Identifier les menaces avec Elastic SIEM

David Pilato

@dadoonet

elastic

Les incidents de sécurité ont 3 niveaux

FYI, WTF ET OMG

Découvrir une faille par

LA PRESSE OU LES UTILISATEURS

Découvrir une faille par

LES PIRATES DEMANDANT UNE RANÇON

Découvrir une faille par

VOTRE FACTURE CLOUD

elastic

Découvrir une faille par

VOUS-MÊME APRÈS LES FAITS

Découvrir une faille par

VOUS-MÊME ET POUVOIR PROUVER

QU'IL N'Y A PAS EU DE DÉGATS

elastic

AUDITD

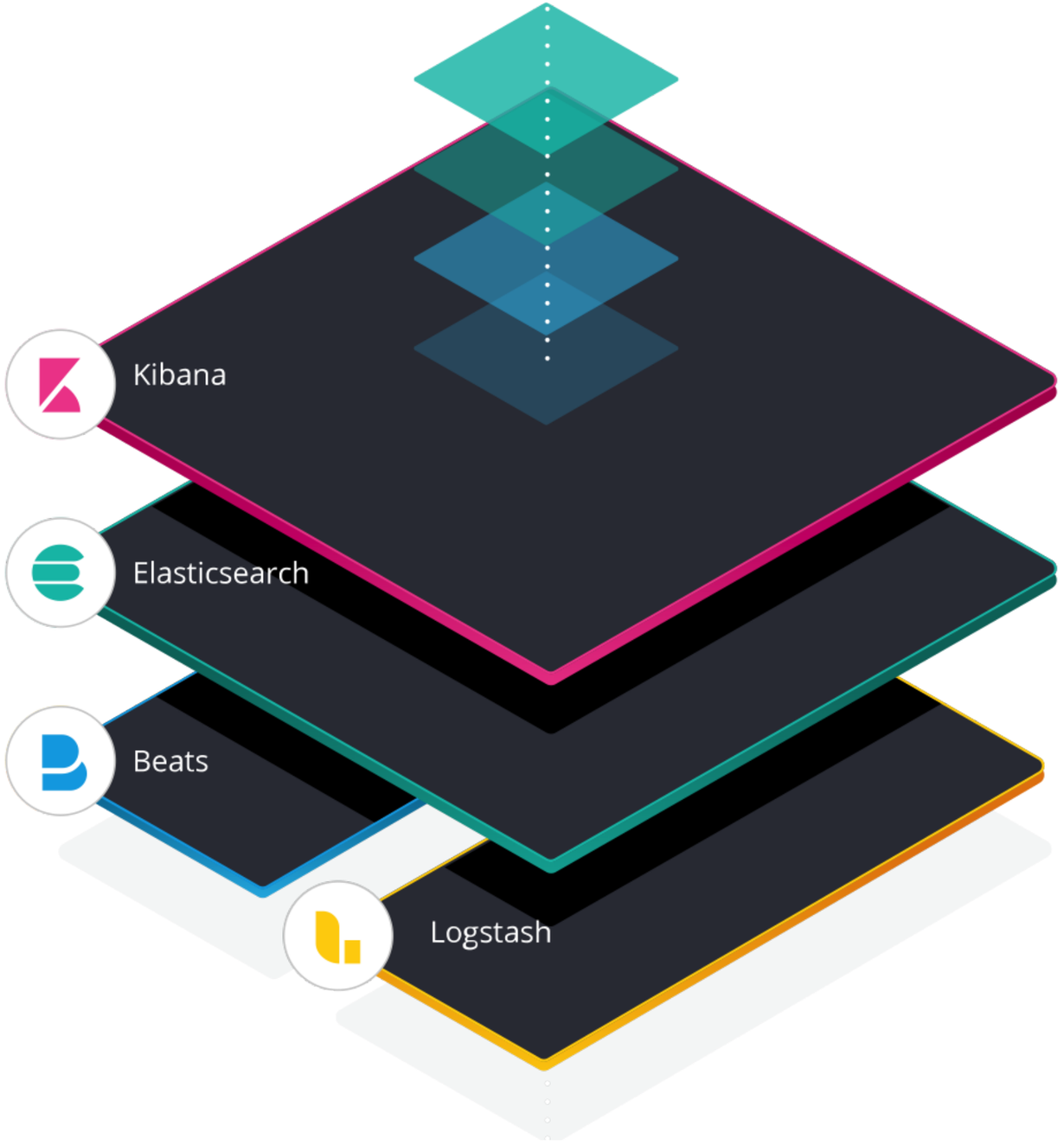
https://github.com/linux-audit

Demo


ALL THE THINGS!

Problem

How to centralize?


Kibana
Elasticsearch
Beats
Logstash

AUDITBEAT

elastic

Demo

System Module

host, process, package, socket, login, user

elastic

Demo

File Integrity Module

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

Demo


ALL THE THINGS!

Elastic Common Schema

https://github.com/elastic/ecs

```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 **I**nformation and **E**vent **M**anagement

elastic

Demo

Code

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

Identifier les menaces avec Elastic SIEM

David Pilato

@dadoonet

elastic