

VISUALIZE YOUR THREATS WITH ELASTIC SIEM

David Pilato

@dadoonet

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

Learn about a breach

CLOUD PROVIDER'S BILL

Learn about a breach

YOURSELF AFTER THE FACT

Learn about a breach

YOURSELF & YOU CAN PROVE NO HARM



UDITD

<https://github.com/linux-audit>

DEMO

ALL THE THINGS!



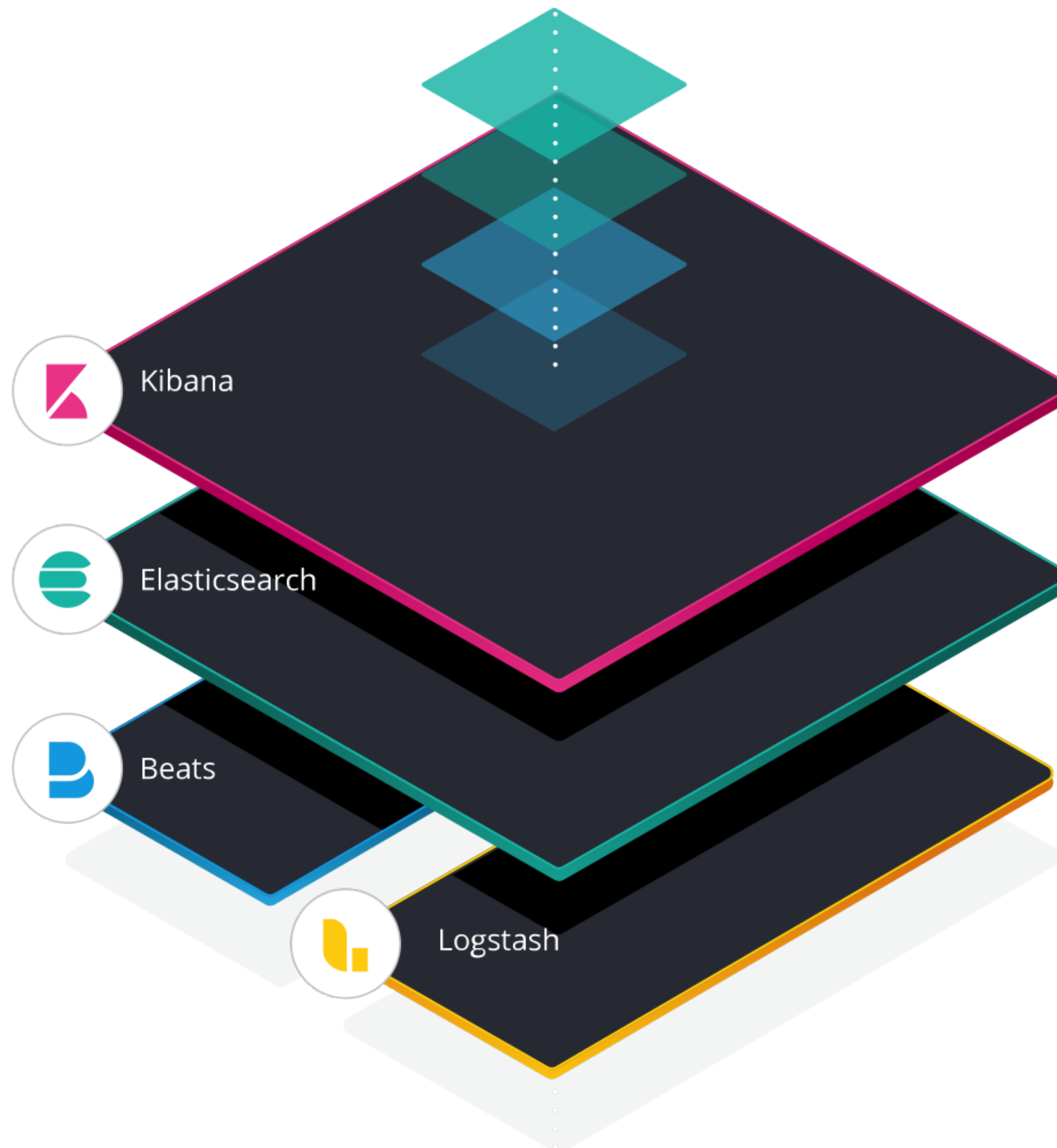
Problem

HOW TO CENTRALIZE?



Developer | Evangelist





FILEBEAT MODULE: AUDITD

DEMO

AUDITBEAT

DEMO

SYSTEM MODULE

host, process, package,
socket, login, user

DEMO

FILE INTEGRITY MODULE

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

DEMO

ALL THE THINGS!



ELASTIC COMMON SCHEMA

<https://github.com/elastic/ecs>

- 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

DEMO



CODE

[https://github.com/xeraa/
auditbeat-in-action](https://github.com/xeraa/auditbeat-in-action)

VISUALIZE YOUR THREATS WITH ELASTIC SIEM

David Pilato

@dadoonet