Identifier les menaces avec Elastic SIEM

David Pilato

@dadoonet

elastic


THIS IS FINE.

Les incidents de sécurité ont 3 niveaux

FYI, WTF ET OMG

elastic


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

Découvrir une faille par

LA PRESSE OU

LES UTILISATEURS

elastic

Découvrir une faille par

LES PIRATES DEMANDANT UNE RANÇON

elastic

Découvrir une faille par

VOTRE FACTURE CLOUD

elastic

Découvrir une faille par

VOUS-MÊME APRÈS LES FAITS

elastic

Découvrir une faille par

VOUS-MÊME ET POUVOIR PROUVER QU'IL N'Y A PAS EU DE DÉGATS

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."

Pour monitorer

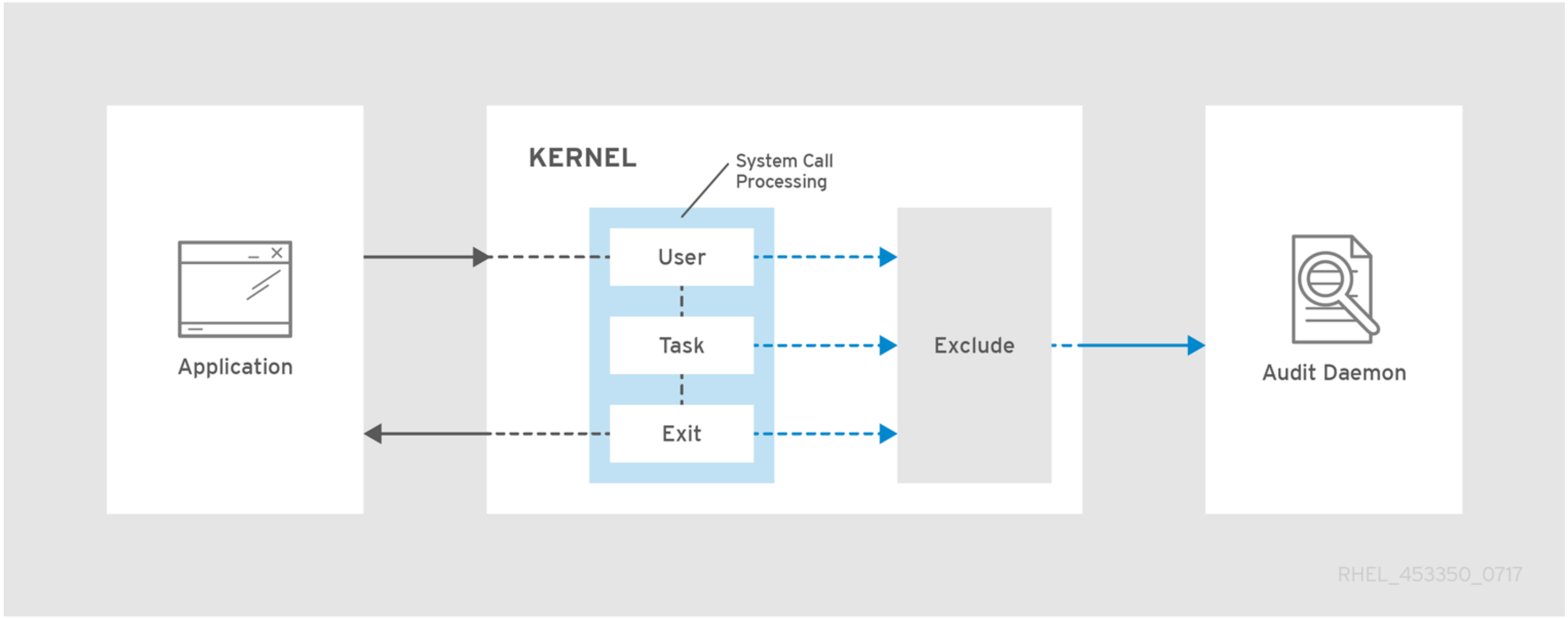
Accès fichier et réseau

Appels système

Commandes lancées par un utilisateur

Evènements de sécurité

elastic



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

Demo

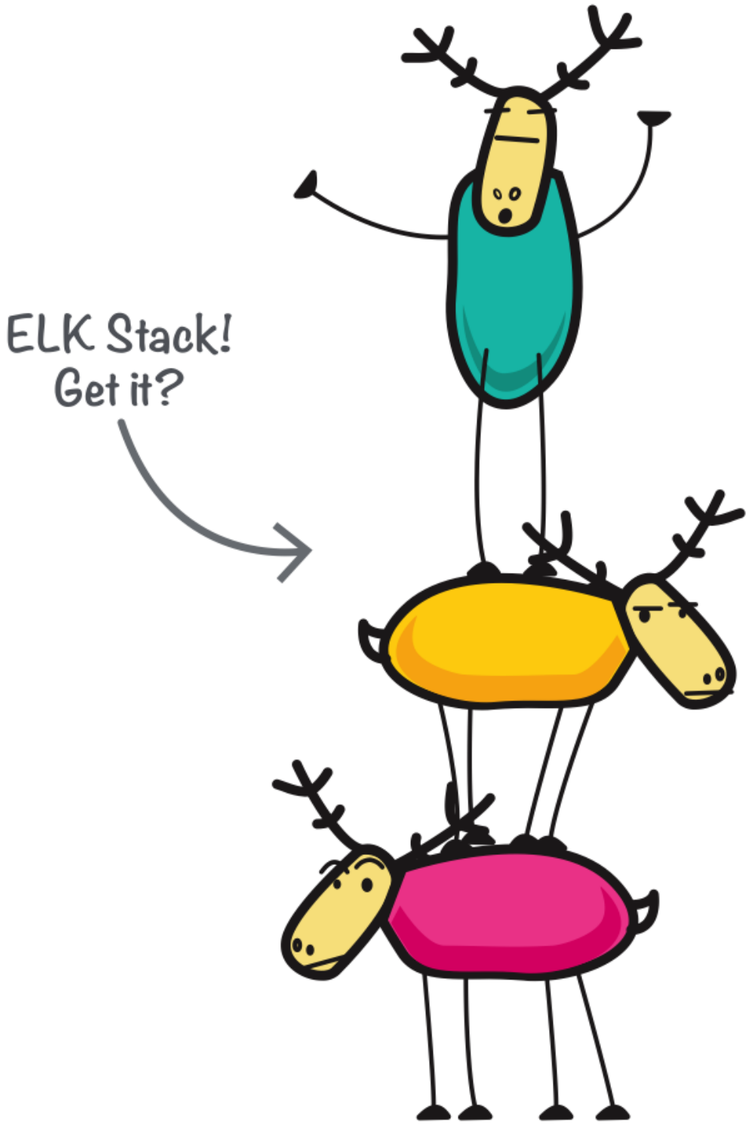

ALL THE THINGS!

Problem

How to centralize?

elastic

Developer | Evangelist

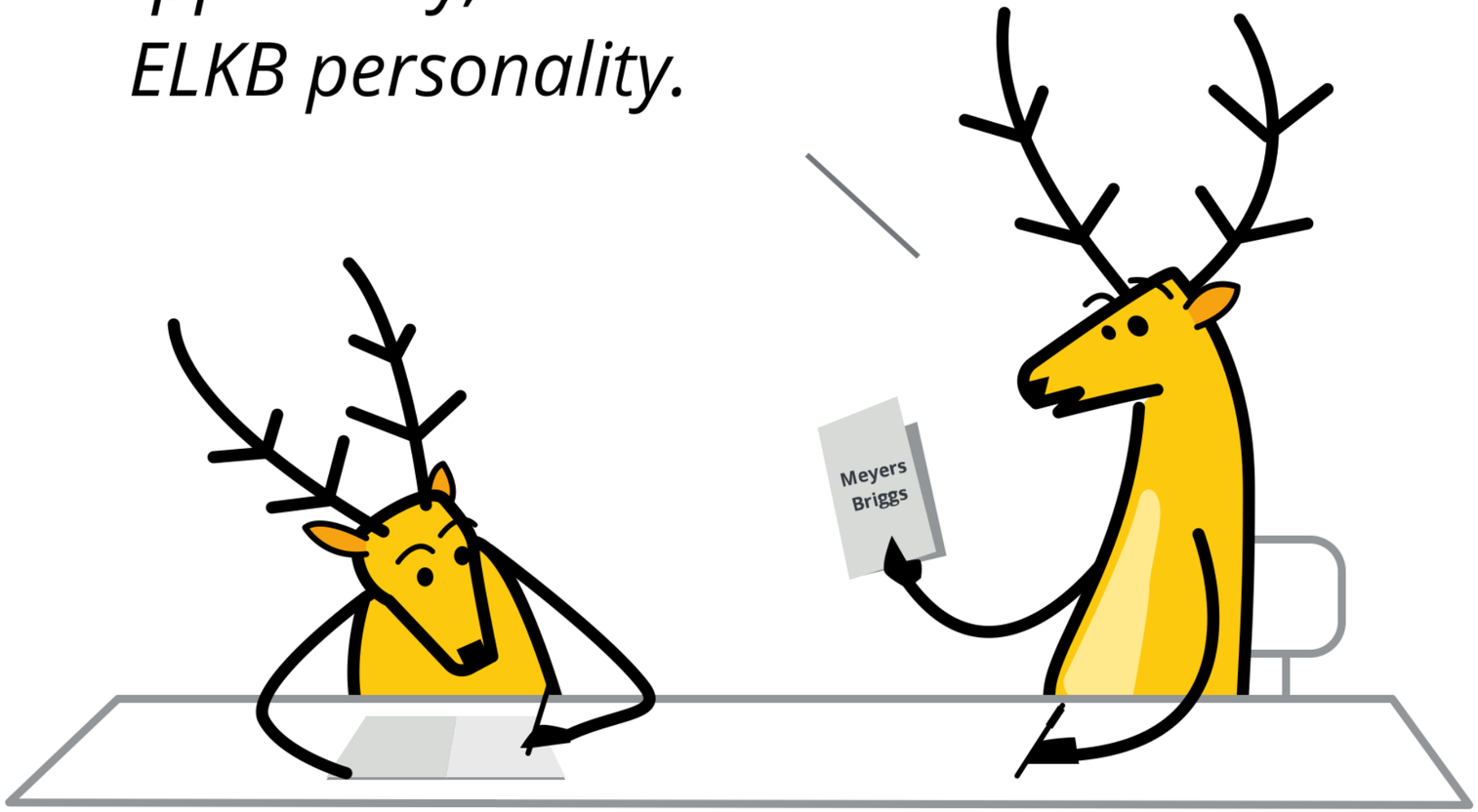


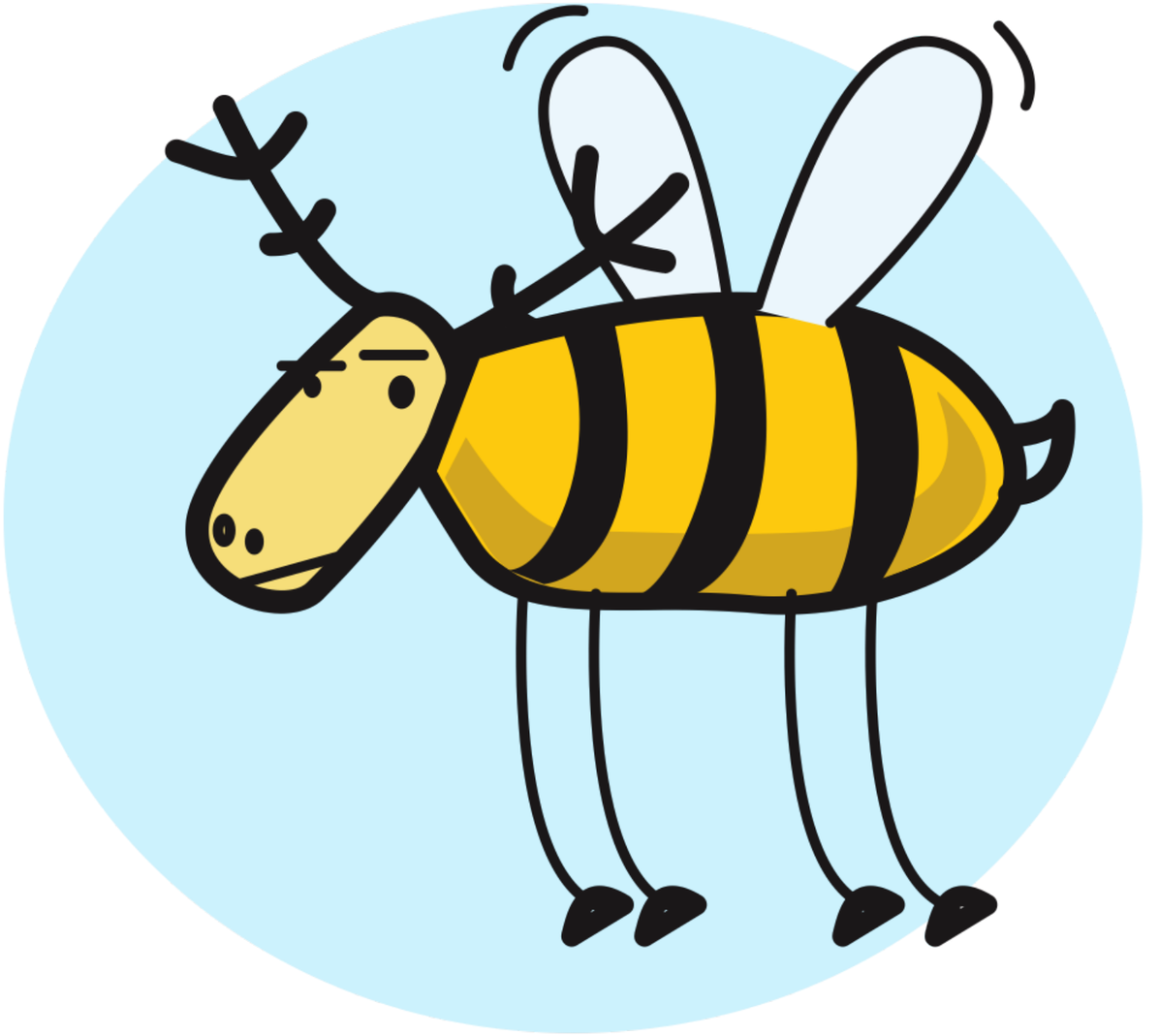
E Elasticsearch

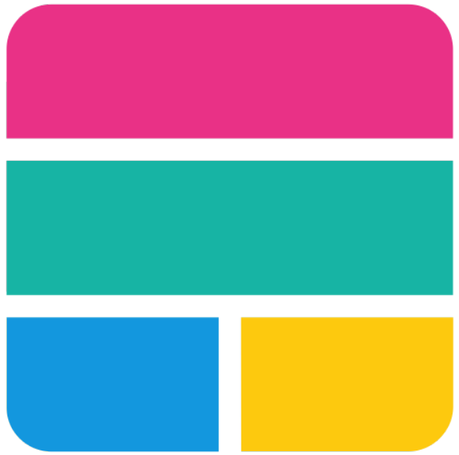
L Logstash

K Kibana

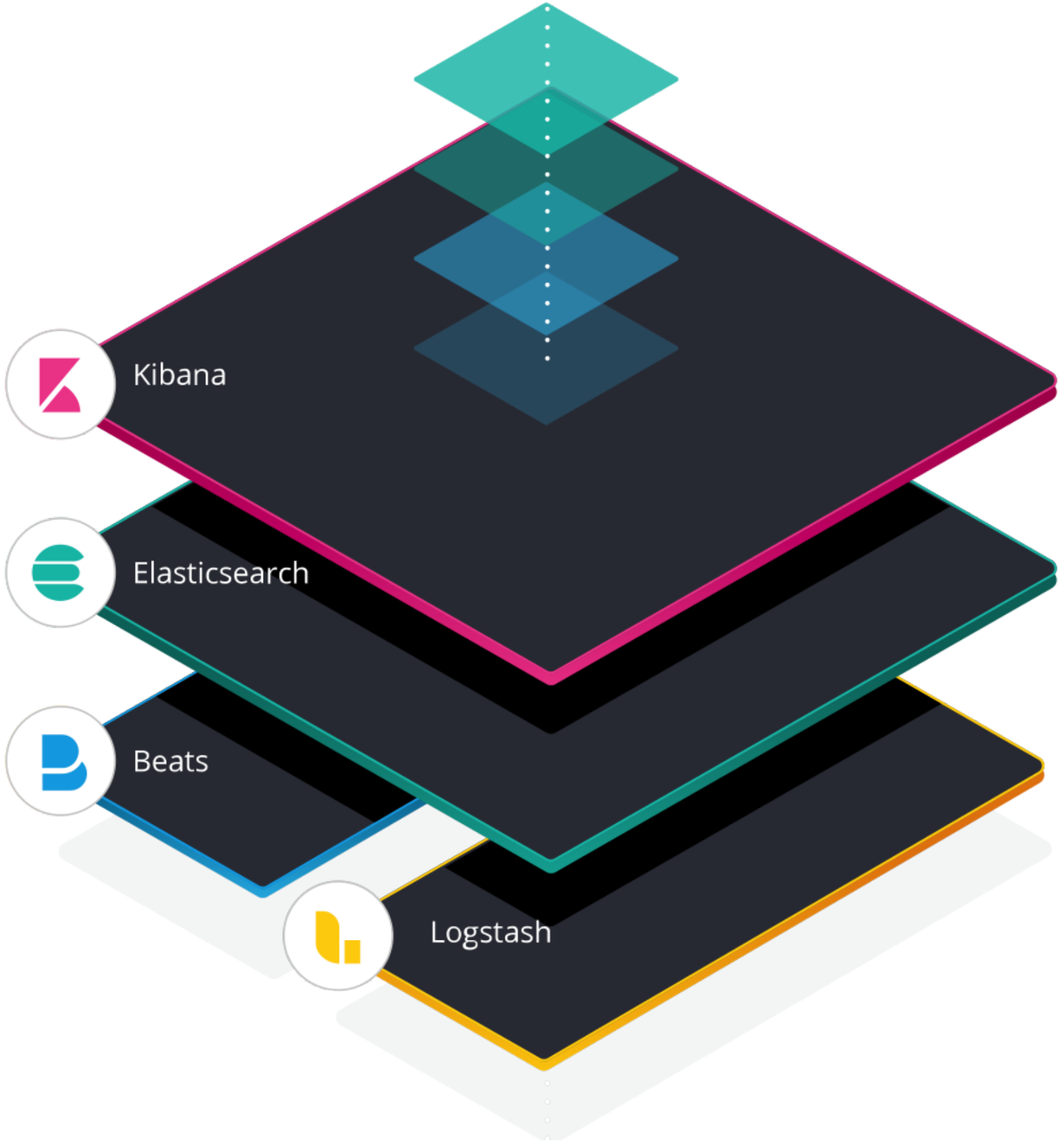
Apparently, I'm an ELKB personality.







elastic stack


Kibana
Elasticsearch
Beats
Logstash

Filebeat Module: Auditd

Demo

AUDITBEAT

elastic

Auditd Module

Correlate related events

Resolve UIDs to user names

Native Elasticsearch integration

Auditd Module

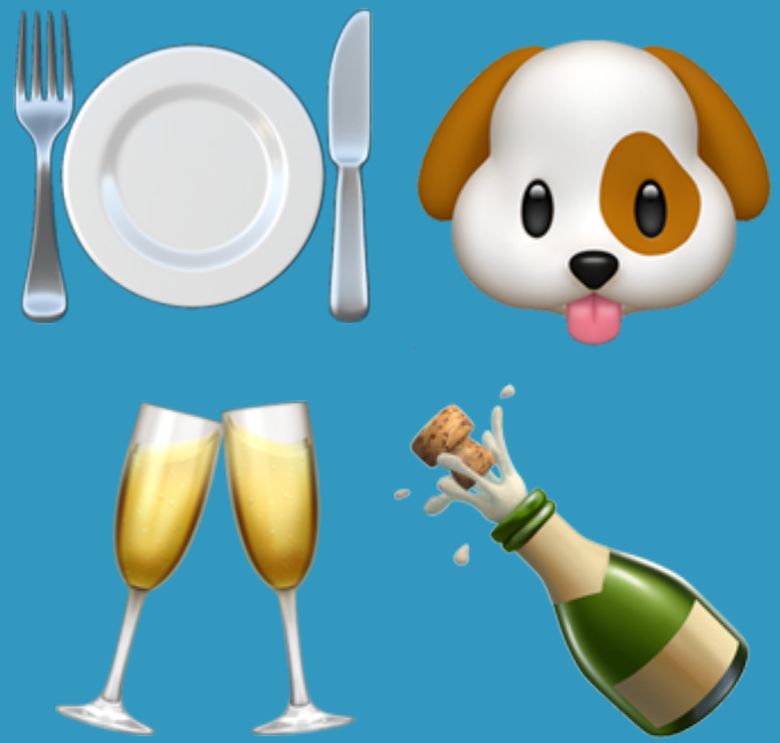
eBPF powers on older kernels

Easier configuration

Written in Golang

elastic

Demo



elastic

elastic cloud

https://cloud.elastic.co

elastic

System Module

Simpler syntax for host, process, socket, user

1. Host dataset works for Windows, macOS, and Linux and is using system APIs for the most part
2. Process dataset works for all three OS as well, and is using `/proc` on Linux, and system APIs on macOS and Windows

Demo

File Integrity Module

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

Demo

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

Running on Kubernetes

Where to run it

DaemonSet

How to run it

https://github.com/elastic/beats/tree/master/deploy/kubernetes/auditbeat

add_docker_metadata

add_kubernetes_metadata


ALL THE THINGS!

Elastic Common Schema

https://github.com/elastic/ecs

elastic

```yaml
---
- name: base
  root: true
  title: Base
  group: 1
  short: All fields defined directly at the top level
  description: >
    The `base` field set contains all fields which are on the top level.
    These fields are common across all types of events.
  type: group
  fields:
    - name: "@timestamp"
      type: date
      level: core
      required: true
      example: "2016-05-23T08:05:34.853Z"
      short: Date/time when the event   originated.
      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.
```

ELASTIC SIEM

Security Information and Event Management

elastic

Demo

PS: Machine Learning

aka Anomaly Detection

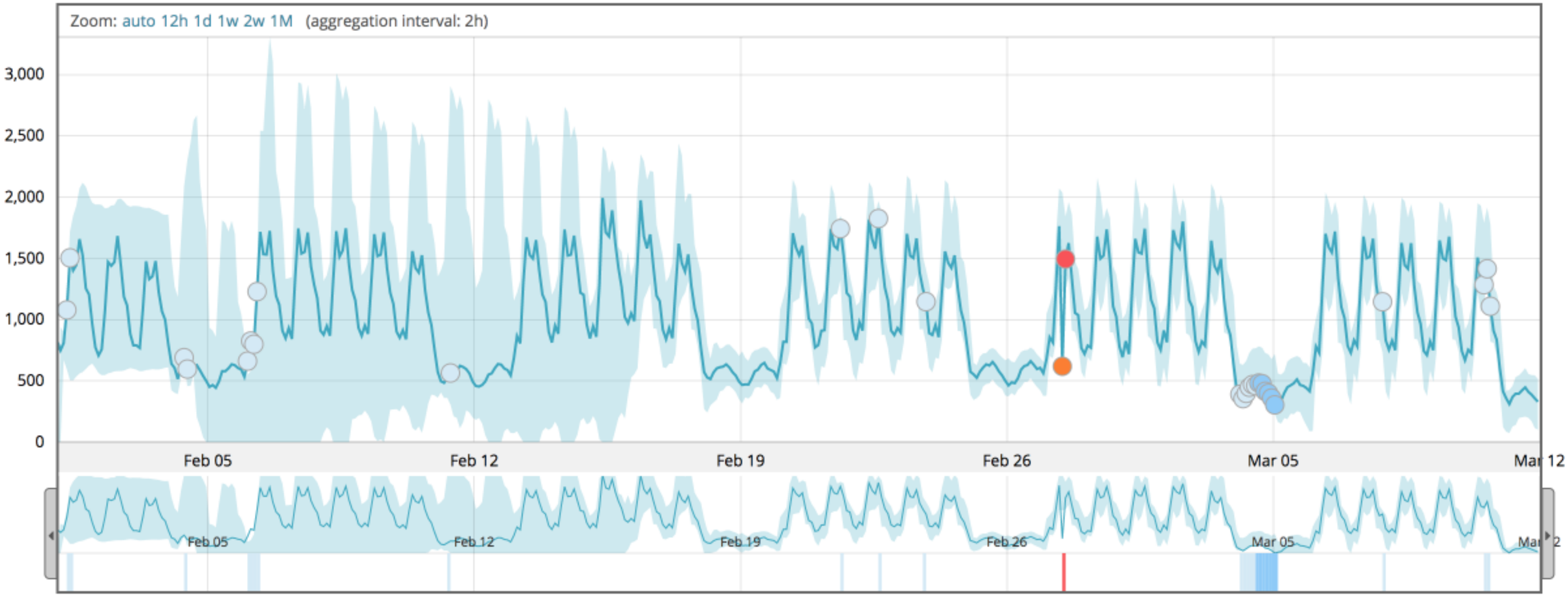
elastic

Job Management Anomaly Explorer Single Metric Viewer

Job nginx-demo

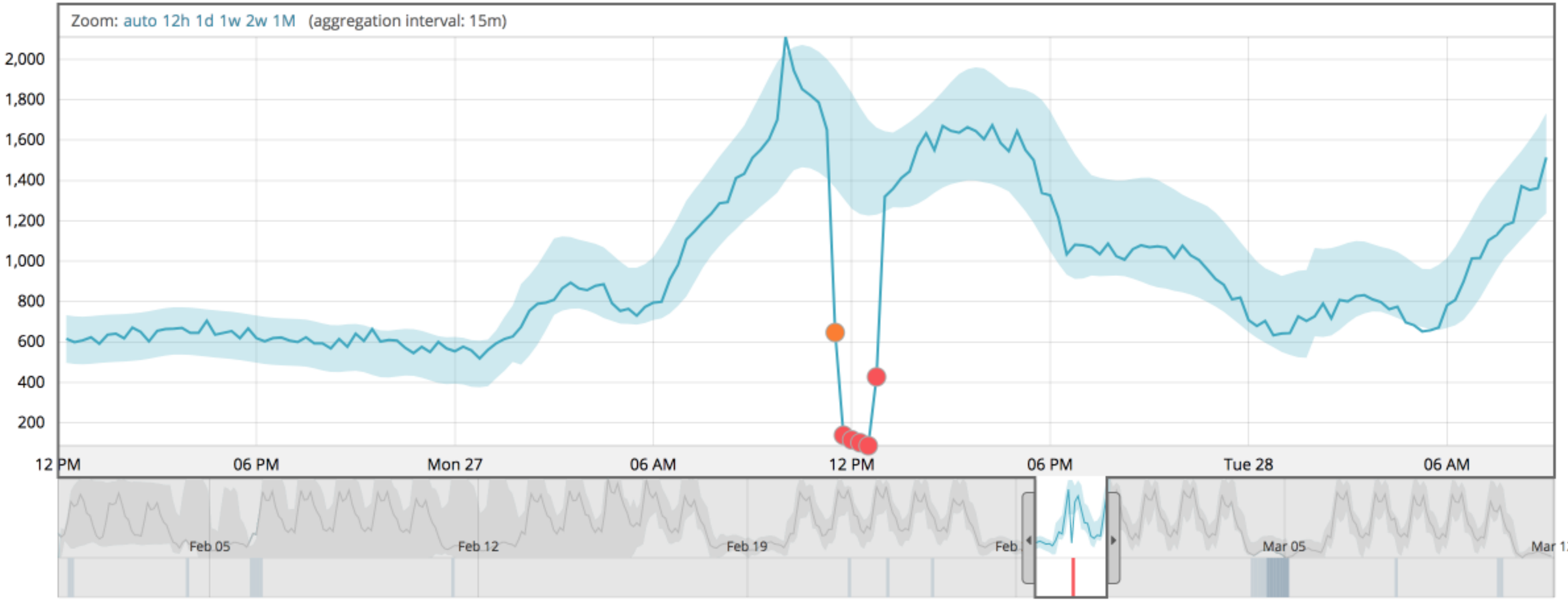
Detector: distinct_count (nginx.access.remote_ip.keyword)

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

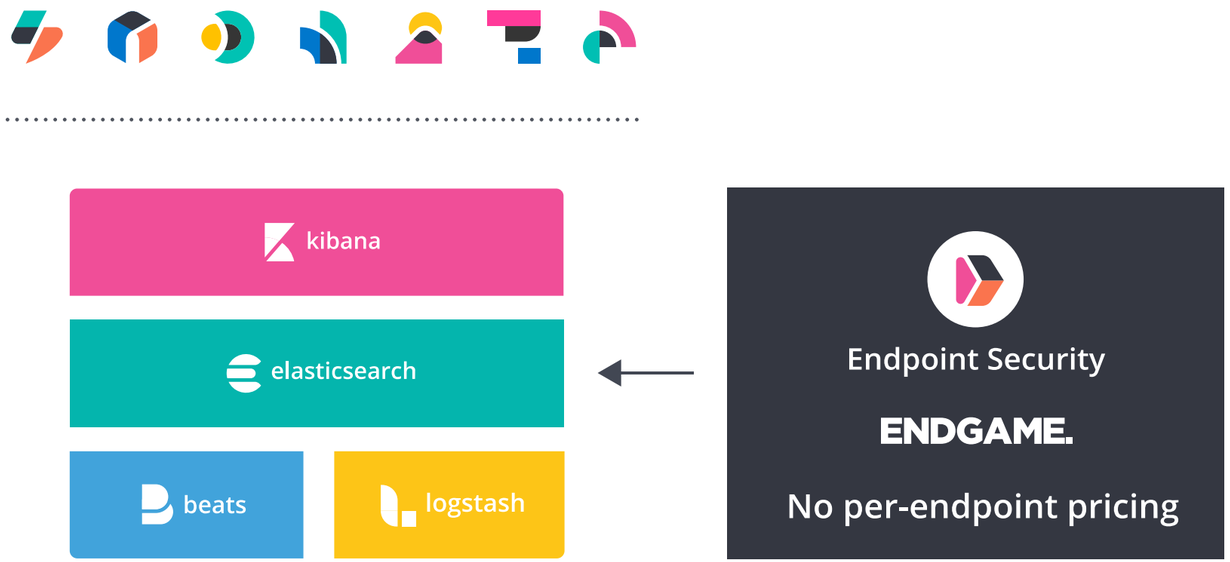
time	max severity	detector	actual	typical	description	job ID
February 27th 2017, 12:00	97	distinct_count (nginx.access.remote_ip.keyword)	86	1453.6	17x lower	nginx-demo
February 27th 2017, 11:00	86	distinct_count (nginx.access.remote_ip.keyword)	138	1575.97	11x lower	nginx-demo

Elastic Endpoint

elastic

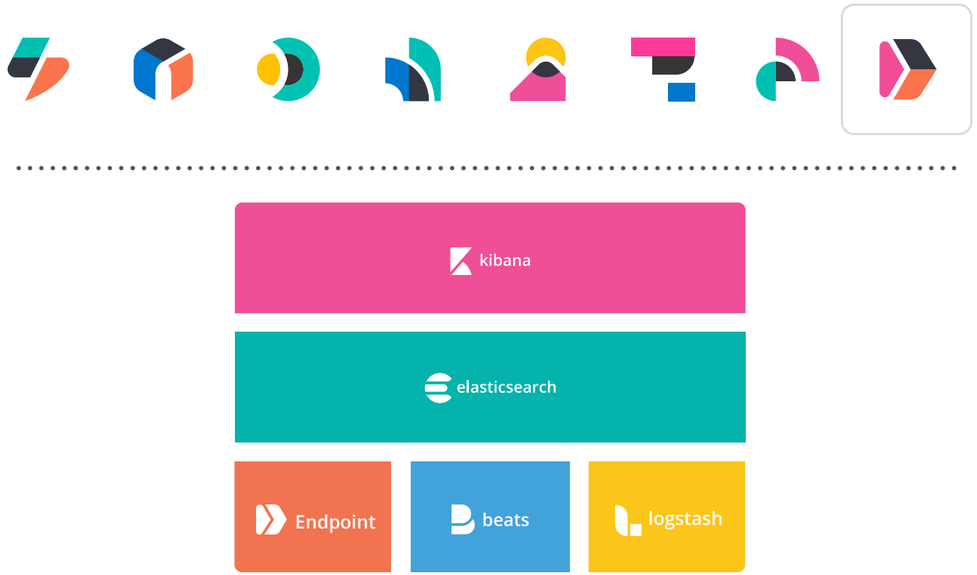
Today

Comprehensive endpoint protection, detection, and response (EPP+EDR) and no per-endpoint pricing. Just pay for what you use.



Future

EPP, EDR, and SIEM delivered in a single, simplified architecture: Elasticsearch, Kibana, Elastic Endpoint.



Conclusion

Topics

Auditd

Filebeat, Auditbeat

SIEM

elastic

Code

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

Identifier les menaces avec Elastic SIEM

David Pilato

@dadoonet

elastic