IFAS

Information Feed Analysis System

CSIRT foundry

What's happening on our national networks?

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?

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”...

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.

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.

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?

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

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

Introducing IFAS

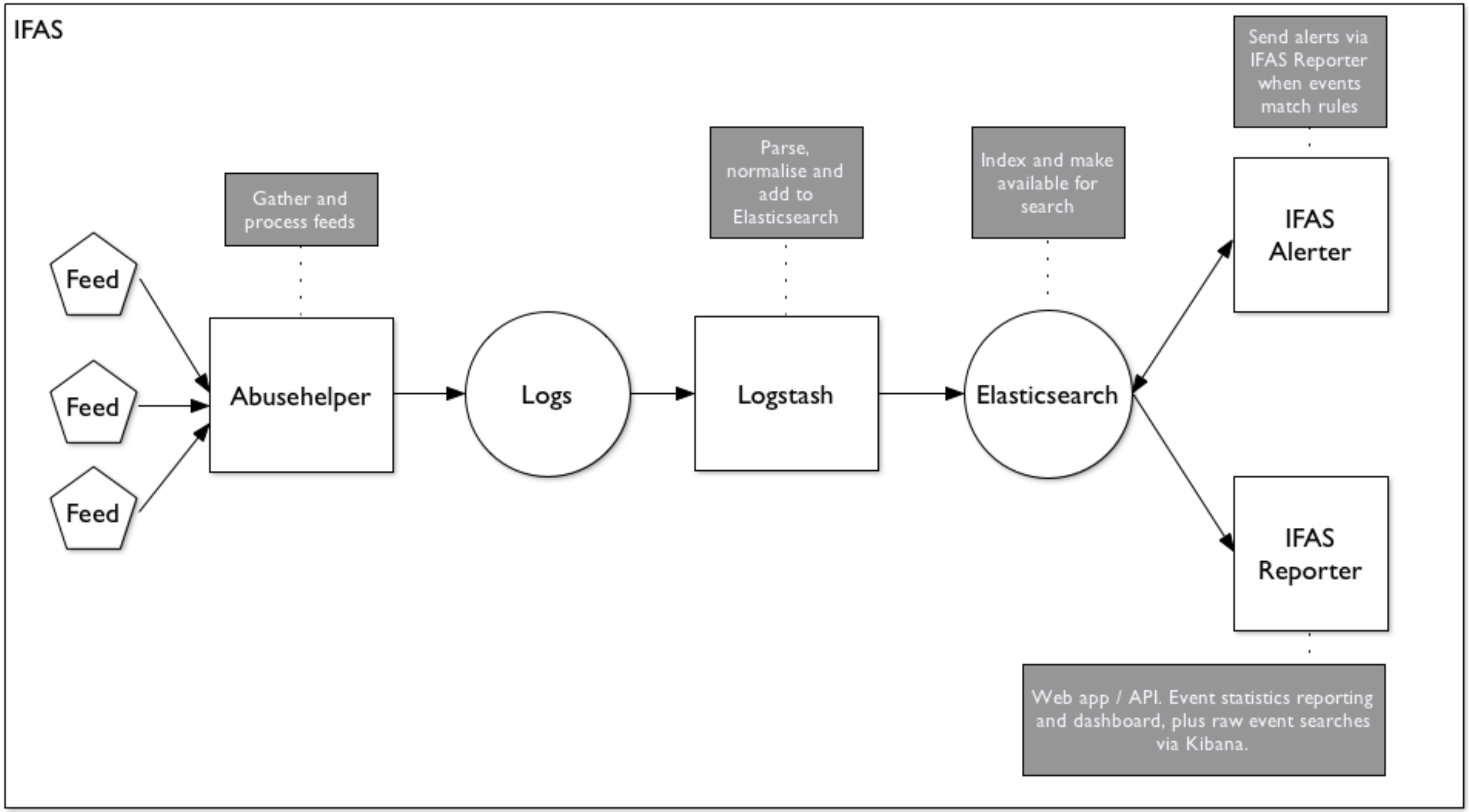
IFAS

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

Architecture


IFAS
Feed
Feed
Feed
Gather and process feeds
Abusehelper
Logs
Parse, normalise and add to Elasticsearch
Logstash
Index and make available for search
Elasticsearch
Send alerts via IFAS Reporter when events match rules
IFAS Alerter
IFAS Reporter
Web app / API. Event statistics reporting and dashboard, plus raw event searches via Kibana.

Architecture

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

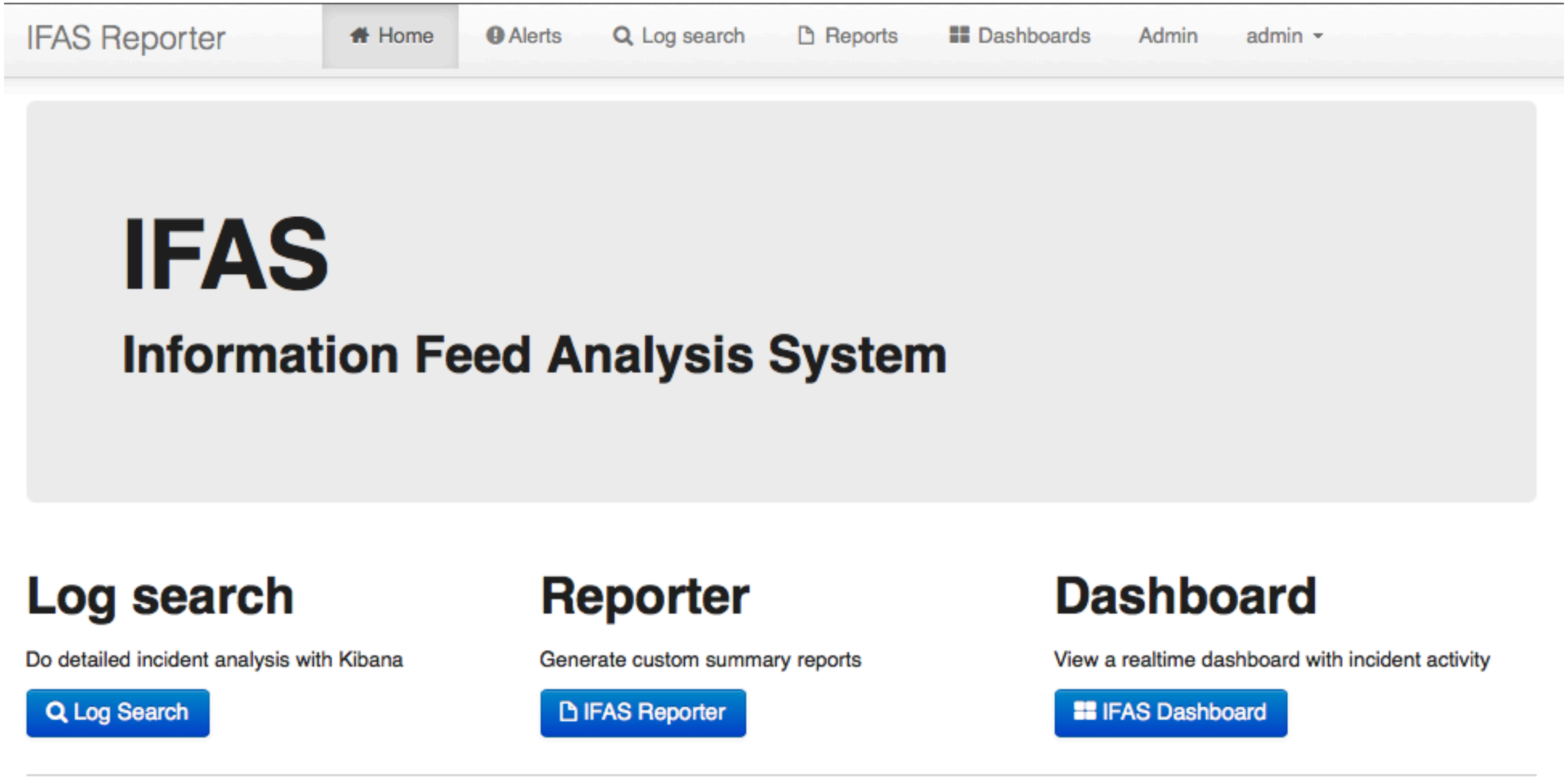
Logstash: process and normalise feeds

Elasticsearch: store events in schema-free index server

Kibana: search through events

IFAS Reporter: get overall statistics, build realtime dashboards

Let’s have a look at IFAS



IFAS

Information Feed Analysis System

Log search

Do detailed incident analysis with Kibana

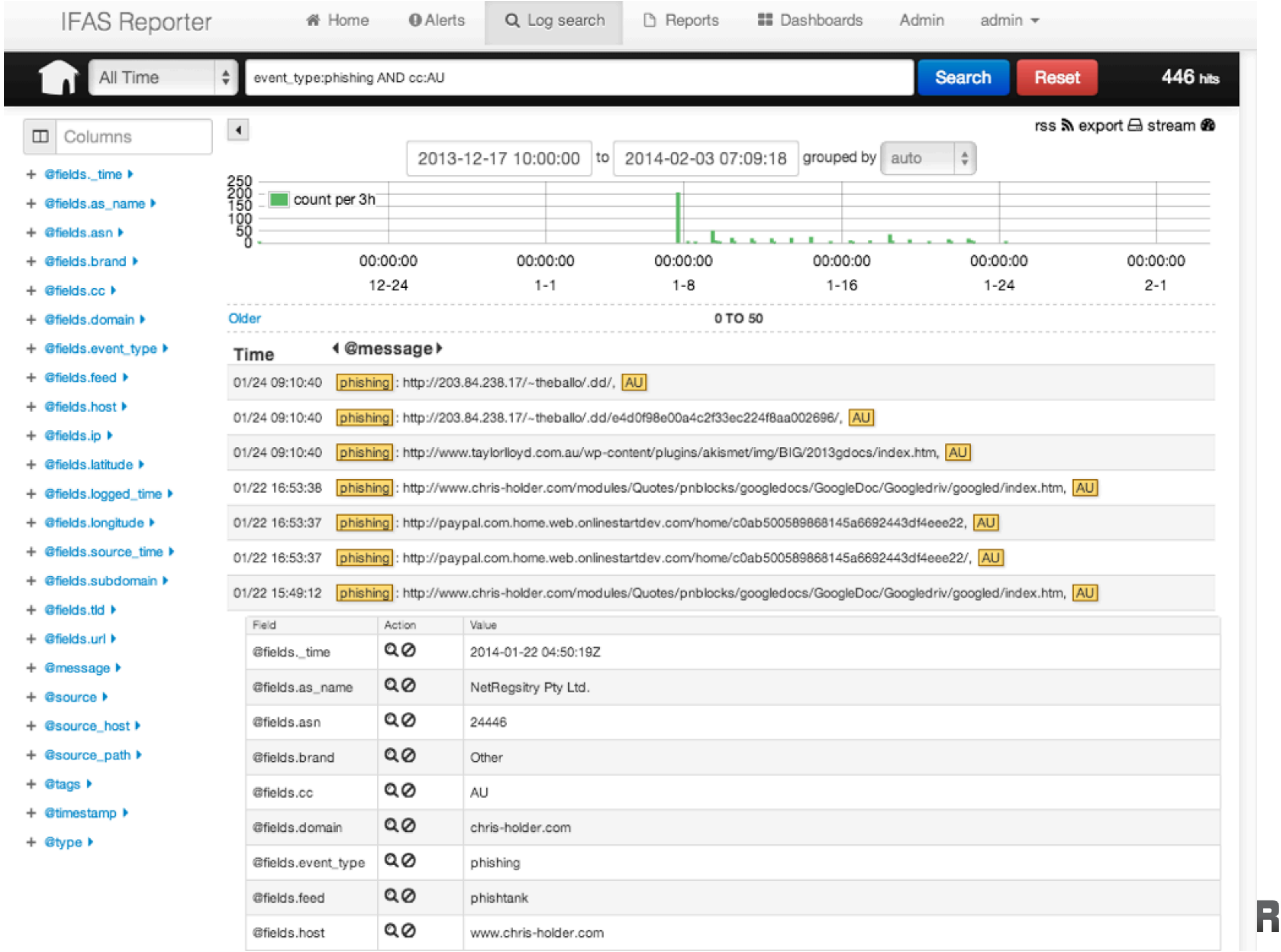
Reporter

Generate custom summary reports

Dashboard

View a realtime dashboard with incident activity

IFAS homepage



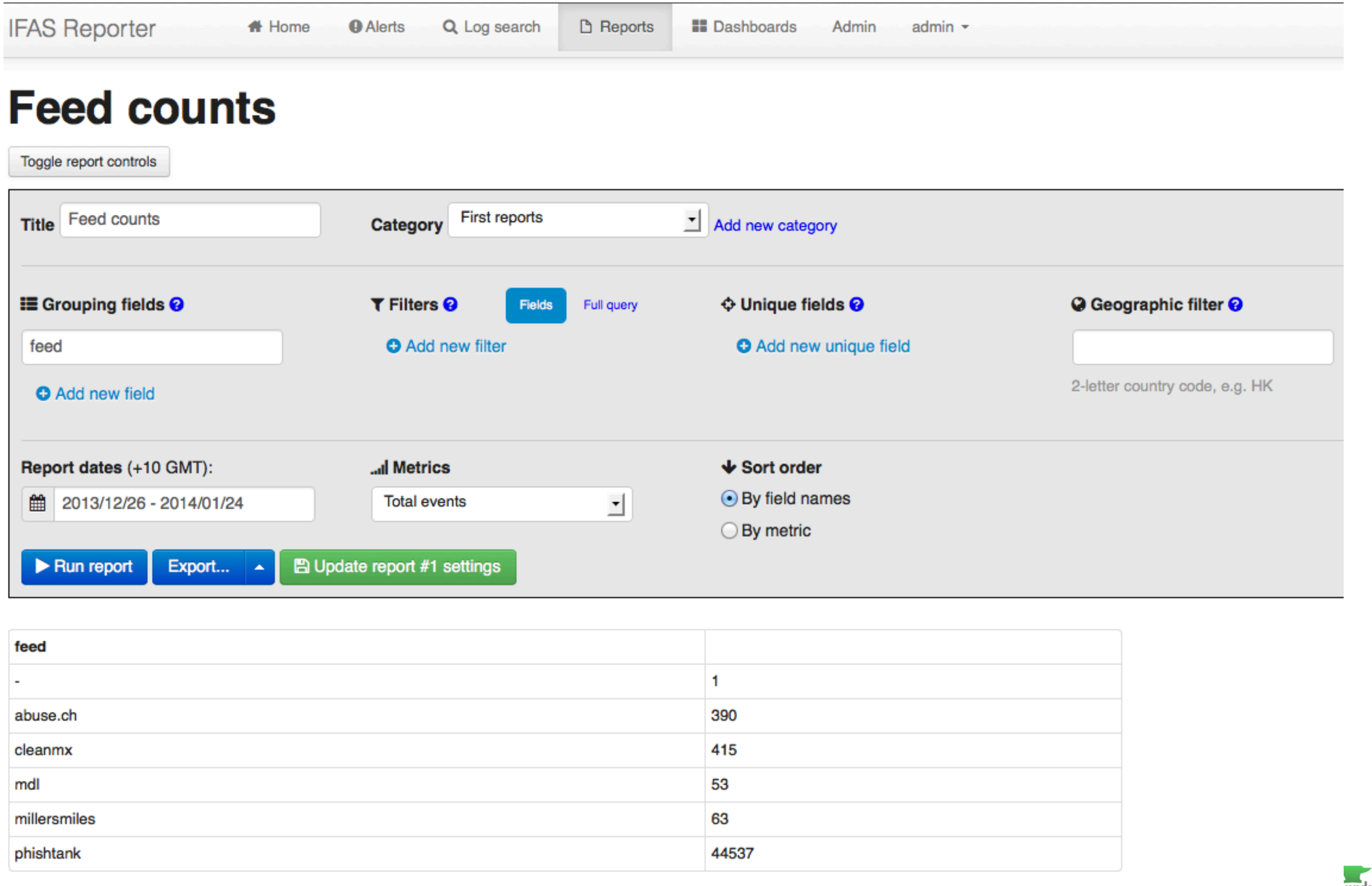
event_type:phishing AND cc:AU

2013-12-17 10:00:00 to 2014-02-03 07:09:18

Time	@message
01/24 09:10:40	phishing: http://203.84.238.17/~theballo/.dd/, AU
01/24 09:10:40	phishing: http://203.84.238.17/~theballo/.dd/e4d0f98e00a4c2f33ec224f8aa002696/, AU
01/24 09:10:40	phishing: http://www.taylorlloyd.com.au/wp-content/plugins/akismet/img/BIG/2013gdocs/index.htm, AU
01/22 16:53:38	phishing: http://www.chris-holder.com/modules/Quotes/pnblocks/googledocs/GoogleDoc/Googledriv/googled/index.htm, AU
01/22 16:53:37	phishing: http://paypal.com.home.web.onlinestartdev.com/home/c0ab500589868145a6692443df4eee22, AU
01/22 16:53:37	phishing: http://paypal.com.home.web.onlinestartdev.com/home/c0ab500589868145a6692443df4eee22/, AU
01/22 15:49:12	phishing: http://www.chris-holder.com/modules/Quotes/pnblocks/googledocs/GoogleDoc/Googledriv/googled/index.htm, AU

Field	Action	Value
@fields._time	🔍⊘	2014-01-22 04:50:19Z
@fields.as_name	🔍⊘	NetRegsitry Pty Ltd.
@fields.asn	🔍⊘	24446
@fields.brand	🔍⊘	Other
@fields.cc	🔍⊘	AU
@fields.domain	🔍⊘	chris-holder.com
@fields.event_type	🔍⊘	phishing
@fields.feed	🔍⊘	phishtank
@fields.host	🔍⊘	www.chris-holder.com

Kibana event searches



Feed counts

Title: Feed counts

Category: First reports

Grouping fields: feed

Filters

Unique fields

Geographic filter:

2-letter country code, e.g. HK

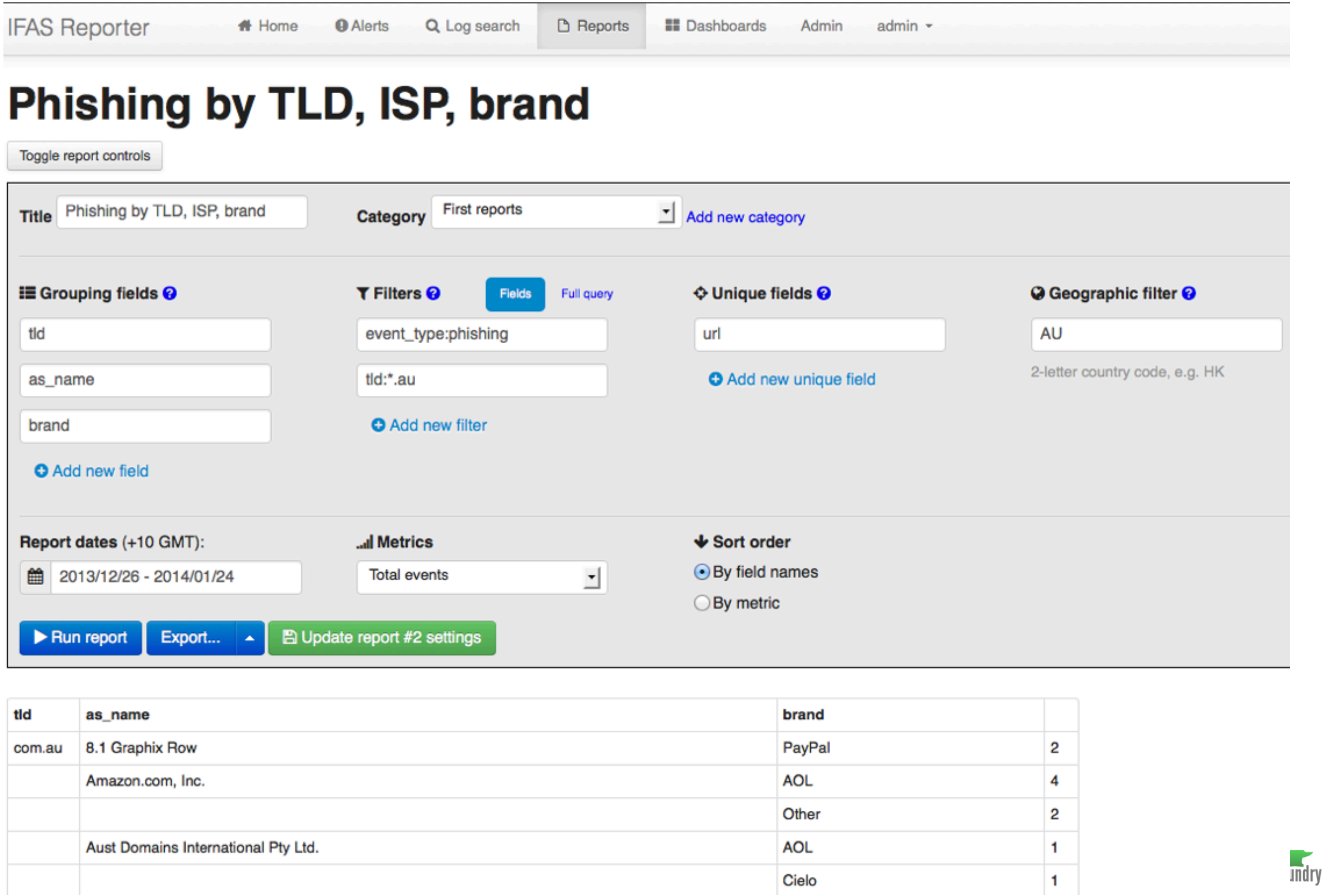
Report dates (+10 GMT): 2013/12/26 - 2014/01/24

Metrics: Total events

Sort order
- ● By field names
- ○ By metric

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

Ad-hoc statistical reporting



Phishing by TLD, ISP, brand

Title: Phishing by TLD, ISP, brand

Category: First reports

Grouping fields: tld, as_name, brand

Filters: event_type:phishing, tld:*.au

Unique fields: url

Geographic filter: AU

2-letter country code, e.g. HK

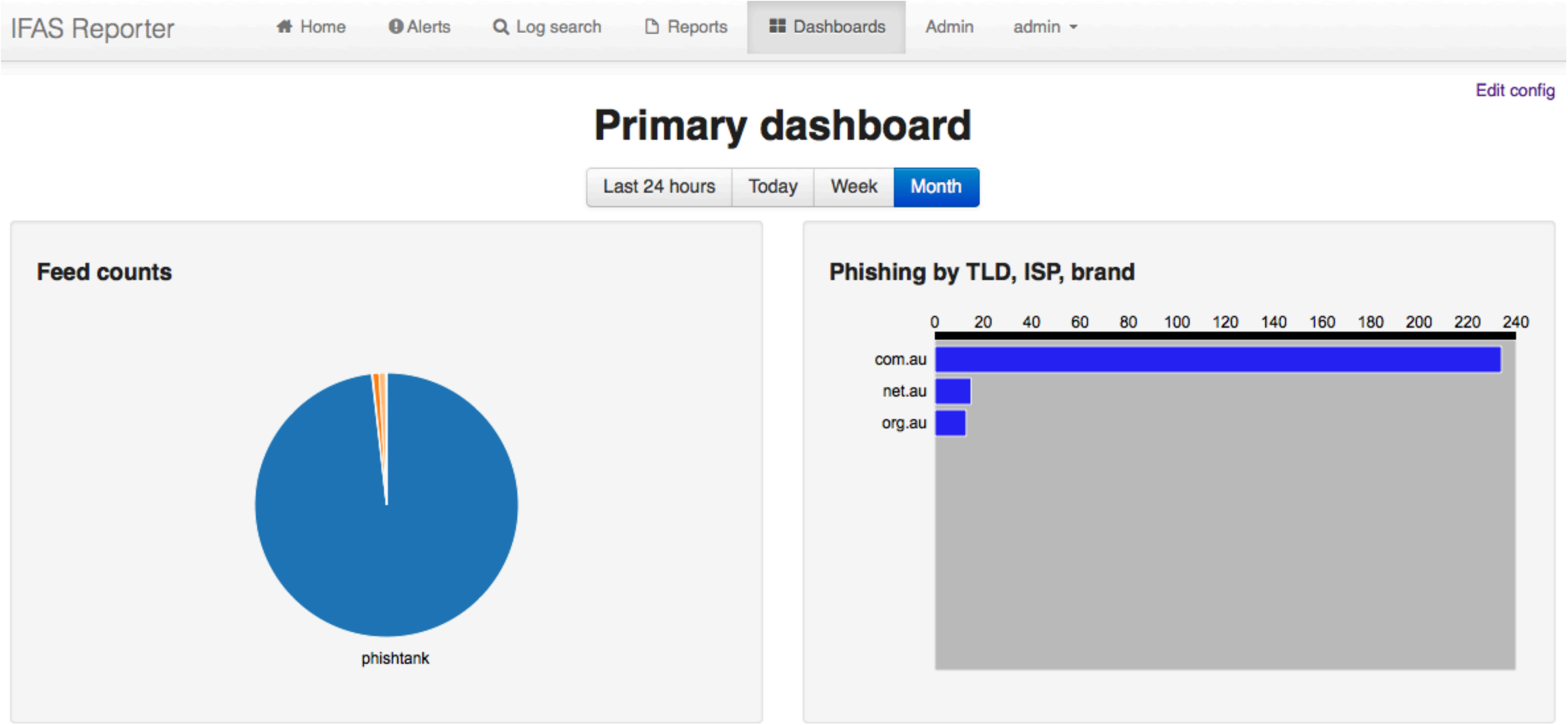
Report dates (+10 GMT): 2013/12/26 - 2014/01/24

Metrics: Total events

Sort order:
● By field names
○ By metric

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



Primary dashboard

Feed counts

Phishing by TLD, ISP, brand

Realtime dashboards

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

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

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

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!

Where to get it

Currently closed pilot program to trusted CSIRTs

- Eventually public release

Please contact contact@ifas.io for details

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

Thank you!

contact@ifas.io

CSIRT foundry