apm-ootb.sh will:

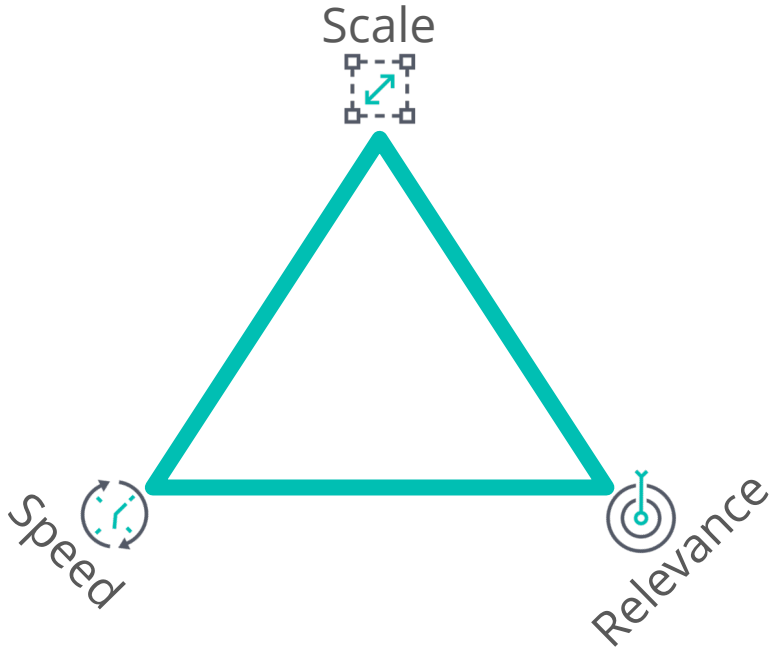
- Install maven (mvn)
  - This will pull in the Java JDK and its dependancies…
- Use maven to fetch the standalone elastic APM attach java file (jar)
- Iterate through all docker containers
  - If they appear to be running java:
  - Install and launch the APM agent
- Optionally (if the ”wait4more” argument is given)
  - Listen for the creation of new containers
  - If they appear to be running java:
  - Install and launch the APM agent

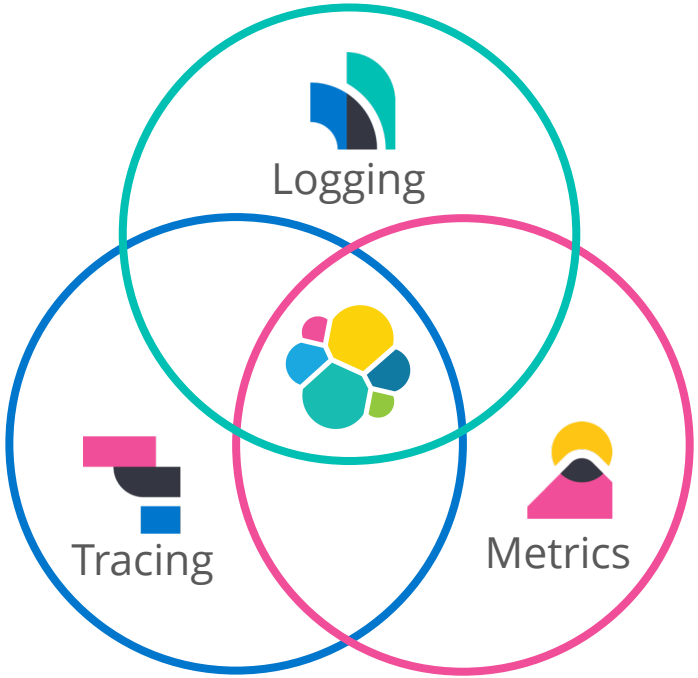
Please read the annotation at the top; then skip the functions and start following the script at the bottom.

https://ela.st/es-ootb

Unique qualities of the Elastic Stack:

Follow along at home: **https://ela.st/es-ootb**





Speed, Scale, Relevance & Observability (aka Visibility)

https://ela.st/es-ootb elastic

What you'd like ICT Security to be like

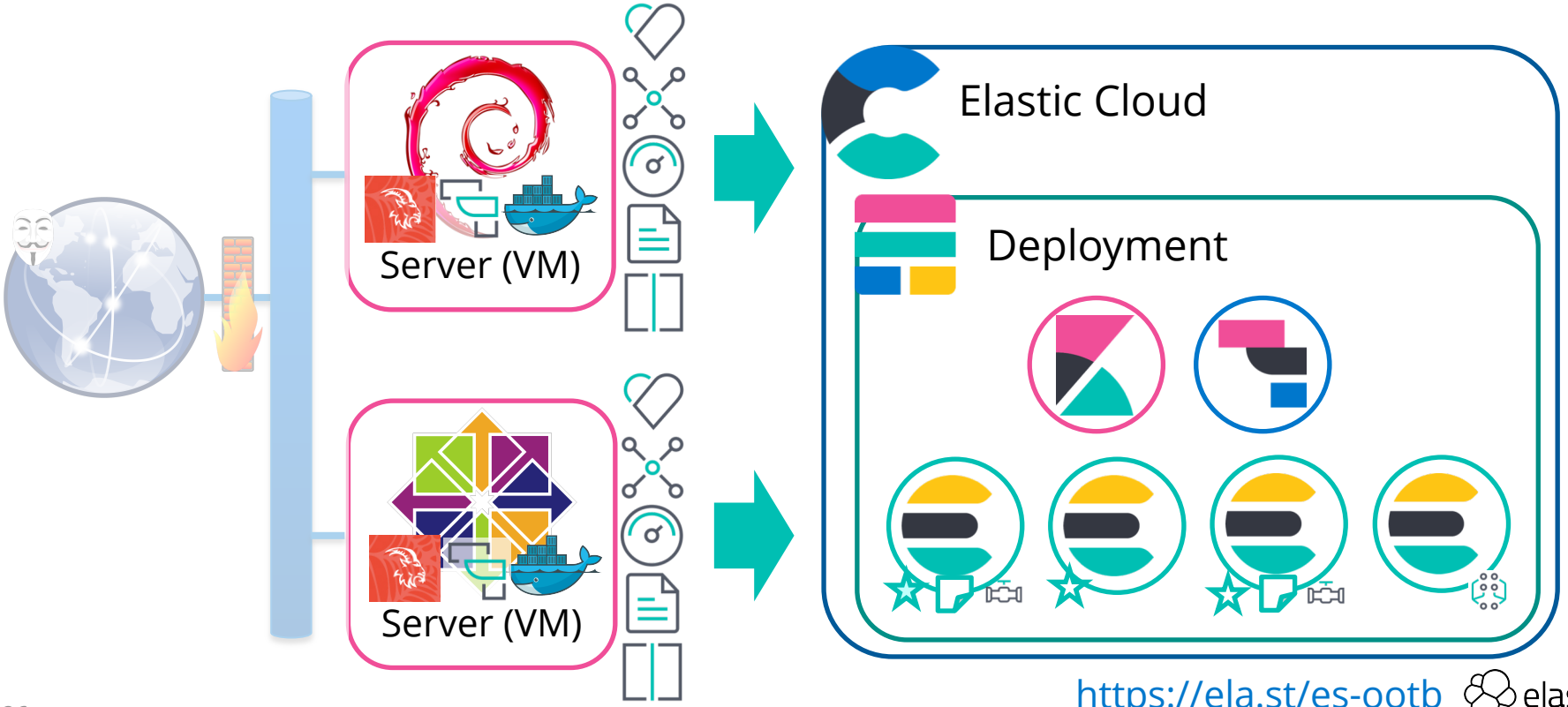
and, also our final demo setup

https://ela.st/es-ootb

elastic

The end result

Follow along at home: **https://ela.st/es-ootb**



https://ela.st/es-ootb elastic

Lets look at our new security analytics tools

This should be the half-way mark

elastic

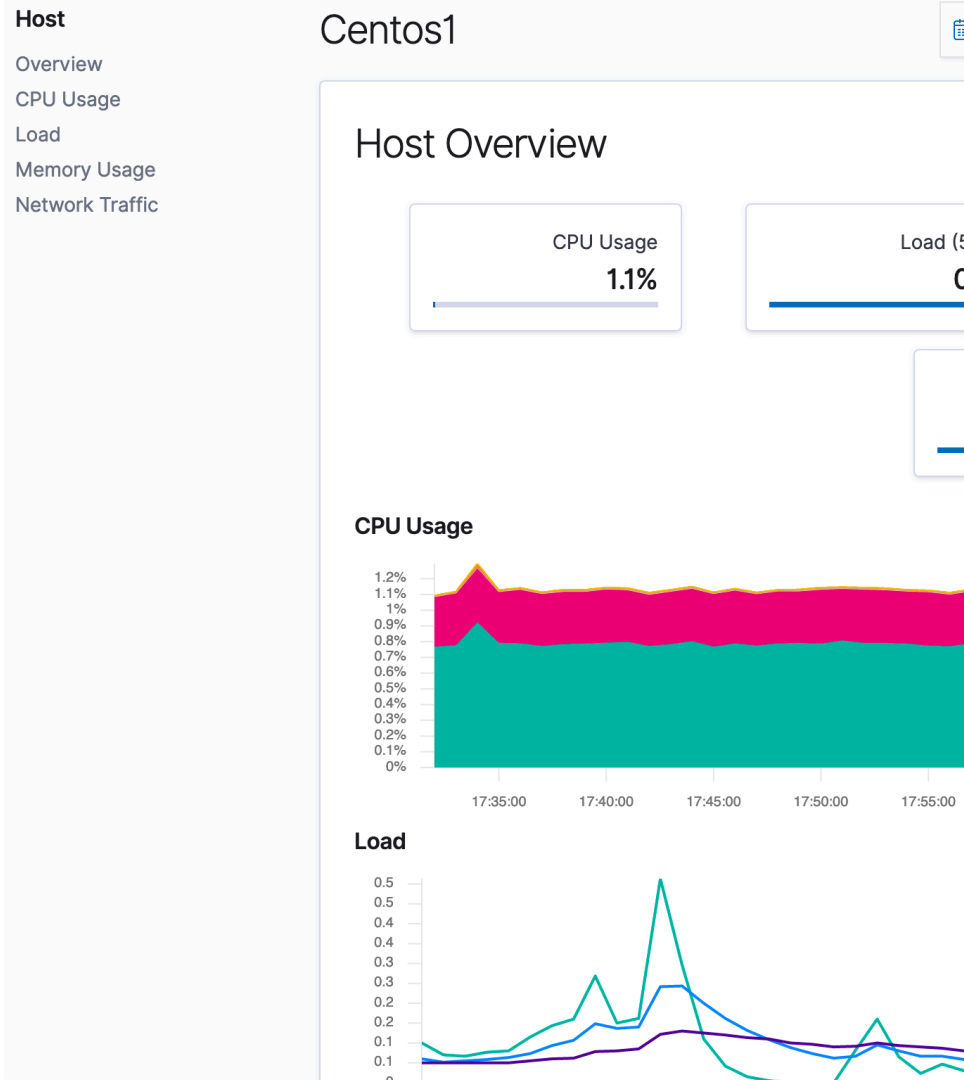
View our infrastructure

Infrastructure / default page

- CPU usage & Memory usage
- Inbound & Outbound traffic
- Load & Log rate

Drill down:

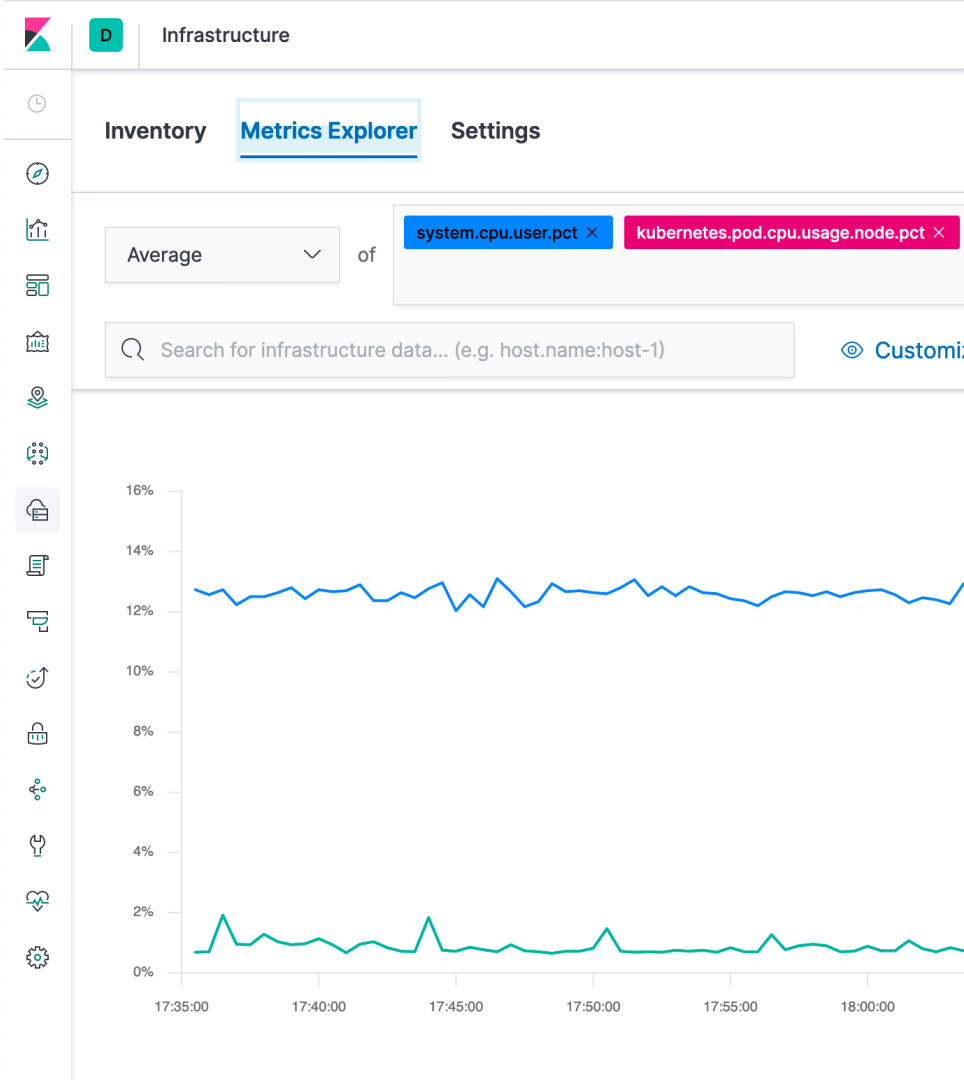
- Host logs
- Host Metrics in deatil
- APM Traces
- Uptime information



Explore your metrics

Infra / Metrics Explorer

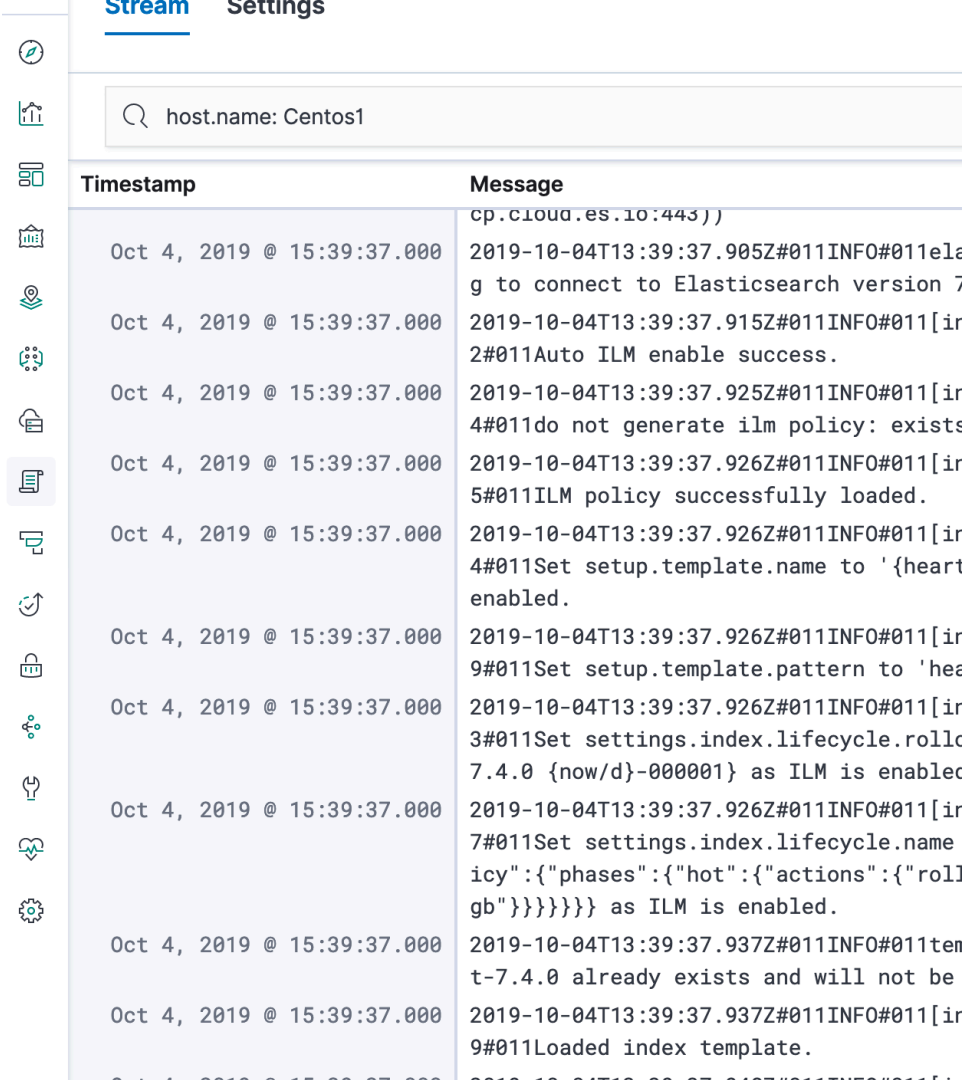
- Useful to identify data points/feeds for
  - Alerting
  - Visualisations / Dashboards
  - Machine learning jobs



View logs

Logs

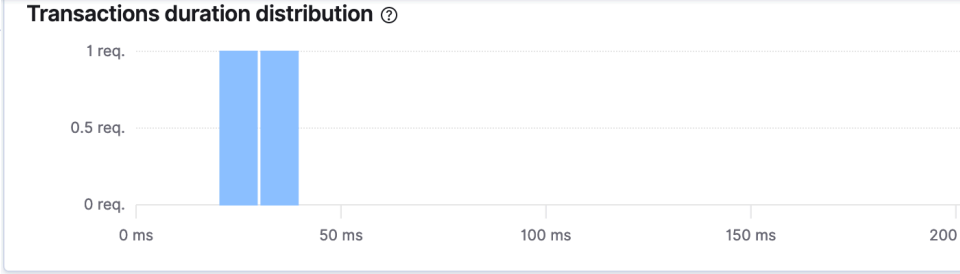
- View logs with infinite scroll
- Can be live streamed and ‘tailed’
- Adjusted columns as needed
- Logs filtered:
  - Via context menus from other apps, or
  - Manually via KQL

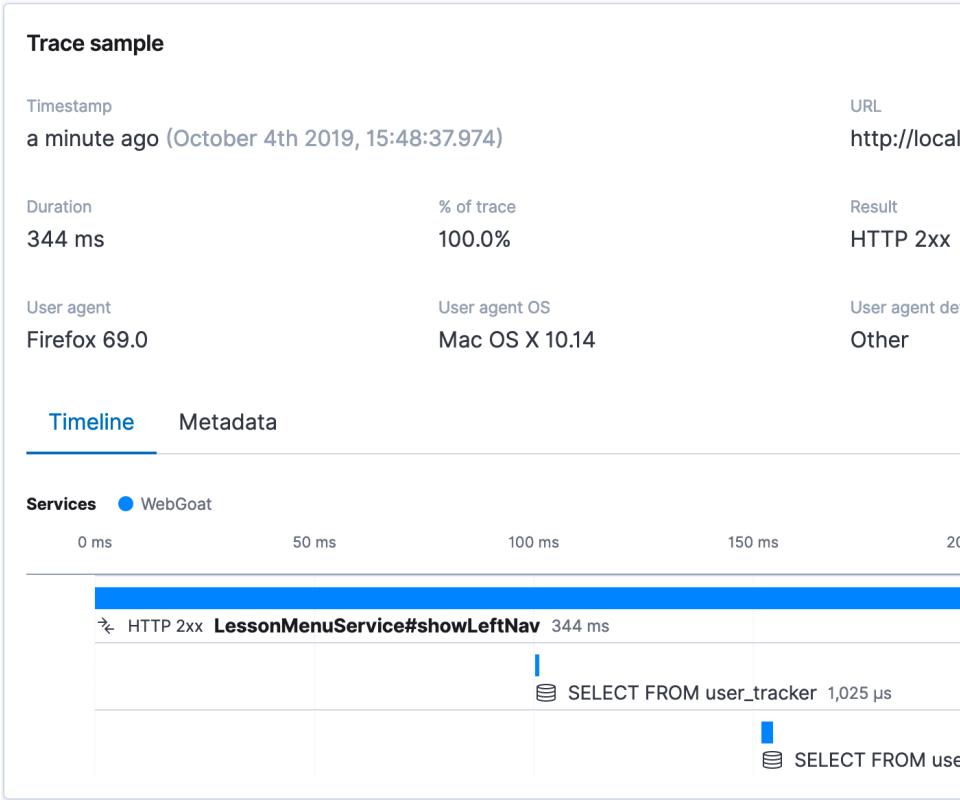


APM
Tracing key applications

APM

- Find out what's happening with that SQL or function call
- Deep dive into details beyond what logs alone offer
  - e.g. See The SQL statement create in reaction to user input
  - Maybe "Little bobby tables" tried to login?

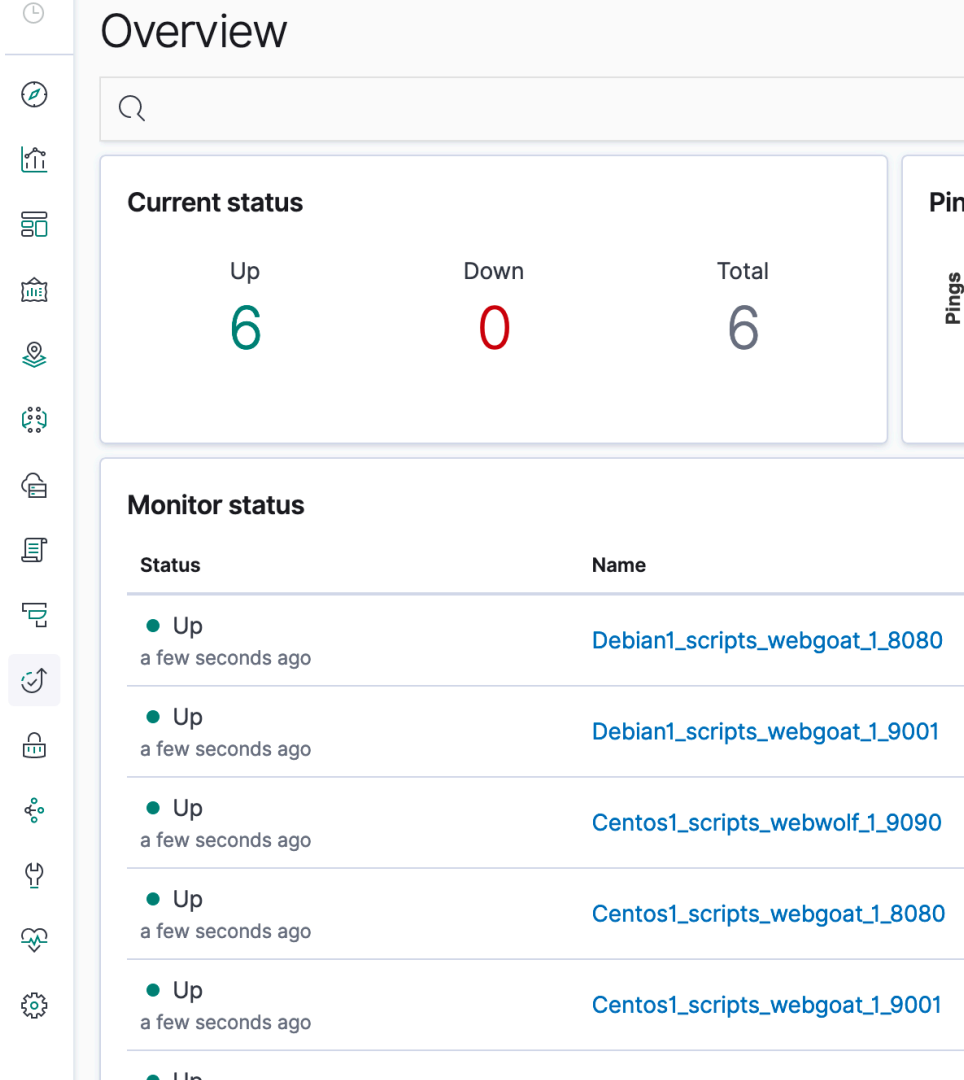




Monitor services' availability

Uptime

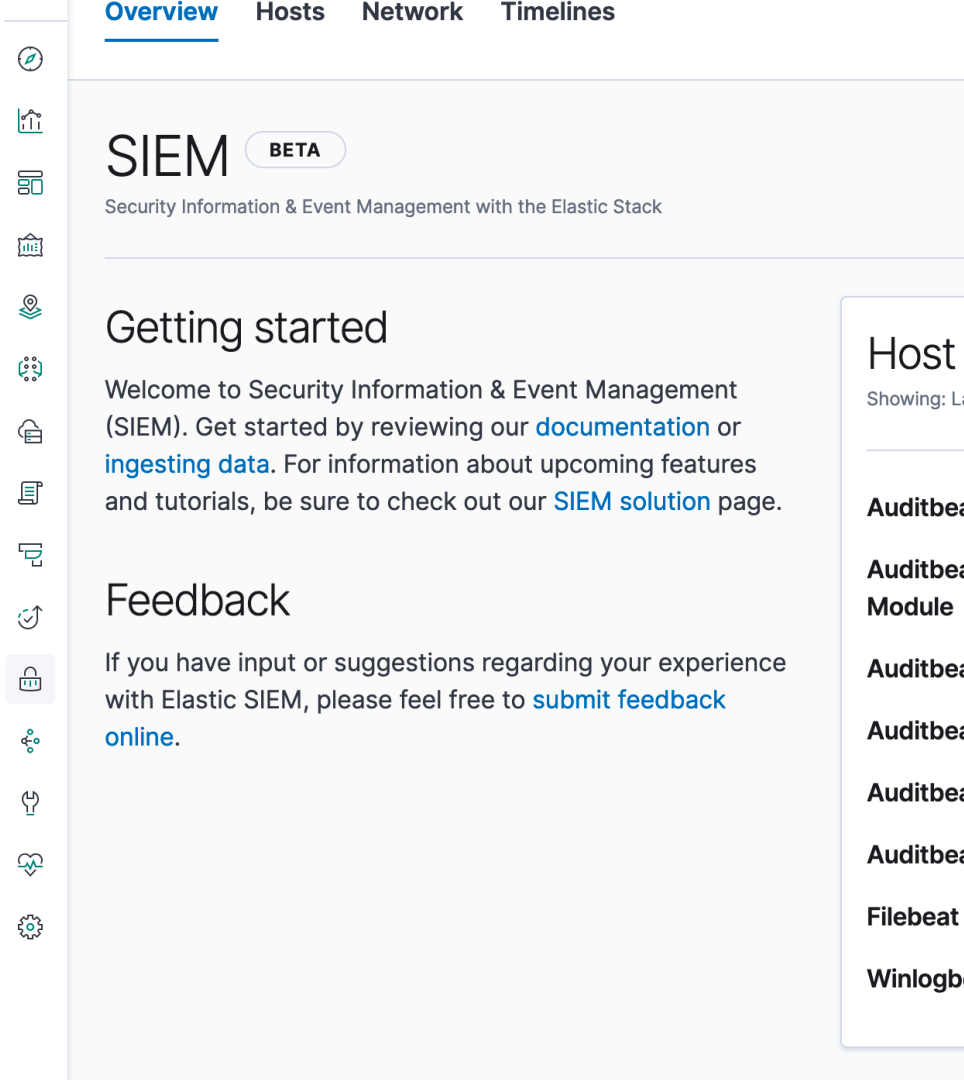
- Metrics from an out side view
  - Where as host collected metrics are an inside view of services
- Are services running stable?
- Are they responding correctly?
- What was happening with my services on that date?



Finally the SIEM app

SIEM

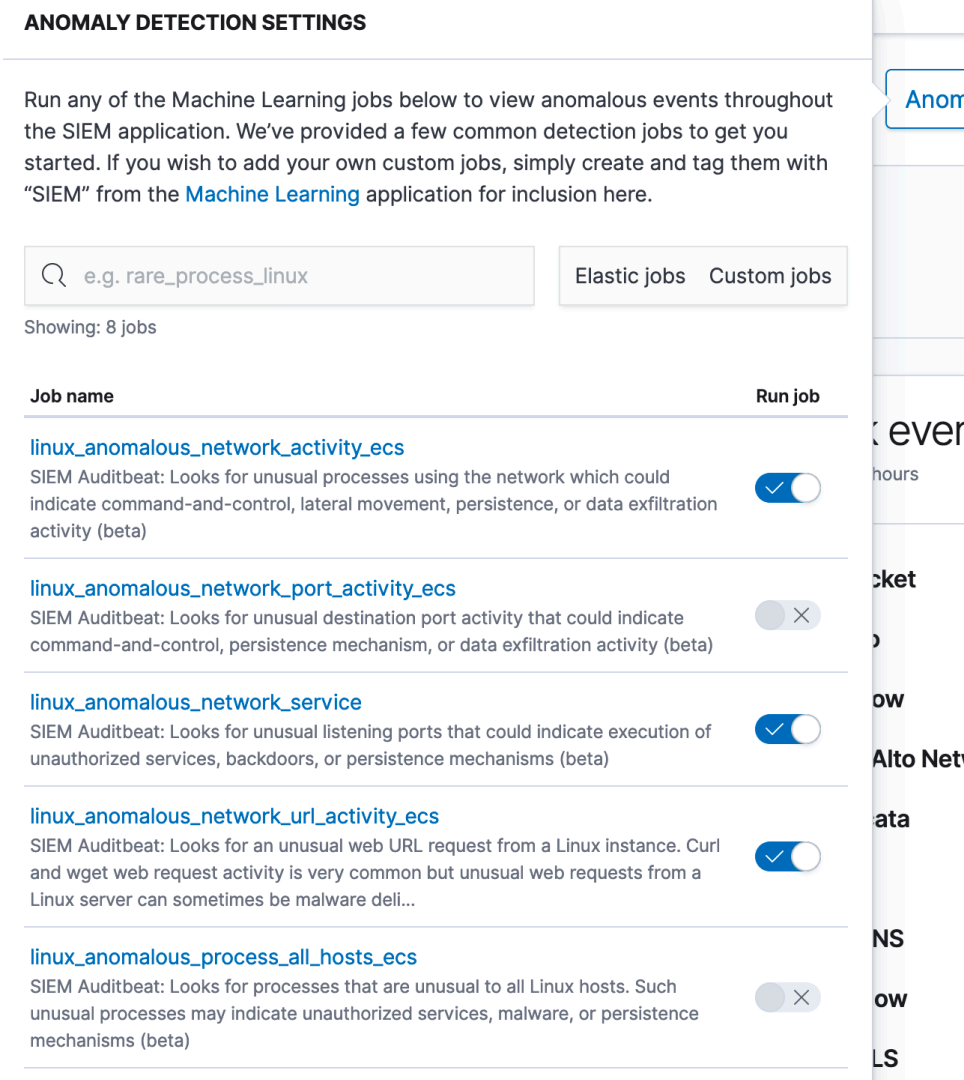
- One can already use ES for security analytics, but the SIEM app brings many features together into one place
- The SIEM app is being developed in public view; many features still to come:
  - Threat Intel, IOC, Case-mgmt., etc.
- This screen gives an overview of the data available to the SIEM



SIEM & ML Anomaly Detection

SIEM / Anomaly Detection

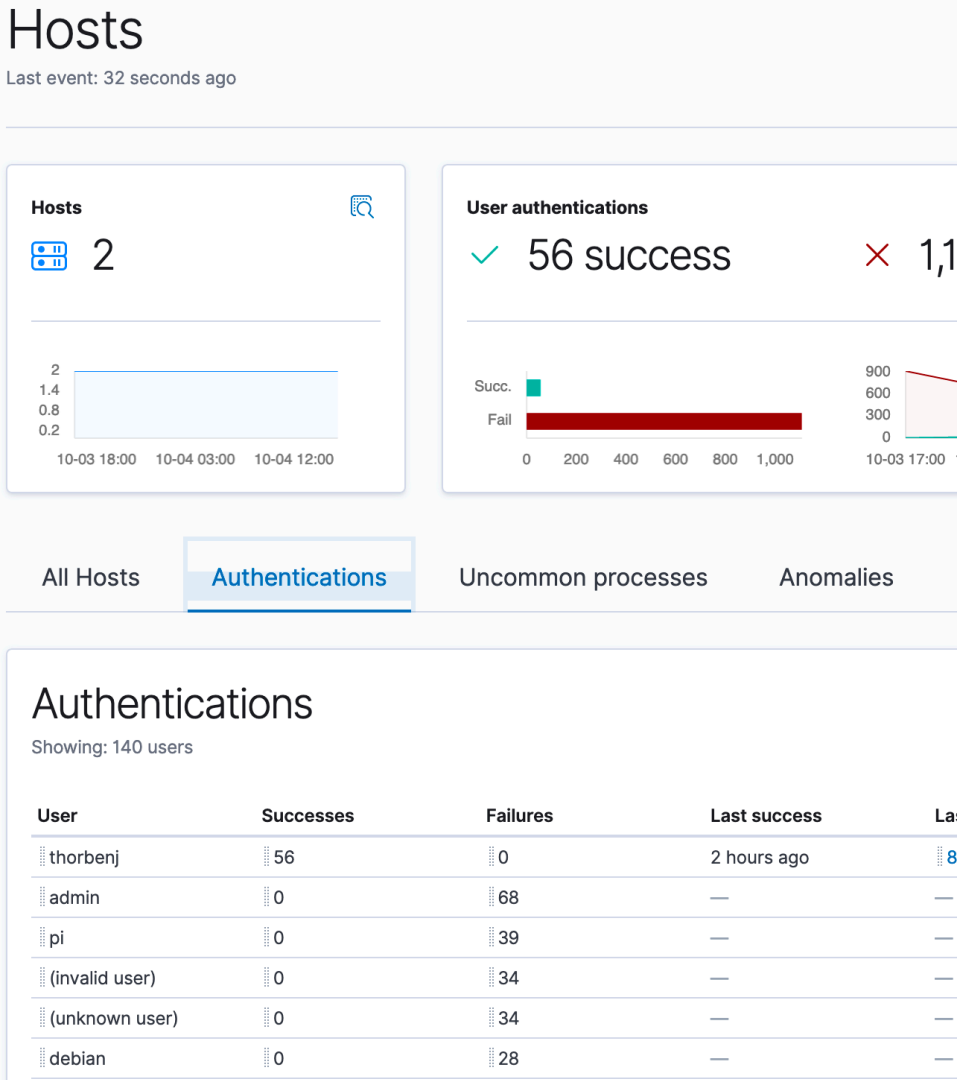
- OOTB Anomaly Detection ML jobs curated for you by Elastic
  - More ML jobs with every release!
- Results of (any) anomaly detection ML job integrated into the various SIEM views
- Help get you started with defining your own ML jobs for anomaly detection



What's happening on my Hosts

SIEM / Hosts

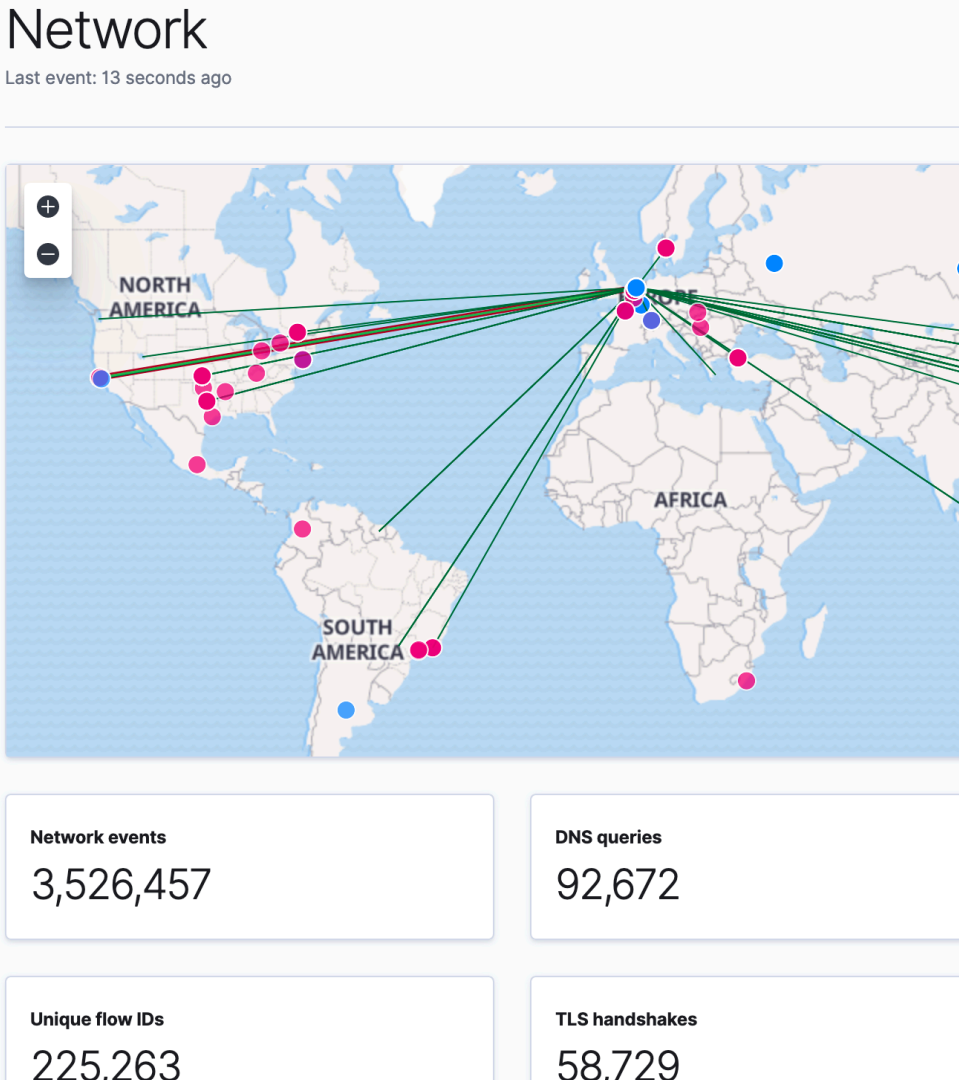
- An overview your host's activities
- Break down of
  - Authentications
  - Uncommon processes
  - ML detected anomalies
  - System event



What's happening on my network?

SIEM / Network

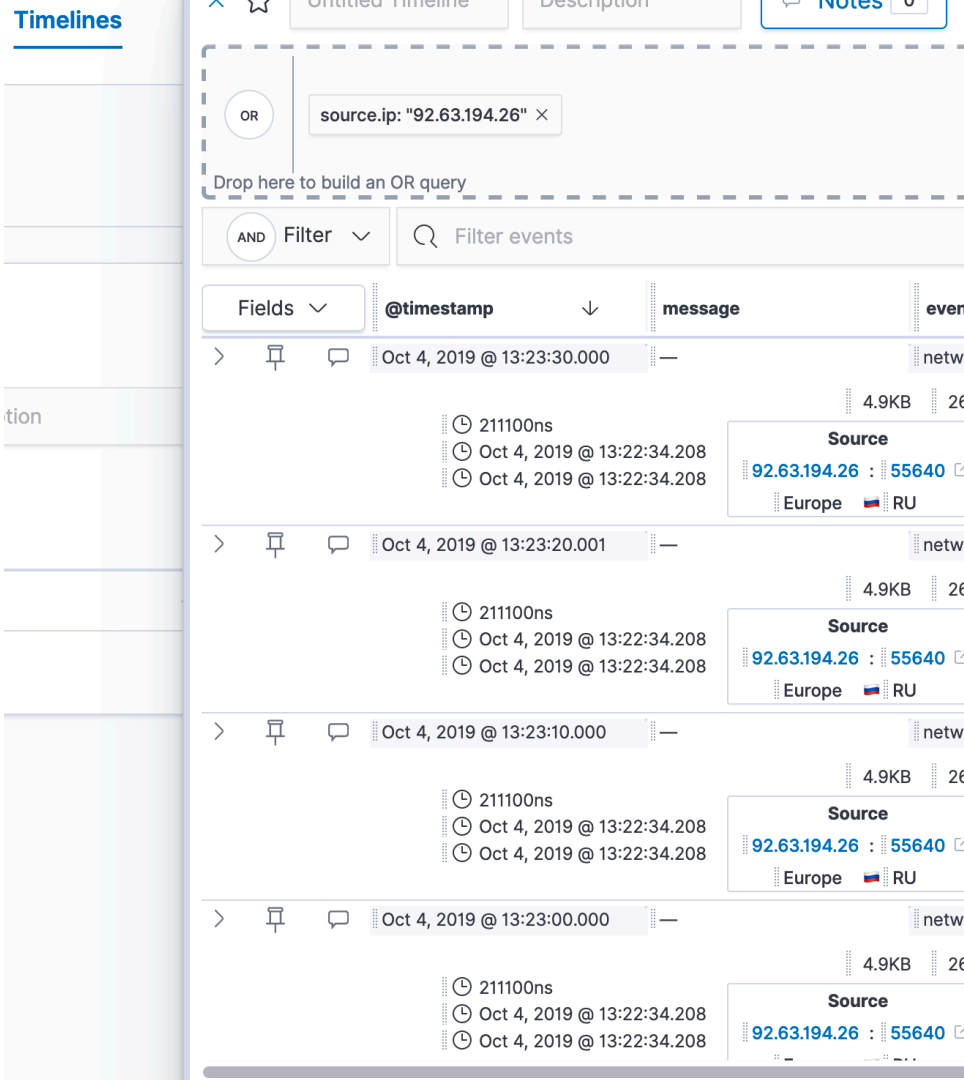
- An overview of network activities
- Network flows from various sources visualised in maps
- Break down of
  - Network events
  - Top DNS queries
  - Open and TLS flows
  - Top Sources and Destinations
  - ML detected anomalies



Super-timelining!

SIEM / Timelines

- First major SIEM feature to be delivered from the roadmap
- Build “supertimes” combining data from all possible sources
- Drag and Drop aretfacts into the timeline tool
- Add comments/notes to time records
- Store and retrieve all created timelines



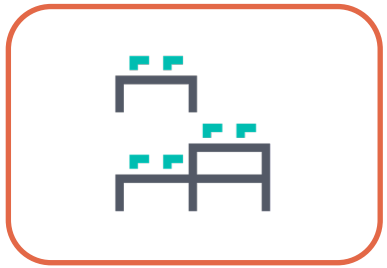
Wrapping up

elastic

The key building blocks

Elasticsearch

Kibana & Apps

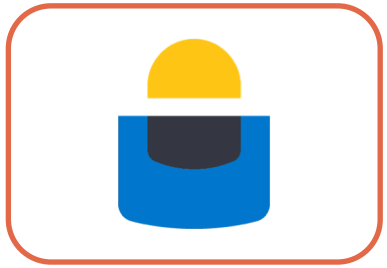


Elastic Common Schema (ECS)

Machine Learning

Beats

Logstash



Security Analytics at Speed & Scale

Community

elastic

Mitre Att&ck coverage with winlogbeat + sysmon (windows)

sysmon config from:
https://github.com/olafhartong/sysmon-modular

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	25 items	41 items	21 items	49 items	16 items	19 items	15 items	13 items	9 items	20 items
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	Binary Padding	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	BITS Jobs	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 from Information Repositories	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 Local System	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 Network Shared Drive	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 Removable Media	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 Staged	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-hop Proxy
	Mshta	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning	Query Registry	Shared Webroot	Man in the Browser		Multi-Stage Channels
	PowerShell	Create Account	Image File Execution Options Injection	Disabling Security Tools	Network Sniffing	Remote System Discovery	Taint Shared Content	Screen Capture		Multiband Communication
	Regsvcs/Regasm	DLL Search Order Hijacking	New Service	DLL Search Order Hijacking	Password Filter DLL	Security Software Discovery	Third-party Software	Video Capture		Multilayer Encryption
	Regsvr32	External Remote Services	Path Interception	DLL Side-Loading	Private Keys	System Information Discovery	Windows Admin Shares			Remote Access Tools
	Rundll32	File System Permissions Weakness	Port Monitors	Exploitation for Defense Evasion	Replication Through Removable Media	System Network Configuration Discovery	Windows Remote Management			Remote File Copy
	Scheduled Task	Hidden Files and Directories	Process Injection	Extra Window Memory Injection	Two-Factor Authentication Interception	System Network Connections Discovery				Standard Application Layer Protocol
	Scripting	Hooking	Scheduled Task	File Deletion		System Owner/User Discovery				Standard Cryptographic Protocol
	Service Execution	Hypervisor	Service Registry Permissions Weakness	File System Logical Offsets		System Service Discovery				Standard Non-Application Layer Protocol
	Signed Binary Proxy Execution	Image File Execution Options Injection	SID-History Injection	Hidden Files and Directories		System Time Discovery				Uncommonly Used Port
	Signed Script Proxy Execution	Logon Scripts	Valid Accounts	Image File Execution Options Injection						Web Service
	Third-party Software	LSASS Driver	Web Shell	Indicator Blocking						
	Trusted Developer Utilities	Modify Existing Service		Indicator Removal from Tools						
	User Execution	Netsh Helper DLL		Indicator Removal on Host						
	Windows Management Instrumentation	New Service		Indirect Command Execution						
	Windows Remote Management	Office Application Startup		Install Root Certificate						
		Path Interception		InstallUtil						
		Port Monitors		Masquerading						
		Redundant Access		Modify Registry						
		Registry Run Keys / Start Folder		Mshta						
		Scheduled Task		Network Share Connection Removal						
		Screensaver		NTFS File Attributes						
		Security Support Provider		Obfuscated Files or Information						
		Service Registry Permissions Weakness		Process Doppelgänging						
		Shortcut Modification		Process Hollowing						
		SIP and Trust Provider Hijacking		Process Injection						
		System Firmware		Redundant Access						
		Time Providers		Regsvcs/Regasm						
		Valid Accounts		Regsvr32						
		Web Shell		Rootkit						
		Windows Management Instrumentation Event Subscription		Rundll32						
		Winlogon Helper DLL		Scripting						
				Signed Binary Proxy Execution						
				Signed Script Proxy Execution						
				SIP and Trust Provider Hijacking						
				Software Packing						
				Timestomp						
				Trusted Developer Utilities						
				Valid Accounts						
				Web Service						

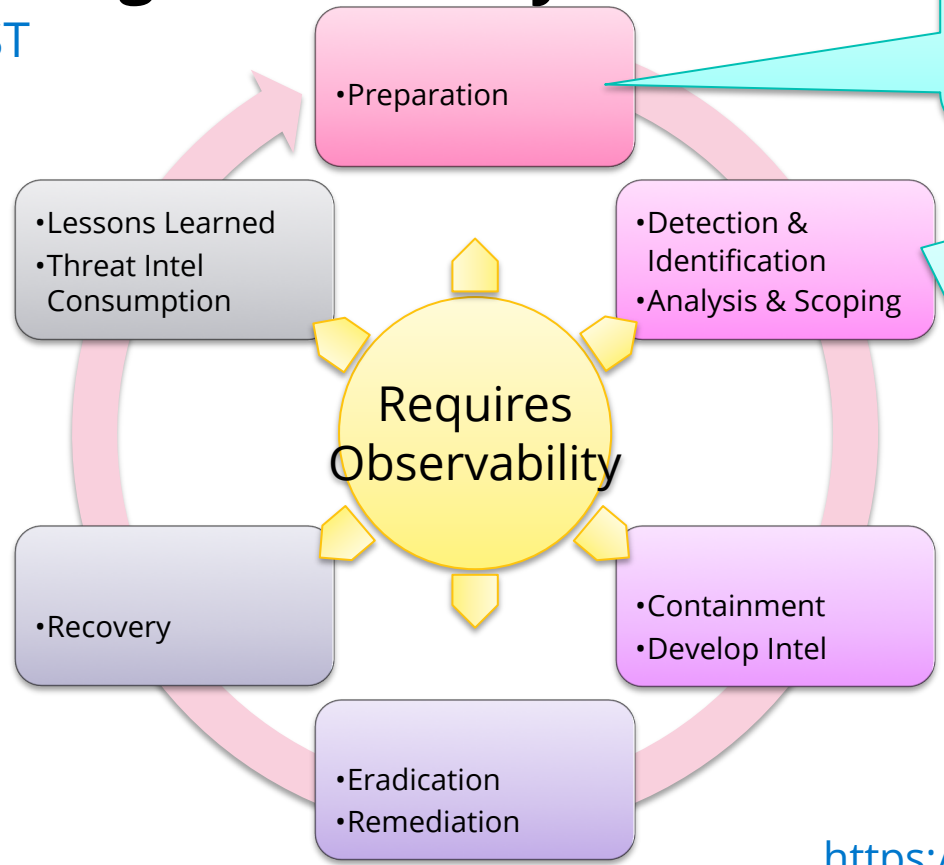
Mitre Att&ck coverage with auditbeat + auditd (linux)

auditd config from:
https://github.com/bfuzzy/auditd-attack

https://ela.st/es-ootb elastic

Incident Management Lifecycle

à la SANS & NIST



Building your Observability capabilities with Elastic Stack tools

Security Analytics

- Discover
- Dashboards
- ML Jobs
- Infra & Log viewer
- Uptime
- & SIEM

https://ela.st/es-ootb

elastic

Thank you for your time!

- **https://ela.st/es-ootb**

Thorben Jändling <thorbenj@elastic.co>

- Solutions Architect @ https://elastic.co/
- https://linkedin.com/in/thorbenj

elastic