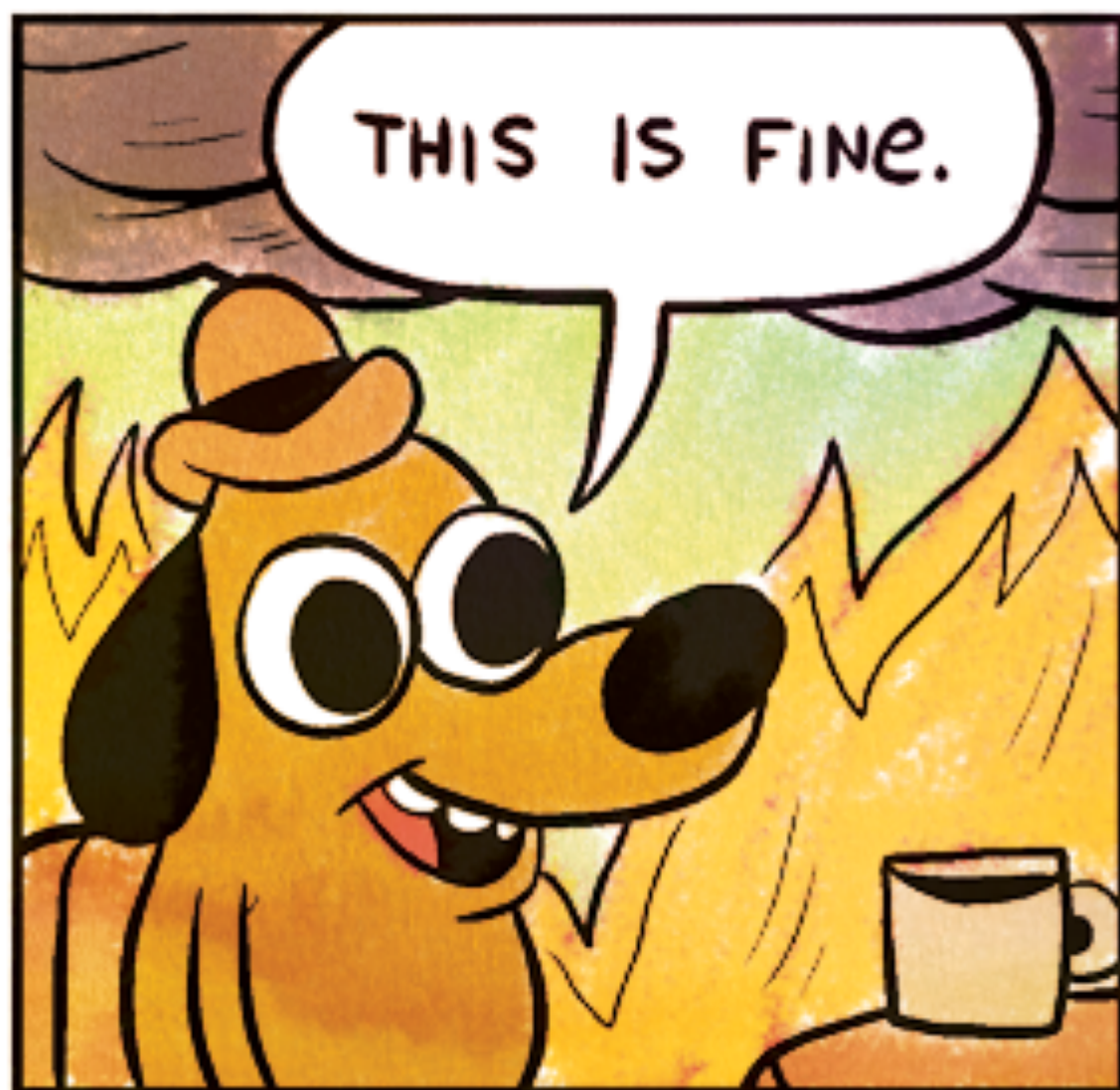


SCALE YOUR AUDITING EVENTS

Philipp Krenn

@xeraa





Learn about a breach

FROM THE PRESS OR USERS

Learn about a breach

ATTACKERS ASKING FOR A RANSOM

Learn about a breach

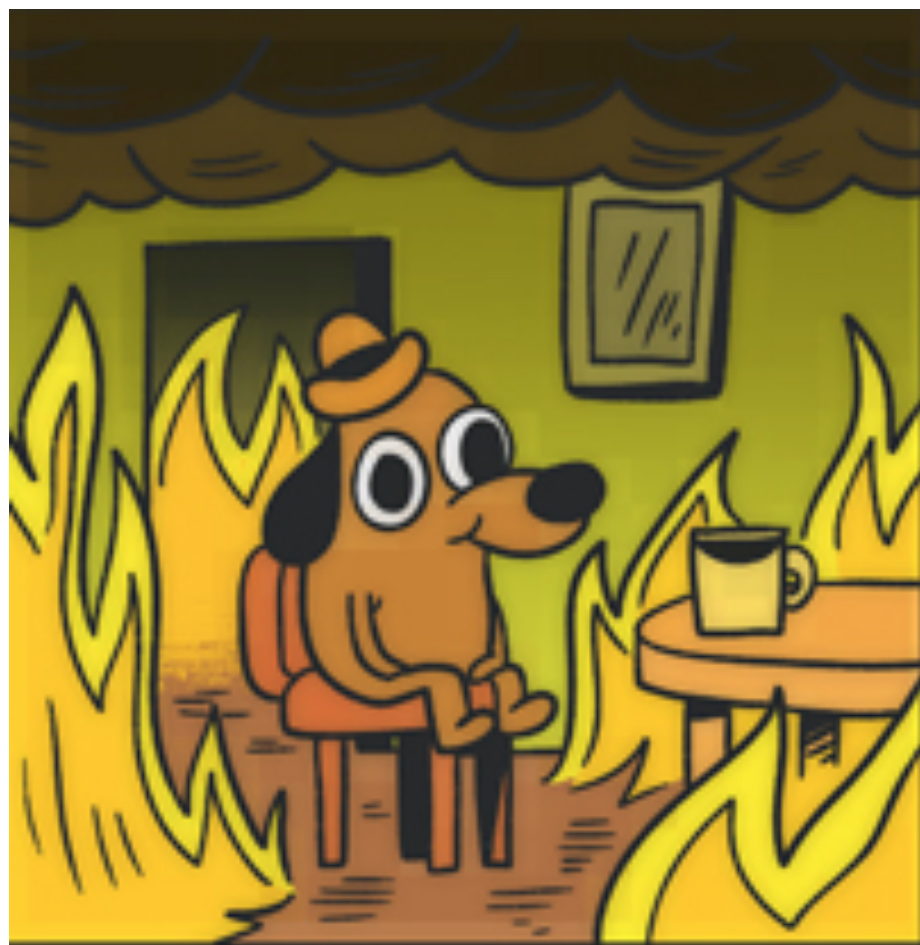
CLOUD PROVIDER'S BILL

Learn about a breach

YOURSELF AFTER THE FACT

Learn about a breach

YOURSELF & YOU CAN PROVE NO HARM



NO SILVER BULLET 

Questions: <https://sli.do/xeraaa>
Answers: <https://twitter.com/xeraaa>



WDIITD

<https://github.com/linux-audit>

"auditd is the userspace component to the Linux Auditing System. It's responsible for writing audit records to the disk. Viewing the logs is done with the ausearch or aureport utilities."

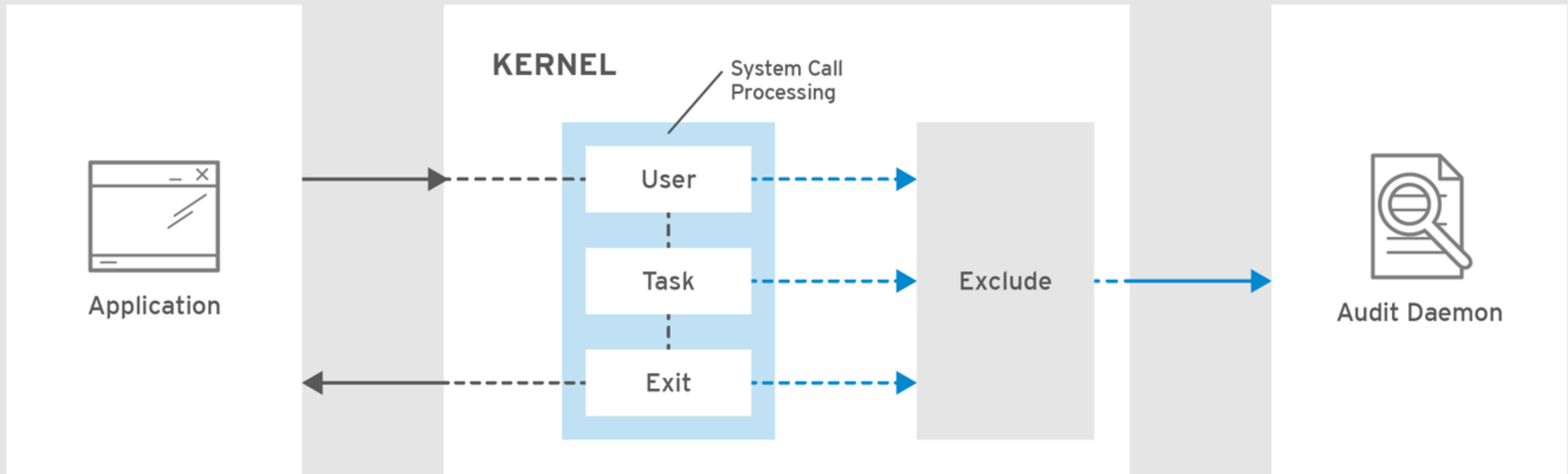
MONITOR

File and network access

System calls

Commands run by a user

Security events



RHEL_453350_0717

DEMO

UNDERSTANDING LOGS

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec-understanding_audit_log_files

MORE RULES

<https://github.com/linux-audit/audit-userspace/tree/master/rules>

NAMESPACES WIP

<https://github.com/linux-audit/audit-kernel/issues/32#issuecomment-395052938>

ALL THE THINGS!



Problem

HOW TO CENTRALIZE?



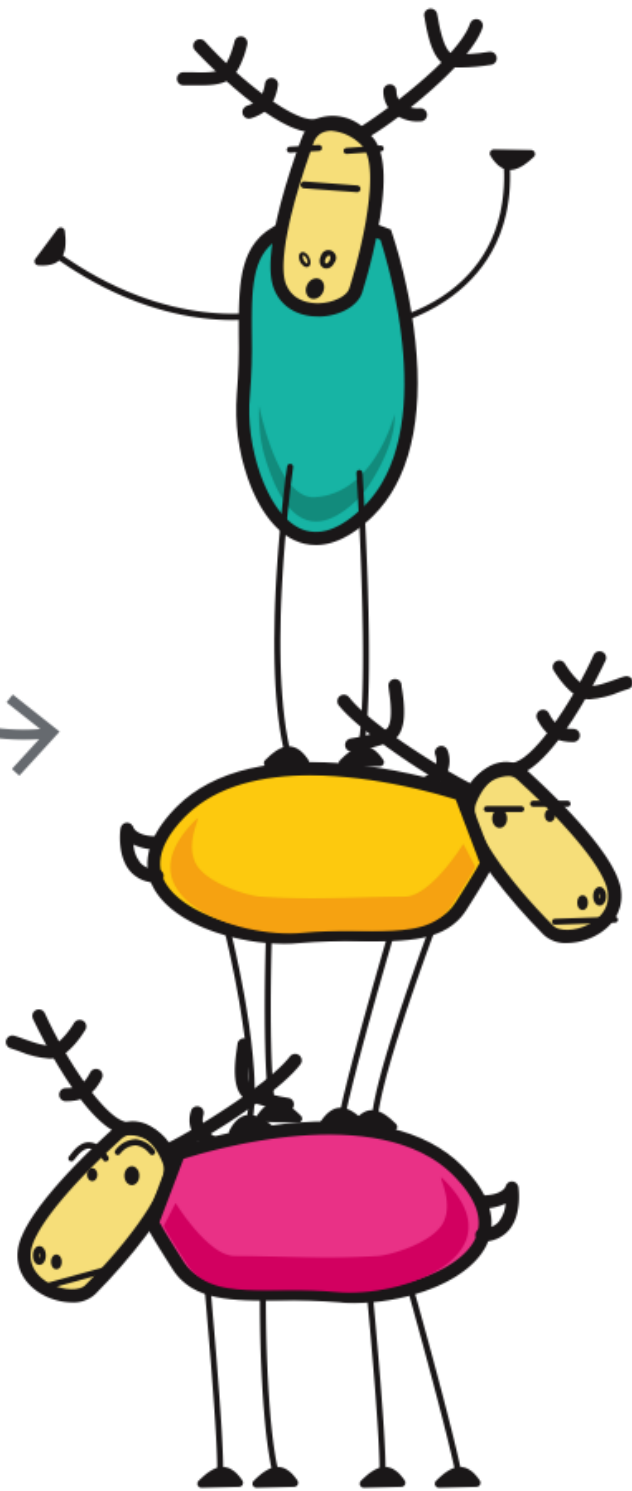
elastic

Developer 🥑

Disclaimer

I BUILD HIGHLY MONITORED HELLO
WORLD APPS

ELK Stack!
Get it?

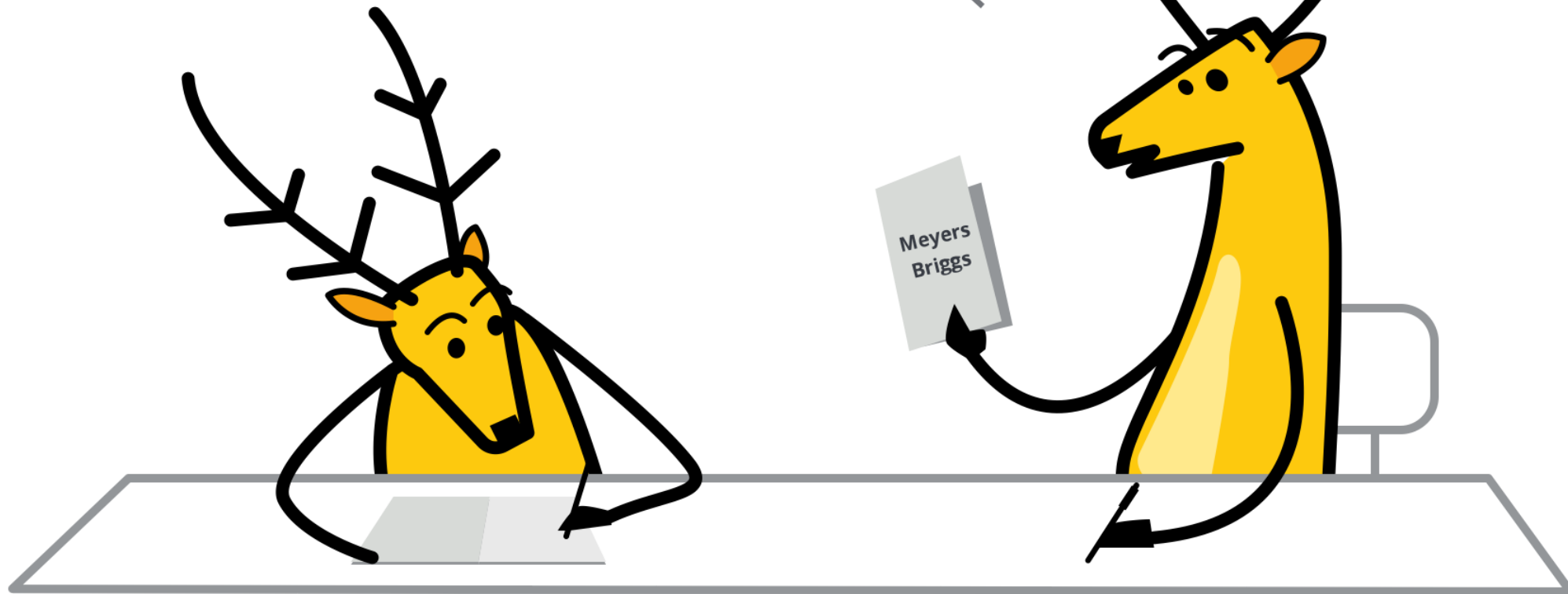


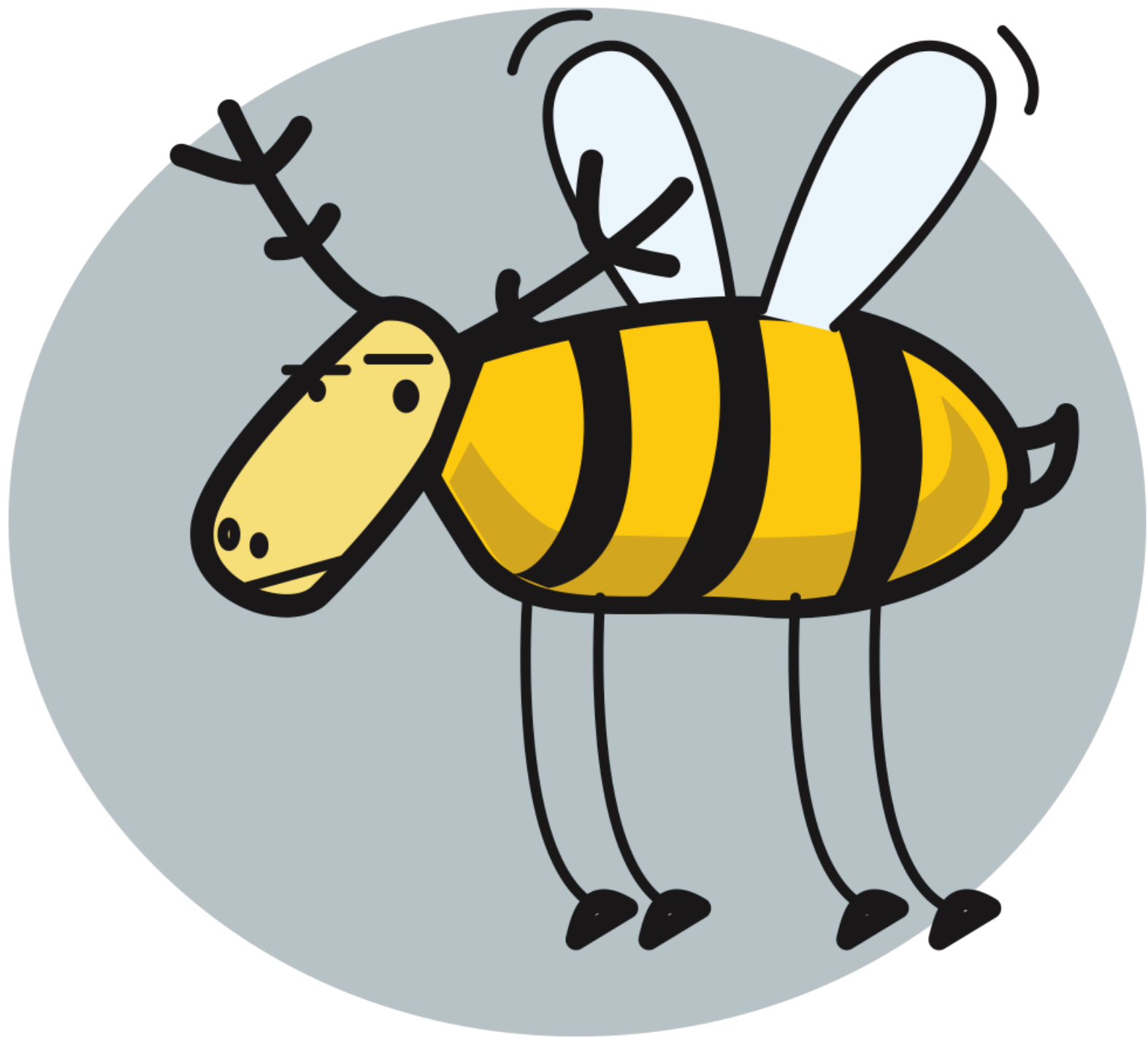
E Elasticsearch

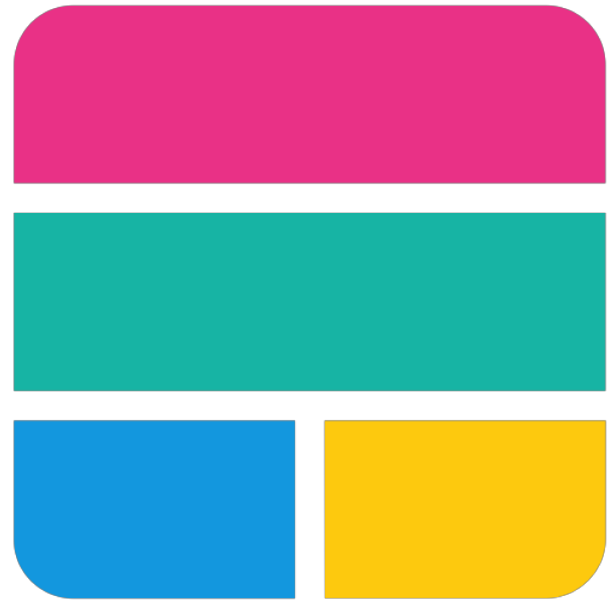
L Logstash

K Kibana

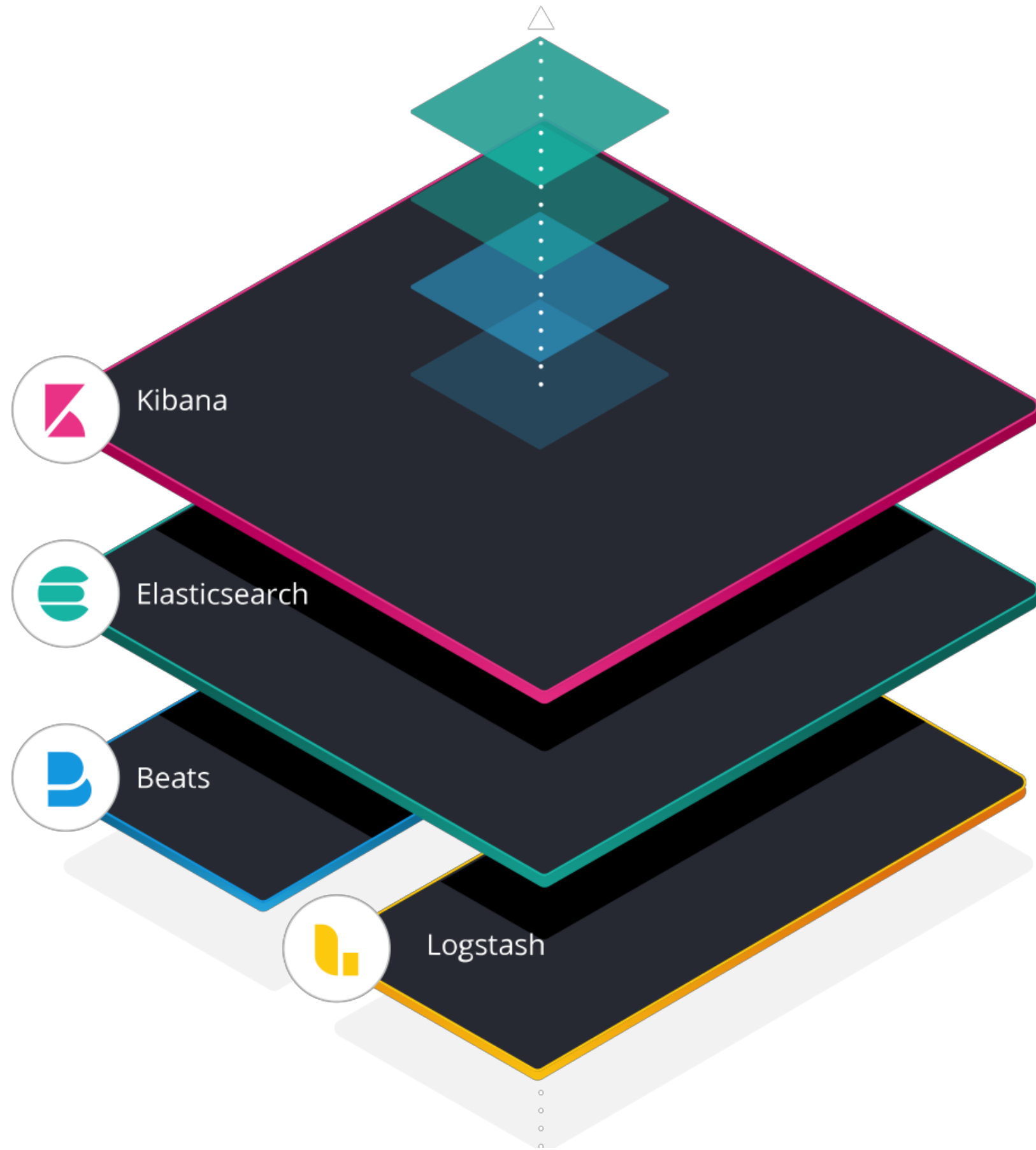
*Apparently, I'm an
ELKB personality.*







elastic stack

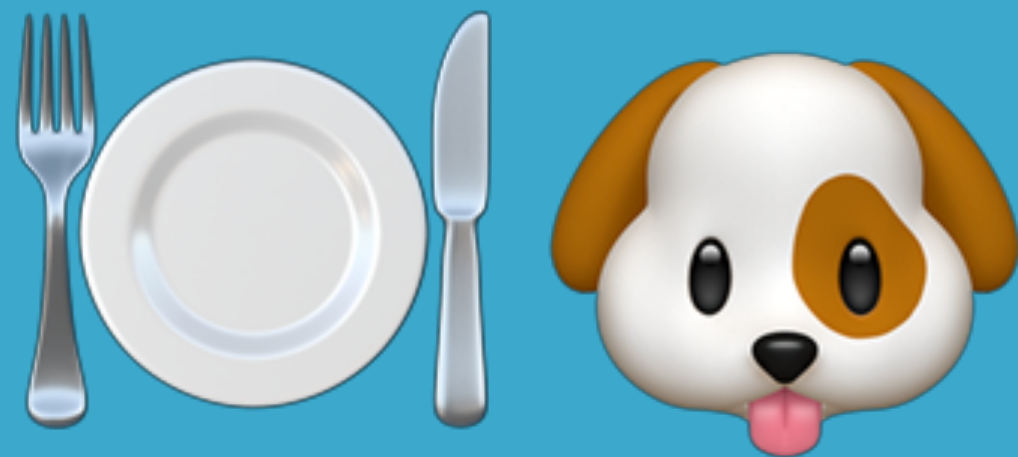




open source

FILEBEAT MODULE: AUDITD

DEMO







elastic cloud

<https://cloud.elastic.co>

AUDITBEAT

AUDITD MODULE

Correlate related events

Resolve UIDs to user names

Native Elasticsearch integration

AUDITD MODULE

eBPF powers on older kernels

Easier configuration

Written in Golang

Docker metadata enrichment

Enhance add_docker_metadata to enrich based on PID

Edit

#6100

Merged exekias merged 2 commits into `elastic:master` from `andrewkroh:feature/libbeat/docker-pid-metadata` on 18 Jan

Conversation 10

Commits 2

Checks 0

Files changed 22

+424 -70



andrewkroh commented on 17 Jan

Member



This PR enhances `add_docker_metadata` with the ability to enrich events containing process IDs.

The processor uses cgroup membership data from `/proc/pid/cgroup` to determine if the process is running inside of a Docker container. It caches the PID -> CID mapping for 5 minutes (based on time of last access).

The default configuration sets `match_pids: [process.pid, process.ppid]`. It falls back to the PPID in case the process has exited before the processing occurs.



Reviewers



rufin



exekias



dedemorton



Assignees



No one—assign yourself

Labels



:Processors

DEMO

FILE INTEGRITY MODULE

inotify (Linux)
fsevents (macOS)
ReadDirectoryChangesW (Windows)

hash_types

blake2b_256, blake2b_384, blake2b_512, md5, sha1,
sha224, sha256, sha384, sha512, sha512_224, sha512_256,
sha3_224, sha3_256, sha3_384, sha3_512, xxh64

DEMO

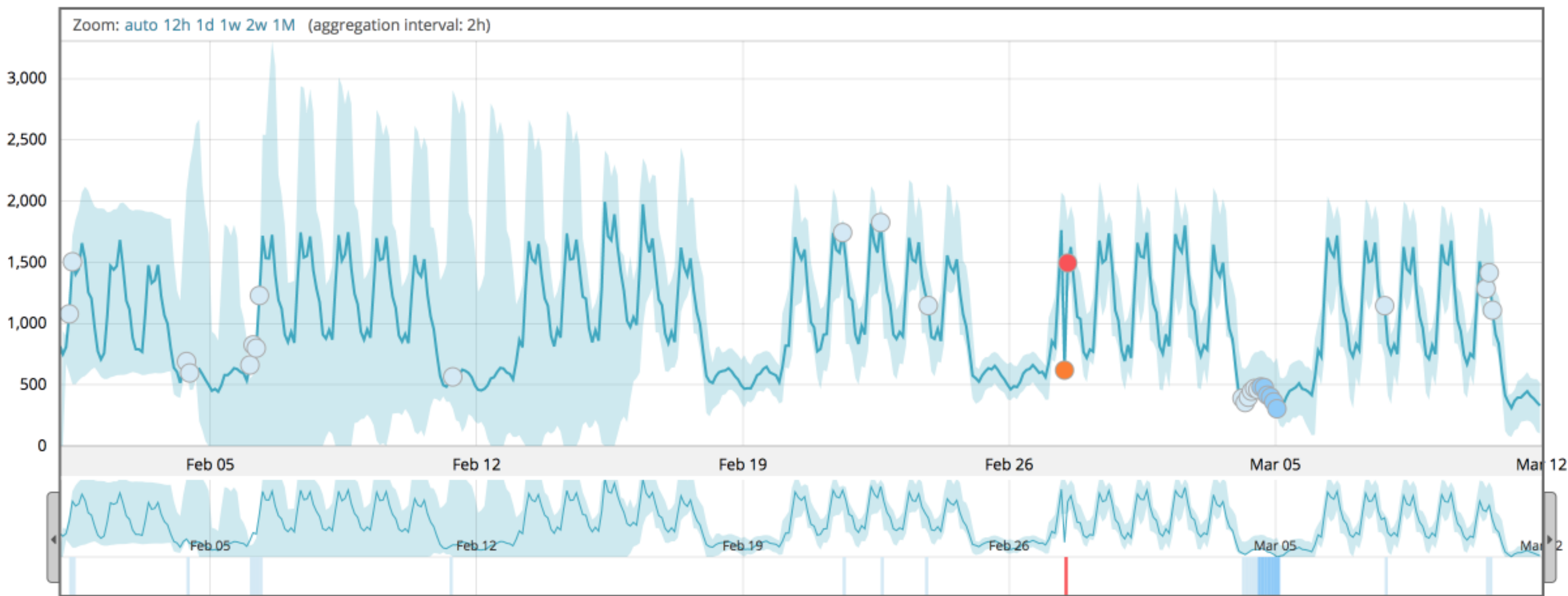
PS: MACHINE LEARNING

Job Management Anomaly Explorer Single Metric Viewer

Job `nginx-demo`

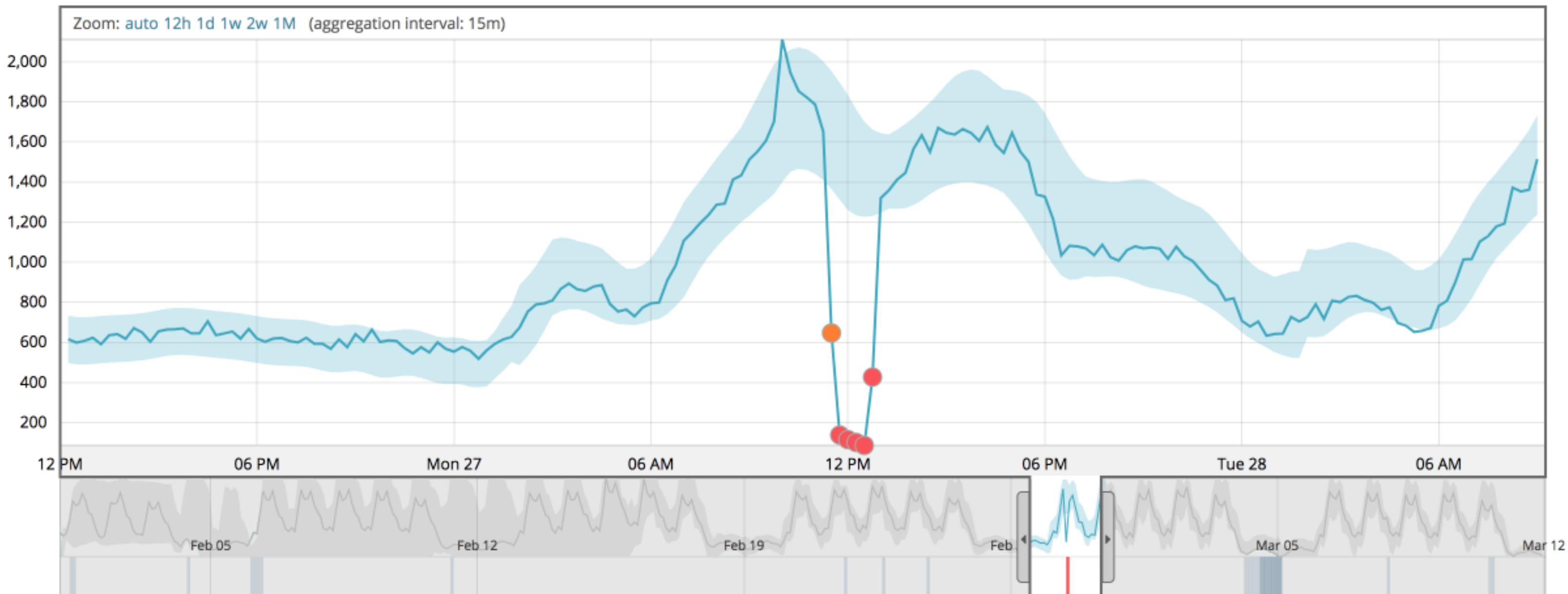
Detector: `distinct_count (nginx.access.remote_ip.keyword)`

Single time series analysis of cardinality `nginx.access.remote_ip.keyword`



Anomalies

Single time series analysis of cardinality nginx.access.remote_ip.keyword



Anomalies

Severity threshold:

▲ warning ▼

Interval:

Auto ▼

time ↕	max severity ↕	detector ↕	actual ↕	typical ↕	description ↕	job ID ↕
▶ February 27th 2017, 12:00	▲ 97	distinct_count (nginx.access.remote_ip.keyword)	86	1453.6	↓ 17x lower	nginx-demo
▶ February 27th 2017, 11:00	▲ 86	distinct_count (nginx.access.remote_ip.keyword)	138	1575.97	↓ 11x lower	nginx-demo

CONCLUSION



AUDITD
AUDITBEAT
LOGS, DASHBOARDS, ...

TRY

<https://dashboard.xeraa.wtf>

SSH: elastic-user@xeraa.wtf secret

CODE

[https://github.com/xeraa/
auditbeat-in-action](https://github.com/xeraa/auditbeat-in-action)

QUESTIONS?

Philipp Krenn

@xeraaa

PS: Sticker