



# Empower your Security Analysts with the Elastic Stack

---

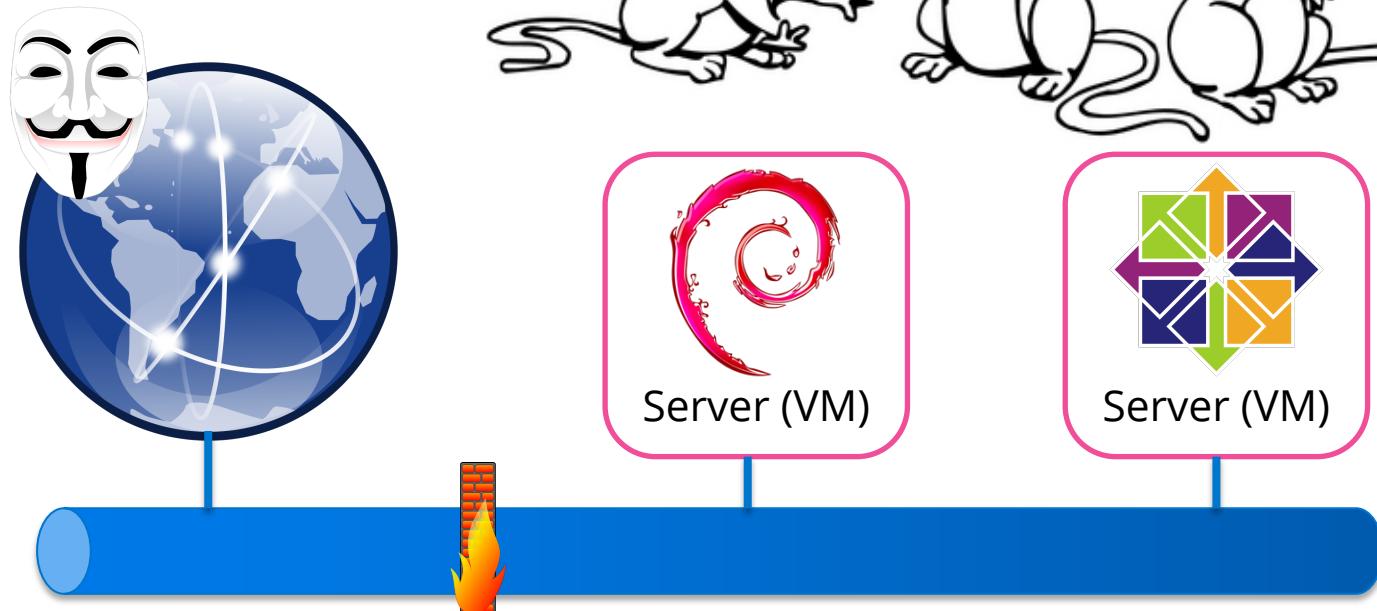
Thorben Jändling – Solutions Architect @Elastic

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

From Zero to Security Analyst in 30min.

# What ICT Security can feel like

But, also our initial demo setup



# I just followed the documentation

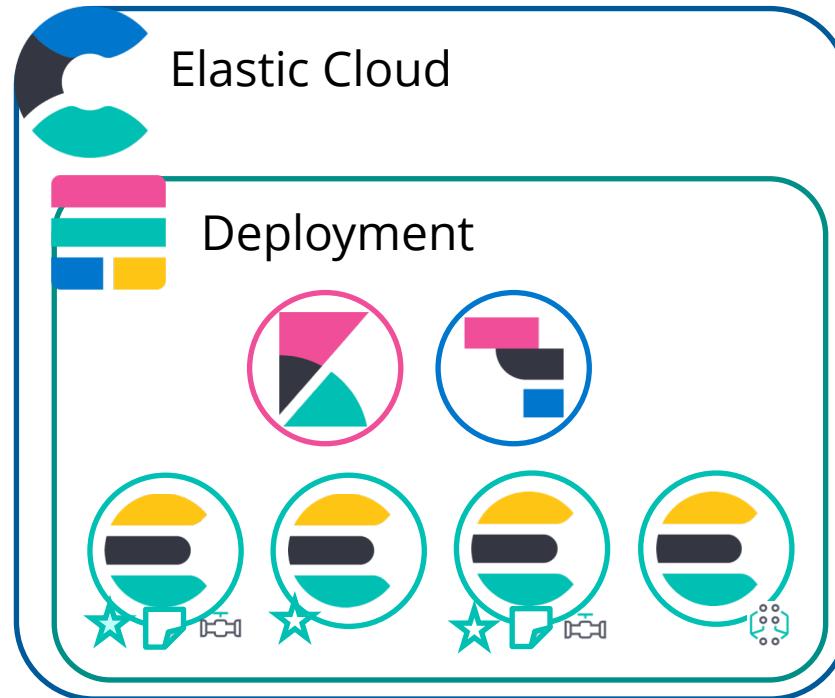
Follow along at home: <https://ela.st/es-ootb>

- 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**

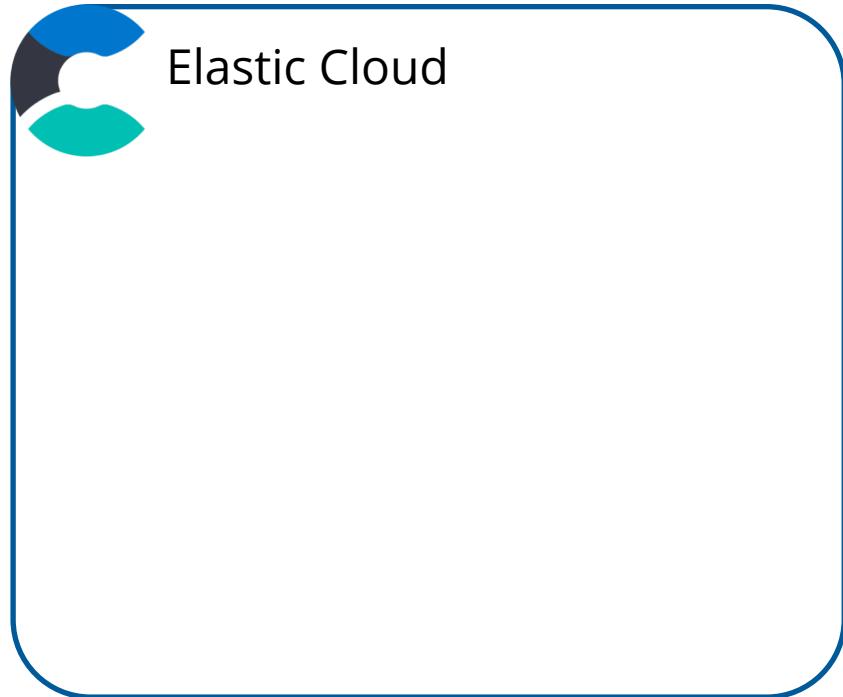
# Phase 1: Deploy Elasticsearch, Kibana & APM server

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



# Goto Elastic Cloud

Phase 1 – Step 1



The image shows the Elastic Cloud login interface. It features two input fields: 'Email' with a user icon and 'Password' with a lock icon. Below these are 'Log in' and 'Forgot password?' buttons. A 'Sign up now.' link is also present. The Elastic logo is at the bottom left, and a circular icon with the same 'C' logo is on the right.

Email

Password

[Log in](#) [Forgot password?](#)

Don't have an account? [Sign up now.](#)

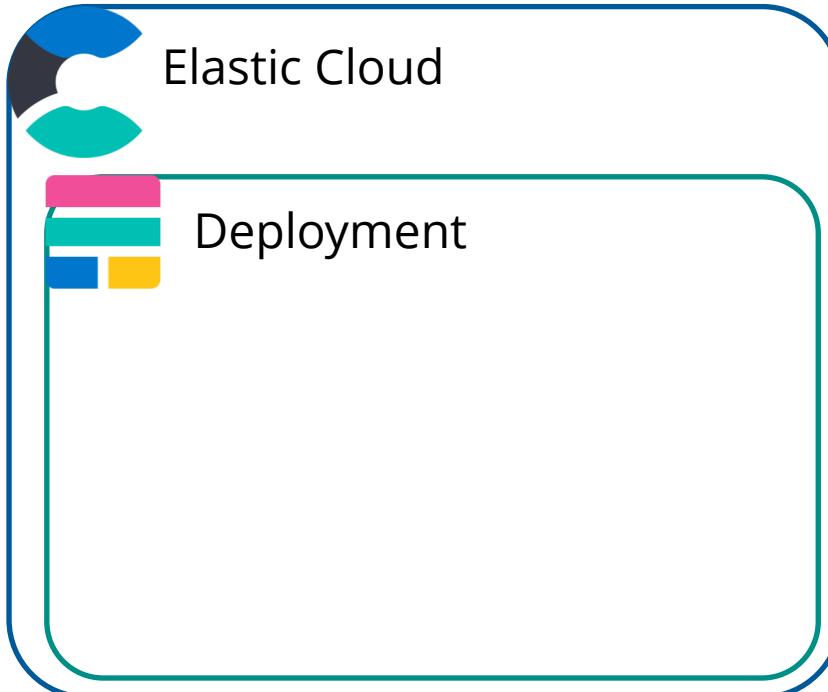
 elastic

# Create deployment

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

# Create Deployment

## Phase 1 – Step 2A



### 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 V

Asia Pacific (Tokyo)

Asia Pacific (Sydney)

### 4 Set up your deployment

Elastic Stack version

7.4.0 [Edit](#)

# Customise Deployment

## Phase 1 – Step 2B

The interface shows a summary of the deployment setup. It includes a large 'Deployment' section with three nodes represented by teal circles with yellow and grey bars. Above this is a 'Cross Cluster Search' section with a pink circular icon containing a search symbol.

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](#)



#### 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

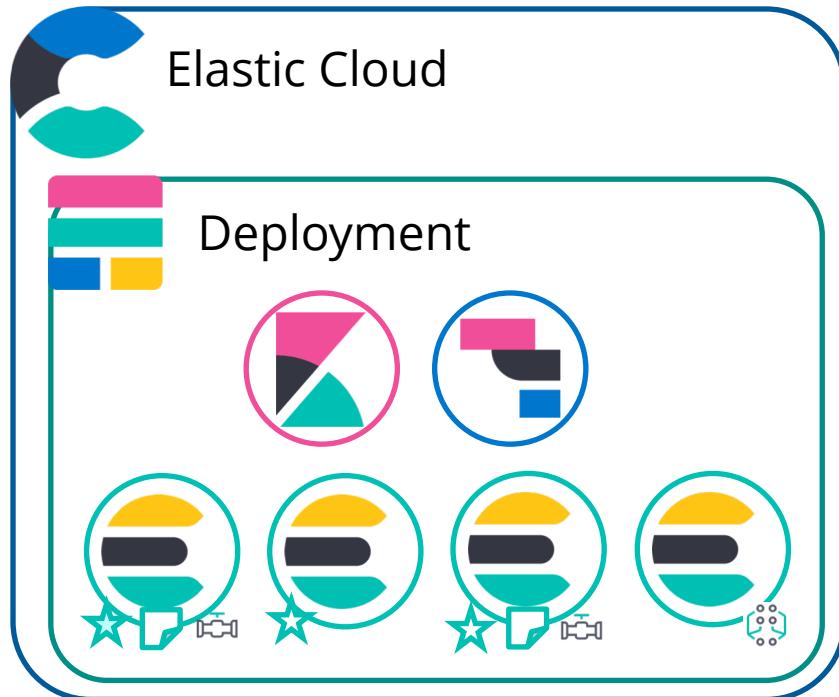
\$0.5696

[Create deployment](#)

[Customize deployment](#)

# Enable APM + Machine Learning

Phase 1 – Step 2C



Machine Learning 1 configuration

Automatically model the behavior of your Elasticsearch data — trends, anomalies, and more.

**gcp.ml.1** Machine Learning

An Elasticsearch machine learning instance.

**Enable**

**gcp.ml.1** Machine Learning

An Elasticsearch machine learning instance.

Fault tolerance

1 zone  2 zones  3 zones

RAM per Node

1 GB 2 GB 4 GB 8 GB 16 GB 32 GB 64 GB

Summary

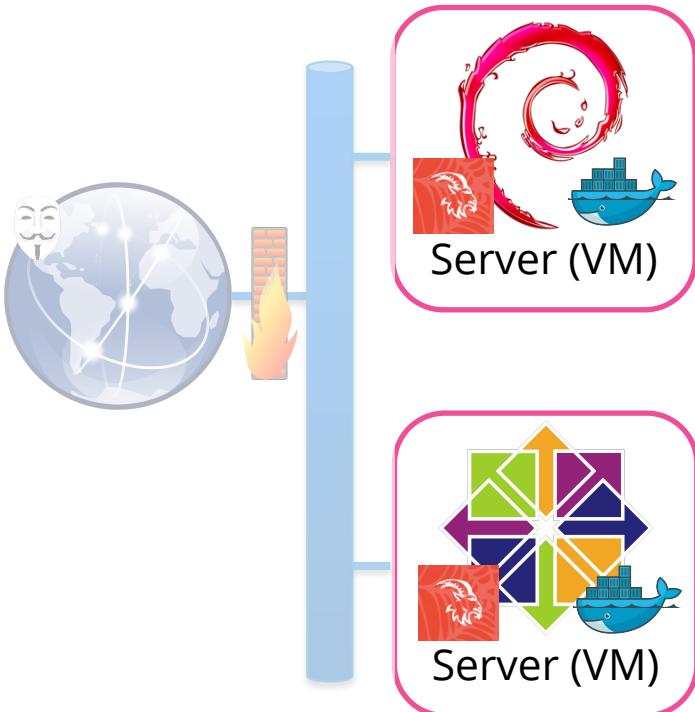
1 GB RAM X 1 node X 1 zone = 1 GB RAM

✓ Create deployment

The screenshot shows the configuration of an Elasticsearch machine learning instance named 'gcp.ml.1'. It highlights several key configuration options: the 'Enable' checkbox, the fault tolerance setting (1 zone selected), the RAM per node slider (set to 1 GB), and the summary calculation '1 GB RAM X 1 node X 1 zone = 1 GB RAM'. A red arrow points from the 'Create deployment' button at the bottom right back up to the 'Enable' checkbox at the top left.

# Phase 2: Deploy our web services

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



The screenshot shows the 'WEBGOAT' application interface. At the top right, the word 'WebGoat' is displayed next to a menu icon. A sidebar on the left lists various security flaws: Introduction, General, Injection Flaws, Authentication Flaws, Cross-Site Scripting (XSS), Access Control Flaws, Insecure Communication, Insecure Deserialization, Request Forgeries, Vulnerable Components - A9, Client side, and Challenges. To the right of the sidebar, a large heading 'What is WebGoat?' is shown, followed by a detailed description of the application's purpose and features.

Introduction  
General  
Injection Flaws  
Authentication Flaws  
Cross-Site Scripting (XSS)  
Access Control Flaws  
Insecure Communication  
Insecure Deserialization  
Request Forgeries  
Vulnerable Components - A9  
Client side  
Challenges

What is WebGoat?  
WebGoat is a deliberately insecure application t...  
popular open source components.  
Now, while we in no way condone causing intent...  
understanding just what happens when even a...

# 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)

```
ES_CLOUD_ID="elasticon"
ES_CLOUD_AUTH="elastic"
ES_APM_SERVER="https://
ES_APM_TOKEN="nzMaaC3x
ES_SITE_LOCATION="52.3
```

# WARNING

## WARNING

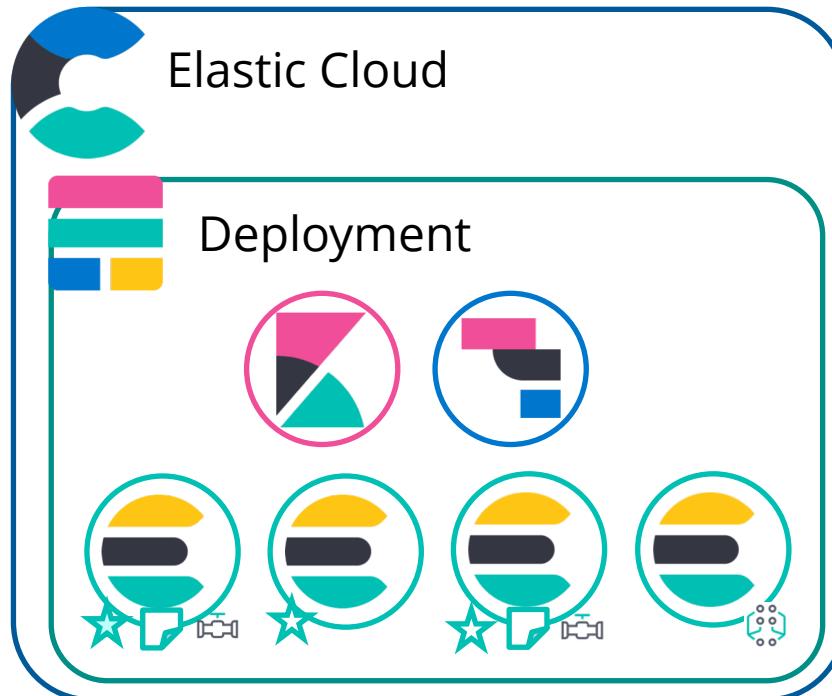
- In this demonstration we have been configuring our agents to use the 'elastic' superuser.
- This user has full admin access over your elasticsearch deployment.
- **Do not use the 'elastic' account for agent deployment**

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.

# Grab you cloud deployment details

Phases 3 & 4 preparation



# 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 Kibana.

Username

elastic

Password

p0xusq2QBZzvx6lq7DLUDS2o

[COPY](#)

[DOWNLOAD](#)

## Creation in progress

Here's what's happening under the hood.



e.g.: healthy\_configuration:y apm

# elasticon

## Grab your Cloud ID

Phases 3 & 4 preparation – Step 2

In “es-ootb.conf”:

```
ES_CLOUD_ID="elasticon:ZXVyb3B1LX
ES_CLOUD_AUTH="elastic:p0xusq2QBZ
ES_APM_SERVER=
ES_APM_TOKEN=
```

Deployment name

elasticon

Edit

Deployment

• Healthy

Deployment version

v7.4.0

Applications

 Elasticsearch [?](#)

[Launch](#) | [Copy Endpoint URL](#)

 Kibana [?](#)

[Launch](#) | [Copy Endpoint URL](#)

 APM [?](#)

[Launch](#) | [Copy APM Server URL](#)

Cloud ID [?](#)

elasticon:ZXVyb3B1LXd1  
4Yjk3MzE0YTE0YzRhOWQ4N  
Mjk0ODQ0ODI1M2VhMWFiNz

## Instances

All instances

5

gcp.master.1

1

gcp.data.highio.1

2

g

# Grab your APM server credentials

## Phases 3 & 4 preparation – Step 3

In “es-ootb.conf”:

```
ES_CLOUD_ID="elasticon:ZXVyb3B1LX  
ES_CLOUD_AUTH="elastic:p0xusq2QBZ  
ES_APM_SERVER="https://8d74c7195c  
ES_APM_TOKEN="nzMaaC3xokzL6gaKq4"
```

### Deployments

elasticon

- Edit
- Elasticsearch
  - Logs
  - Snapshots
  - API Console
- Kibana
- APM
- Activity
- Security
- Performance

### Custom plugins

### Account

### Help

elasticon

APM 

Application Performance Monitoring (APM)  
next. [Learn more ↗](#)

Complete your APM configuration by creating a

[Dismiss](#)

### Server details

 APM ⓘ  
[Launch](#) | [Copy APM Server URL](#)

  
APM Server secret token  
[nzMaaC3xokzL6gaKq4](#)  [Reset token](#)

### Instances

gcp.apm.1 1



# Give your datacenter's private IPs a location

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

In "es-ootb.conf":

```
ES_CLOUD_ID="elasticon:ZXVyb3B1LX  
ES_CLOUD_AUTH="elastic:p0xusq2QBZ  
ES_APM_SERVER="https://8d74c7195c  
ES_APM_TOKEN="nzMaaC3xokzL6gaKq4"  
  
ES_SITE_LOCATION="52.3667:4.8945"
```

lat long amsterdam

All

Maps

Images

News

About 21'600'000 results (0.65 seconds)

Amsterdam / Coordinates

52.3667° N, 4.8945° E

People also search for



Netherlands



52.1326° N,  
5.2913° E

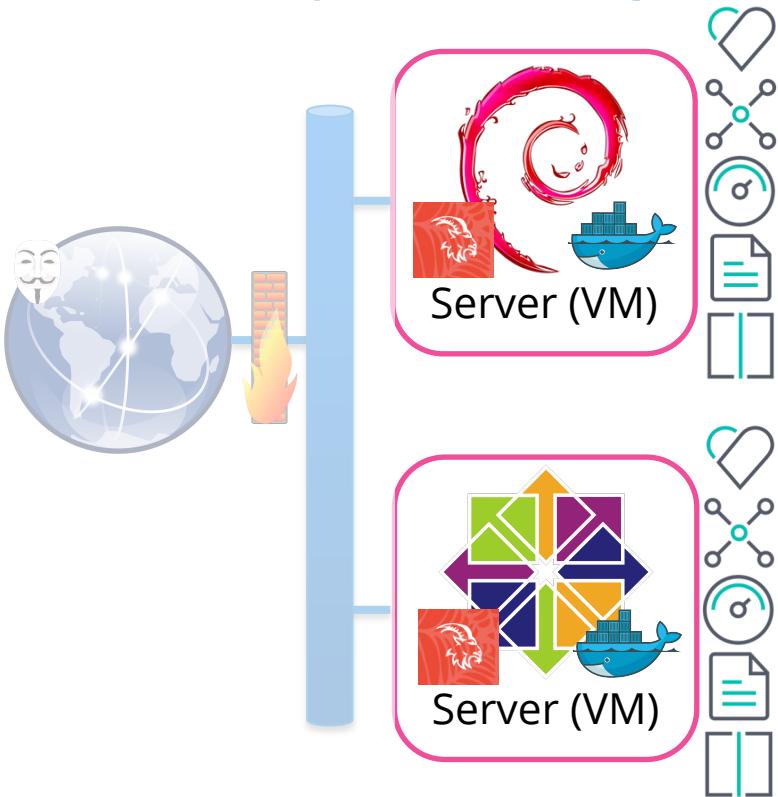


Rotterda

51.9244°  
4.4777°

# 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
```

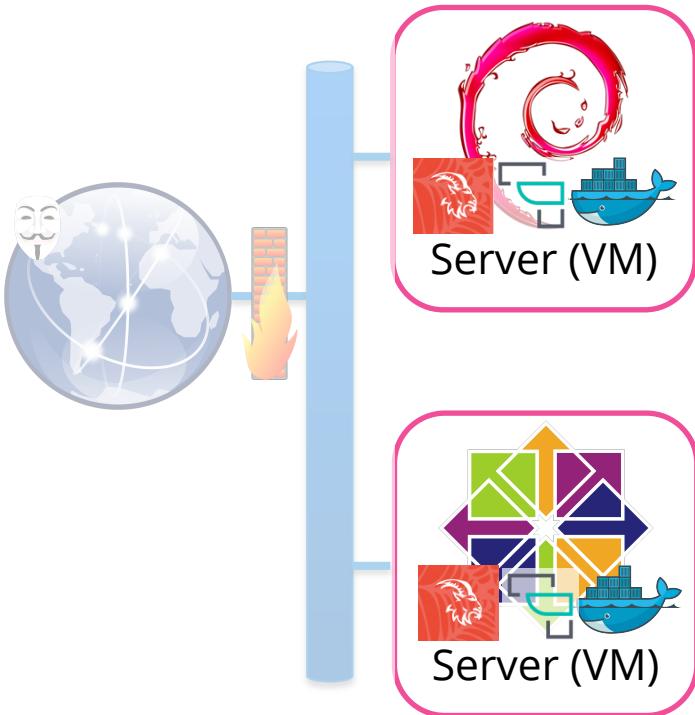
beats-ootb.sh will:

- 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.

# 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 apt-ootb.sh
```

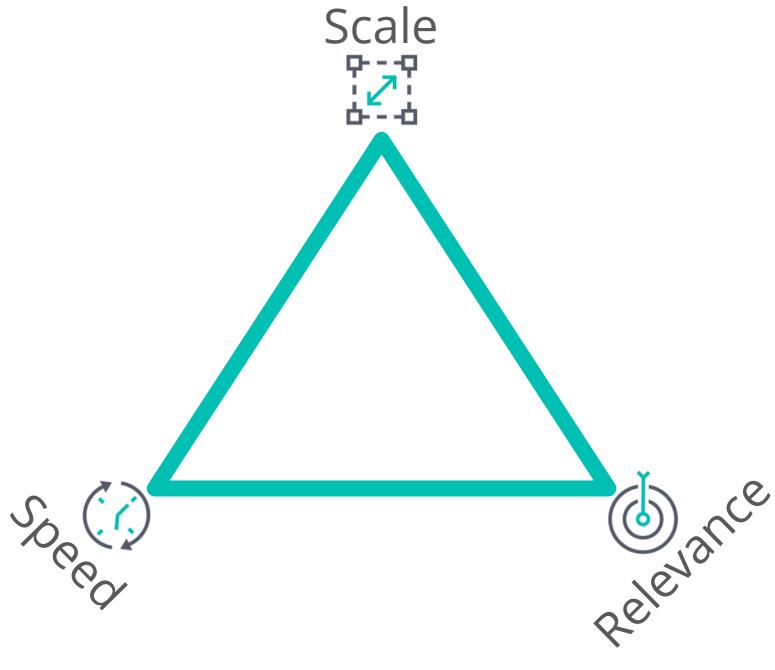
### apt-ootb.sh will:

- 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.

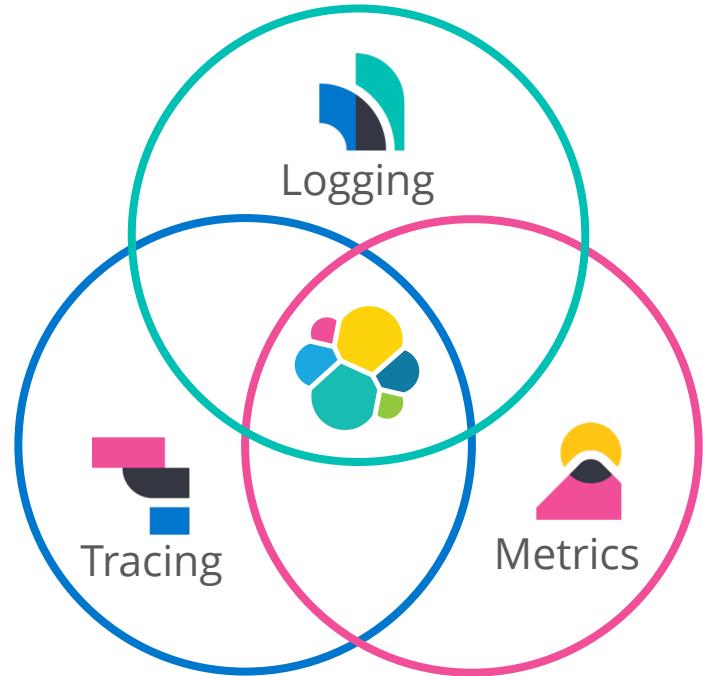
# Unique qualities of the Elastic Stack:

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



Speed, Scale, Relevance

&



Observability (aka Visibility)

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

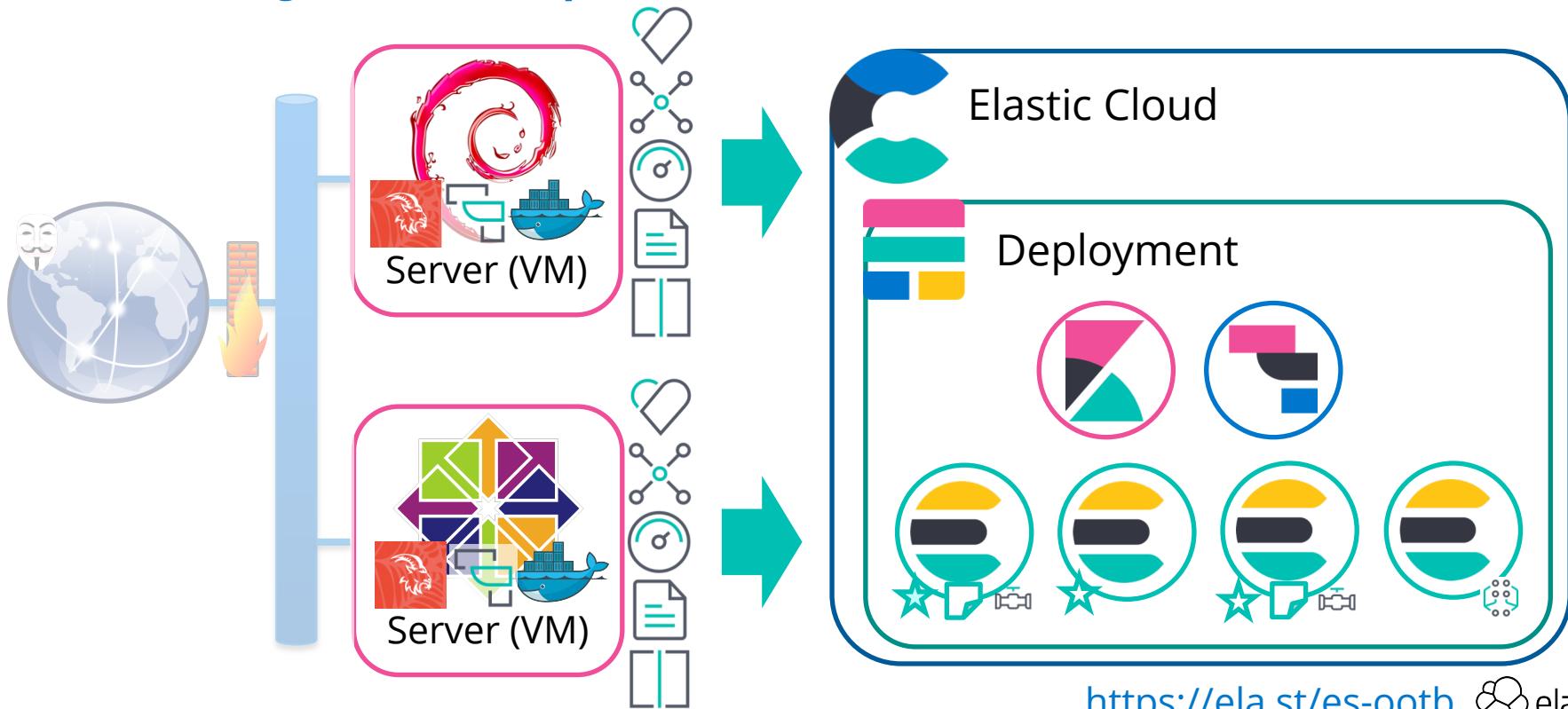
# What you'd like ICT Security to be like

and, also our final demo setup



# The end result

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



# Lets look at our new security analytics tools



This should be the half-way mark

# View our infrastructure

## Infrastructure / default page

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

Drill down:

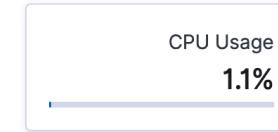
- Host logs
- Host Metrics in detail
- APM Traces
- Uptime information

### Host

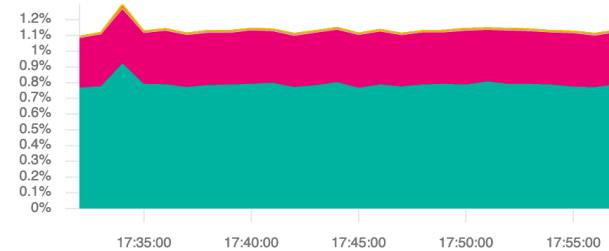
Overview  
CPU Usage  
Load  
Memory Usage  
Network Traffic

Centos1

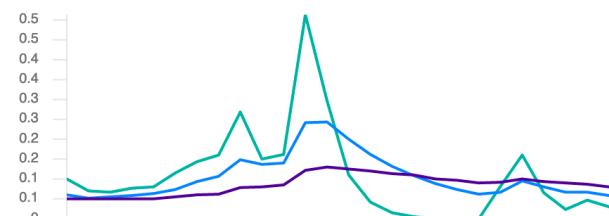
### Host Overview



### CPU Usage



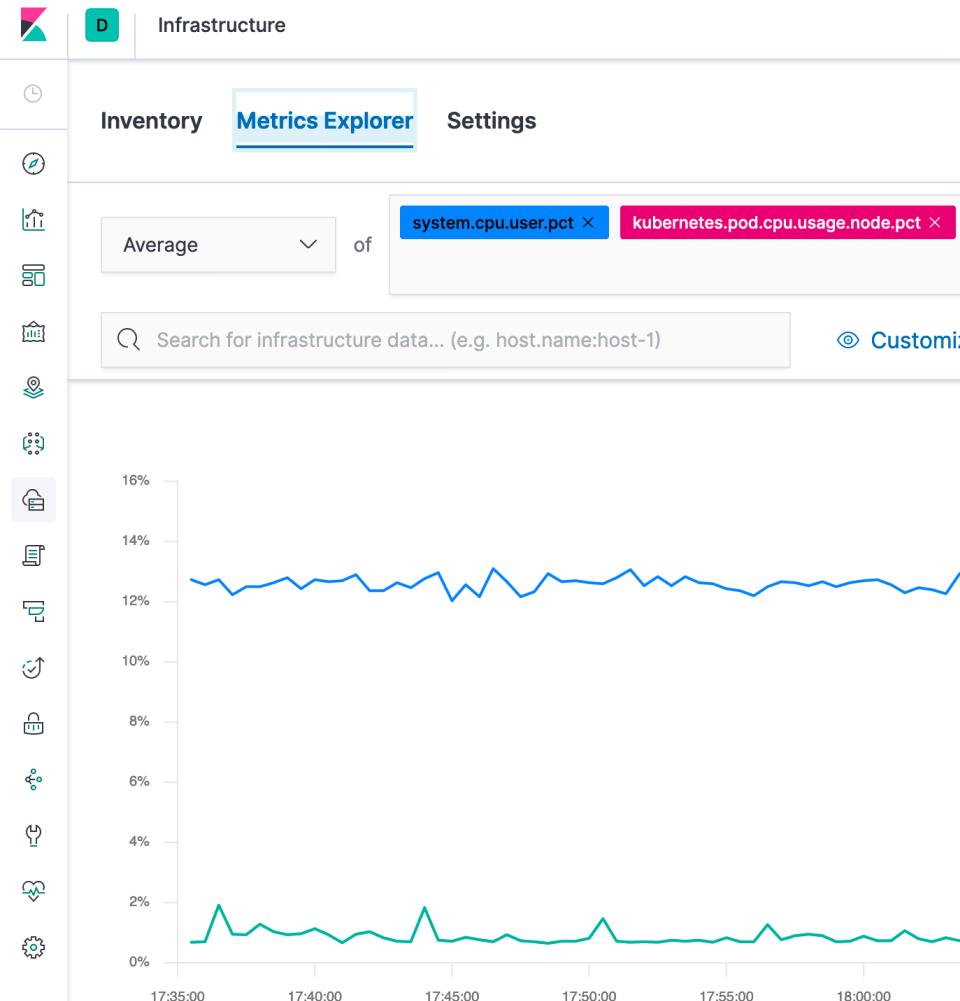
### Load



# Explore your metrics



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



# View 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

Stream		Settings
	Timestamp	Message
	Oct 4, 2019 @ 15:39:37.000	host.name: Centos1 cp.cloud.es.10:443))
	Oct 4, 2019 @ 15:39:37.000	2019-10-04T13:39:37.905Z#011INFO#011elast
	Oct 4, 2019 @ 15:39:37.000	g to connect to Elasticsearch version 7
	Oct 4, 2019 @ 15:39:37.000	2019-10-04T13:39:37.915Z#011INFO#011[in
	Oct 4, 2019 @ 15:39:37.000	2#011Auto ILM enable success.
	Oct 4, 2019 @ 15:39:37.000	2019-10-04T13:39:37.925Z#011INFO#011[in
	Oct 4, 2019 @ 15:39:37.000	4#011do not generate ilm policy: exists
	Oct 4, 2019 @ 15:39:37.000	2019-10-04T13:39:37.926Z#011INFO#011[in
	Oct 4, 2019 @ 15:39:37.000	5#011ILM policy successfully loaded.
	Oct 4, 2019 @ 15:39:37.000	2019-10-04T13:39:37.926Z#011INFO#011[in
	Oct 4, 2019 @ 15:39:37.000	4#011Set setup.template.name to '{heart
	Oct 4, 2019 @ 15:39:37.000	enabled.
	Oct 4, 2019 @ 15:39:37.000	2019-10-04T13:39:37.926Z#011INFO#011[in
	Oct 4, 2019 @ 15:39:37.000	9#011Set setup.template.pattern to 'hea
	Oct 4, 2019 @ 15:39:37.000	2019-10-04T13:39:37.926Z#011INFO#011[in
	Oct 4, 2019 @ 15:39:37.000	3#011Set settings.index.lifecycle.rolle
	Oct 4, 2019 @ 15:39:37.000	7.4.0 {now/d}-000001} as ILM is enabled
	Oct 4, 2019 @ 15:39:37.000	2019-10-04T13:39:37.926Z#011INFO#011[in
	Oct 4, 2019 @ 15:39:37.000	7#011Set settings.index.lifecycle.name
	Oct 4, 2019 @ 15:39:37.000	icy": {"phases": {"hot": {"actions": {"roll
	Oct 4, 2019 @ 15:39:37.000	gb": {}}}}}}} as ILM is enabled.
	Oct 4, 2019 @ 15:39:37.000	2019-10-04T13:39:37.937Z#011INFO#011tem
	Oct 4, 2019 @ 15:39:37.000	t-7.4.0 already exists and will not be
	Oct 4, 2019 @ 15:39:37.000	2019-10-04T13:39:37.937Z#011INFO#011[in
	Oct 4, 2019 @ 15:39:37.000	9#011Loaded index template.

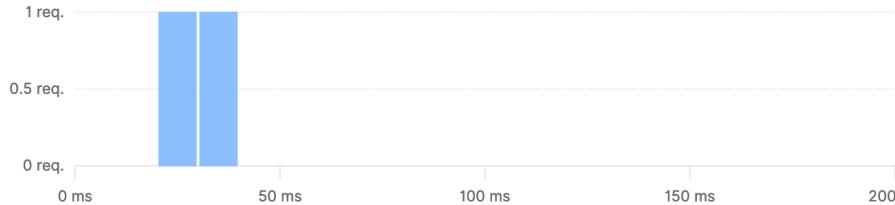
# APM

## Tracing key applications



- 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?

Transactions duration distribution ②



### Trace sample

#### Timestamp

a minute ago (October 4th 2019, 15:48:37.974)

#### URL

http://local

#### Duration

344 ms

#### % of trace

100.0%

#### Result

HTTP 2xx

#### User agent

Firefox 69.0

#### User agent OS

Mac OS X 10.14

#### User agent de

Other

### Timeline

### Metadata

#### Services

WebGoat

0 ms

50 ms

100 ms

150 ms

200 ms

HTTP 2xx LessonMenuService#showLeftNav 344 ms

SELECT FROM user\_tracker 1,025 µs

SELECT FROM user\_

# Monitor services' availability

## Uptime

- Metrics from an outside 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?

The screenshot shows a monitoring interface with a sidebar of icons and a main content area.

**Current status:**

Up	Down	Total
6	0	6

**Monitor status:**

Status	Name
Up a few seconds ago	Debian1_scripts_webgoat_1_8080
Up a few seconds ago	Debian1_scripts_webgoat_1_9001
Up a few seconds ago	Centos1_scripts_webwolf_1_9090
Up a few seconds ago	Centos1_scripts_webgoat_1_8080
Up a few seconds ago	Centos1_scripts_webgoat_1_9001
Up	

# Finally the SIEM app



- 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 BETA

Security Information & Event Management with the Elastic Stack

### Getting started

Welcome to Security Information & Event Management (SIEM). Get started by reviewing our [documentation](#) or [ingesting data](#). For information about upcoming features and tutorials, be sure to check out our [SIEM solution page](#).

### Feedback

If you have input or suggestions regarding your experience with Elastic SIEM, please free to [submit feedback online](#).

Host

Showing: L

Auditbea

Auditbea  
Module

Auditbea

Auditbea

Auditbea

Auditbea

Filebeat

Winlogb

# 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

### ANOMALY DETECTION SETTINGS

Run any of the Machine Learning jobs below to view anomalous events throughout the SIEM application. We've provided a few common detection jobs to get you started. If you wish to add your own custom jobs, simply create and tag them with "SIEM" from the [Machine Learning](#) application for inclusion here.

Elastic jobsCustom jobs

Showing: 8 jobs

Job name	Run job
<a href="#">linux_anomalous_network_activity_ecs</a>	<input checked="" type="checkbox"/>
SIM Auditbeat: Looks for unusual processes using the network which could indicate command-and-control, lateral movement, persistence, or data exfiltration activity (beta)	<input checked="" type="checkbox"/>
<a href="#">linux_anomalous_network_port_activity_ecs</a>	<input type="checkbox"/>
SIM Auditbeat: Looks for unusual destination port activity that could indicate command-and-control, persistence mechanism, or data exfiltration activity (beta)	<input type="checkbox"/>
<a href="#">linux_anomalous_network_service</a>	<input checked="" type="checkbox"/>
SIM Auditbeat: Looks for unusual listening ports that could indicate execution of unauthorized services, backdoors, or persistence mechanisms (beta)	<input checked="" type="checkbox"/>
<a href="#">linux_anomalous_network_url_activity_ecs</a>	<input checked="" type="checkbox"/>
SIM Auditbeat: Looks for an unusual web URL request from a Linux instance. Curl and wget web request activity is very common but unusual web requests from a Linux server can sometimes be malware deli...	<input checked="" type="checkbox"/>
<a href="#">linux_anomalous_process_all_hosts_ecs</a>	<input type="checkbox"/>
SIM Auditbeat: Looks for processes that are unusual to all Linux hosts. Such unusual processes may indicate unauthorized services, malware, or persistence mechanisms (beta)	<input type="checkbox"/>

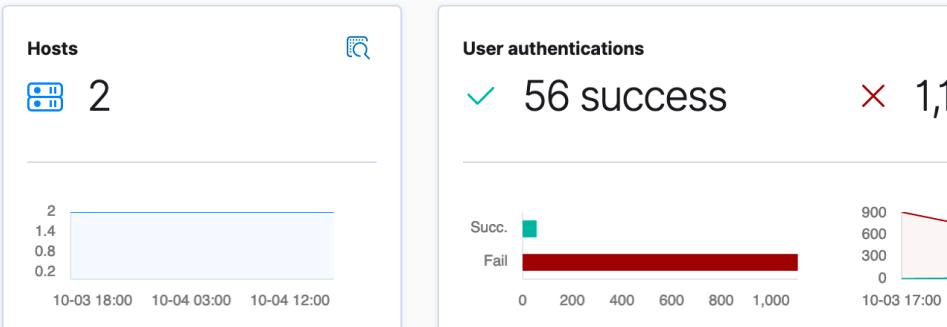
# What's happening on my Hosts



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

## Hosts

Last event: 32 seconds ago



All Hosts

Authentications

Uncommon processes

Anomalies

## Authentications

Showing: 140 users

User	Successes	Failures	Last success	Last failure
thorbenj	56	0	2 hours ago	8 hours ago
admin	0	68	—	—
pi	0	39	—	—
(invalid user)	0	34	—	—
(unknown user)	0	34	—	—
debian	0	28	—	—

# 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

## Network

Last event: 13 seconds ago



### Network events

3,526,457

### DNS queries

92,672

### Unique flow IDs

225,263

### TLS handshakes

58,729

# Super-timeline!



## SIEM / Timelines

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

## Timelines

The screenshot shows the Splunk Timeline interface. At the top, there's a search bar with the query "source.ip: \"92.63.194.26\"". Below the search bar, there's a section titled "Drop here to build an OR query" with an "OR" button. There are two main timeline sections, each starting with an "AND Filter" dropdown and a "Filter events" search bar. The first timeline starts at "Oct 4, 2019 @ 13:23:30.000" and contains three events: "211100ns", "Oct 4, 2019 @ 13:22:34.208", and "Oct 4, 2019 @ 13:22:34.208". The second timeline starts at "Oct 4, 2019 @ 13:23:20.001" and also contains three events: "211100ns", "Oct 4, 2019 @ 13:22:34.208", and "Oct 4, 2019 @ 13:22:34.208". The third timeline starts at "Oct 4, 2019 @ 13:23:10.000" and contains the same three events. The fourth timeline starts at "Oct 4, 2019 @ 13:23:00.000" and contains the same three events. Each event entry includes a timestamp, a "Source" field (92.63.194.26), a "Type" field (55640), and a location field (Europe, RU). The interface also shows network and file sizes (4.9KB) and file counts (26).

# Wrapping up



# The key building blocks



Elasticsearch



Kibana & Apps



Elastic Common  
Schema (ECS)



Machine  
Learning



Beats



Logstash



Security Analytics  
at Speed & Scale



Community

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

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



# Mitre Att&ck coverage with auditbeat + auditd-attack

auditd config from:  
<https://github.com/bfuzzz/auditd-attack>

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
9 items	10 items	13 items	7 items	22 items	9 items	13 items	6 items	10 items	9 items	21 items
Drive-by Compromise	Command-Line Interface	.bash_profile and .bashrc	Exploitation for Privilege Escalation	Binary Padding	Bash History	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Exploitation for Client Execution	Bootkit	Process Injection	Clear Command History	Brute Force	Browser Bookmark Discovery	Automated Collection	Data Compressed	Communication Through Removable Media	
Hardware Additions	Graphical User Interface	Browser Extensions	Setuid and Setgid	Disabling Security Tools	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Connection Proxy
Spearphishing Attachment	Create Account	Sudo			Credentials in Files	Network Service Scanning	Remote File Copy	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Link	Local Job Scheduling	Hidden Files and Directories	Sudo Caching	Exploitation for Defense Evasion	Exploitation for Credential Access	Network Sniffing	Remote Services	SSH Hijacking	Data from Local System	Custom Cryptographic Protocol
Spearphishing via Service	Scripting	Kernel Modules and Extensions	Valid Accounts	File Deletion	Input Capture	Network Sniffing	Third-party Software		Data from Network Shared Drive	Data Encoding
Supply Chain Compromise	Source	Local Job Scheduling	Web Shell	File Permissions Modification	Network Sniffing	Private Keys			Exfiltration Over Alternative Protocol	Data Obfuscation
Trusted Relationship	Space after Filename	Port Knocking		HISTCONTROL	Two-Factor Authentication Interception	Permission Groups Discovery			Exfiltration Over Command and Control Channel	Domain Fronting
	Port Knocking	Redundant Access		Indicator Removal from Tools	Indicator Removal on Host	Process Discovery			Data from Removable Media	Fallback Channels
	Trap	Setuid and Setgid			Install Root Certificate	Remote System Discovery			Data Staged	Multi-hop Proxy
	User Execution	Trap	Valid Accounts		Masquerading	System Information Discovery			Input Capture	Multi-Stage Channels
			Web Shell		Obfuscated Files or Information	System Network Configuration Discovery			Screen Capture	Multiband Communication
					Port Knocking	System Network Connections Discovery				Multilayer Encryption
					Process Injection	System Owner/User Discovery				Port Knocking
					Redundant Access					Remote Access Tools
					Rootkit					Remote File Copy
					Scripting					Standard Application Layer Protocol
					Space after Filename					Standard Cryptographic Protocol
					Timestamp					Standard Non-Application Layer Protocol
					Valid Accounts					Uncommonly Used Port
					Web Service					Web Service



<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

# 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>