Scale Your Auditing Events

Philipp Krenn @xeraa


THIS IS FINE.

Security incidents come in three levels

FYI, WTF, AND OMG

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

Learn about a breach

YOURSELF & YOU CAN PROVE NO HARM

No silver bullet 

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."

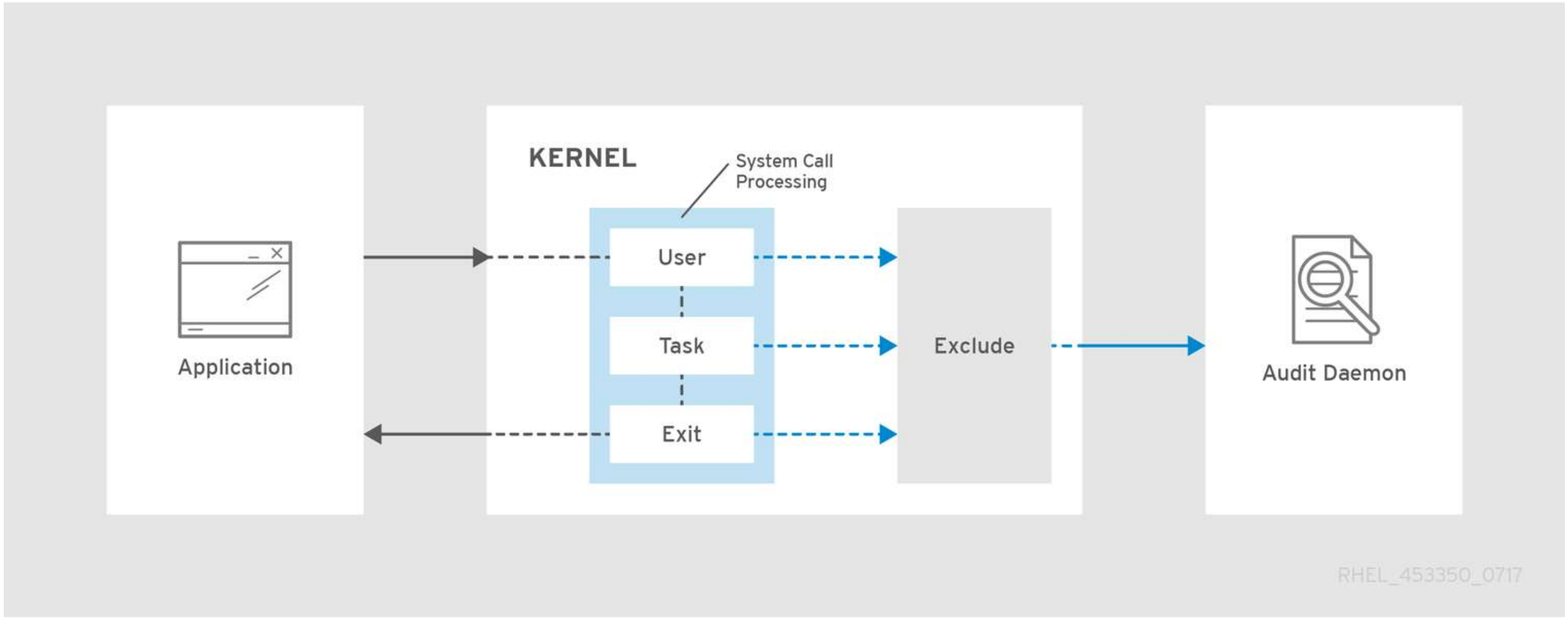
Monitor

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

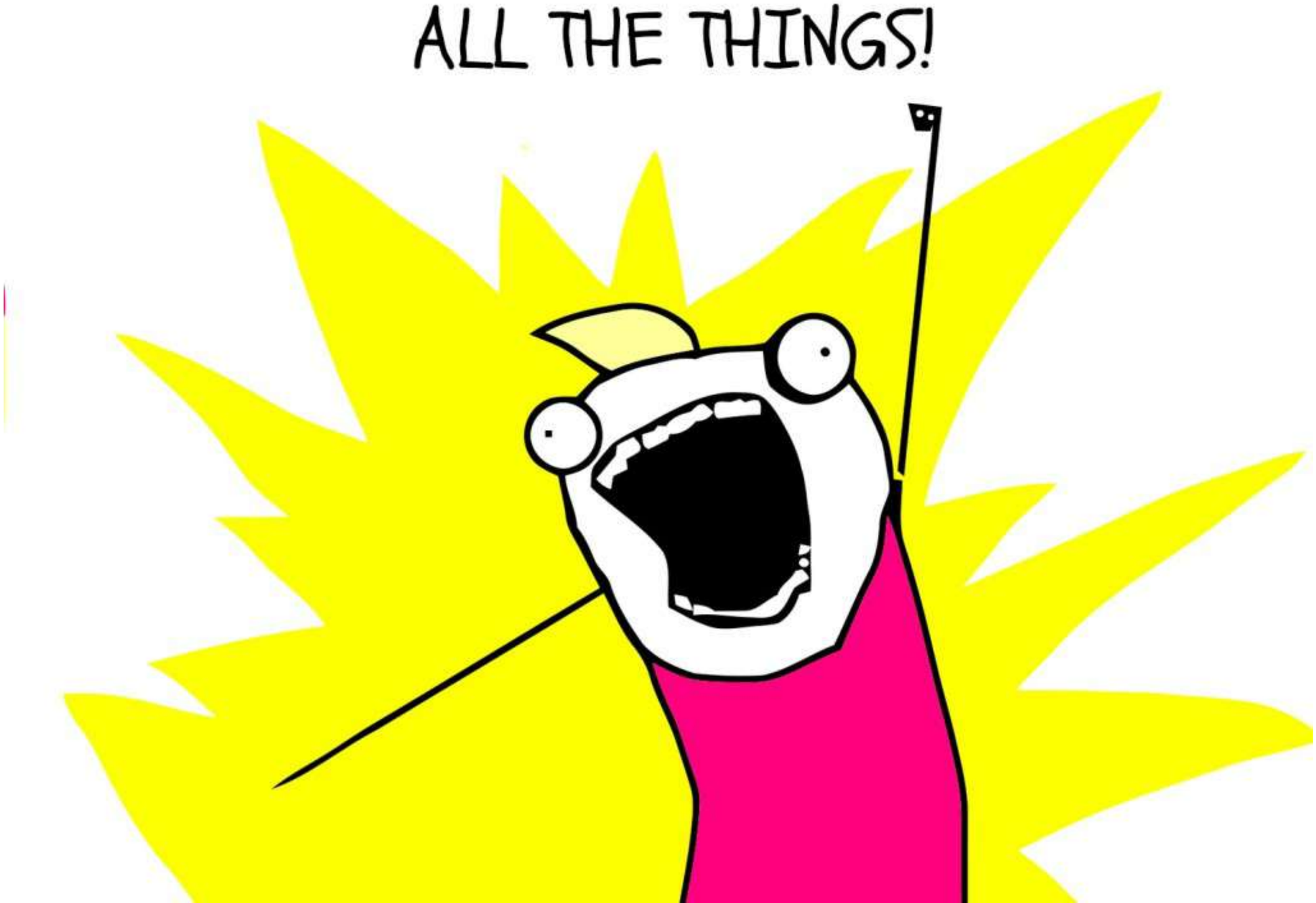
https://github.com/linux-audit/audit-userspace/tree/master/rules

Actual Rules

https://github.com/mtkirby/audisp-simplify

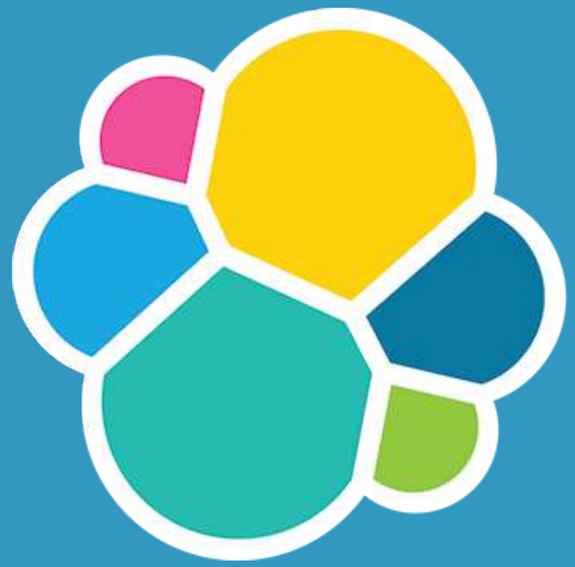
Namespaces WIP

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


ALL THE THINGS!

Problem

How to centralize?

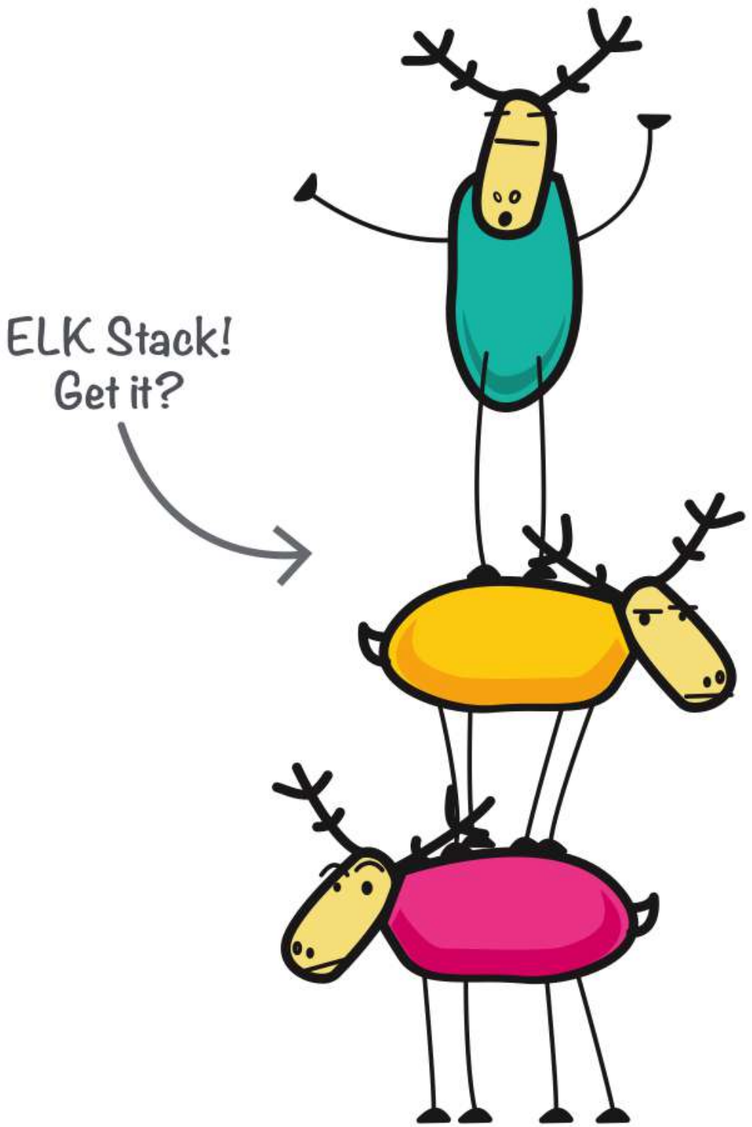


elastic

Developer 🥑

Disclaimer

I BUILD HIGHLY MONITORED HELLO WORLD APPS

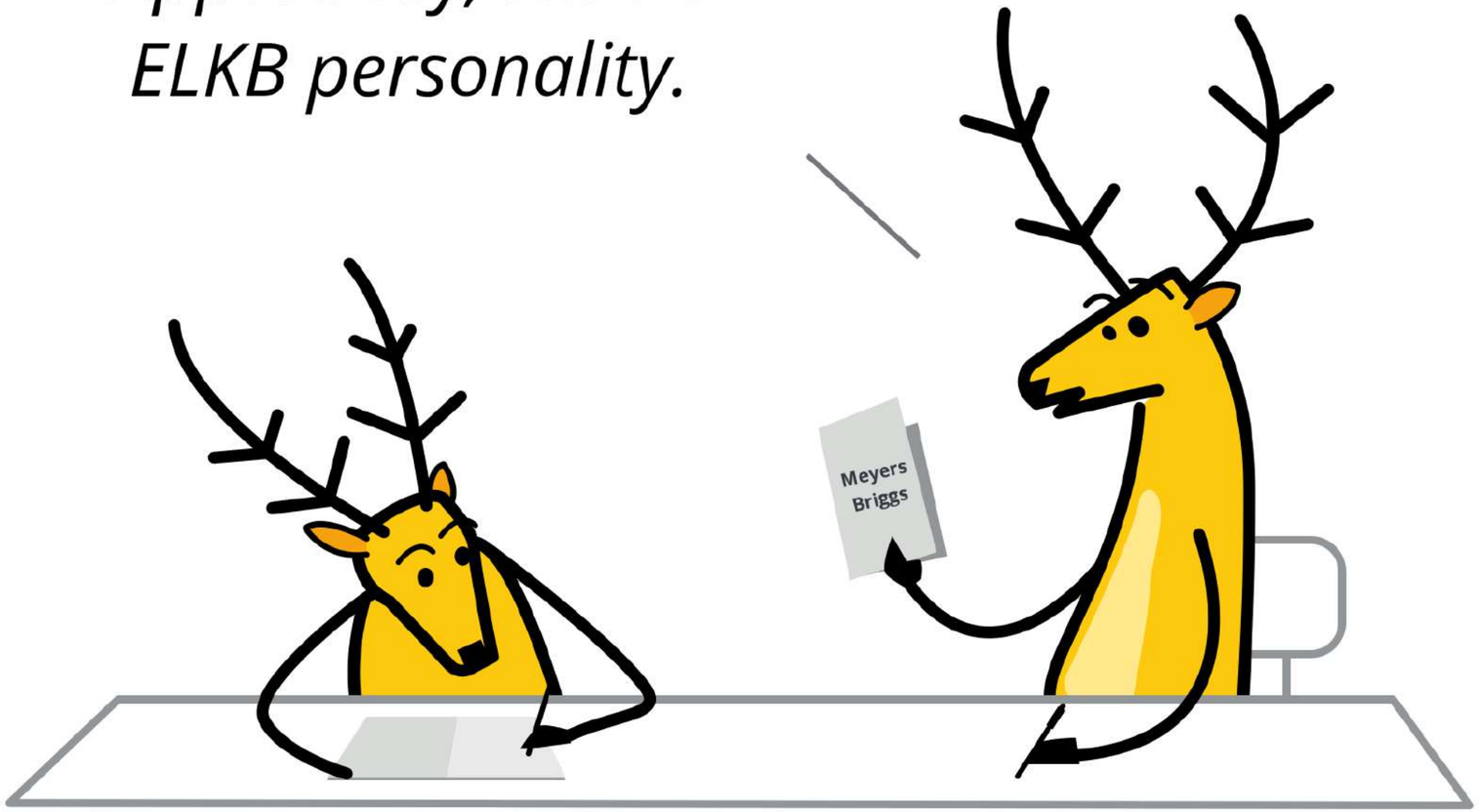


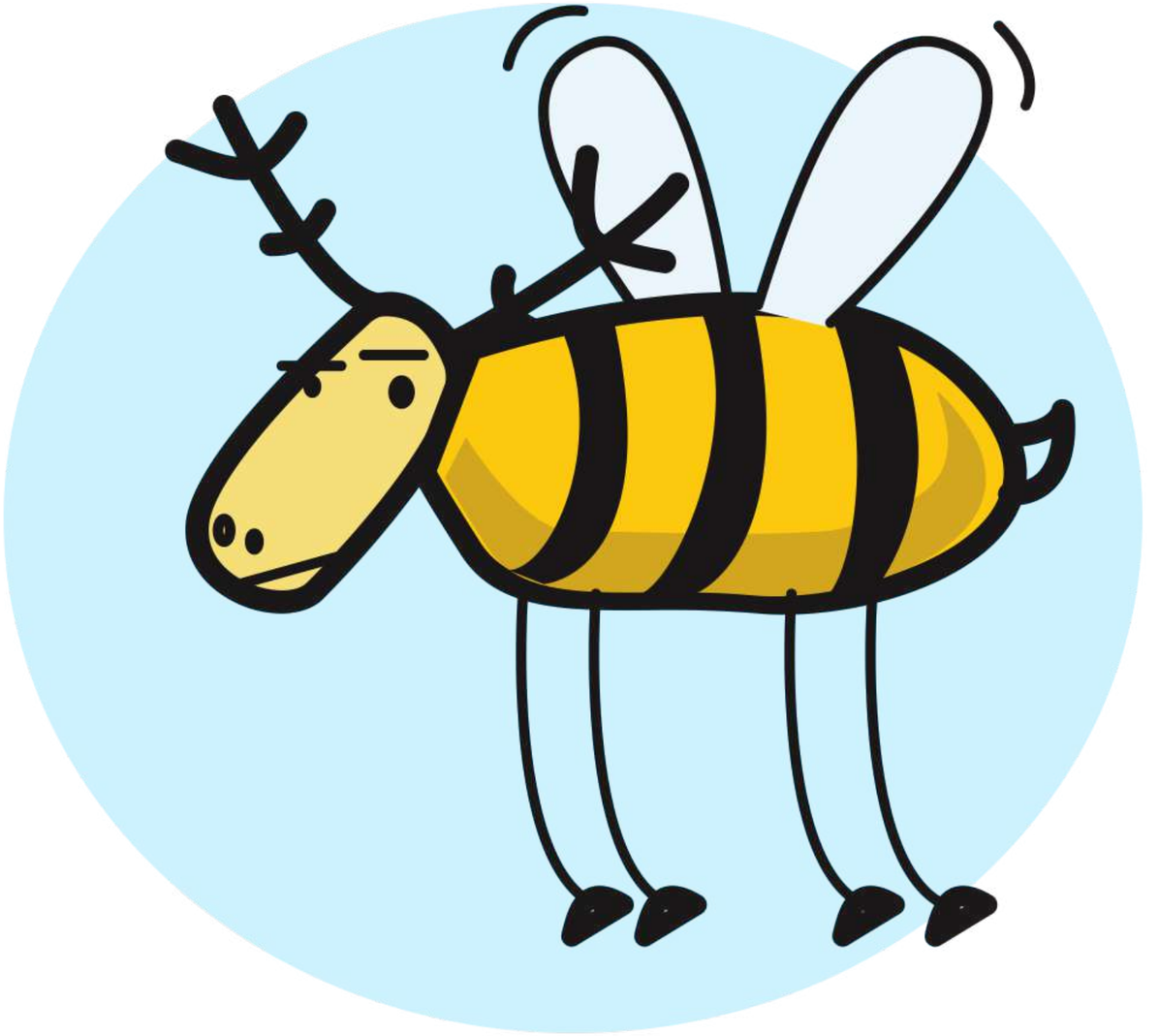
E Elasticsearch

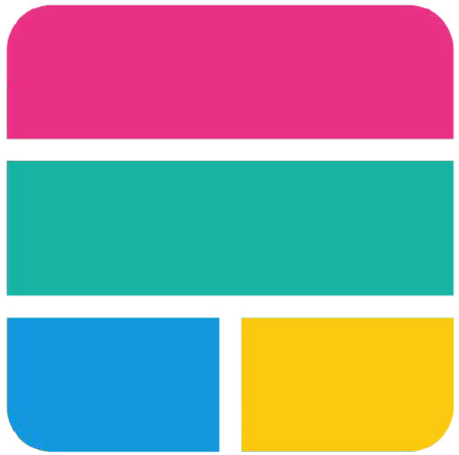
L Logstash

K Kibana

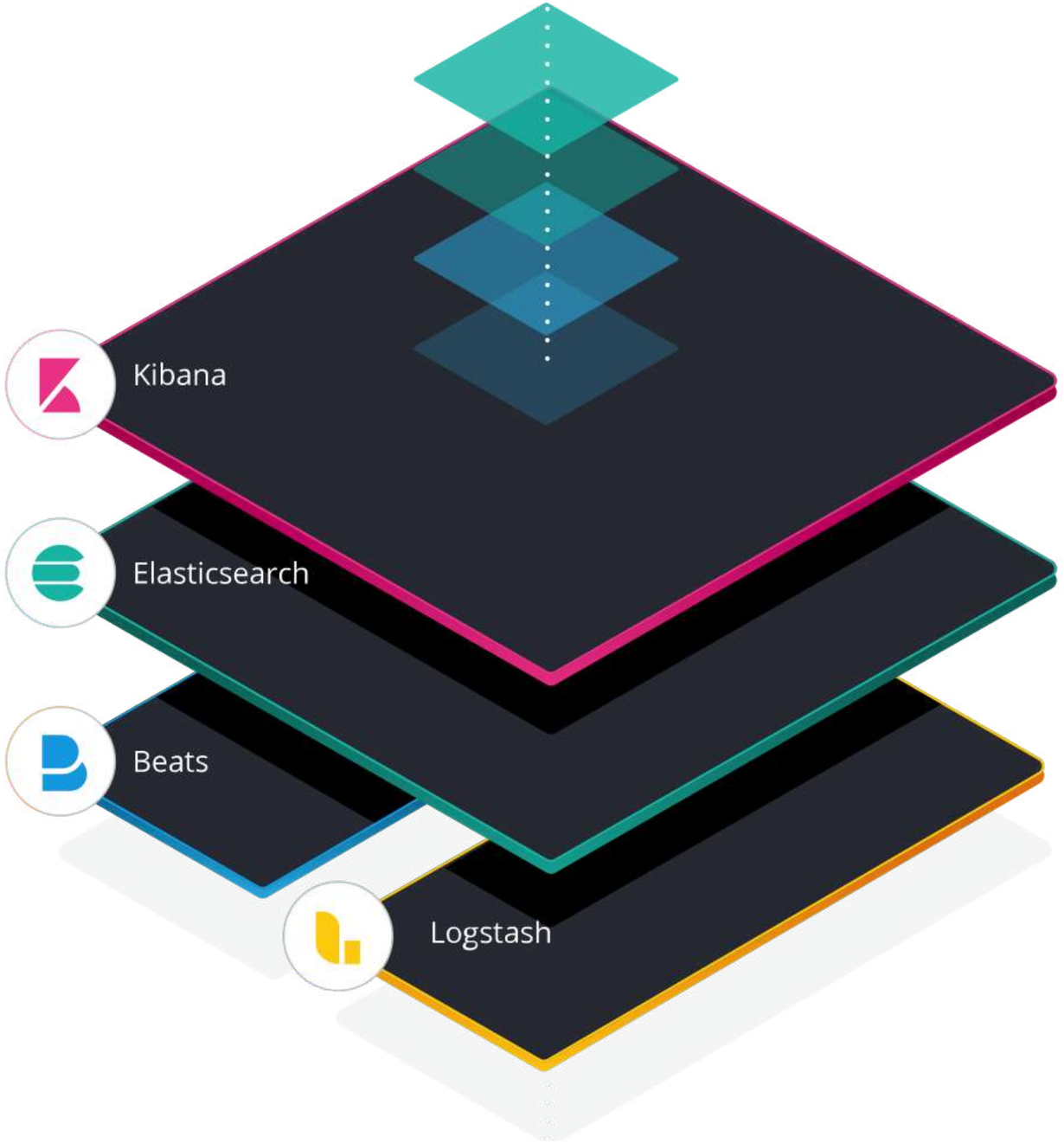
Apparently, I'm an ELKB personality.





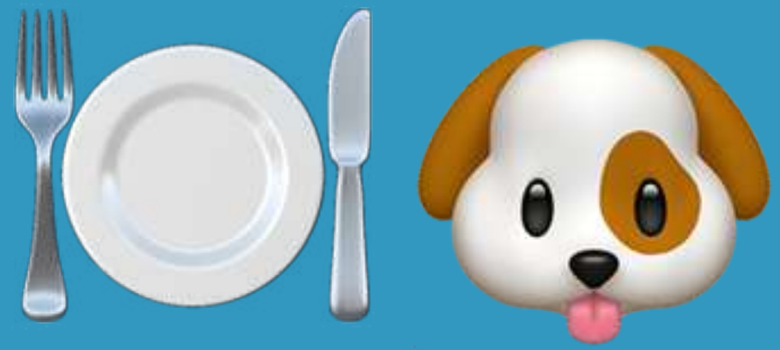


elastic stack


Kibana
Elasticsearch
Beats
Logstash

Filebeat Module: Auditd

Demo



elastic

elastic

elastic cloud

https://cloud.elastic.co

elastic

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

elastic

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

GO-LIBAUDIT

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

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

Demo

System Module

Simpler syntax 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

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
```

Kubernetes Audit Logs

https://kubernetes.io/docs/tasks/debug-application-cluster/audit/


same

```yaml
apiVersion: audit.k8s.io/v1
kind: Policy

omitStages:
  - "RequestReceived"

rules:
  - level: RequestResponse
    resources:
    - group: ""
      resources: ["pods"]
  - level: Metadata
    resources:
    - group: ""
      resources: ["pods/log", "pods/status"]
```

ELASTIC SIEM

elastic

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.
```

Search KQL Last 24 hours Show dates Refresh

+ Add filter

designed for security analysts and practitioners who have used other SIEMs or are familiar with SIEM concepts.

Elastic Endpoint Security overview webinar

2019-11-17

Elastic is bringing endpoint protection and SIEM together to streamline how you secure your organization.

Elastic SIEM for home and small business

2019-10-24

What might you find with a SIEM dedicated to your small business or home? See how to get started with Elastic SIEM.

Enterprise protection for your endpoints

2019-10-15

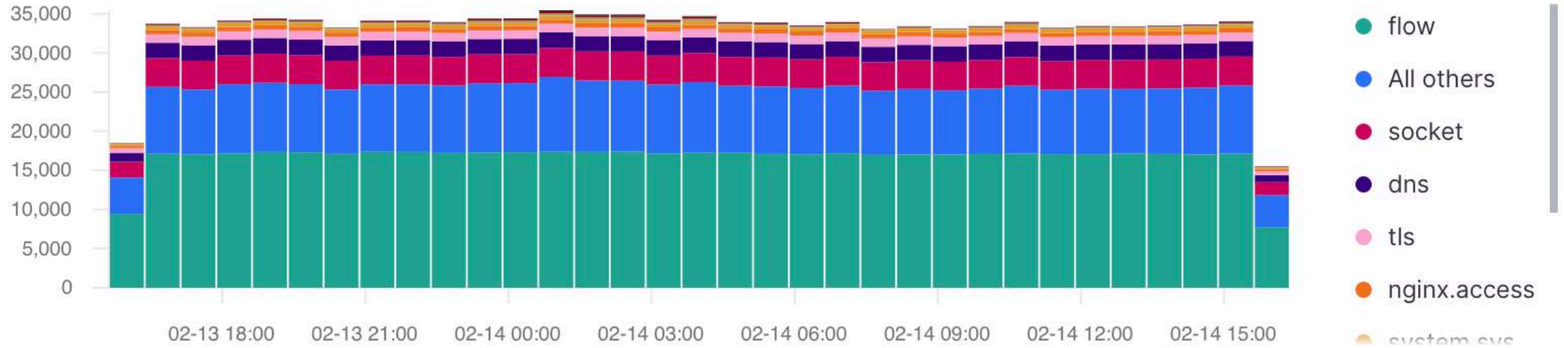
Integrating Elastic Endpoint Security (formerly Endgame) with Elastic SIEM provides a whole new comprehensive security operations solution designed to support multiple users and use cases.

Events count

Showing: 1,087,931 events

Stack by event.dataset

View events



Host events

Showing: 304,014 events

View hosts

Auditbeat	283,243
Elastic Endpoint Security	0
Filebeat	20,771
Winlogbeat	0

Network events

Showing: 766,124 events

View network

Auditbeat	117,929
Filebeat	0
Packetbeat	648,195

Timeline

Search KQL Last 24 hours Show dates Refresh

+ Add filter

Definition

Index patterns

auditbeat-* filebeat-* packetbeat-* winlogbeat-*

Custom query

network.transport: tcp and destination.port:22 and (network.direction: outbound or (source.ip: (10.0.0.0/8 or 172.16.0.0/12 or 192.168.0.0/16) and not destination.ip: (10.0.0.0/8 or 172.16.0.0/12 or 192.168.0.0/16)))

About

Description

This rule detects network events that may indicate the use of SSH traffic from the Internet. SSH is commonly used by system administrators to remotely control a system using the command line shell. If it is exposed to the Internet, it should be done with strong security controls as it is frequently targeted and exploited by threat actors as an initial access or back-door vector.

Severity

Low

Risk score

21

Investigate detections using this timeline template

Default blank timeline

False positive examples

SSH connections may be made directly to Internet destinations in order to access Linux cloud server instances but such connections are usually made only by engineers. In such cases, only SSH gateways, bastions or jump servers may be expected Internet destinations and can be exempted from this rule. SSH may be required by some work-flows such as remote access and support for specialized software products and servers. Such work-flows are usually known and not unexpected. Usage that is unfamiliar to server or network owners can be unexpected and suspicious.

MITRE ATT&CK™

Command and Control (TA0011)

- Commonly Used Port (T1043)

Schedule

Runs every

5m

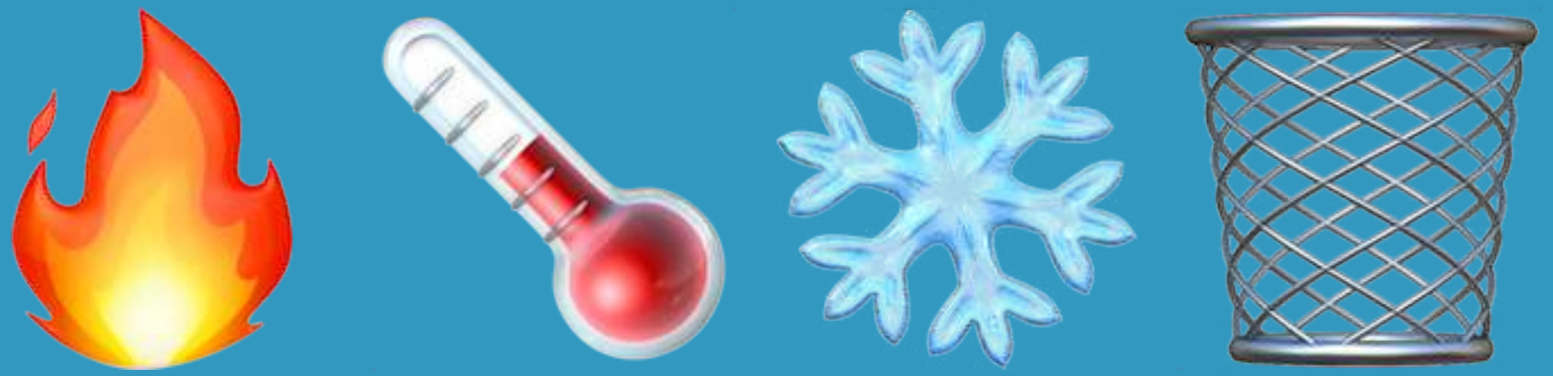
Additional look-back time

1m

Timeline

Demo

SCALE



elastic

ILM

Index Lifecycle Management

elastic

Features & Order

https://github.com/elastic/elasticsearch/blob/7.4/x-pack/plugin/core/src/main/java/org/elasticsearch/xpack/core/ilm/TimeseriesLifecycleType.java

```
static final List<String> ORDERED_VALID_HOT_ACTIONS = Arrays.asList(
  SetPriorityAction.NAME, UnfollowAction.NAME, RolloverAction.NAME
);
static final List<String> ORDERED_VALID_WARM_ACTIONS = Arrays.asList(
  SetPriorityAction.NAME, UnfollowAction.NAME, ReadOnlyAction.NAME,
        AllocateAction.NAME, ShrinkAction.NAME, ForceMergeAction.NAME
);
static final List<String> ORDERED_VALID_COLD_ACTIONS = Arrays.asList(
  SetPriorityAction.NAME, UnfollowAction.NAME, AllocateAction.NAME, FreezeAction.NAME
);
static final List<String> ORDERED_VALID_DELETE_ACTIONS = Arrays.asList(
  DeleteAction.NAME
);
```

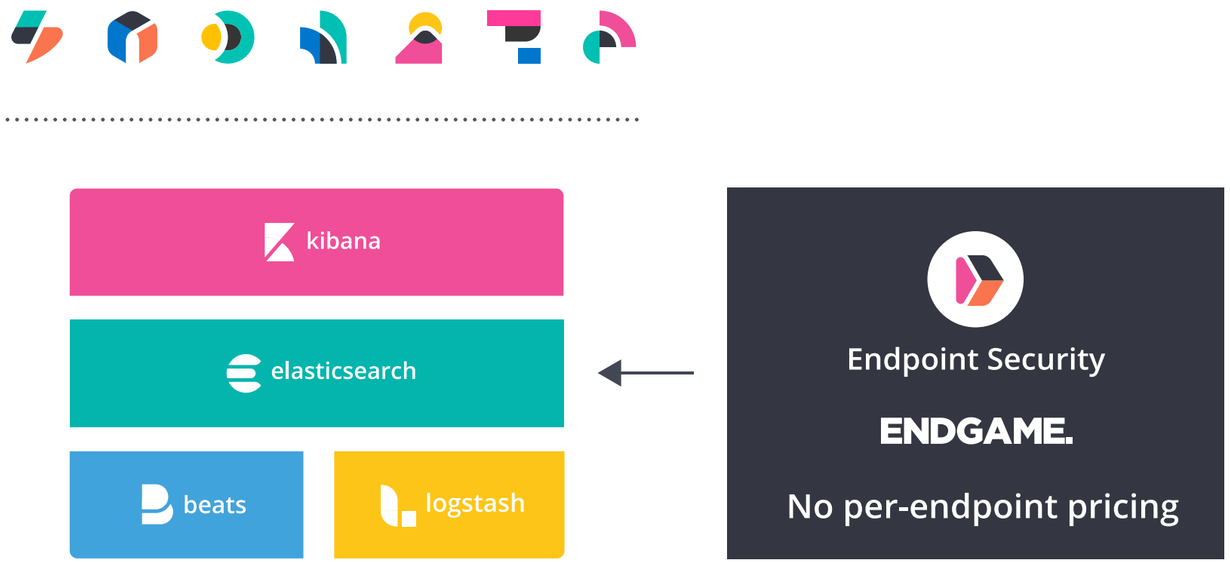
Frozen Indizes

Elastic Endpoint

elastic

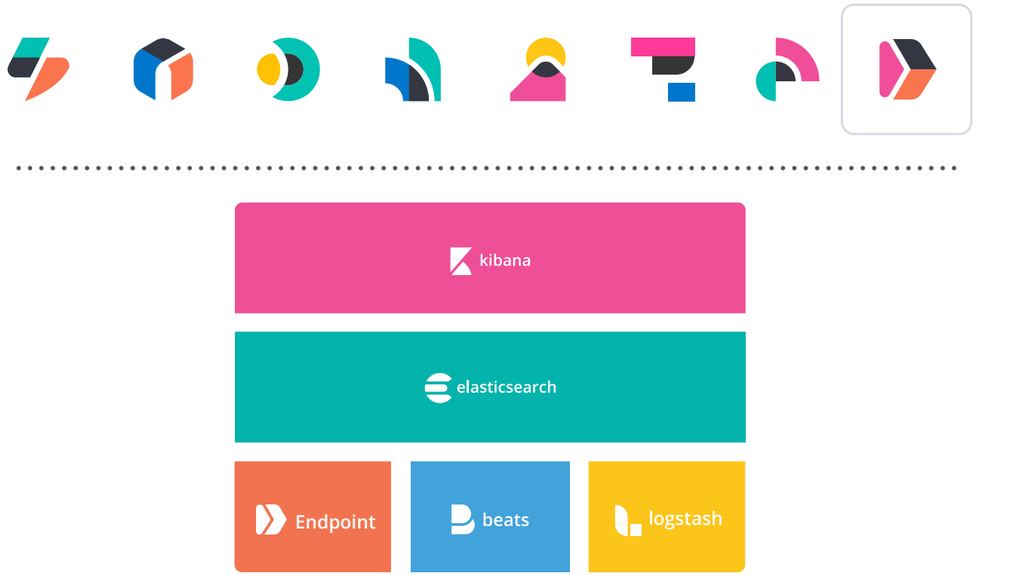
Today

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.



PS: Machine Learning

aka Anomaly Detection

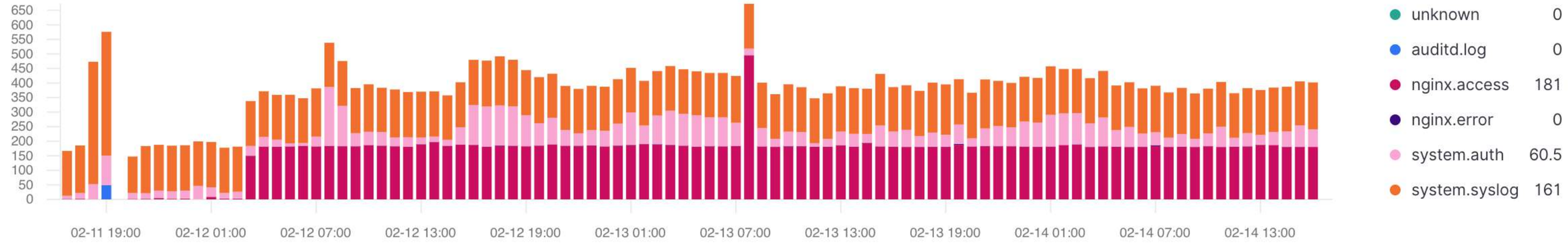
elastic

Analyzed 108.90k log entries from **February 11, 2020 4:44 PM** to **February 14, 2020 4:44 PM**

Last 3 days Show dates Refresh

Log entries BETA

Bucket span: 15 minutes



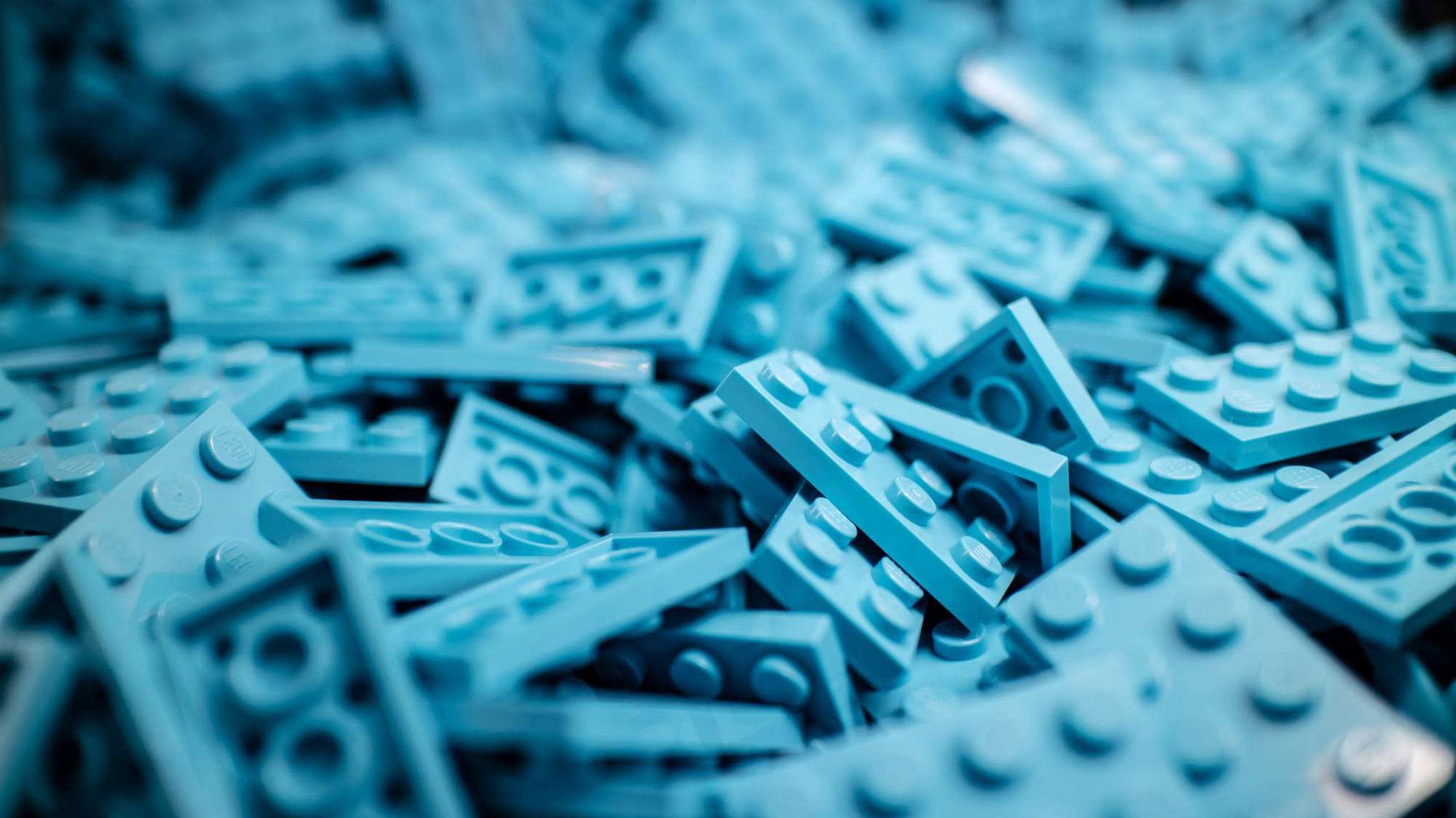
Anomalies

Recreate ML job Analyze in ML

108.90k
Number of log entries

88
Max anomaly score

Conclusion



Topics

Auditd

Auditbeat

Scale, Kubernetes, SIEM,...

Code

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

Similar Solutions

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

https://github.com/Scribery/aushape

Scale Your Auditing Events

Philipp Krenn @xeraa

elastic