IFAS

Information Feed Analysis System

HKCERT

CSIRT foundry

What’s happening on our national networks?

HKCERT CSIRT foundry

How do national CSIRTs know what's happening?

National CSIRTs must collect national incident data

Many national CSIRTs don't operate networks themselves, and normally don't have global (or any) direct monitoring access

How does the CSIRT know what's going on in their country?

HKCERT CSIRT foundry

The kindness of strangers

Luckily, lots of ISPs, research teams, vendors, and other CSIRTs collect information, and will share it with us.

And here comes the “but”...

HKCERT CSIRT foundry

So much data, so many formats

Many feeds, with many formats and mediums:

Formats: CSV, JSON, XML, STIX, IODEF

Mediums: HTML, RSS, email, HTTP APIs

Strong efforts to standardise data feed formats, but that doesn't help us process all these feeds today.

HKCERT CSIRT foundry

The need for standards

Different feeds use different terms to mean the same thing:

ip, source_ip, src_ip, endpoint, attacker_ip, cnc_ip...

We need to rename fields so we can compare events from different feeds.

HKCERT CSIRT foundry

The need for storage

To understand the situation of our national networks, we must collect, store, and measure incident data.

We need to keep this data for a long time - years.

We also want to ask questions about our incident data:

- How many C&C servers nationally in last week?
- How many bots infected with Trojan.abc on BigISP?
- When were web sites defaced targeting gov.zz?
- Which national ISP has the most bot infections?

HKCERT CSIRT foundry

Need for automation

Too much network event data out there to manually process

Options:

a) use lots of analyst time doing tedious log processing

b) write lots of small, independent scripts

c) ignore inbound logs completely

d) use an centralised, automated processing system

HKCERT CSIRT foundry

So what do we need?

We need something which automatically:

- Gathers many different types of feeds
- Normalises the data in those feeds
- Stores that data somewhere
- Allows search and performs statistical analysis

HKCERT CSIRT foundry

Introducing IFAS

HKCERT

CSIRT foundry

IFAS

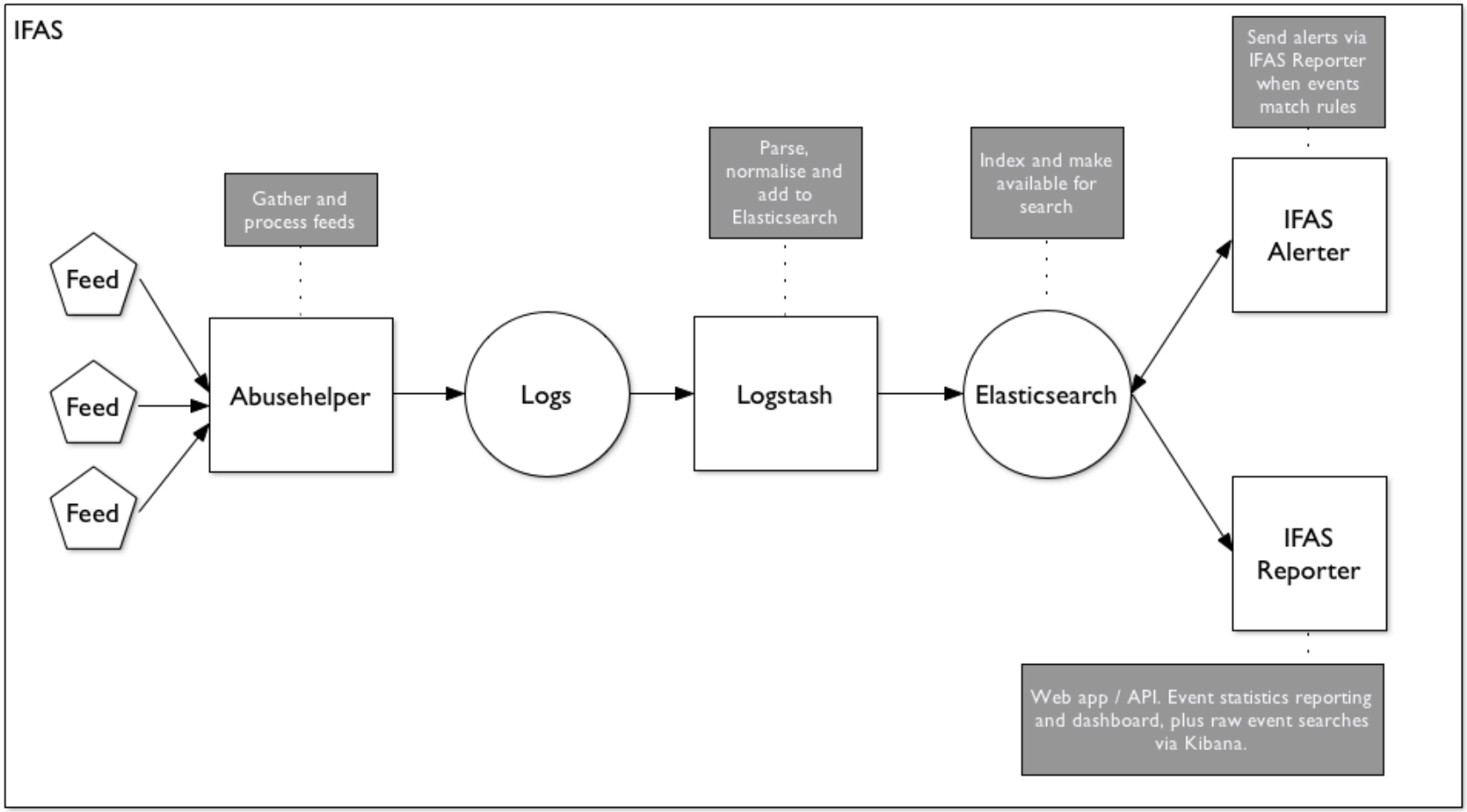
IFAS = Information Feed Analysis System

Project sponsored by HKCERT and developed by CSIRT Foundry and HKCERT

An integration of open source tools, released as open source for CSIRTs

HKCERT CSIRT foundry

Architecture



HKCERT CSIRT foundry

Architecture

Abusehelper: gather, process, and enrich feeds, generate events

Logstash: process and normalise feeds

Elasticsearch: store events in schema-free index server

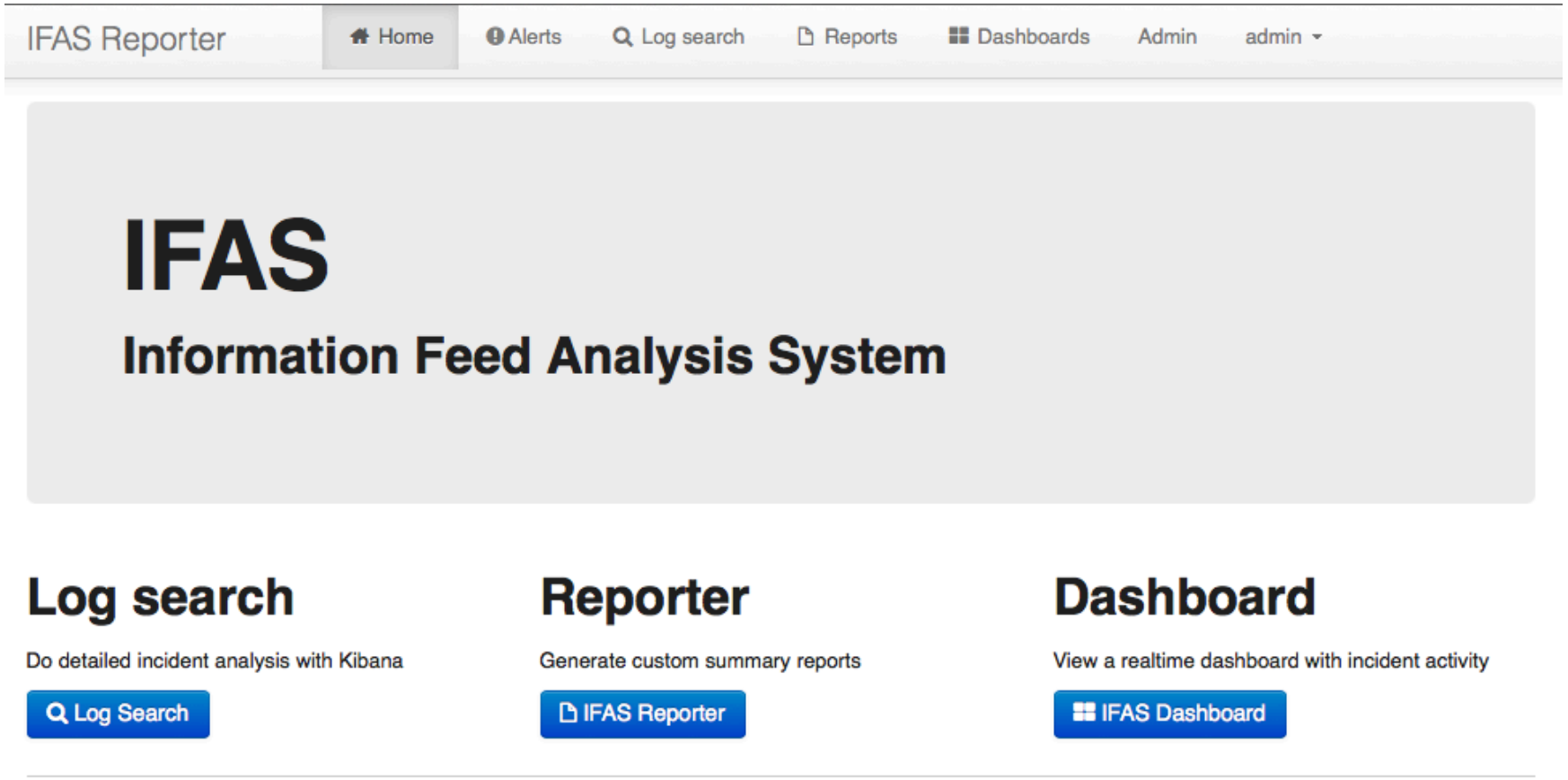
Kibana: search through events

IFAS Reporter: get overall statistics, build realtime dashboards

HKCERT CSIRT foundry

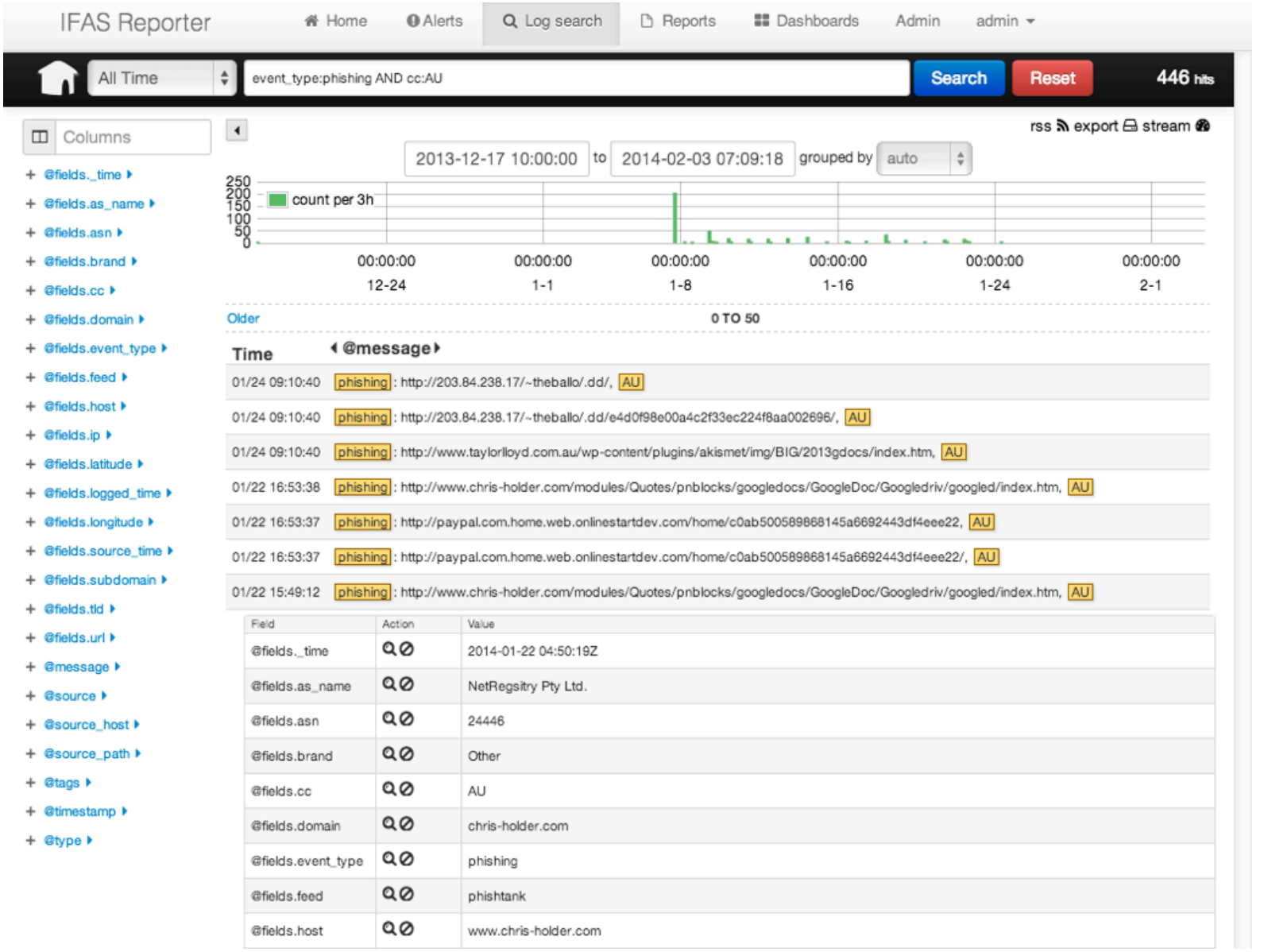
Let’s have a look at IFAS

HKCERT CSIRT foundry



IFAS homepage

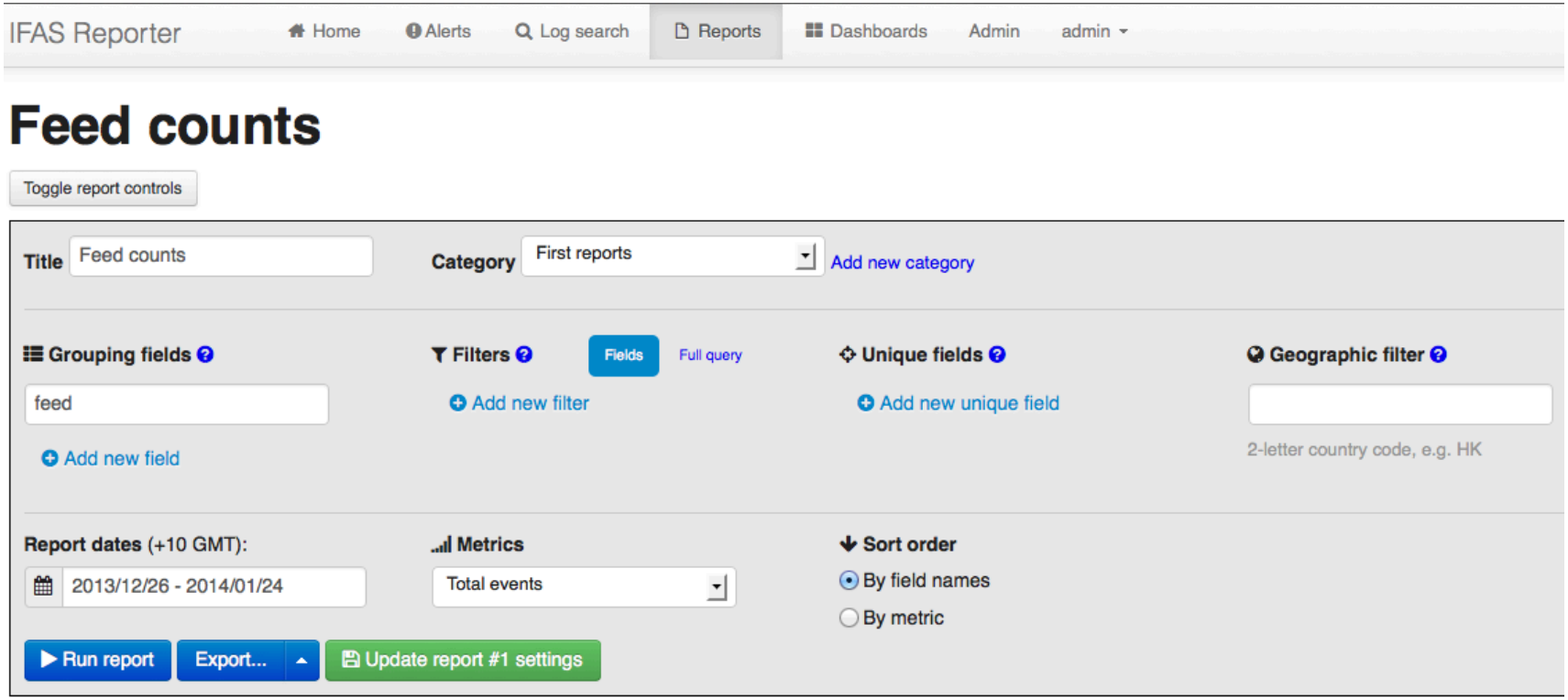
HKCERT CSIRT foundry



Kibana event searches

HKCERT

CSIRT foundry

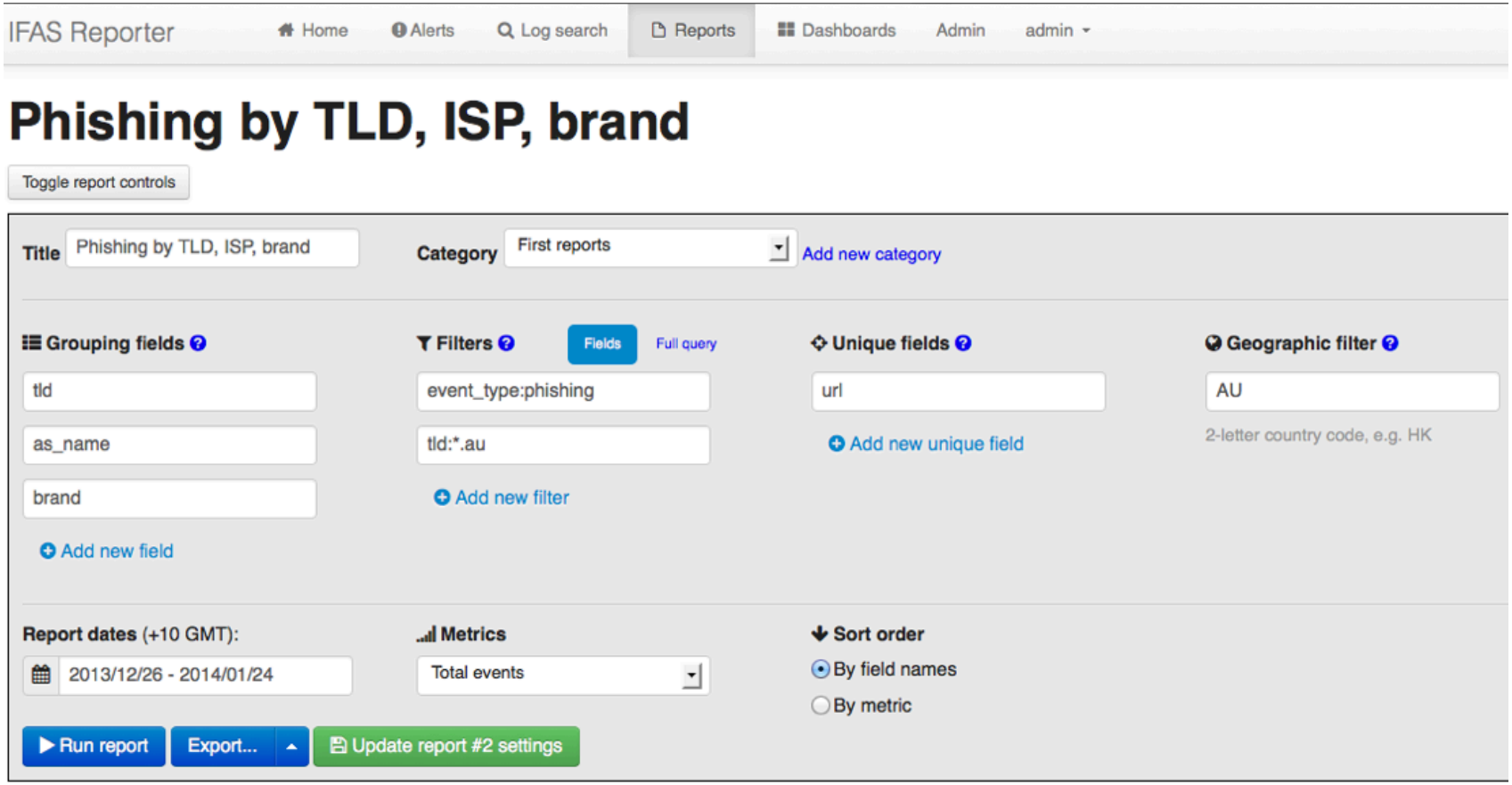


feed	
-	1
abuse.ch	390
cleanmx	415
mdl	53
millersmiles	63
phishtank	44537

Ad-hoc statistical reporting

HKCERT

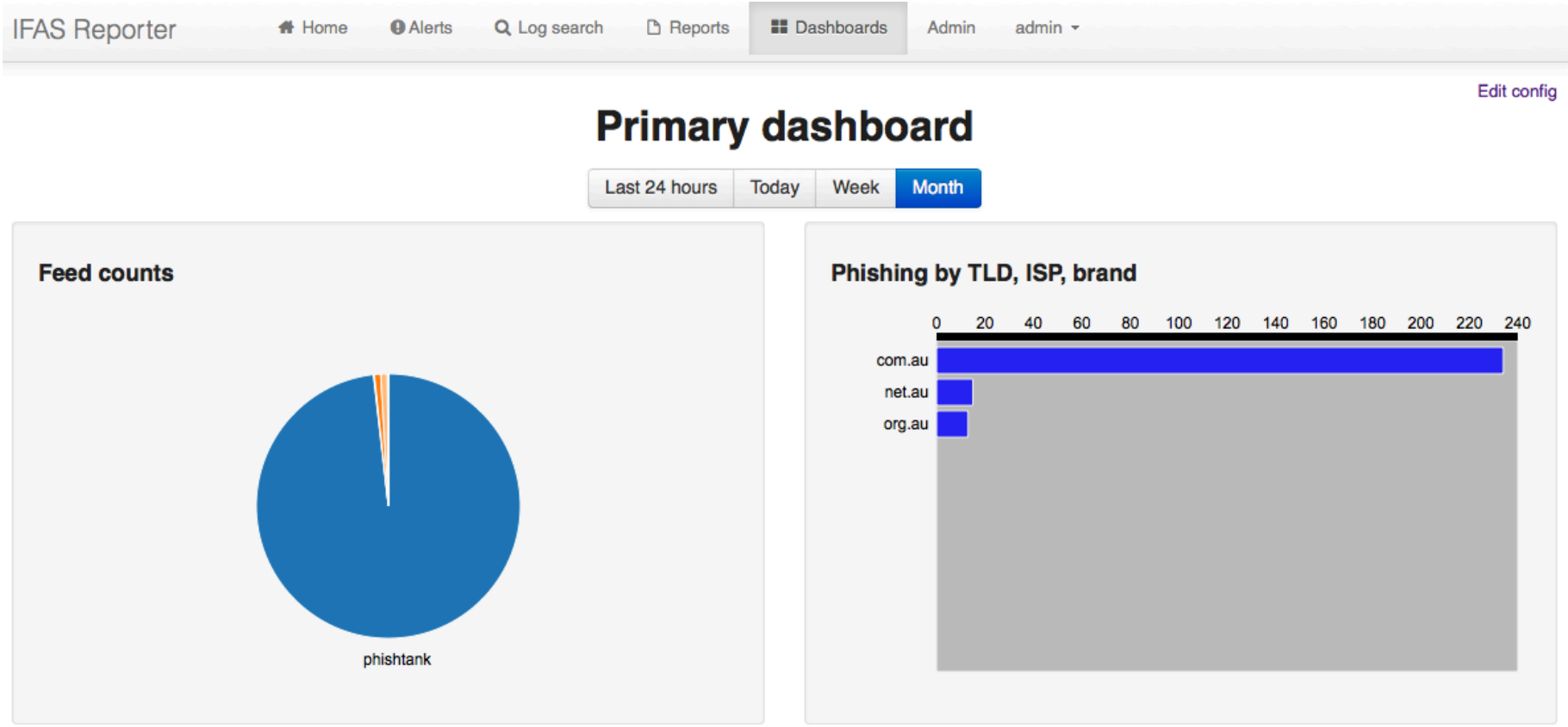
CSIRT foundry



tld	as_name	brand	
com.au	8.1 Graphix Row	PayPal	2
	Amazon.com, Inc.	AOL	4
		Other	2
	Aust Domains International Pty Ltd.	AOL	1
		Cielo	1

Nesting, filtering, deduplication

HKCERT CSIRT foundry



Realtime dashboards

HKCERT

CSIRT foundry

IFAS Alerter

IFAS Alerter: detect events which are high priority incidents

e.g. anything with domain:*.gov.zz

Highlighted in menu when matching events arrive

HKCERT CSIRT foundry

Other IFAS features

Run reports over months of data

Data export from any report

Authenticated API for automated reports and data export

Highly granular access control

- Report groups (e.g. analysts, managers, ISP staff)
- Dashboard access control
- Admins and editors

HKCERT CSIRT foundry

What you need to start

Hardware

Multi-core machine (4+ ideal)

Production: 8-16GB memory machine

Dev: 4GB okay for testing

Runs in a VM no problem

HKCERT

CSIRT foundry

Software

Open source release under Apache 2.0 License

Automatically installs and configures all necessary software via install script

Contributions, bug reports, feature requests most welcome!

HKCERT

CSIRT foundry

Where to get it

Currently closed pilot program to trusted CSIRTs

Eventually public release

Please contact ifas@ifas.io for details

HKCERT CSIRT foundry

IFAS benefits summary

Greater awareness of incidents for operational response

Analyse incident trends at high level

- HKCERT publishes stats based on IFAS data to HK stakeholders

Automation = less tedious work, more time for deep analysis

Visualise incident statistics

Store events and analyse so we can:

- Identify ISPs with poor response
- Identify new trends in phishing, defacements, malware

HKCERT CSIRT foundry

Thank you!

ifas@ifas.io

HKCERT CSIRT foundry