# Auditd for the Masses

Philipp Krenn @xeraa

elastic


THIS IS FINE.


TH-
THIS IS NOT FINE!!
OH MY GOD EVERY THINGS ON FIRE
WHAT THE HELL IS MY PROBLEM

Learn about a breach

FROM THE PRESS OR USERS

Learn about a breach

# ATTACKERS ASKING FOR A RANSOM

elastic

Learn about a breach

# CLOUD PROVIDER'S BILL

elastic

Learn about a breach

YOURSELF AFTER THE FACT

elastic

Learn about a breach

YOURSELF BUT UNSURE ABOUT HARM

elastic

Learn about a breach

YOURSELF & YOU CAN PROVE NO HARM

elastic

# No silver bullet 

elastic

Questions: https://sli.do/xeraa

Answers: https://twitter.com/xeraa

elastic

# AUDIT

https://github.com/linux-audit

elastic

"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."

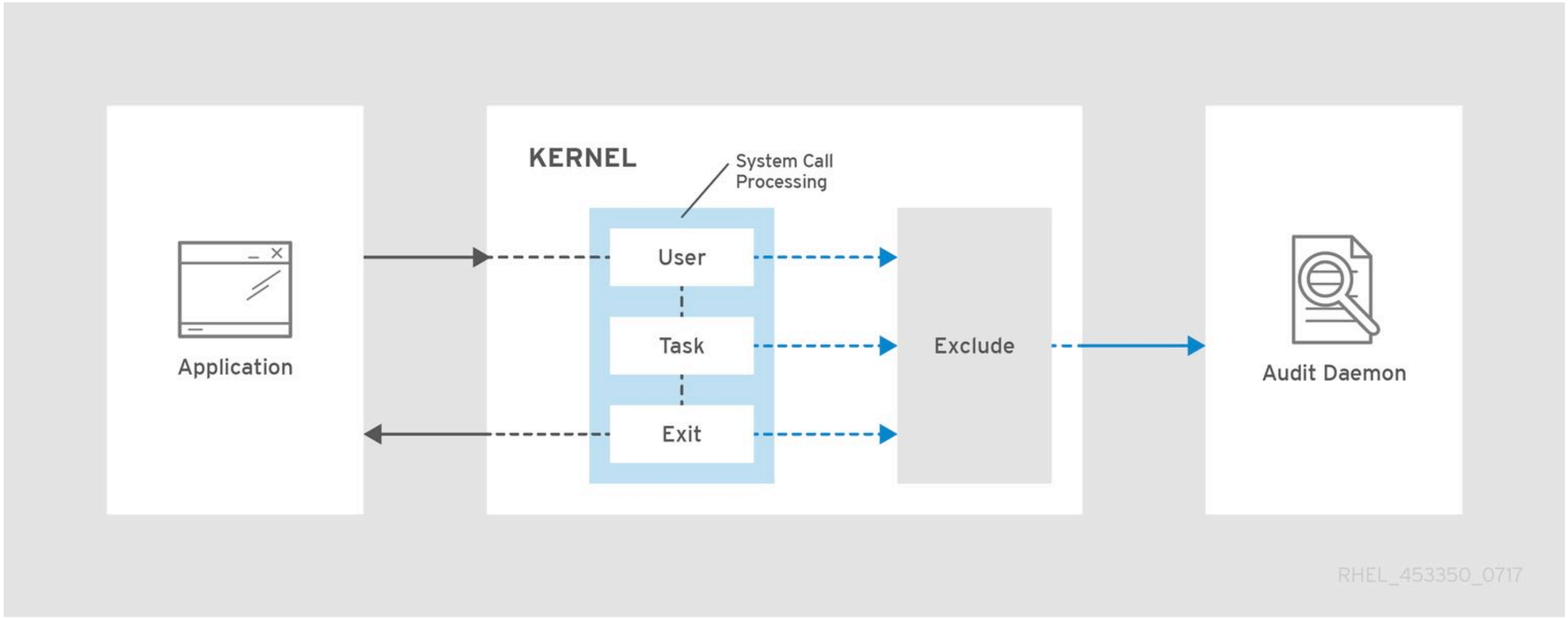
Watching file access

Monitoring system calls

Recording commands run by a user

Recording security events

Monitoring network access




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

# Demo

# 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?

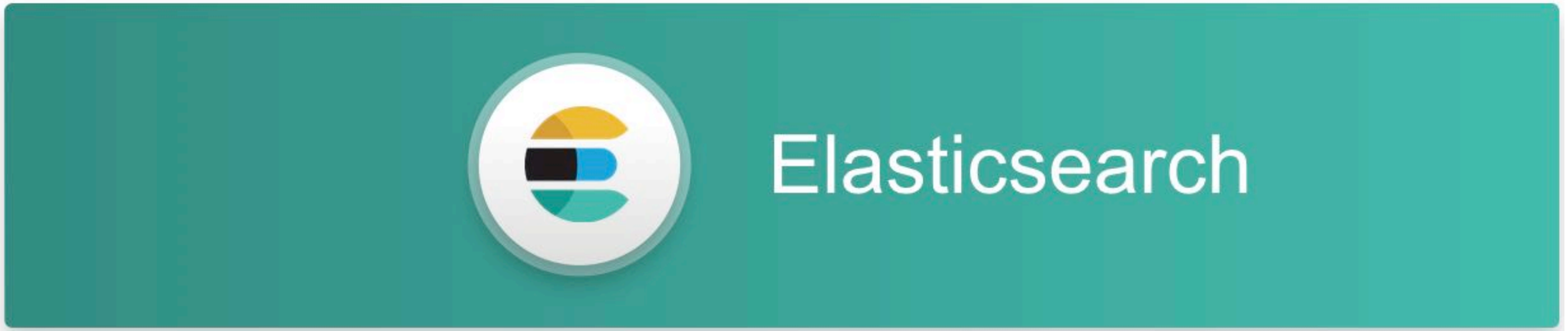
elastic

# Infrastructure | Developer 🥑

# Disclaimer

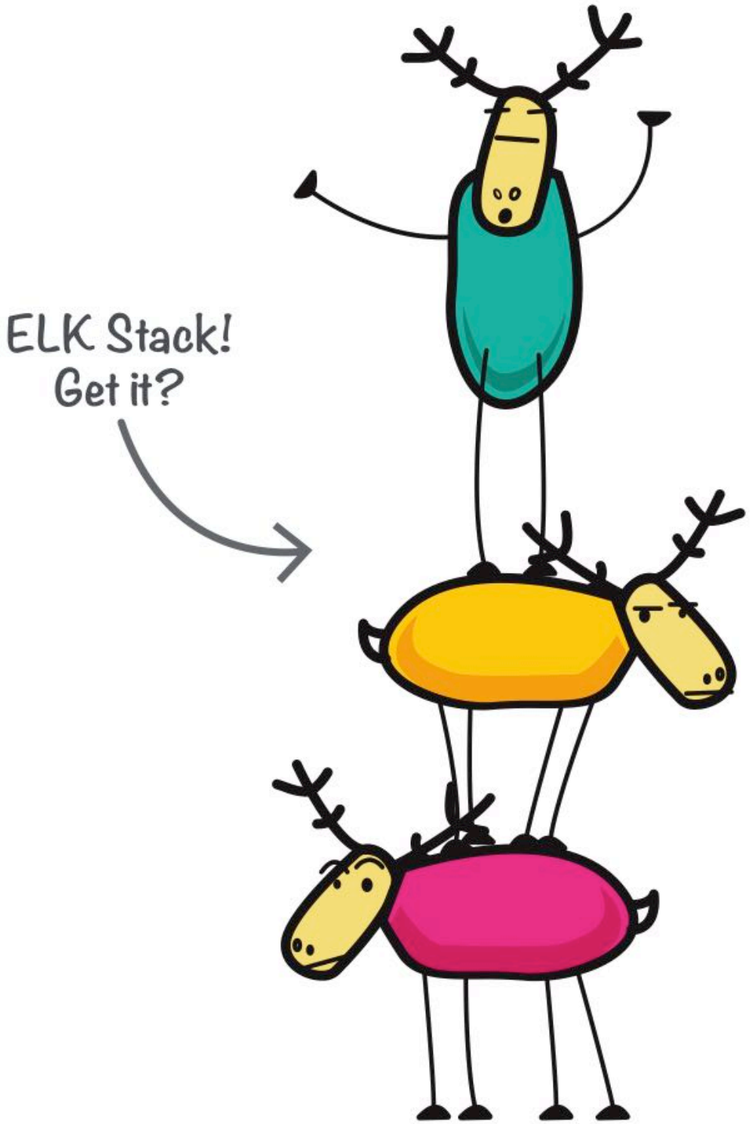
# I BUILD HIGHLY MONITORED HELLO WORLD APPS


Kibana


Elasticsearch


Logstash


Beats



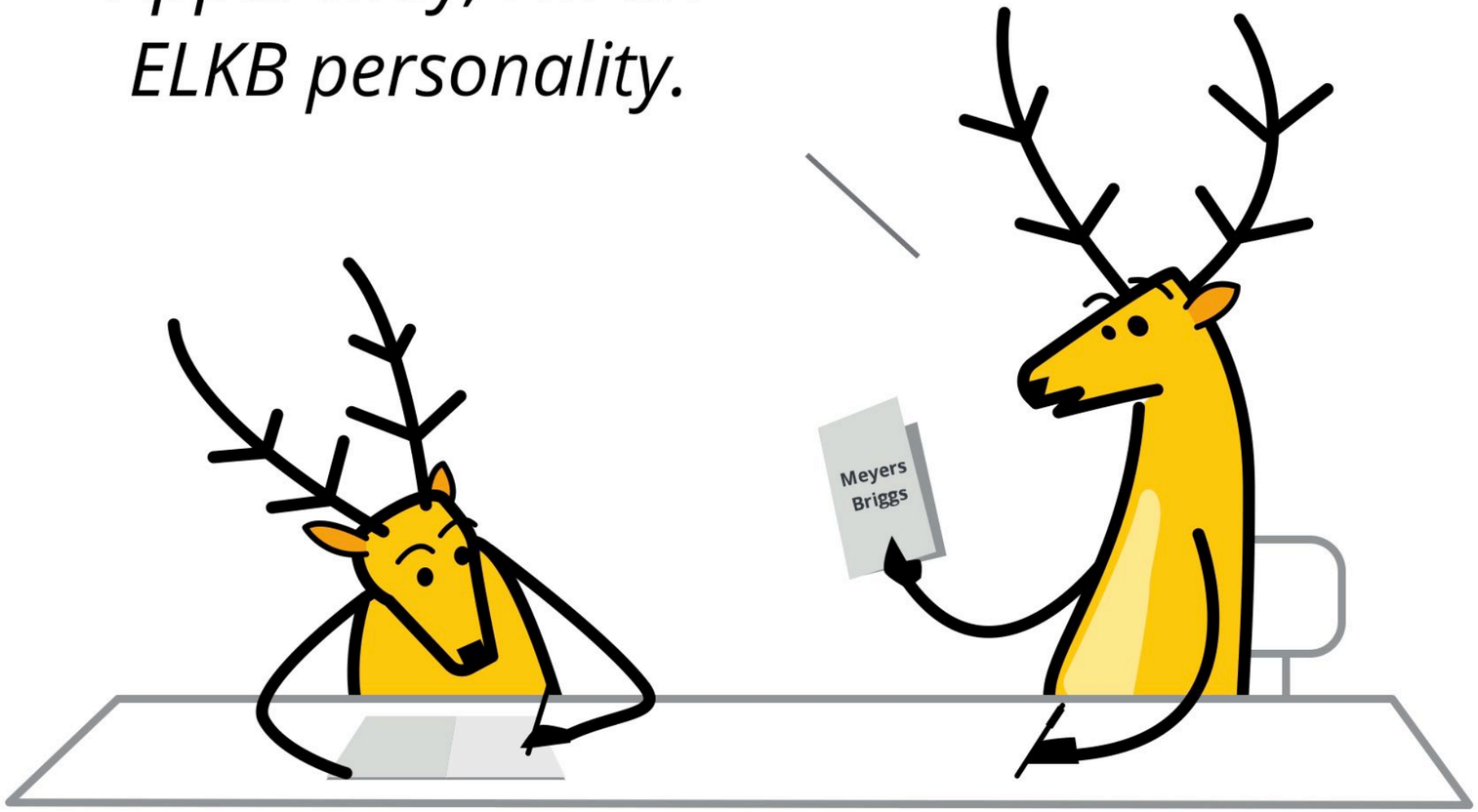

**E** Elasticsearch

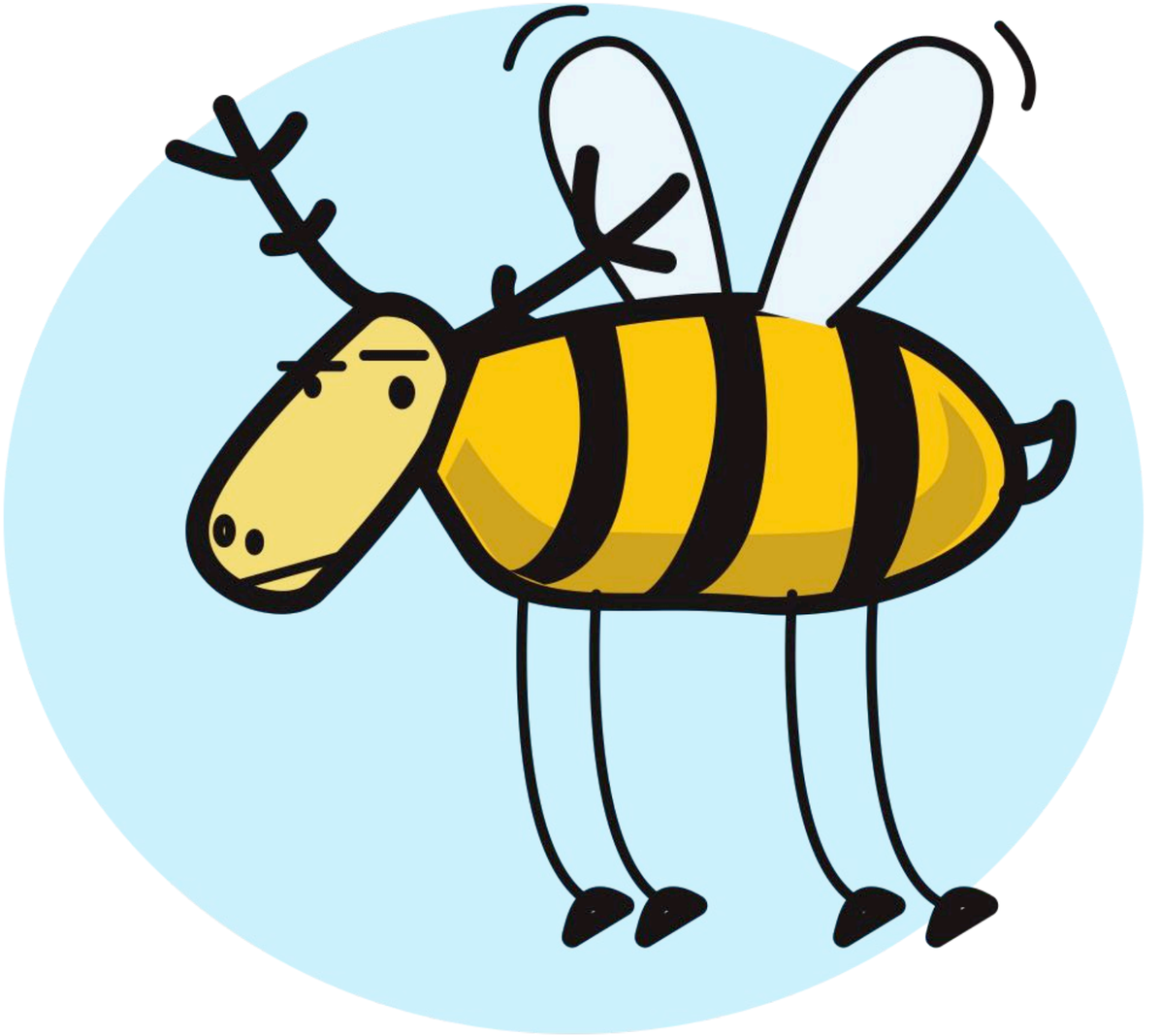
**L** Logstash

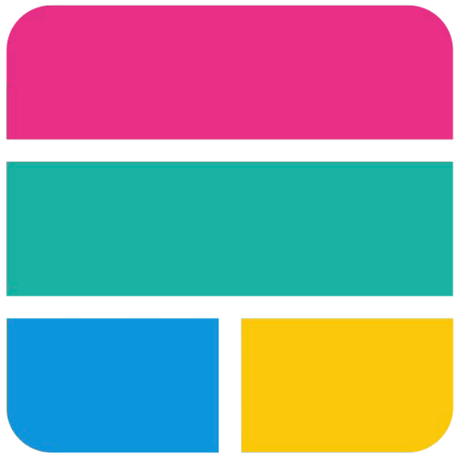
**K** Kibana

elastic

*Apparently, I'm an ELKB personality.*





# elastic stack

open source

# Filebeat Module: Auditd

# Demo

# AUDITBEAT

elastic

# Auditd Module

Correlate related events

Resolve UIDs to user names

Native Elasticsearch integration

elastic

# Auditd Module

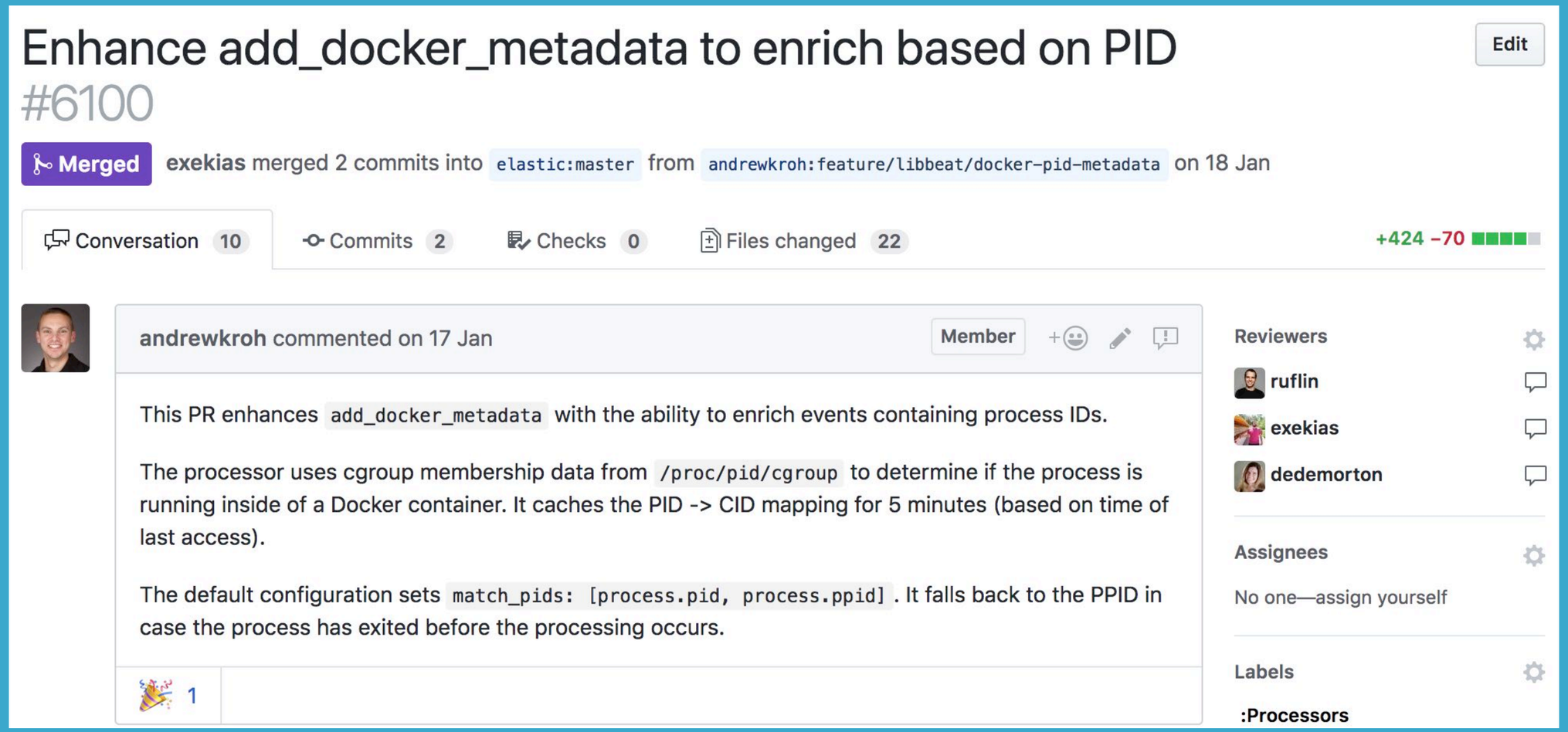
eBPF powers on older kernels

Run side by side with Auditd

Easier configuration

elastic

# Docker metadata enrichment



## Enhance add_docker_metadata to enrich based on PID #6100

Edit

**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.

1

**Reviewers**

ruflin

exekias

dedemorton

**Assignees**

No one—assign yourself

**Labels**

:Processors

elastic

# Demo

# File Integrity Module

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

elastic

# 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

# See MOAR

## Kibana visualizations & dashboards

elastic

# Demo

# PS: Machine Learning

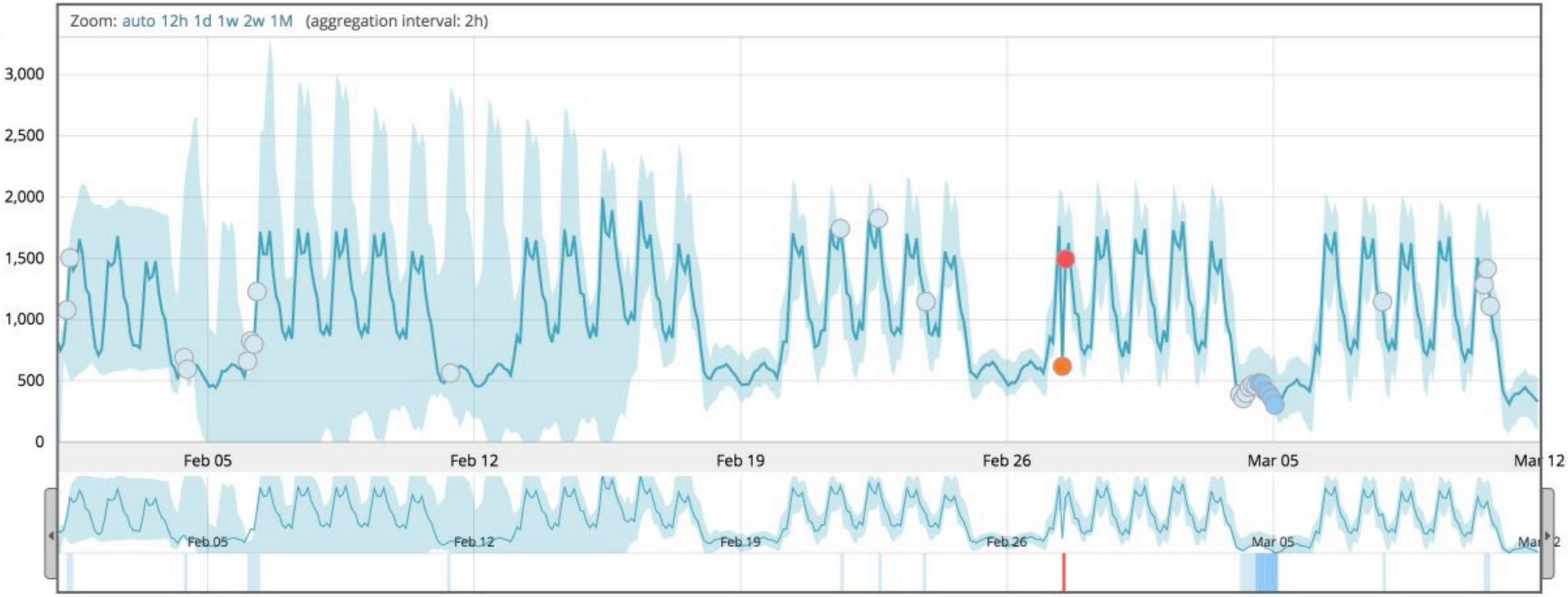
elastic

Job Management Anomaly Explorer Single Metric Viewer

Job nginx-demo

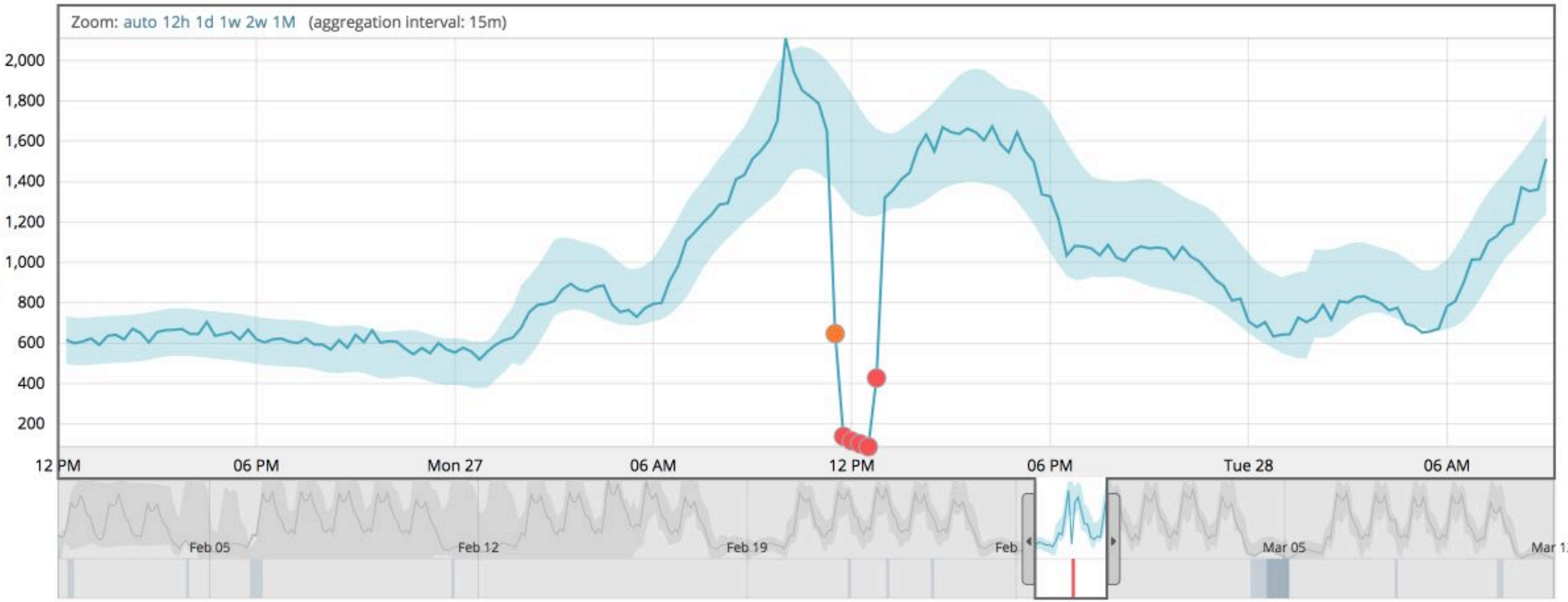
**Detector:** distinct_count (nginx.access.remote_ip.keyword)

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




Anomalies

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




## Anomalies

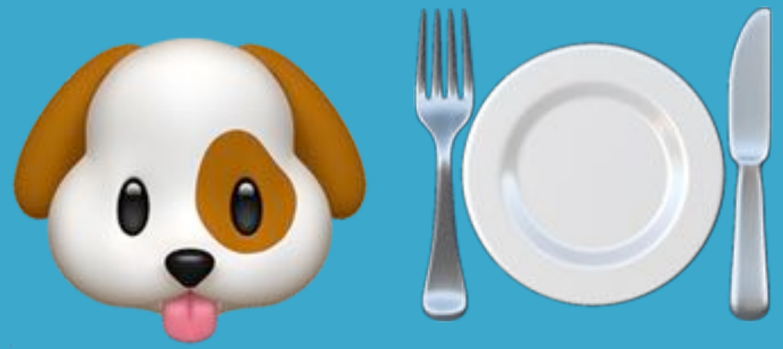
**Severity threshold:** warning **Interval:** Auto

| 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,...

elastic



elastic

elastic

cloud

# https://cloud.elastic.co

elastic

# Next Steps

**https://dashboard.xeraa.wtf**

**SSH: elastic-user@xeraa.wtf secret**

# Questions?

Philipp Krenn @xeraa

PS: Sticker

elastic