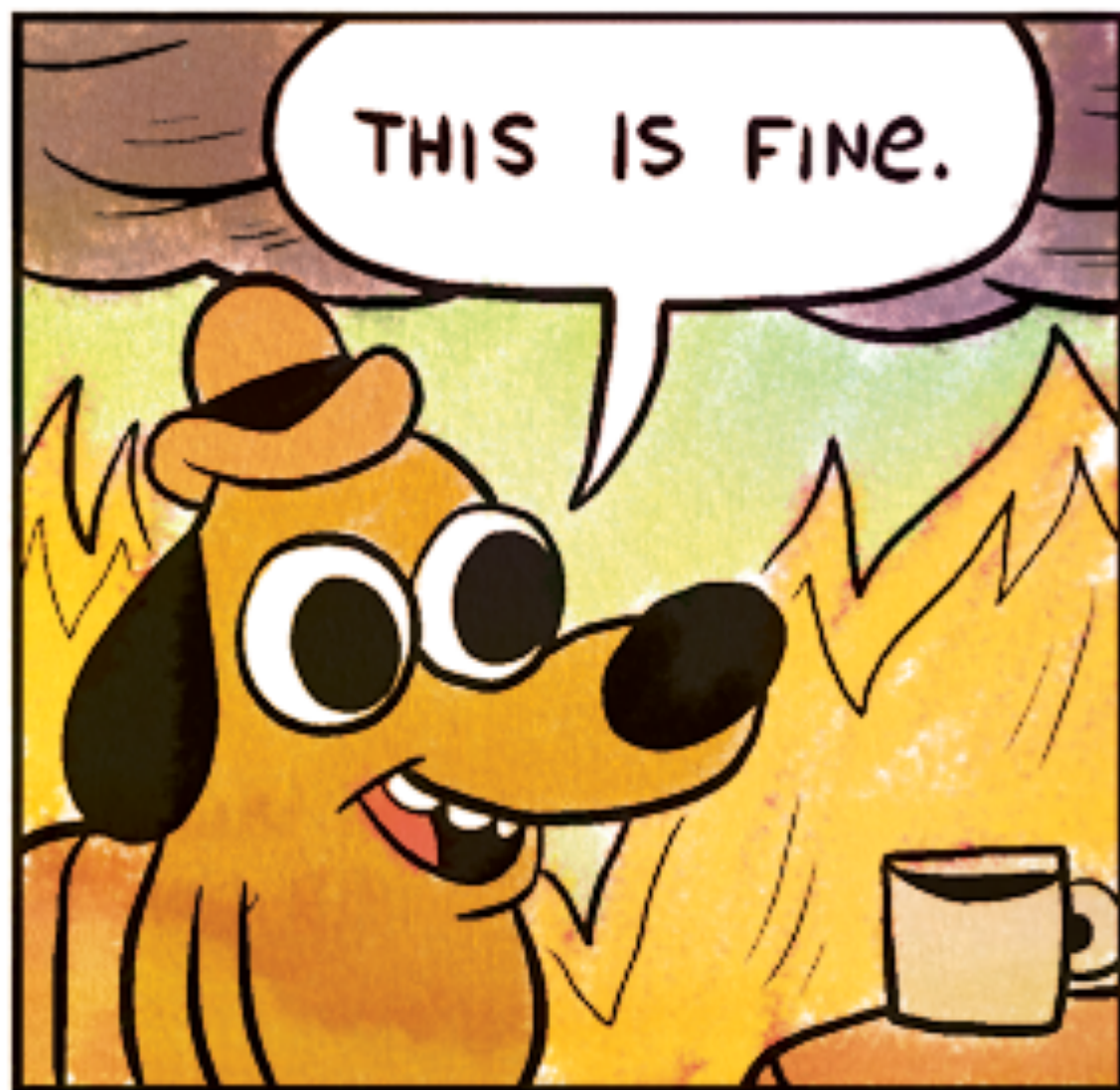# Scale Your Auditing Events

Philipp Krenn   @xeraa

elastic

Learn about a breach

From the press or users

Learn about a breach
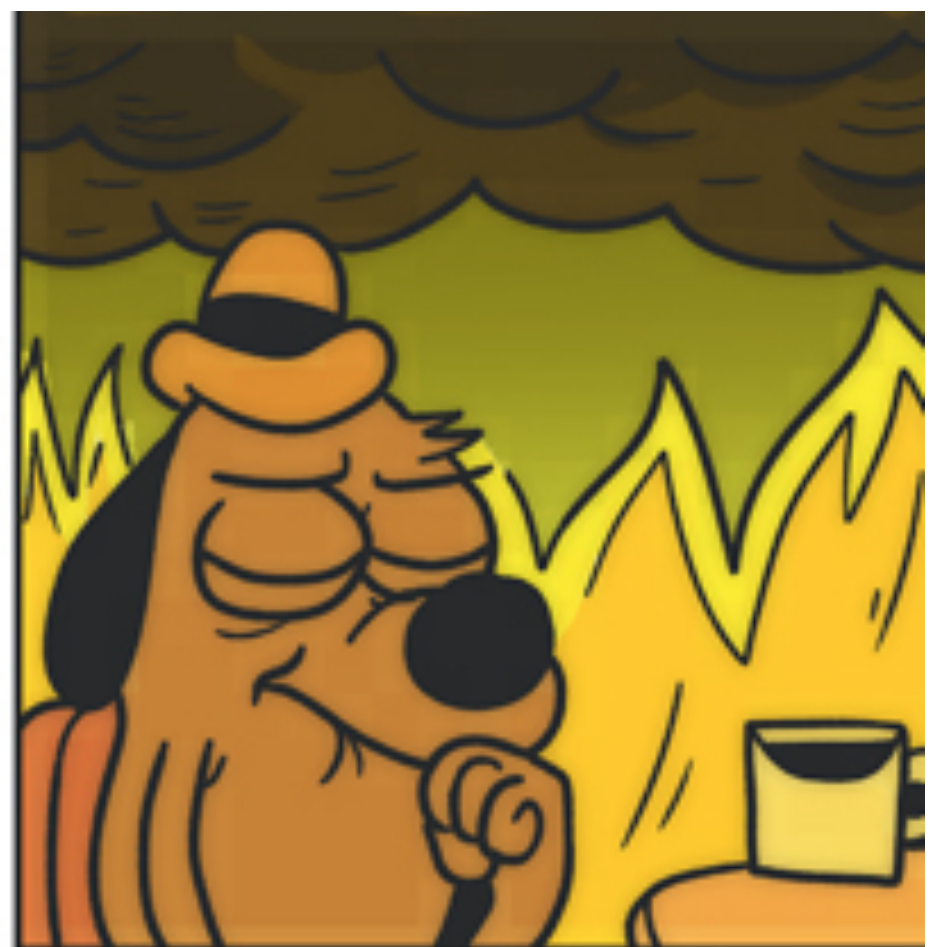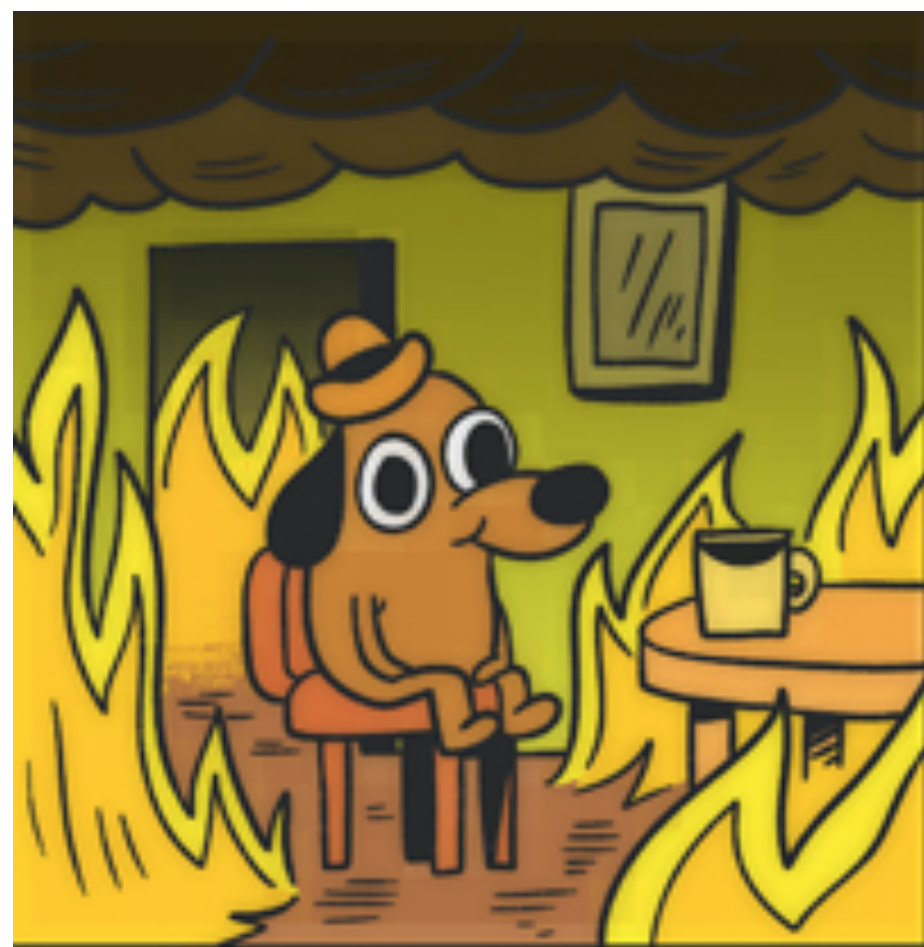
Attackers asking for a ransom

elastic

Learn about a breach

Cloud provider's bill

elastic

Learn about a breach
Yourself after the fact

elastic

Learn about a breach

Yourself & YOU CAN PROVE NO HARM

elastic

No silver bullet 🔫

elastic

AUDITD
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."
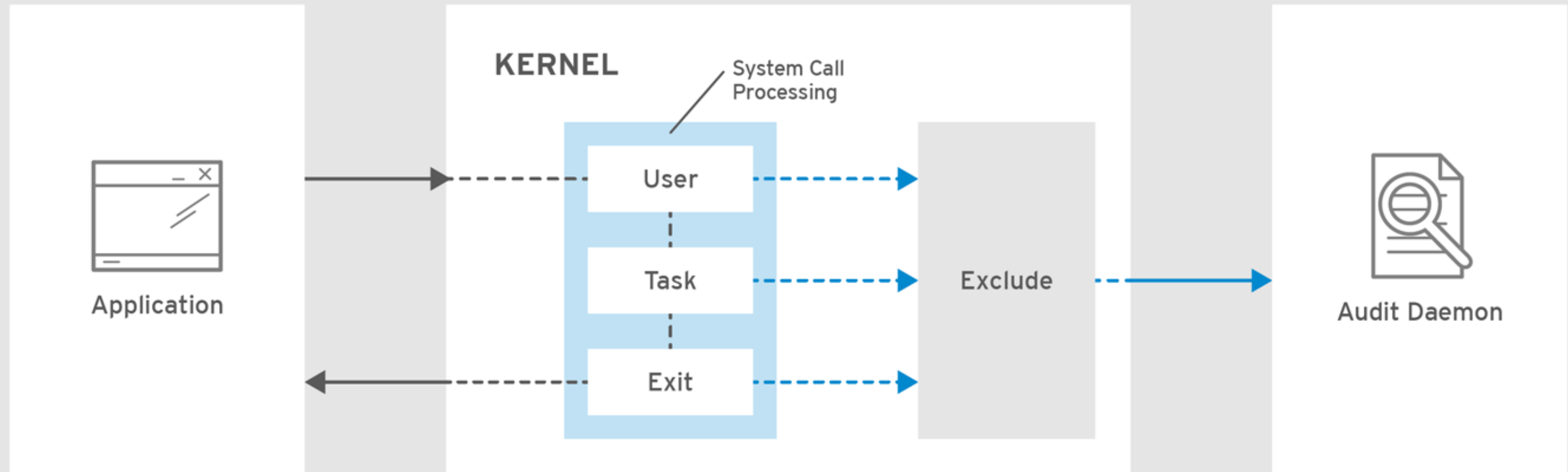
elastic

Monitor

File and network access

System calls

Commands run by a user

Security events

elastic

KERNEL

System Call
Processing

User

Task

Exit

Exclude

Application

Audit Daemon

RHEL_453350_0717

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

Demo

elastic

Understanding Logs

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

elastic

More Rules

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

elastic

Namespaces WIP

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

elastic

Problem

How to centralize?
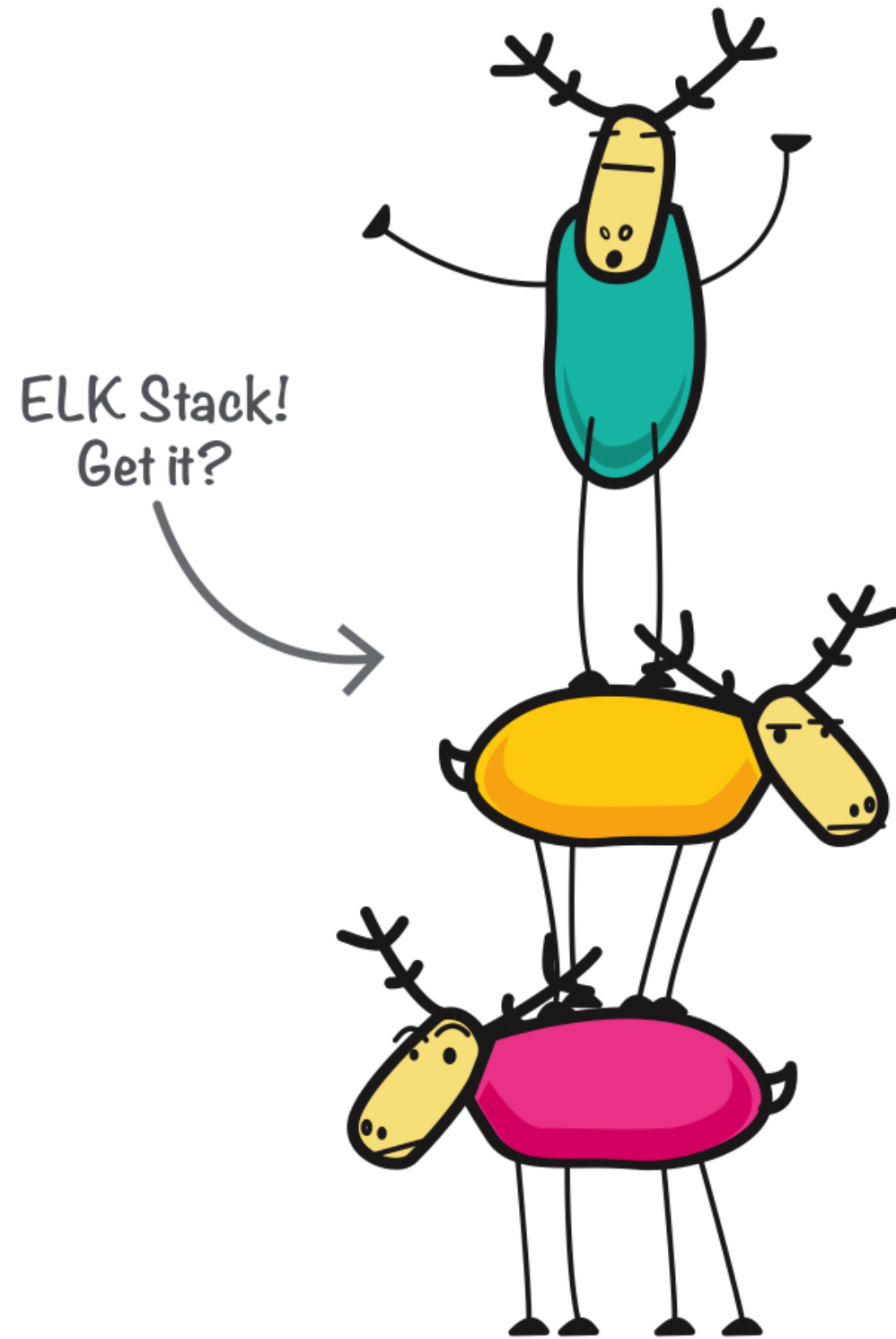
elastic

Disclaimer

I build **highly** monitored Hello World apps

elastic
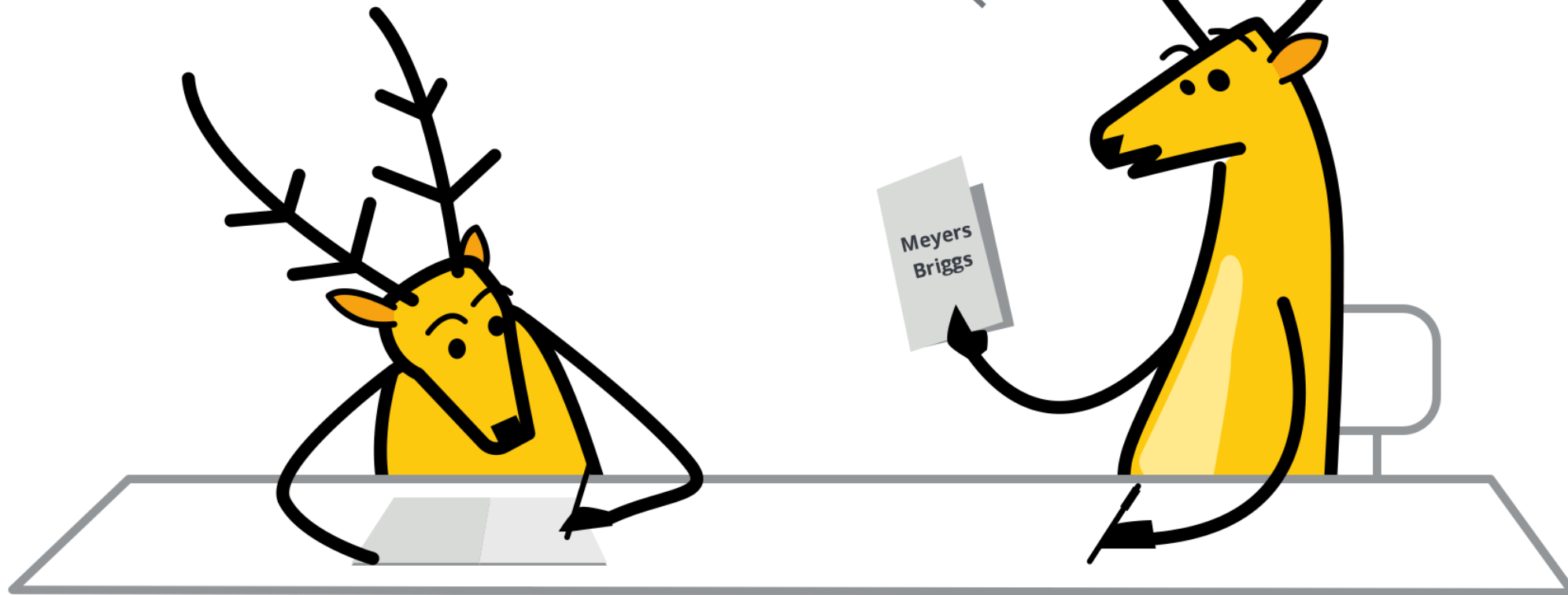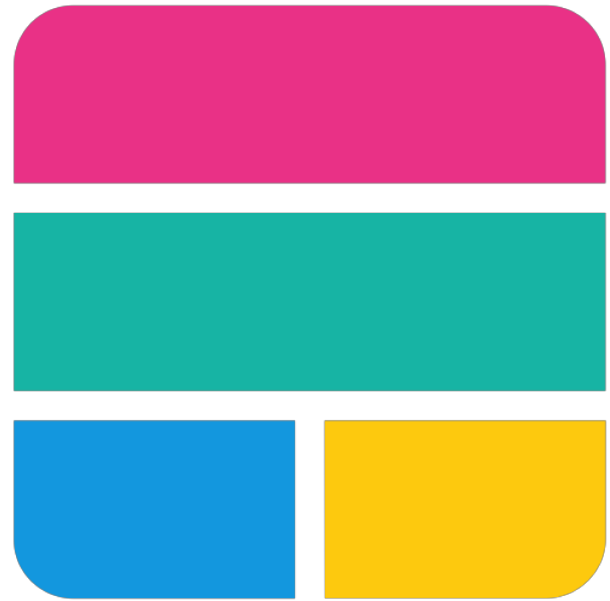
elastic stack

Kibana

Elasticsearch

Beats

Logstash

Filebeat Module: Auditd

elastic

Demo

elastic

elastic cloud

https://cloud.elastic.co
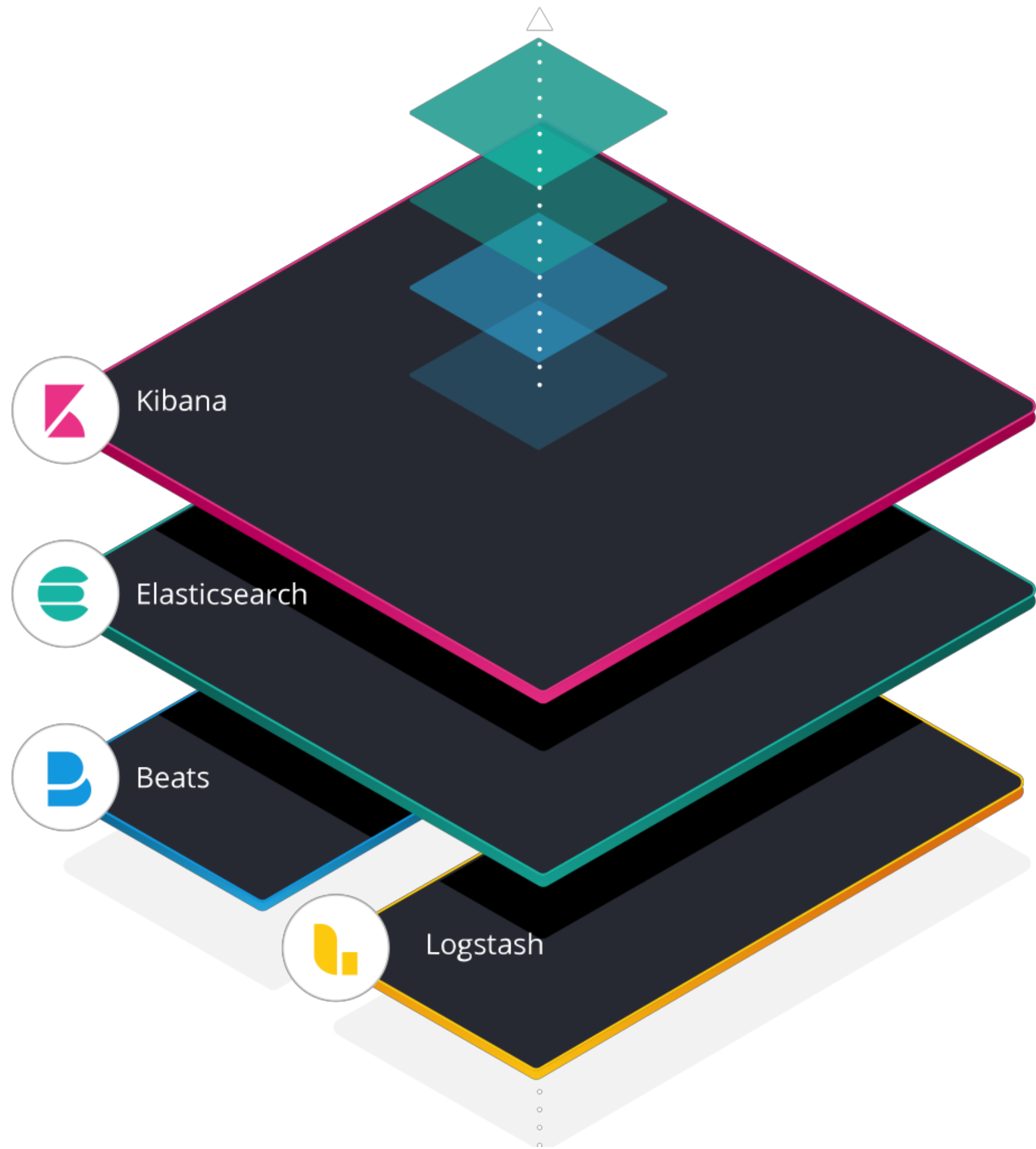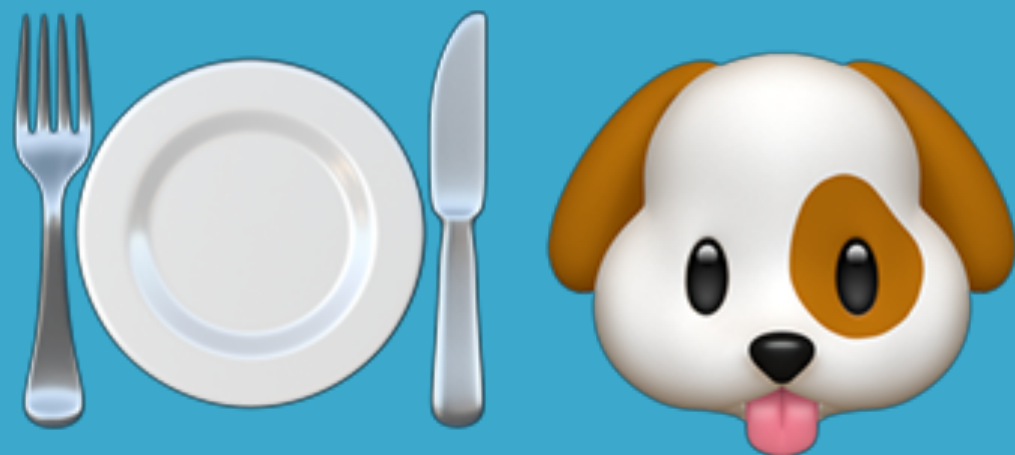
elastic

AUDITBEAT

elastic

Auditd Module

Correlate related events

Resolve UIDs to user names

Native Elasticsearch integration

elastic

Auditd Module

eBPF powers on older kernels

Easier configuration

Written in Golang

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

GO-LIBAUDIT

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

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

elastic

Demo

elastic

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

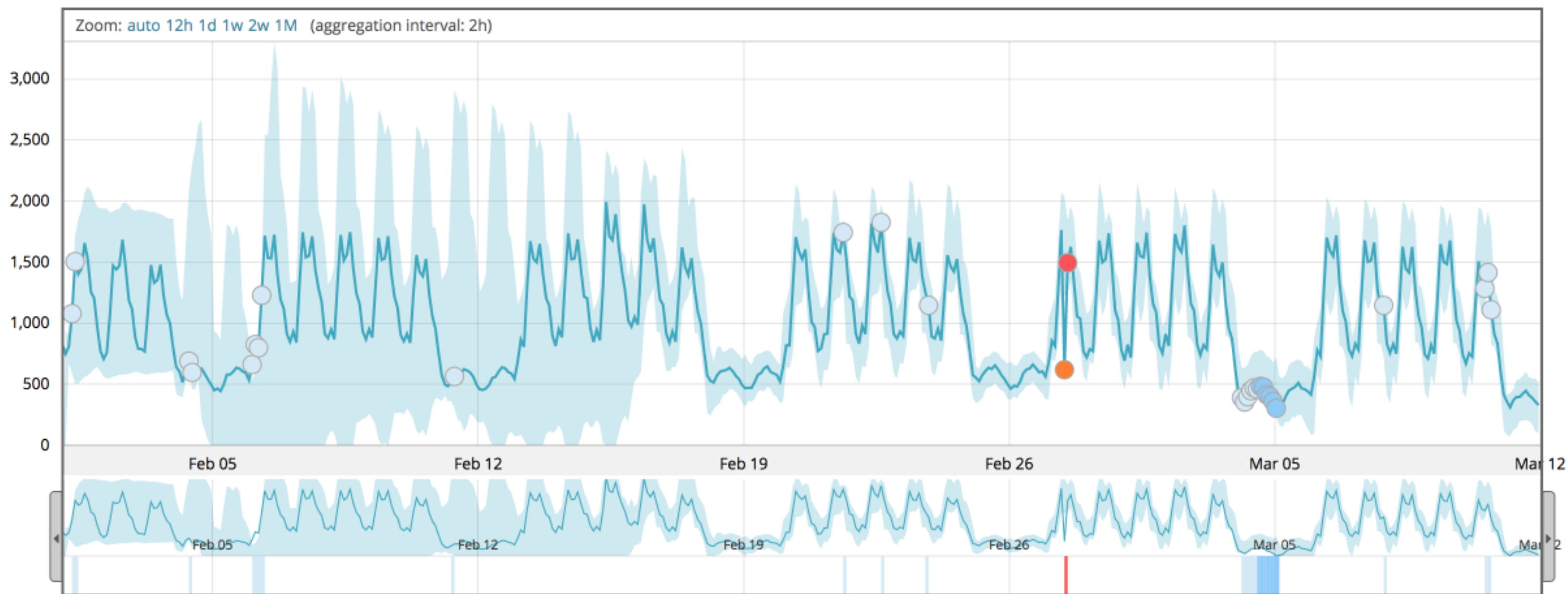# Demo

elastic

PS: Machine Learning

elastic

Job Management Anomaly Explorer **Single Metric Viewer**

Job nginx-demo ▾

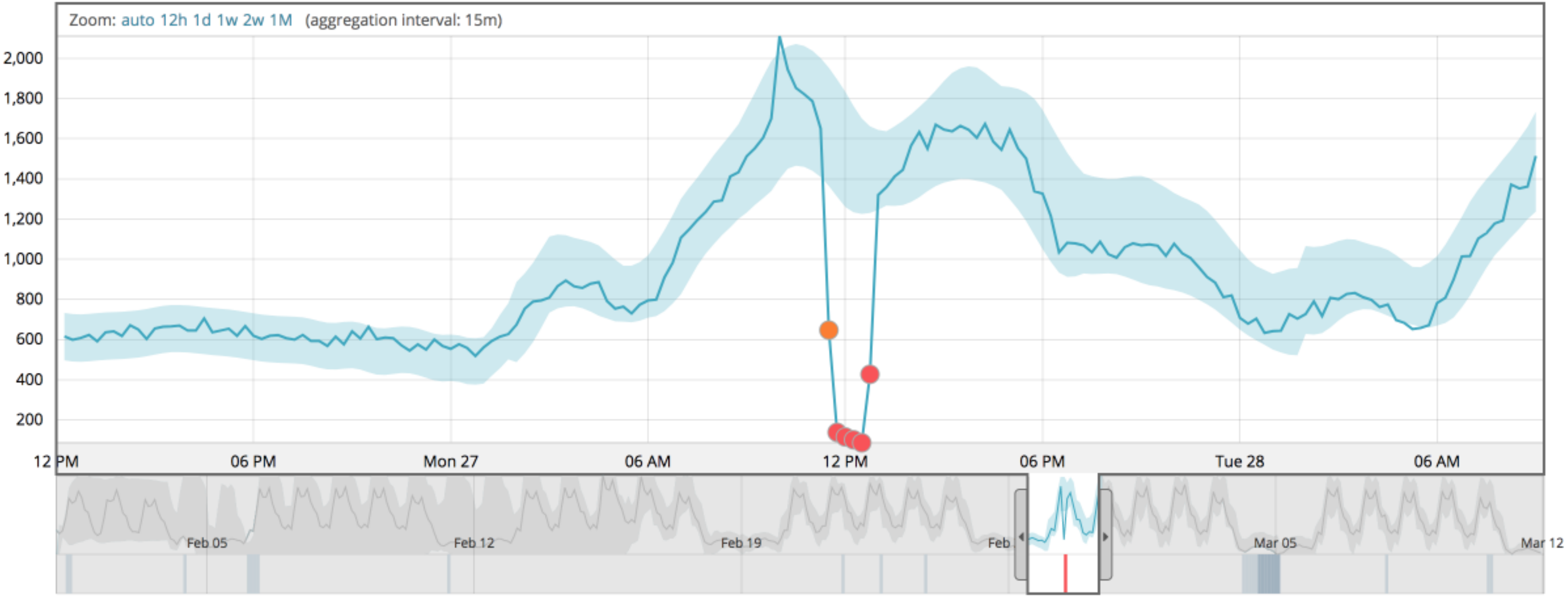**Detector:** distinct_count (nginx.access.remote_ip.keyword) ▾ ▶

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

Zoom: auto 12h 1d 1w 2w 1M (aggregation interval: 2h)

Anomalies

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

Zoom: auto 12h 1d 1w 2w 1M (aggregation interval: 15m)

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

elastic

Auditd
Auditbeat
Logs, Dashboards,...

elastic

Try

https://dashboard.xeraa.wtf

SSH: elastic-user@xeraa.wtf   secret

elastic

Code

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

elastic

Similar Solutions

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

https://github.com/Scribery/aushape

elastic

Questions?

Philipp Krenn   **@xeraa**

PS: Sticker

elastic