Scale Your Auditing Events

Philipp Krenn @xeraa

elastic

THIS IS FINE.

No silver bullet 🔫

AUDITD

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."

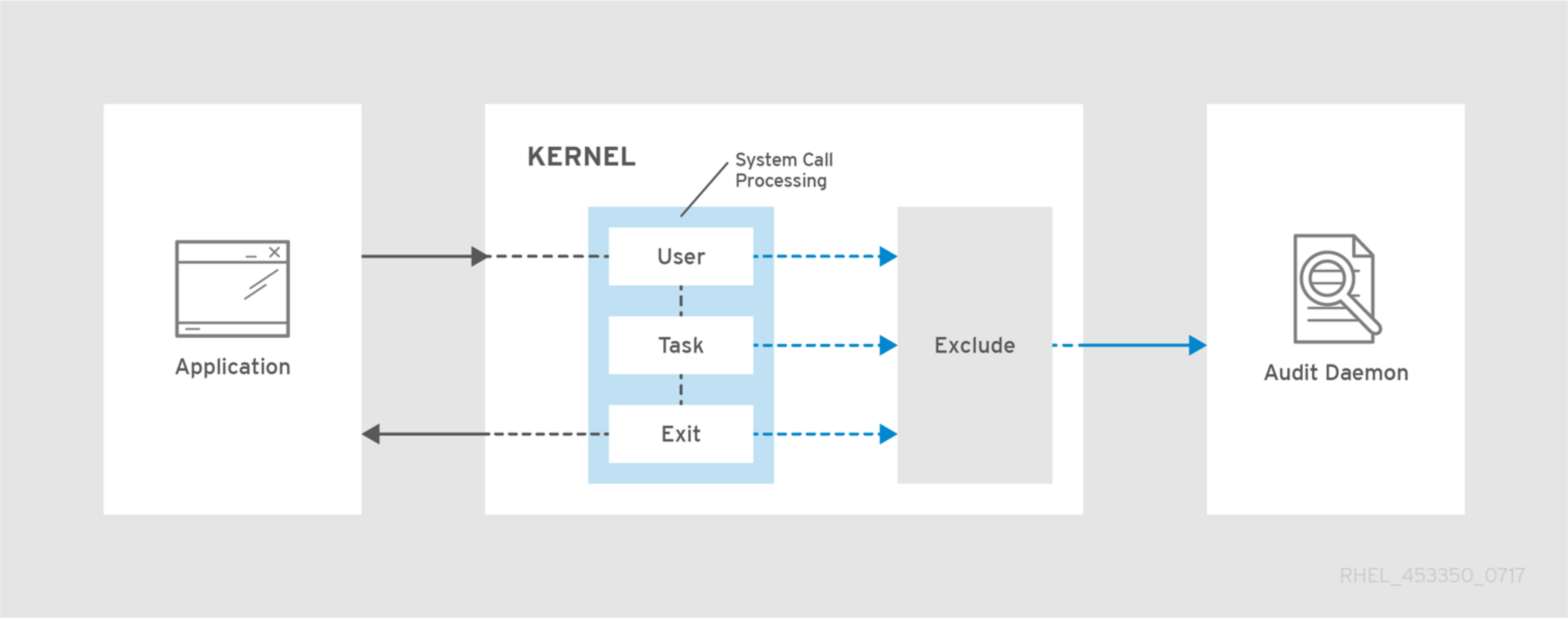
MONITOR

File and network access

System calls

Commands run by a user

Security events



https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/chap-system_auditing

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

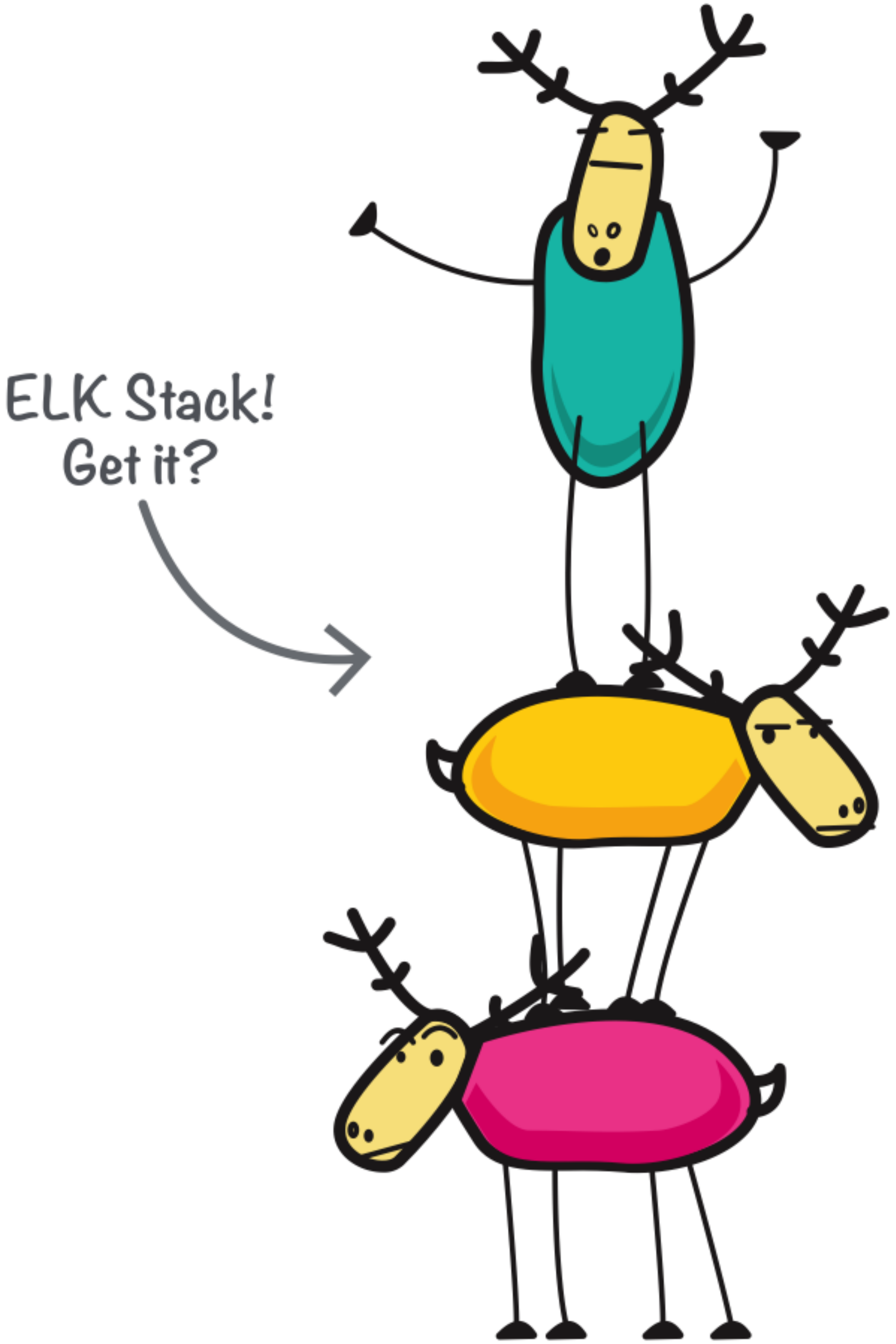
HOW TO CENTRALIZE?

elastic

Developer 🥑

Disclaimer

I build highly monitored Hello World apps



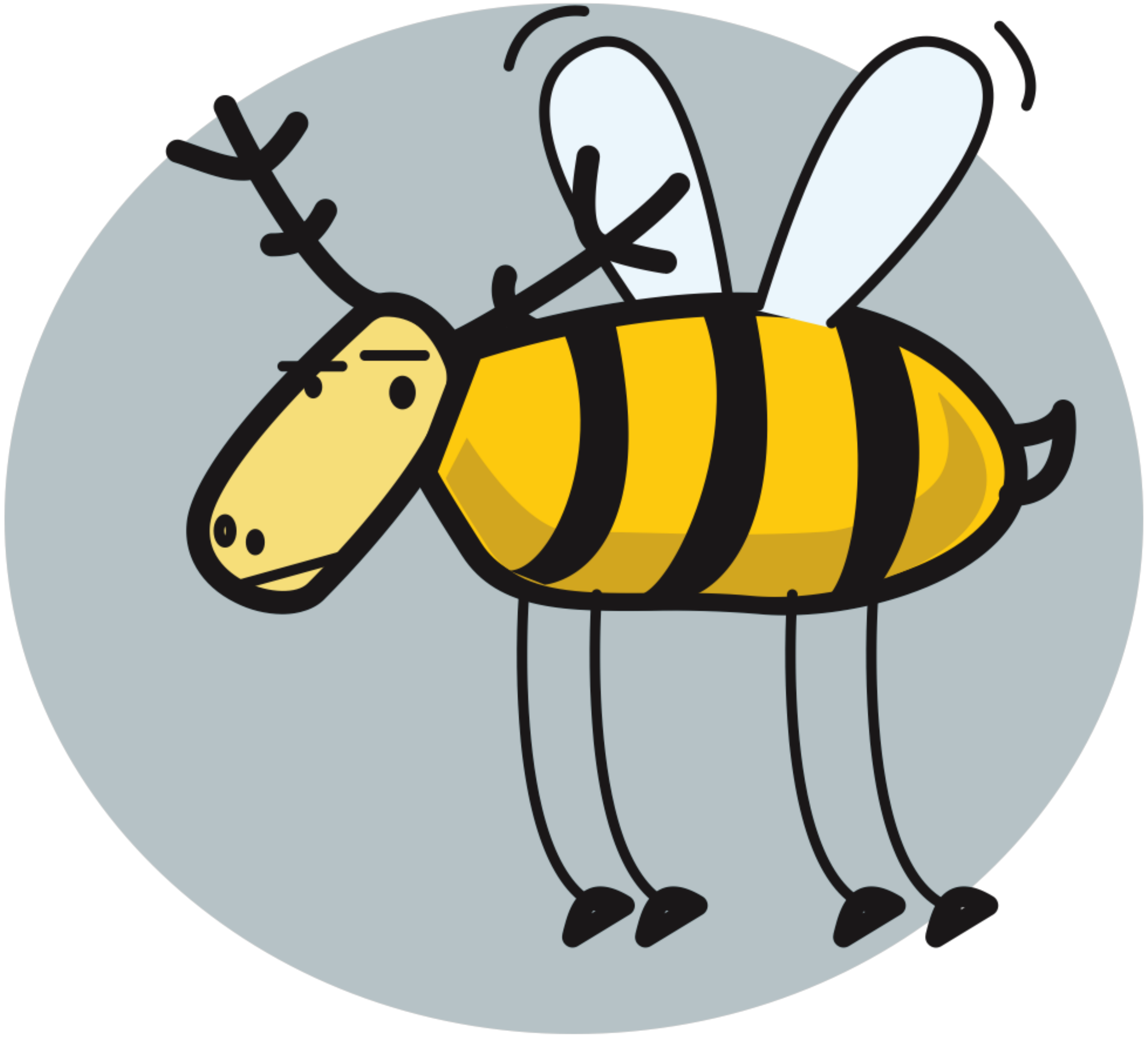
ELK Stack!
Get it?

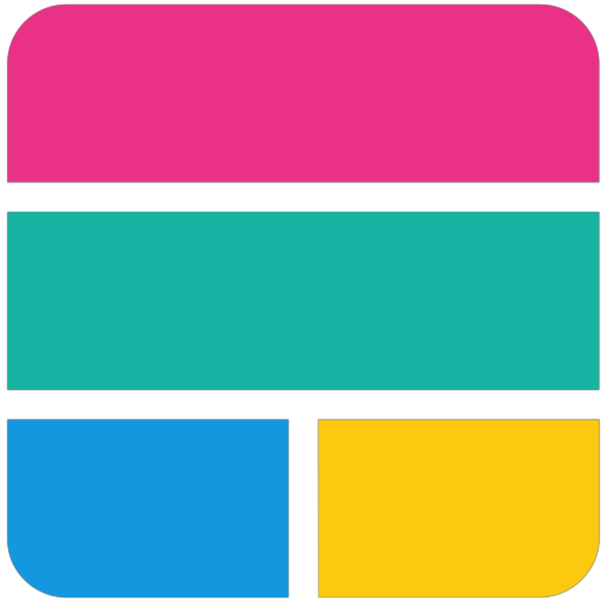
E Elasticsearch

L Logstash

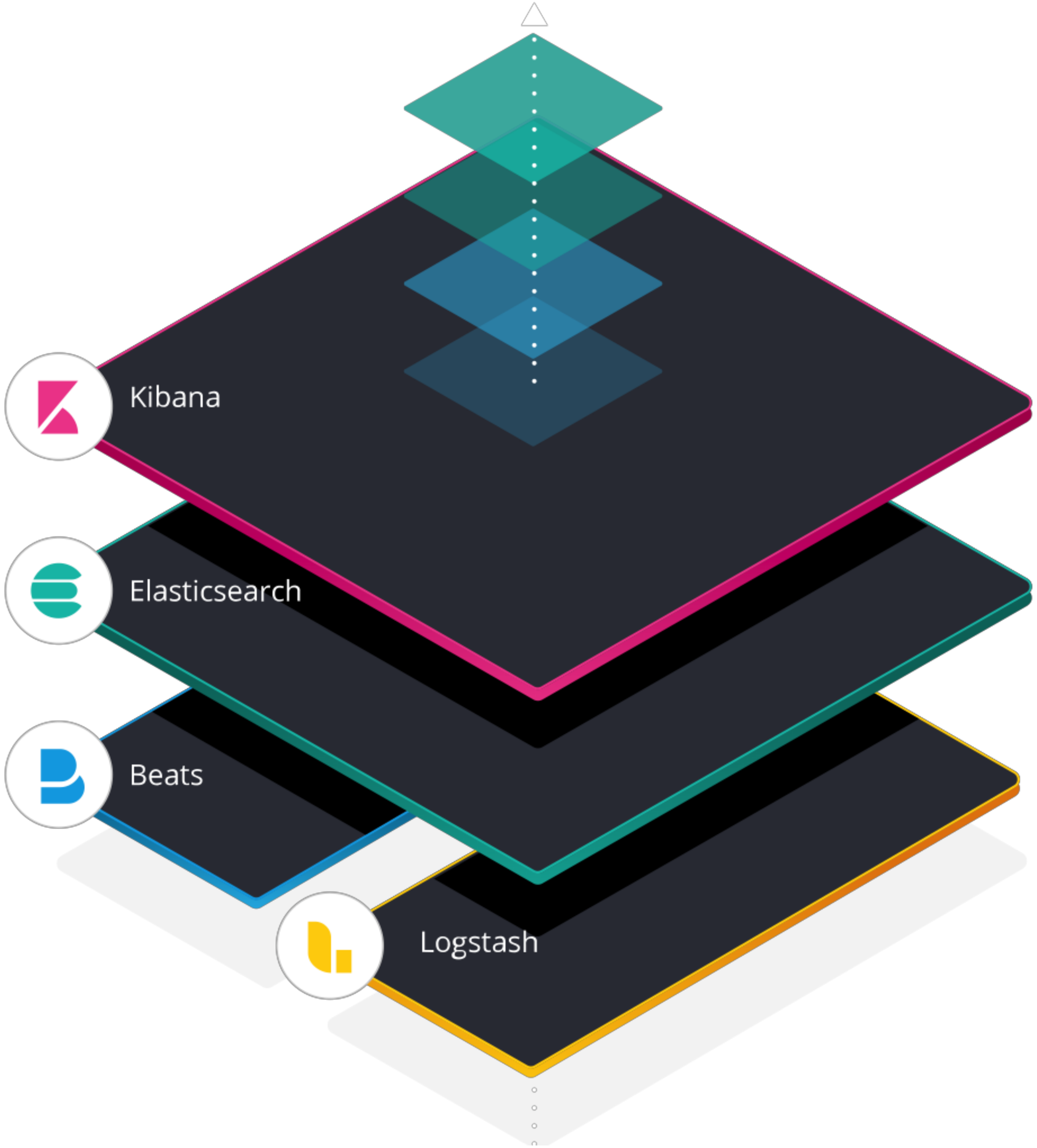
K Kibana

Apparently, I'm an ELKB personality.
Meyers Briggs
Meyers Briggs





elastic stack


Kibana
Elasticsearch
Beats
Logstash

Filebeat Module: Auditd

Demo

🍽️🐶

🥂 🍾

elastic cloud

https://cloud.elastic.co

AUDITBEAT

Auditd Module

Correlate related events

Resolve UIDs to user names

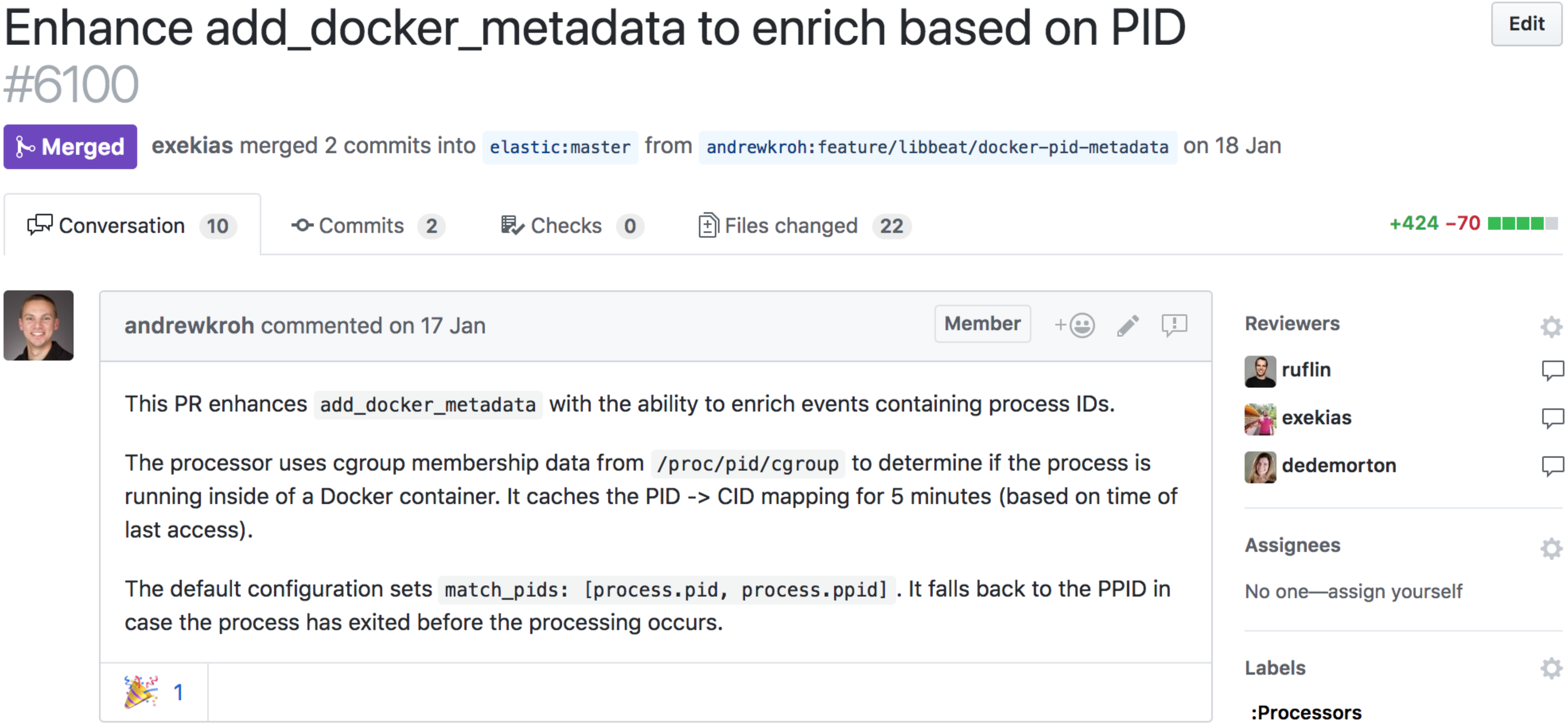
Native Elasticsearch integration

Auditd Module

eBPF powers on older kernels

Easier configuration

Written in Golang



Enhance add_docker_metadata to enrich based on PID #6100

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

andrewkroh commented on 17 Jan

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.

🎉 1

Reviewers

- ruflin
- exekias
- dedemorton

Assignees

No one—assign yourself

Labels

:Processors

GO-LIBAUDIT

https://github.com/elastic/go-libaudit

go-libaudit is a library for communicating with the Linux Audit Framework

Demo

System Module

Easier configuration for host, process, socket, user

Added in 6.6 — not based on Auditd

Demo

File Integrity Module

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

hash_types

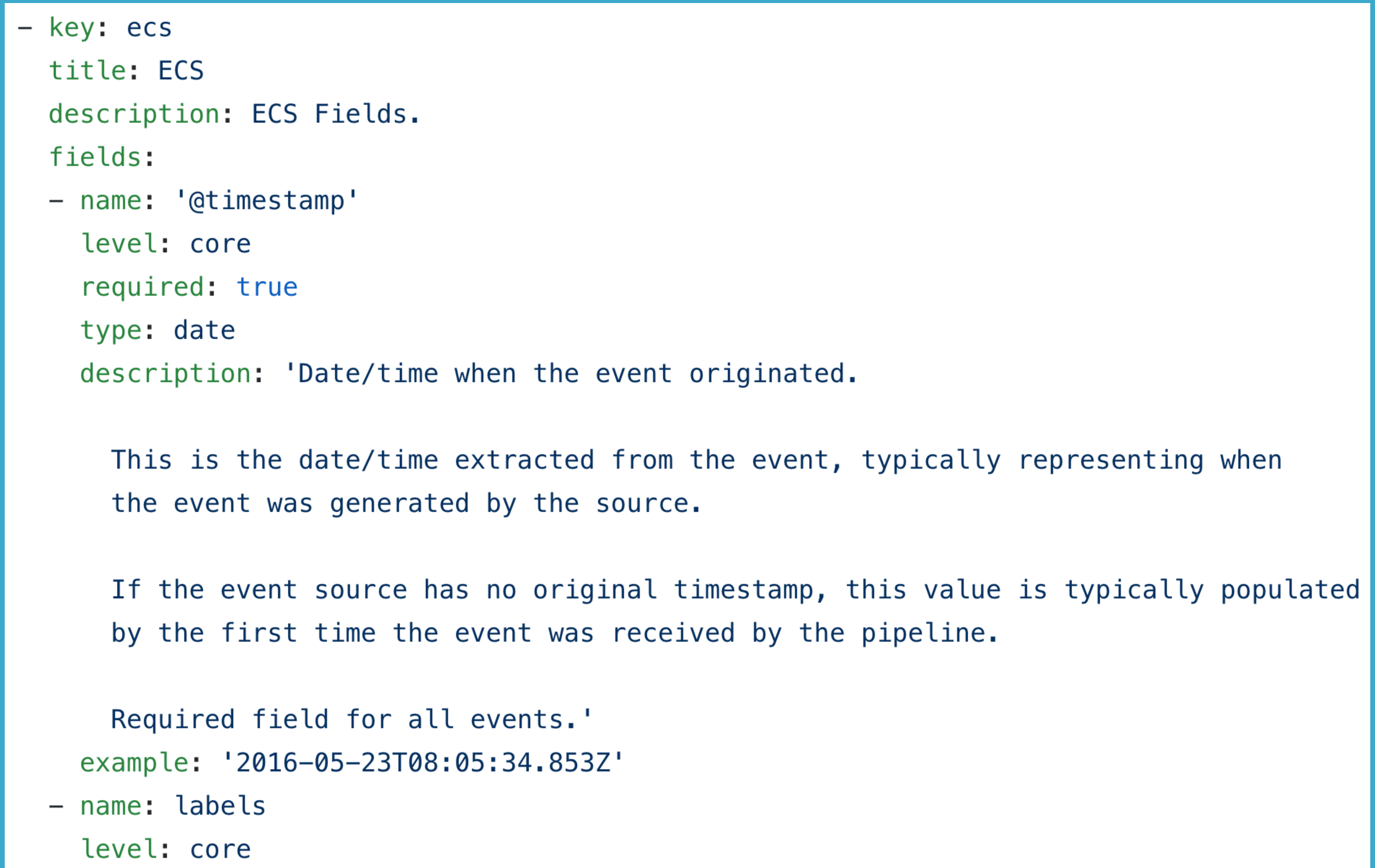
blake2b_256, blake2b_384, blake2b_512, md5, sha1, sha224, sha256, sha384, sha512, sha512_224, sha512_256, sha3_224, sha3_256, sha3_384, sha3_512, xxh64

Demo

Elastic SIEM

elastic

https://github.com/elastic/ecs

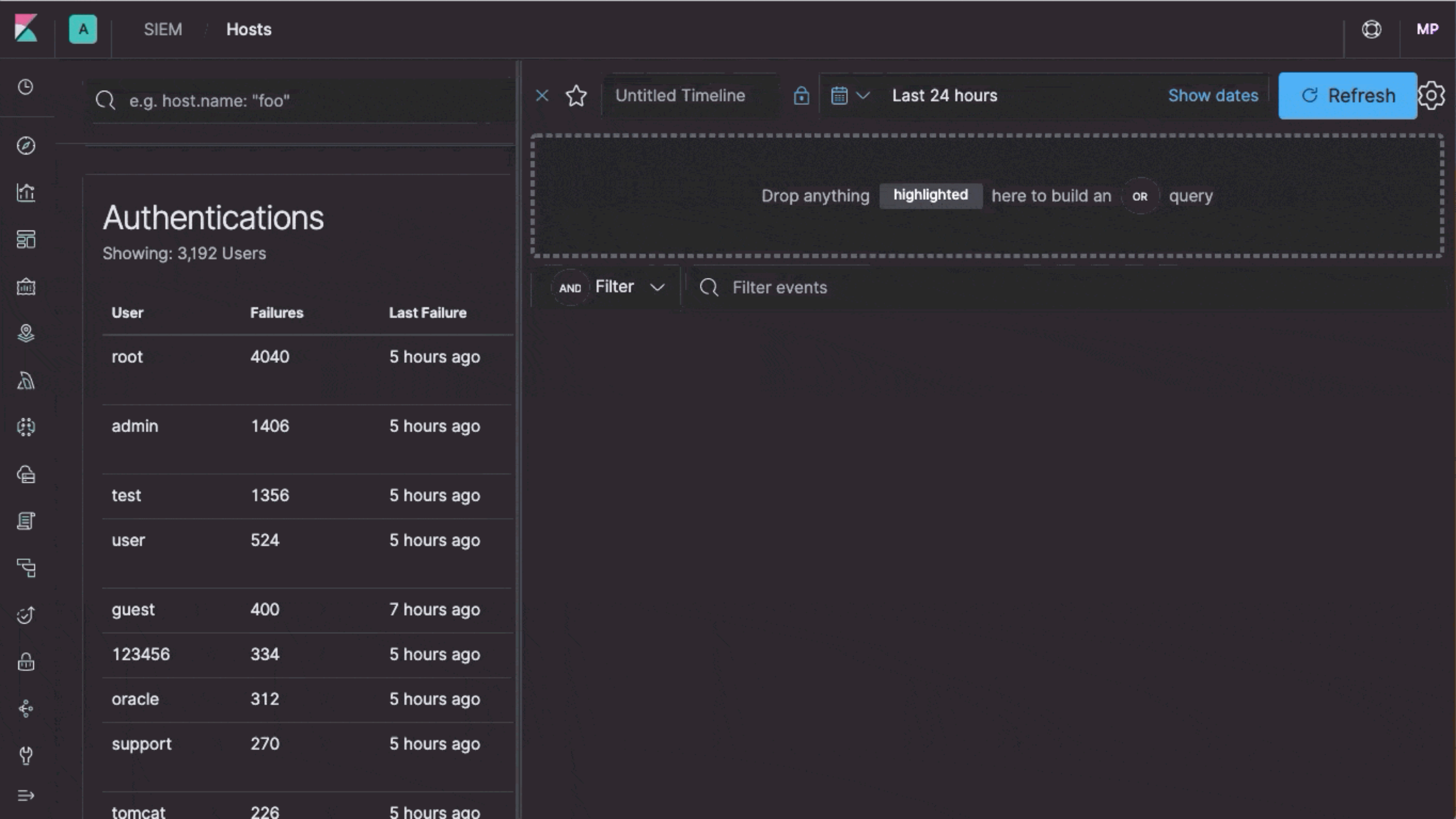


```yaml
- key: ecs
  title: ECS
  description: ECS Fields.
  fields:
  - name: '@timestamp'
    level: core
    required: true
    type: date
    description: 'Date/time when the event originated.

      This is the date/time extracted from the event, typically representing when
      the event was generated by the source.

      If the event source has no original timestamp, this value is typically populated
      by the first time the event was received by the pipeline.

      Required field for all events.'
    example: '2016-05-23T08:05:34.853Z'
  - name: labels
    level: core
```



Drop anything highlighted here to build an OR query

Authentications

Showing: 3,192 Users

User	Failures	Last Failure
root	4040	5 hours ago
admin	1406	5 hours ago
test	1356	5 hours ago
user	524	5 hours ago
guest	400	7 hours ago
123456	334	5 hours ago
oracle	312	5 hours ago
support	270	5 hours ago
tomcat	226	5 hours ago

Demo

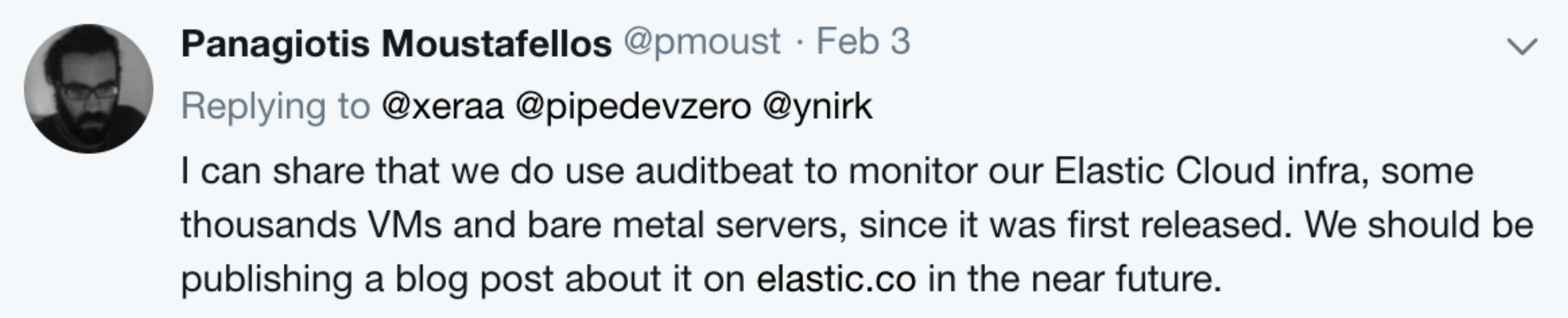
elastic

Conclusion

Auditd

Auditbeat

Logs, Dashboards, SIEM



Panagiotis Moustafellos @pmoust · Feb 3

Replying to @xeraa @pipedevzero @ynirk

I can share that we do use auditbeat to monitor our Elastic Cloud infra, some thousands VMs and bare metal servers, since it was first released. We should be publishing a blog post about it on elastic.co in the near future.

Code

https://github.com/xeraa/auditbeat-in-action

Similar Solutions

https://github.com/slackhq/go-audit

https://github.com/Scribery/aushape

QUESTIONS?

Philipp Krenn @xeraa

PS: Sticker

elastic