27th ANNUAL
FIRST CONFERENCE BERLIN
14 - 19 JUNE 2015

UNIFIED SECURITY:
IMPROVING THE FUTURE

Sinfonier Storm Builder for Security Intelligence

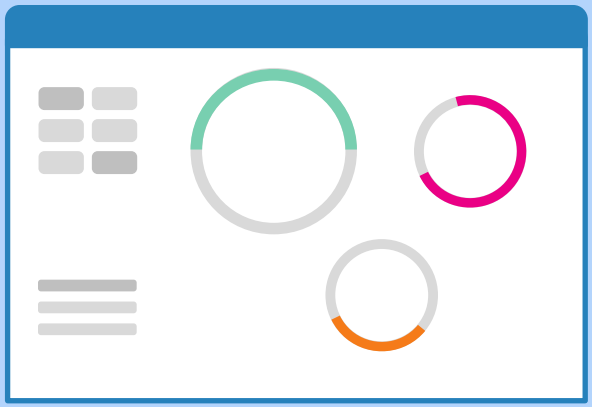
Fran Gomez @ffranz

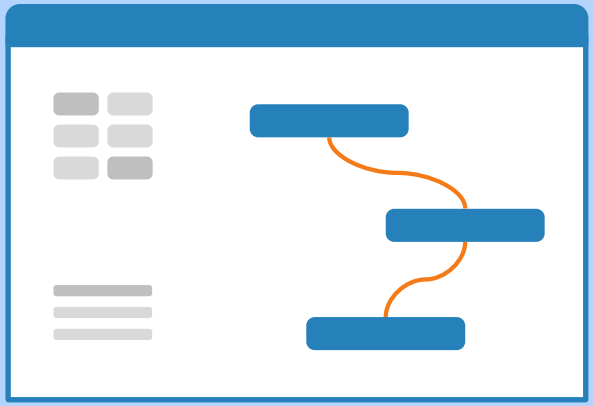
Leonardo Amor @LeoAmorV

Sinfonier

Storm Builder for Security Intelligence

“Connecting information, delivering intelligence”





Telefónica

21
Countries

50.377m
Income

>340m
Customers

120.000
Employees

movistar | O2 | vivo

- Mostly:
- Telco engineers
- Computer Science
- Engineers
- ….
- Science or Scientist people

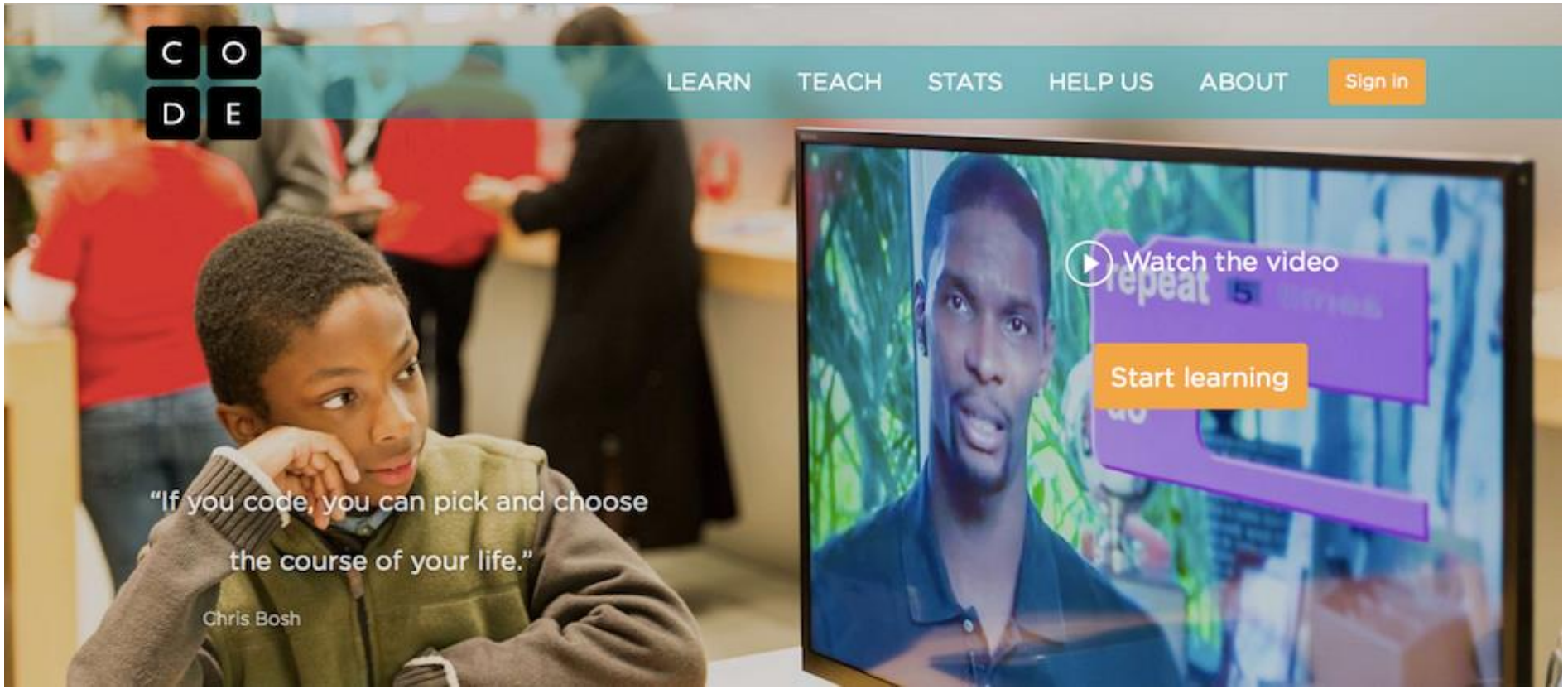
But there also space to:

- Lawyers
- Business administration
- Economist
- Psychologist
- Philologist

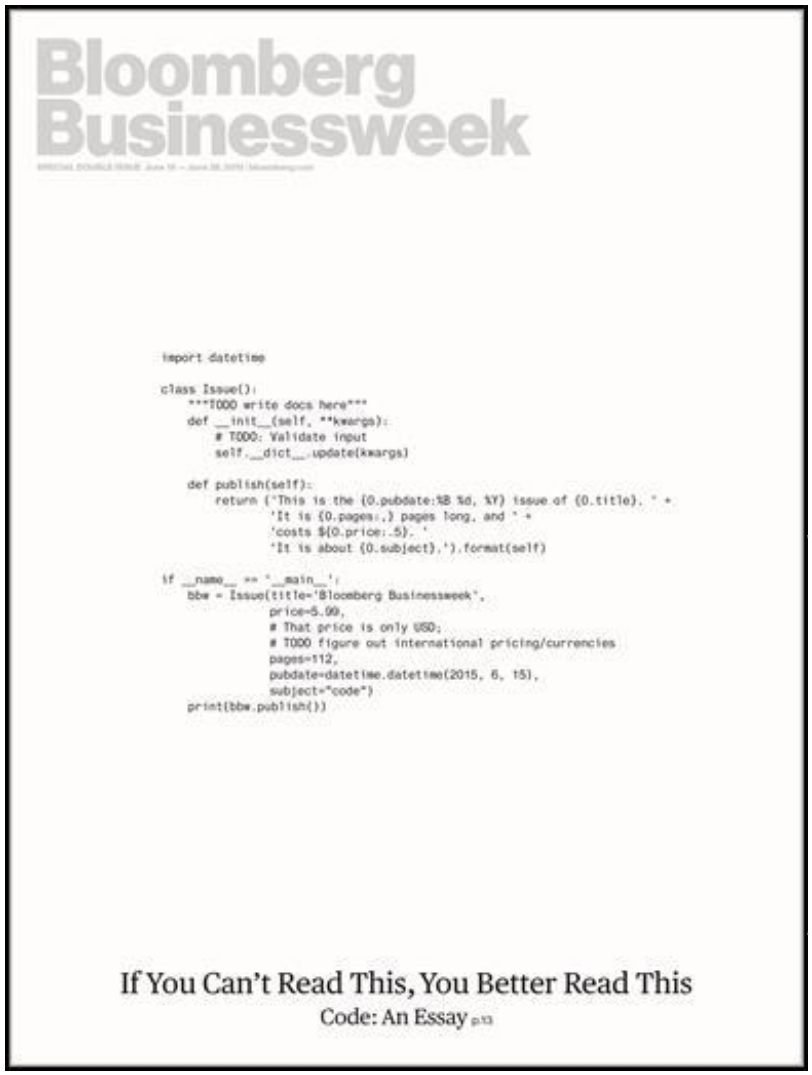

Leo
Fran


Leo
Fran

Ideas explosion



- ✓Unfortunately yet not everyone knows to code
- ✓Fortunately everyday schools are getting it should be one more basic class

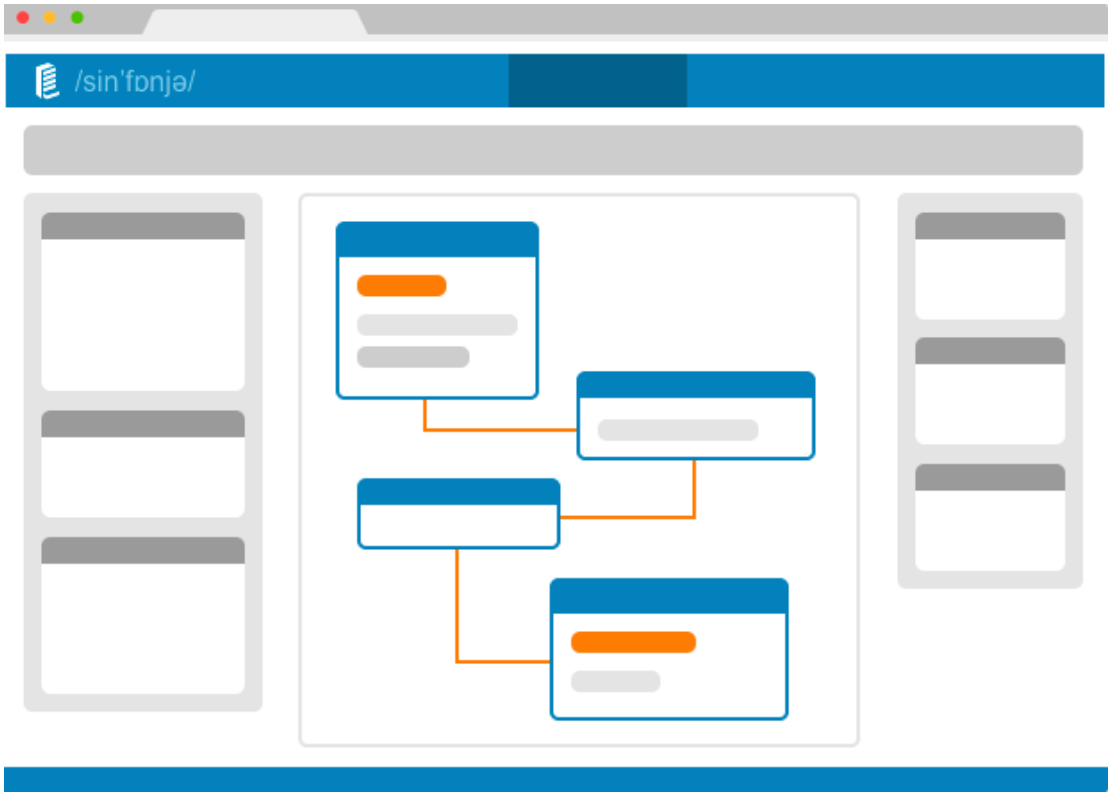


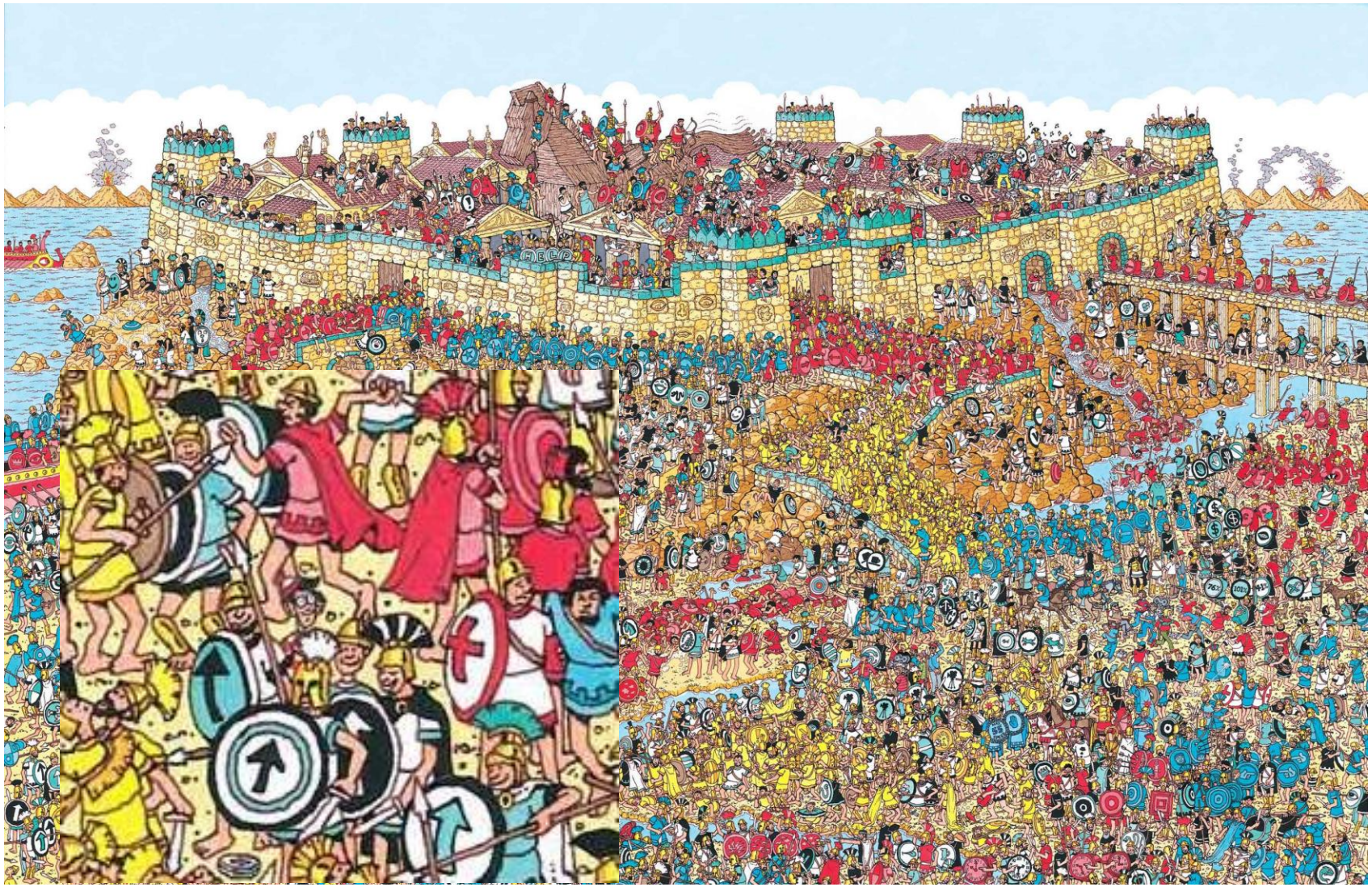
June 2015 Cover

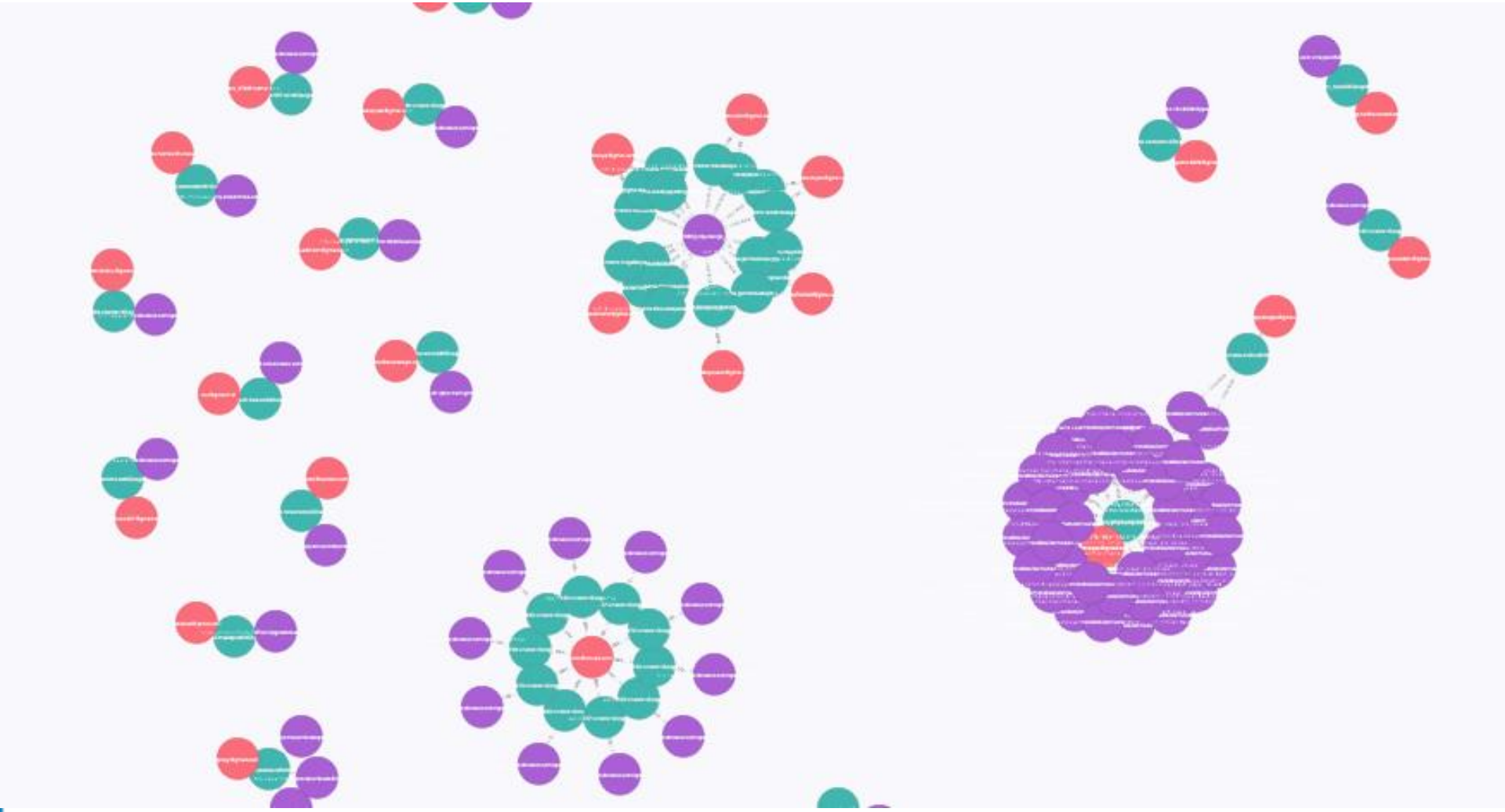
- Hot topic
- +- 2020 Digital natives workforce

How we are introducing code in our kids?

The need of visual coding







Real Time Processing

"Apache Storm is a free and open source distributed real time computation system. Storm makes it easy to reliably process unbounded streams of data, doing for real time processing what Hadoop did for batch processing. Storm is simple, can be used with any programming language, and is a lot of fun to use! "

http://storm.apache.org/

Where used


The Weather Channel
WebMD
Alibaba.com
FullContact
yelp
YAHOO! JAPAN
Spotify
GROUPON
Flipboard
Cerner
Aeris COMMUNICATIONS
Baidu 百度
parc A Xerox Company
淘宝网 Taobao.com
rubicon PROJECT
rocketfuel
HolidayCheck.com
and many

- Extremely broad set of use cases
- Scalable
- Guarantees no data loss
- Extremely robust
- Fault-tolerant
- Programming language agnostic

Sinfonier

Le chiffonnier est un meuble à tiroirs apparu sous la Régence. Il est destiné à ranger le linge. Il est le plus souvent plus haut que large et possède généralement un marbre en guise de dessus.

Sinfonier is **a change in the focus** in respect to current solutions in the area of processing information in real-time. We combine an **easy-to-use interface**, **modular and adaptable**, and we integrate it with an **advanced technological** solution to allow you to do the necessary tune up suitable for your needs in matters of information security.

Sinfonier is borne out of the cooperation and knowledge, where any **work can be re-used** and the efforts are done in **improving the processing and collection** of the new information which is generated.

Our Open project to stream processing

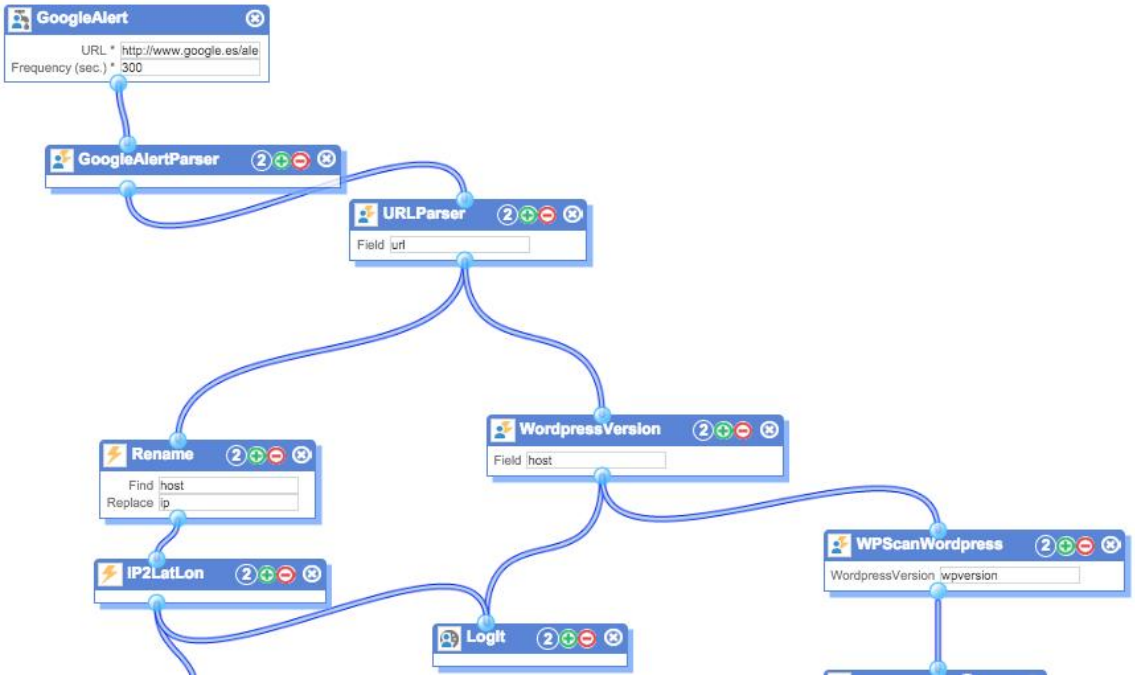
Drag & Drop Interface

Automatic Deploy API

Storm Cluster

Visual Progamming

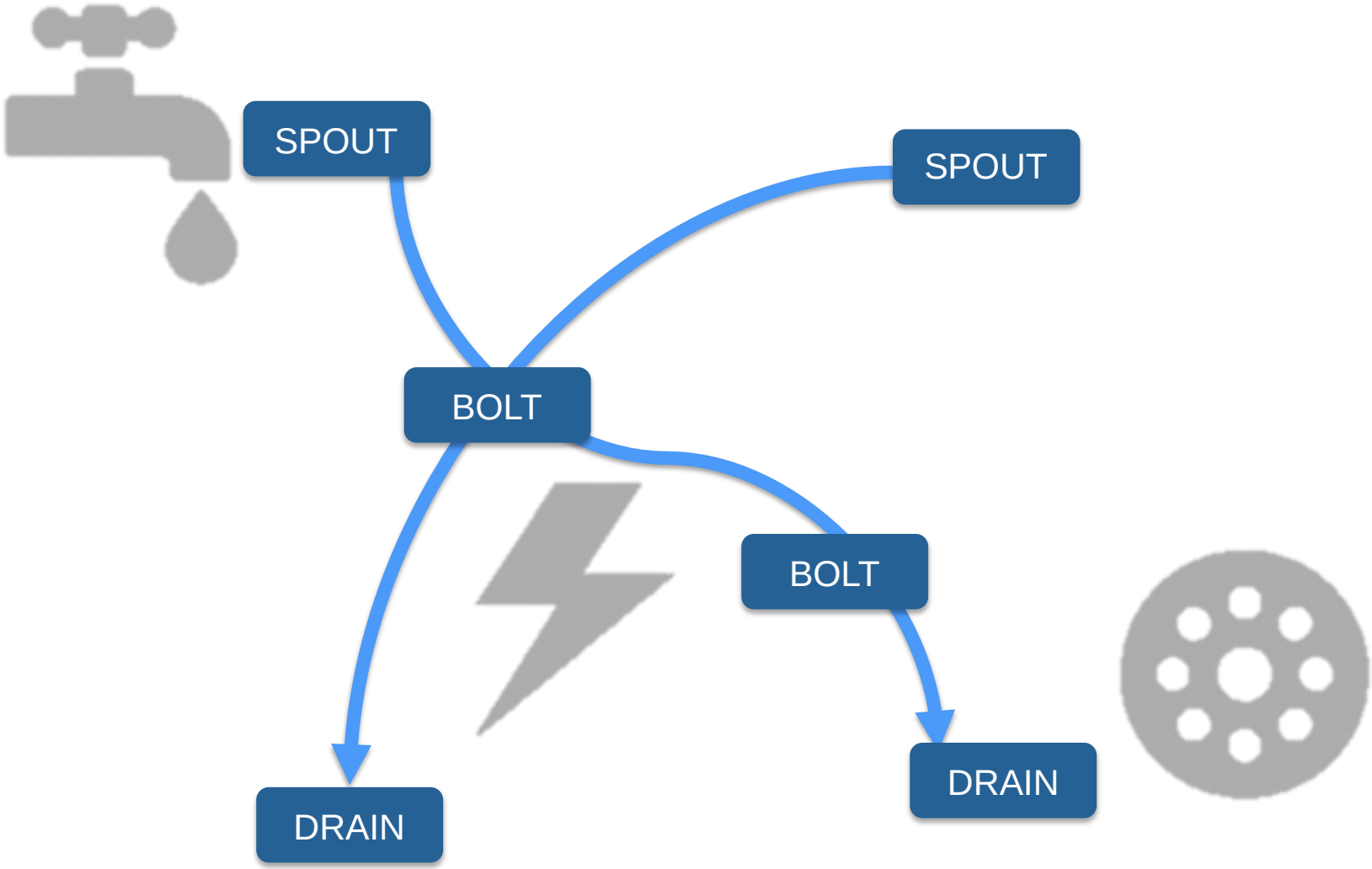

```
public static void main(String[] args) throws Exception {
  TopologyBuilder builder = new TopologyBuilder();

  builder.setSpout("word", new TestWordSpout(), 10);
  builder.setBolt("exclaim1", new ExclamationBolt(), 3).shuffleGrouping("word");
  builder.setBolt("exclaim2", new ExclamationBolt(), 2).shuffleGrouping("exclaim1");

  Config conf = new Config();
  conf.setDebug(true);

  if (args != null && args.length > 0) {
    conf.setNumWorkers(3);

    StormSubmitter.submitTopologyWithProgressBa
  }
  else {

    LocalCluster cluster = new LocalCluster();
    cluster.submitTopology("test", conf, builde
    Utils.sleep(10000);
    cluster.killTopology("test");
    cluster.shutdown();
  }
}
```



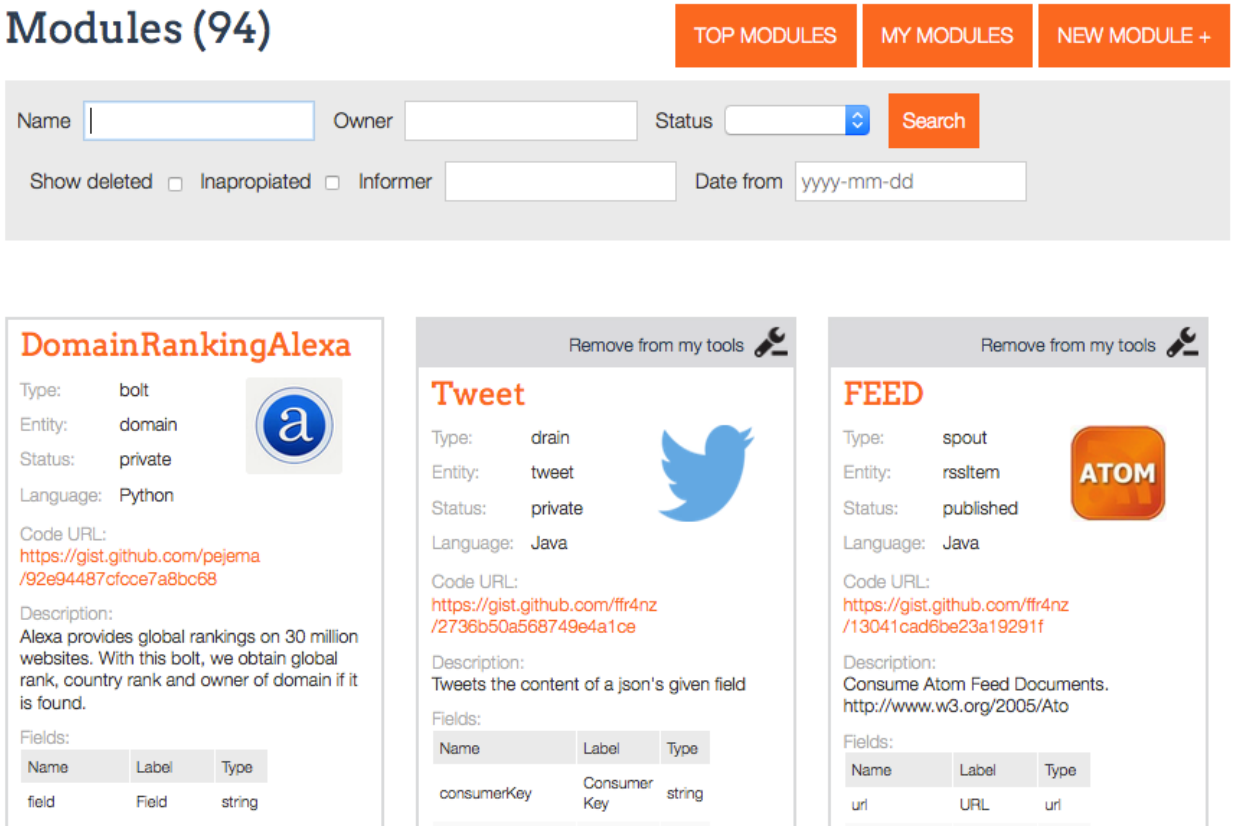
Modules

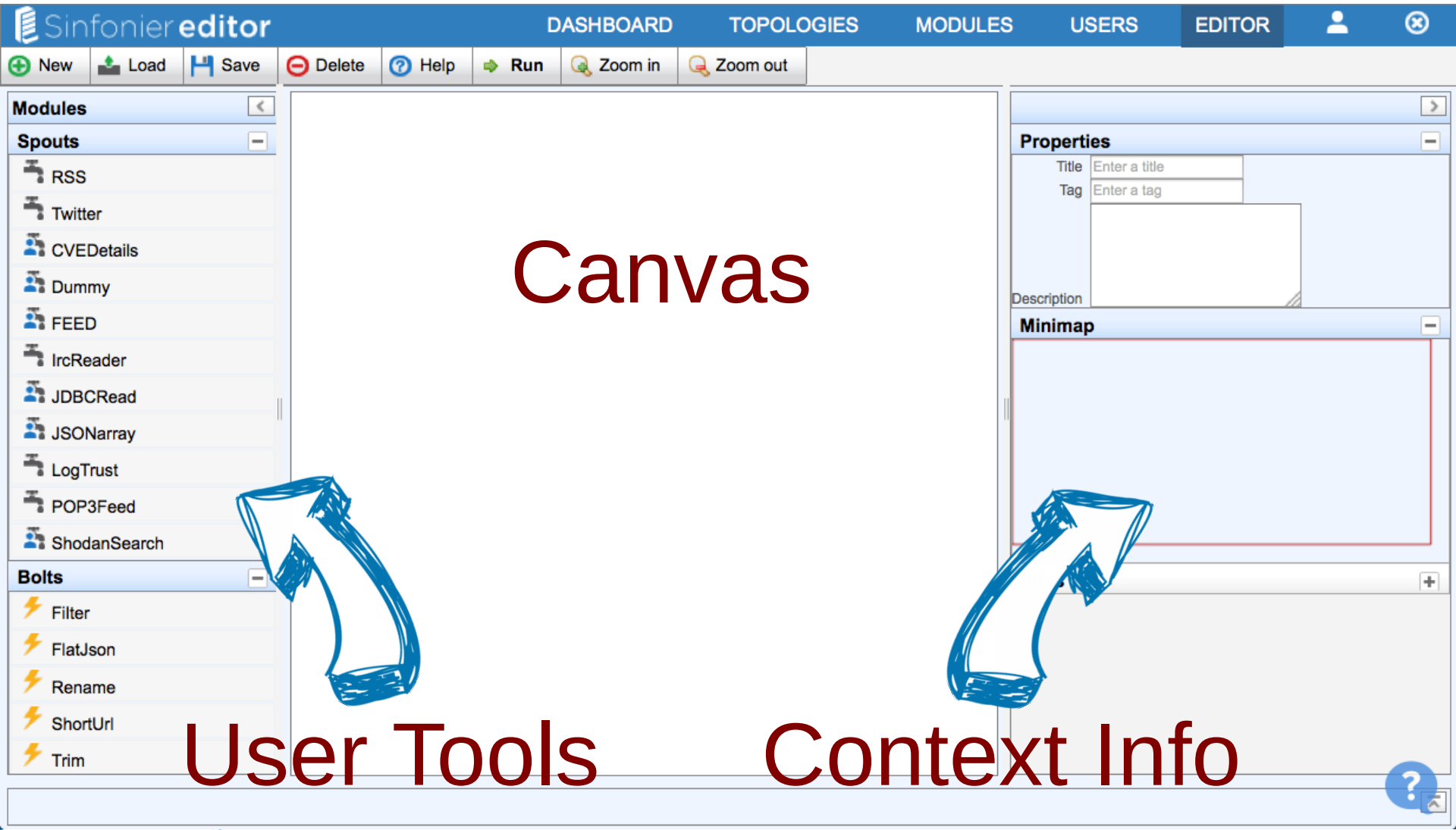
Spout Bolt Drain




SPOUT
SPOUT
BOLT
BOLT
DRAIN
DRAIN

Topology life cycle




Sinfonier editor
DASHBOARD
TOPOLOGIES
MODULES
USERS
EDITOR
New
Load
Save
Delete
Help
Run
Zoom in
Zoom out
Modules
Spouts
RSS
Twitter
CVEDetails
Dummy
FEED
IrcReader
JDBCRead
JSONarray
LogTrust
POP3Feed
ShodanSearch
Bolts
Filter
FlatJson
Rename
ShortUrl
Trim
Canvas
Properties
Title
Enter a title
Tag
Enter a tag
Description
Minimap
User Tools
Context Info

Topology Wordpressrss

Wordpressrss

Description:
No description yet

Sharing:
private
Publish

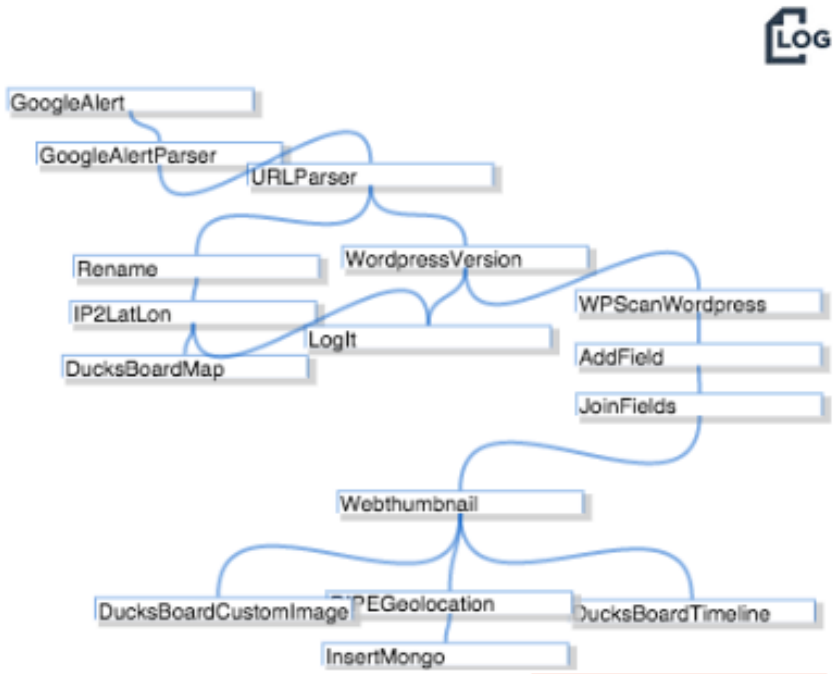
Tag:
undefined

Updated:
26 days ago

Last Execution:
never

Created by ffranz at Fri Jul 18 2014 00:47:16 GMT+0200 (CEST)

Delete Stop Edit Update



Advantages

Collaborative scheme

Enable automation through actionable intelligence thanks to a flexible integration framework

Facilitate generation, enrichment and dissemination of cybersecurity data

Leverage on structured cyber security data output normalization


KEEP
CALM
AND
SHARE
IT

Some Modules

Remove from my tools

Webthumbnail

Type: bolt
Entity: url
Status: published
Language: Java

Code URL:
https://gist.github.com/ffr4nz/be1dfdedd0a4a5fea9bc

Description:
Webthumbnail.org offers a simple to use API for generating website screenshots on demand. Add screenshot field.

Remove from my tools

ShodanSearch

Type: spout
Entity: ip
Status: published
Language: Java

Code URL:
https://gist.github.com/ffr4nz/c6194dc69fda732c984f

Description:
Search Shodan using the same query syntax as the website and use facets to get summary information for different properties. Emit each new match item.

Remove from my tools

LinkedINUserParser

Type: bolt
Entity: user
Status: published
Language: Java

Code URL:
https://gist.github.com/ffr4nz/2c751a335ce7c91003a8

Description:
Get user info from public profile URL.

Remove from my tools

CSV

Type: spout
Entity: unknown
Status: private
Language: Java

Code URL:
https://gist.github.com/ffr4nz/a99d61800def6f03e314

Description:
Get CSV file and emit each line into a JSON object. Key list are key names for comman separated vallues.

Remove from my tools

DucksBoardStatus

Type: drain
Entity: unknown
Status: published
Language: Java

Code URL:
https://gist.github.com/ffr4nz/932afa7c6d0c65c2e509

Description:
Display the status of an item in your Ducksboard.

Remove from my tools

TwitterUser

Type: spout
Entity: tweet
Status: published
Language: Java

Code URL:
https://gist.github.com/ffr4nz/62b7cacdff08f9b9f91d

Description:
Real-time updates of all data from user timeline.

Remove from my tools

InstaPush

Type: drain
Entity: unknown
Status: published
Language: Java

Code URL:
https://gist.github.com/ffr4nz/19e374a8d71655f0faa6

Description:
Send push using instapush.im events. Needs a trackers list, each element match with a json received fields and an event title.

Remove from my tools

VirusTotalIP

Type: bolt
Entity: ip
Status: published
Language: Java

Code URL:
https://gist.github.com/ffr4nz/8538194d9c778394eab9

Description:
Retrieve a report on a given IP address (including the information recorded by VirusTotal's Passive DNS infrastructure)

Telefónica

Some Modules

Sinfonier

Remove from my tools

DomainTLD

Type: bolt
Entity: domain
Status: published
Language: Java

Code URL:
https://gist.github.com/ffr4nz/45edfc9e3909ff13c55b

Description:
Get TLD from Domain using Google InternetDomainName Class. http://docs.guava-libraries.googlecode.com/git-history/release/javadoc/index.html

Remove from my tools

HibpwnedAccount

Type: bolt
Entity: user
Status: published
Language: Java

Code URL:
https://gist.github.com/ffr4nz/3c934492cce20dda17f8

Description:
Getting all breaches for an account.

Remove from my tools

FreeGeoIP

Type: bolt
Entity: ip
Status: published
Language: Java

Code URL:
https://gist.github.com/ffr4nz/963ab4693435b6d57109

Description:
Receives a json with a field to be geolocated, and returns the same json with latitude and longitude field. Uses free webservice from FreeGeoIP (10.000 queries rate limit shared by Sinfonier used). If it could not determine location, both fields will return as 0.0

Remove from my tools

PeerReach

Type: bolt
Entity: user
Status: published
Language: Java

Code URL:
https://gist.github.com/ffr4nz/1b9491155b5e7ef16702

Description:
Consume Peer Reach API. Returns a detailed overview for a single user based on a Twitter Screen Name.

Remove from my tools

LogTrust

Type: spout
Entity: unknown
Status: published
Language: Java

Code URL:
https://gist.github.com/ajsanchezsanz/3c55e1a49d3d3802112b

Description:
Read LogTrust API and retrieves info

Remove from my tools

JSONarray

Type: spout
Entity: unknown
Status: published
Language: Java

Code URL:
https://gist.github.com/ffr4nz/5f444345d76e42c592a6

Description:
Consume JSON Array from server. [{},{},...]

Remove from my tools

CVEDetails

Type: spout
Entity: unknown
Status: published
Language: Java

Code URL:
https://gist.github.com/ffr4nz/656b92085bf38ac6c03e

Description:
Consume JSON CVEFeed from CVEDetails.com.

Remove from my tools

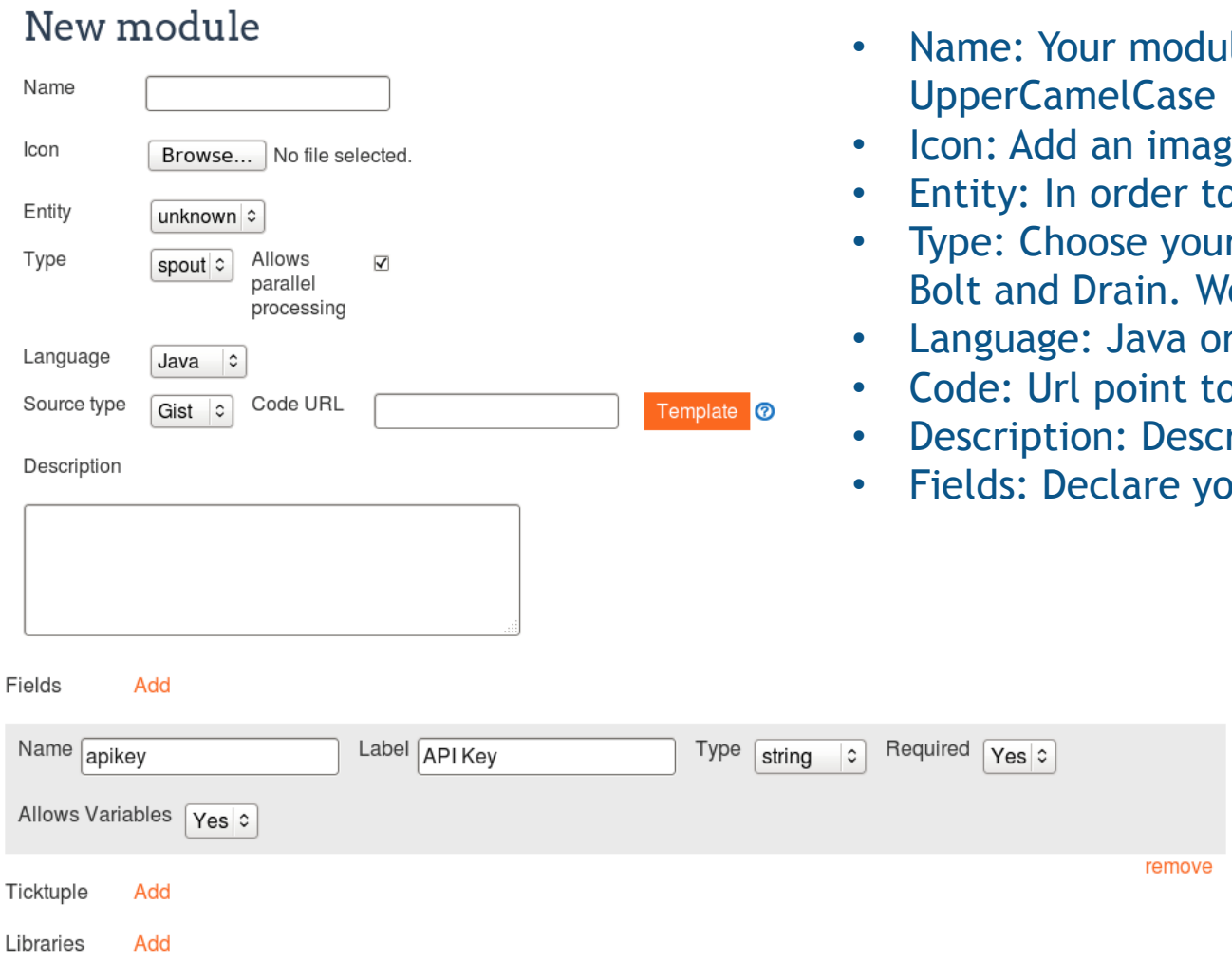
RdataDNSDB

Type: bolt
Entity: domain
Status: published
Language: Java

Code URL:
https://gist.github.com/ffr4nz/668e5d104518e63fc6da

Description:
Get Rdata from field. Domain, IP or Range and RawHex supported.

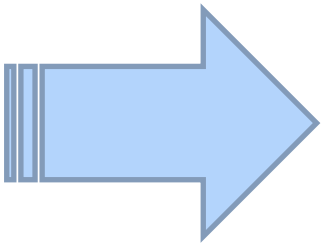
Adding Knowledge: Modules



- Name: Your module name. Must be UpperCamelCase
- Icon: Add an image.
- Entity: In order to catalog.
- Type: Choose your type of module. Spout, Bolt and Drain. Won't be change.
- Language: Java or Python
- Code: Url point to Gist.github.com
- Description: Describe what you module do.
- Fields: Declare your parameters.

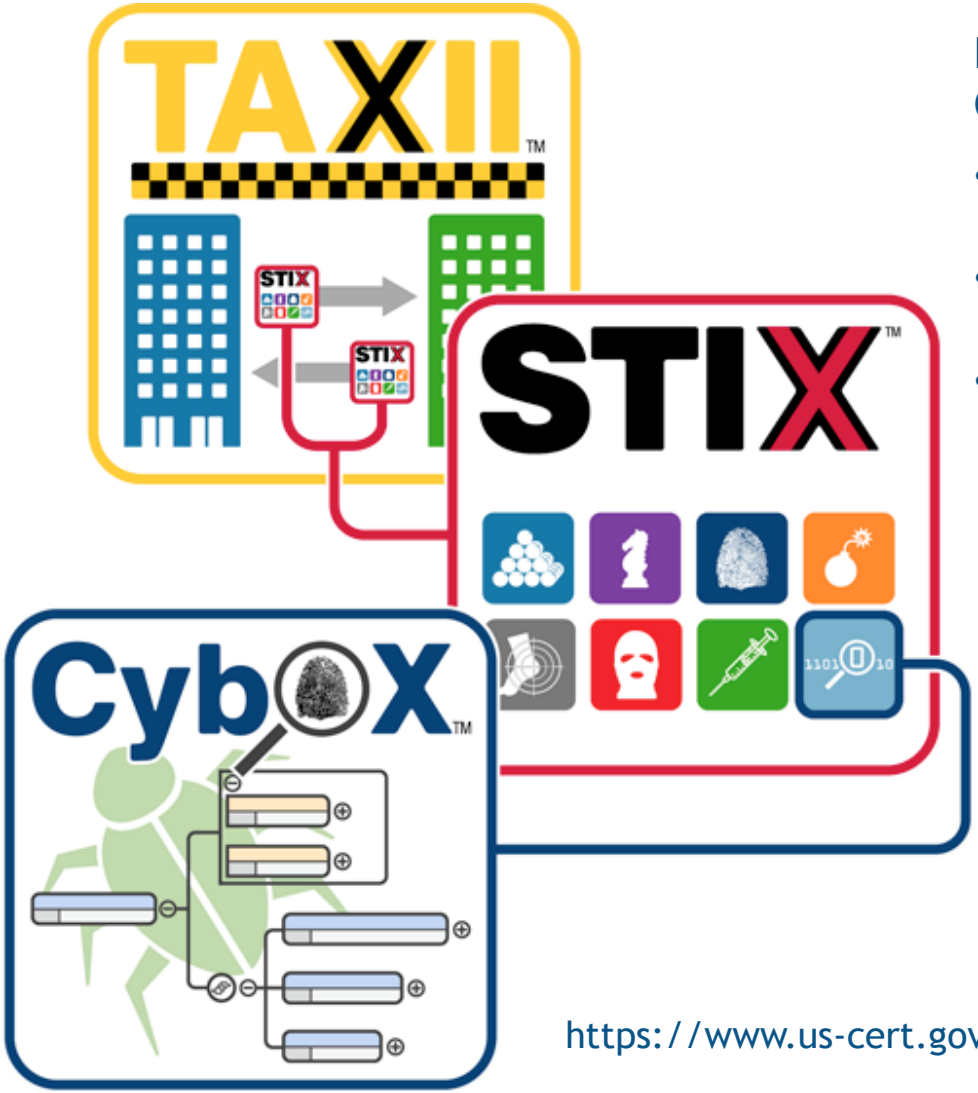
Adding Knowledge: Modules


```
/*
    The MIT License (MIT)

    Copyright (c) 2015 sinfonier-project

    Permission is hereby granted, free of charge, to any person obtaining a copy
    of this software and associated documentation files (the "Software"), to deal
    in the Software without restriction, including without limitation the rights
    to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
    copies of the Software, and to permit persons to whom the Software is
    furnished to do so, subject to the following conditions:

    The above copyright notice and this permission notice shall be included in
    all copies or substantial portions of the Software.

    THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
    IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
    FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
    AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
    LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
    OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
    THE SOFTWARE.
*/


package com.sinfonier.spouts;

import java.io.File;
import java.io.FileNotFoundException;
import java.util.Scanner;

public class FirstConModule extends BaseSinfonierSpout {

    private File file;
    private Scanner sc;

    public FirstConModule(String spoutName, String xmlPath) {
        super(spoutName, xmlPath);

    }

    public void useropen(){

        // TO-DO: Init values. Code here runs once.
        // In Spouts this function is very important. Must get an object than can
        // iterate to use it in usernextTuple()

        file = new File((String)this.getParam("file"));
        try {
            sc = new Scanner(file);
        } catch (FileNotFoundException e) {
            e.printStackTrace();
        }

    }
```



github:gist


STIX
IODEF
OpenIOC
TAXII
CybOX
OpenIOC
IODEF
OpenIOC
STIX
TAXII
OpenIOC
STIX
STIX
CybOX
IODEF
OpenIOC
IODEF



Information Sharing Specifications for Cybersecurity

- **TAXII™**, the Trusted Automated eXchange of Indicator Information;
- **STIX™**, the Structured Threat Information eXpression; and
- **CybOX™**, the Cyber Observable eXpression.

https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity

Mostly:
Not standards at all…

20% Rejected due to missing information

ACNS

Automated Copyright Notice System (ACNS) 2.0

ARF

Abuse Reporting Format
(RFC5965)

Time to Play

Sinfonier /sin'fonje/ DASHBOARD TOPOLOGIES MODULES USERS EDITOR

My Topologies

TOPOLOGIES NEW TOPOLOGY +

DetectingEmbeddedAPKs (used as template 1 time)

Description:
eCrime 2015 Keynote: Join the phishing dots to detect suspicious mobile apps

Sharing:
private Publish

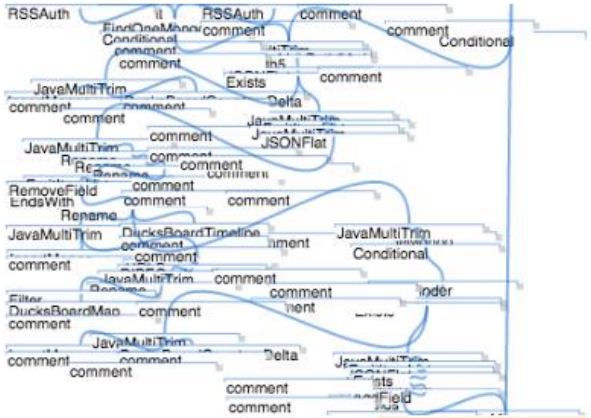
Tag:
undefined

Updated:
a day ago

Last Execution:
never

Created by citronio at Sun May 10 2015 17:28:59 GMT+0200 (CEST)

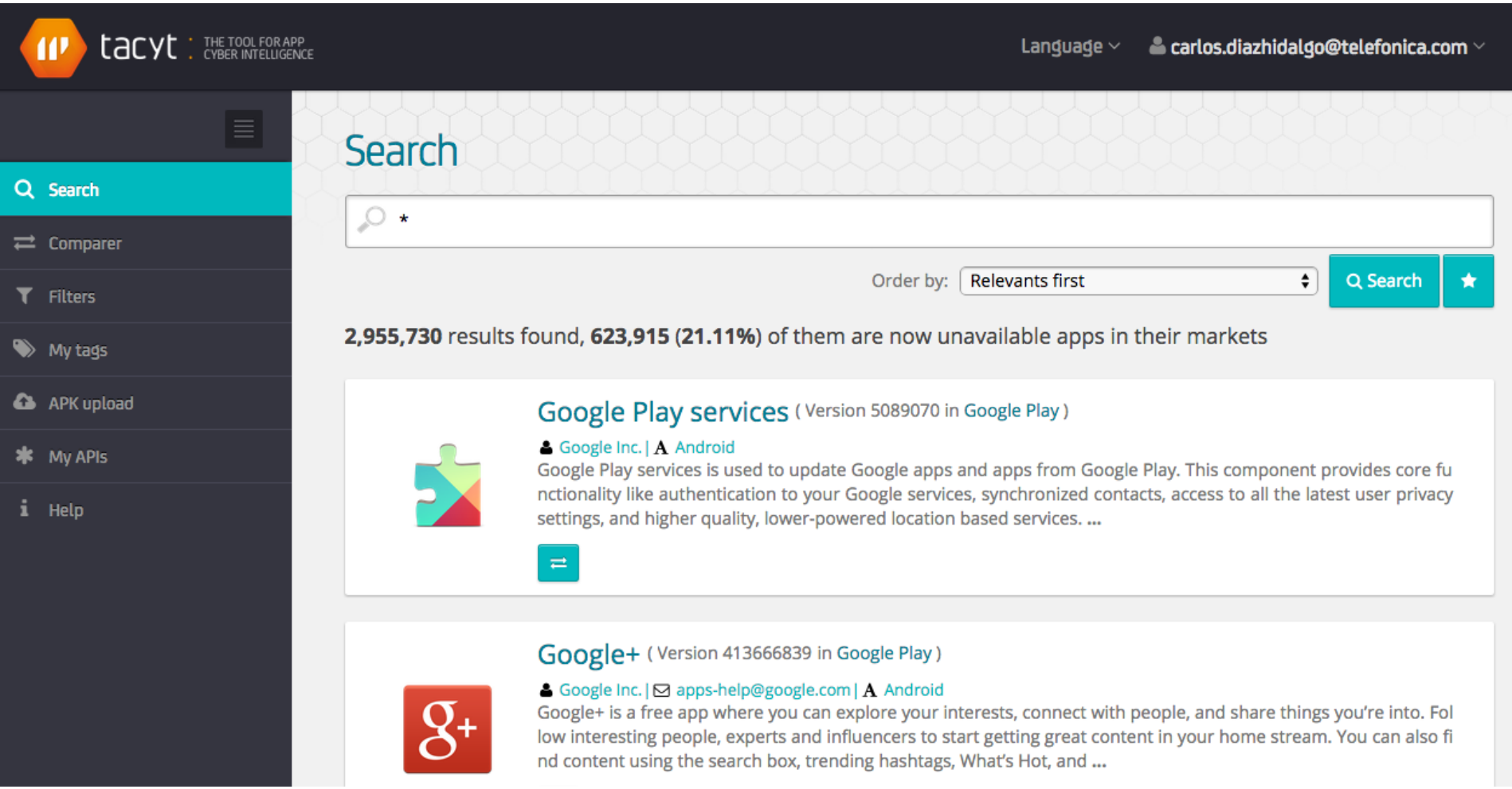
Delete Stop Edit Update

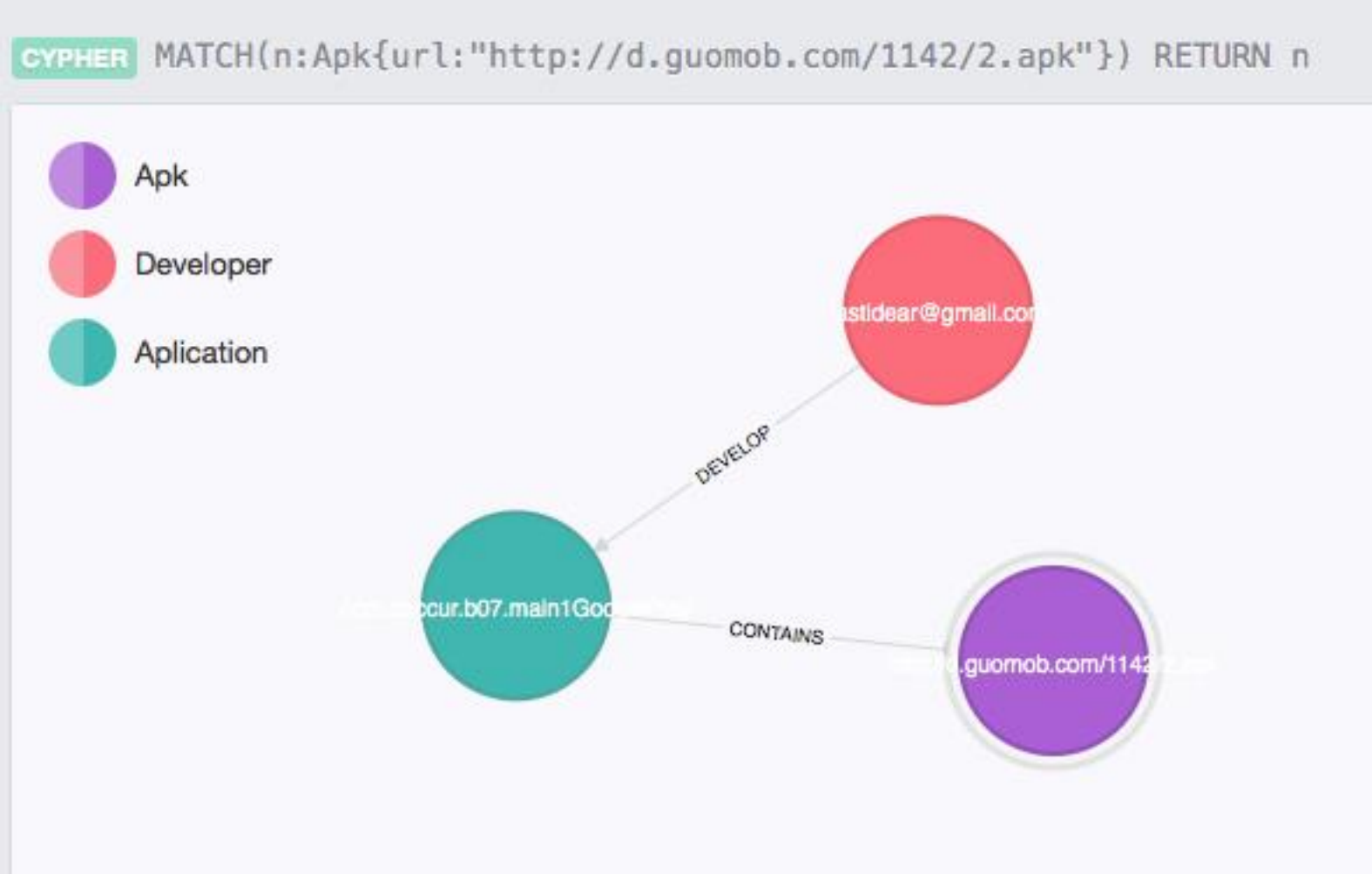


Use as template

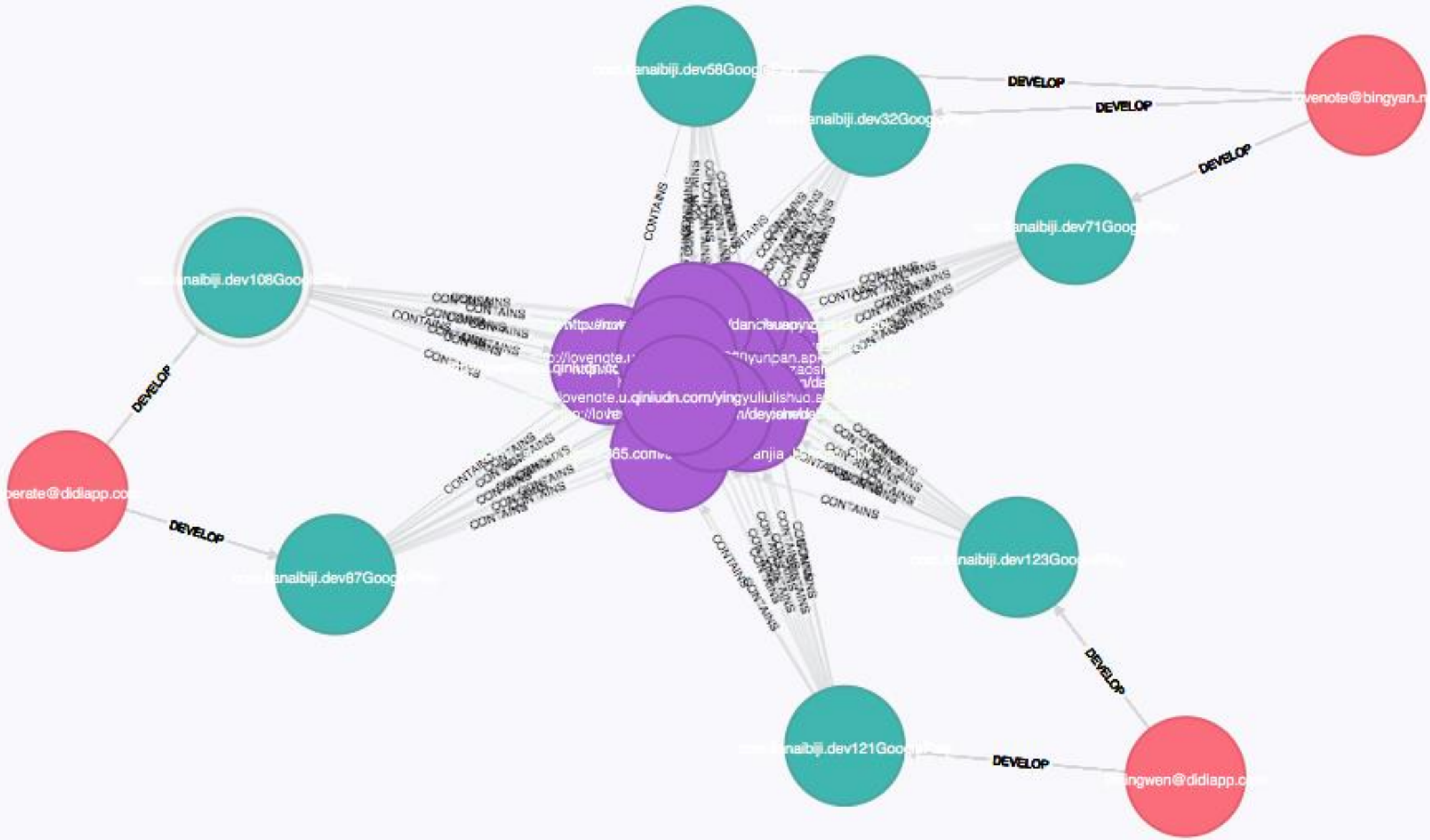
EmailInjectorTacyct

Description:
No description yet

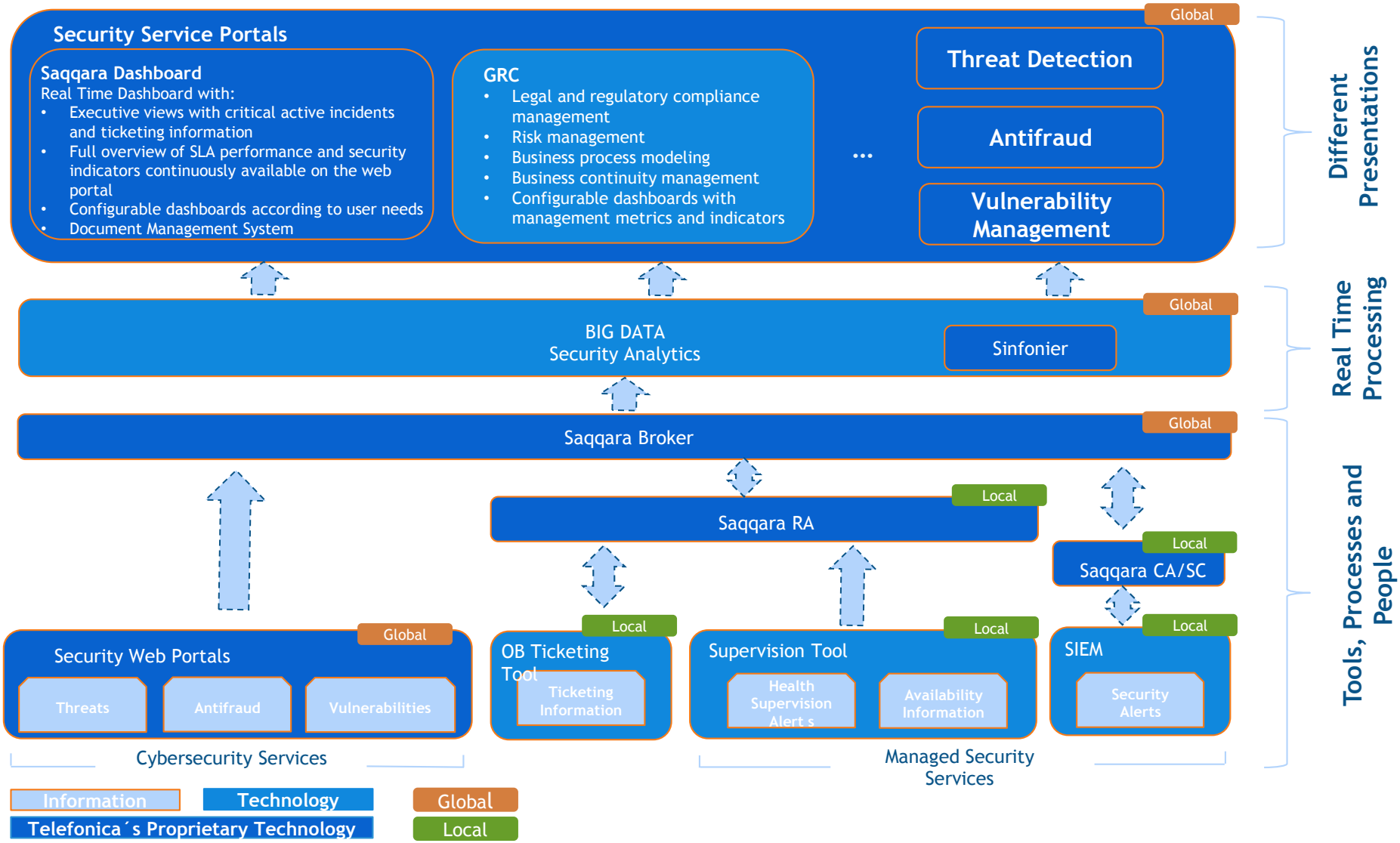

tacyt : THE TOOL FOR APP CYBER INTELLIGENCE
Language
carlos.diazhidalgo@telefonica.com
Search
Comparer
Filters
My tags
APK upload
My APIs
Help
Search
*
Order by:
Relevants first
Search
2,955,730 results found, 623,915 (21.11%) of them are now unavailable apps in their markets
Google Play services (Version 5089070 in Google Play)
Google Inc. | Android
Google Play services is used to update Google apps and apps from Google Play. This component provides core fu nctionality like authentication to your Google services, synchronized contacts, access to all the latest user privacy settings, and higher quality, lower-powered location based services. ...
Google+ (Version 413666839 in Google Play)
Google Inc. | apps-help@google.com | Android
Google+ is a free app where you can explore your interests, connect with people, and share things you're into. Fol low interesting people, experts and influencers to start getting great content in your home stream. You can also fi nd content using the search box, trending hashtags, What's Hot, and ...


CYPHER MATCH(n:Apk{url:"http://d.guomob.com/1142/2.apk"}) RETURN n
Apk
Developer
Aplication
DEVELOP
CONTAINS

Mobile Threats




EAT
OUR OWN
DOG FOOD
(AND LIKE IT TOO)


Global
Security Service Portals
Saqqara Dashboard
Real Time Dashboard with:
• Executive views with critical active incidents and ticketing information
• Full overview of SLA performance and security indicators continuously available on the web portal
• Configurable dashboards according to user needs
• Document Management System
GRC
• Legal and regulatory compliance management
• Risk management
• Business process modeling
• Business continuity management
• Configurable dashboards with management metrics and indicators
...
Threat Detection
Antifraud
Vulnerability Management
Different Presentations
Global
BIG DATA
Security Analytics
Sinfonier
Real Time Processing
Global
Saqqara Broker
Local
Saqqara RA
Local
Saqqara CA/SC
Global
Security Web Portals
Threats
Antifraud
Vulnerabilities
Local
OB Ticketing Tool
Ticketing Information
Local
Supervision Tool
Health Supervision Alert s
Availability Information
Local
SIEM
Security Alerts
Tools, Processes and People
Cybersecurity Services
Managed Security Services
Information
Technology
Telefonica´s Proprietary Technology
Global
Local

Sinfonier

1 Select Data Source

kafka

saqq-ticket

saqq-security-alarm

saqq-avail

saqq-health-alarm

Sinfonier

2 Process data

saqq-security-alarm

MATCH Alarm_id In real time

saqq-ticket

Alarm_id

Ticket_id Alarm_id

Detection date

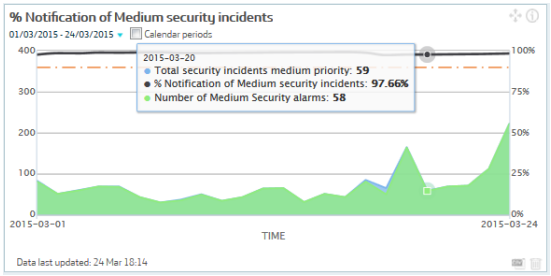
Notification Time = Notification date - Detection date

Notification date

BIG DATA CASSANDRA

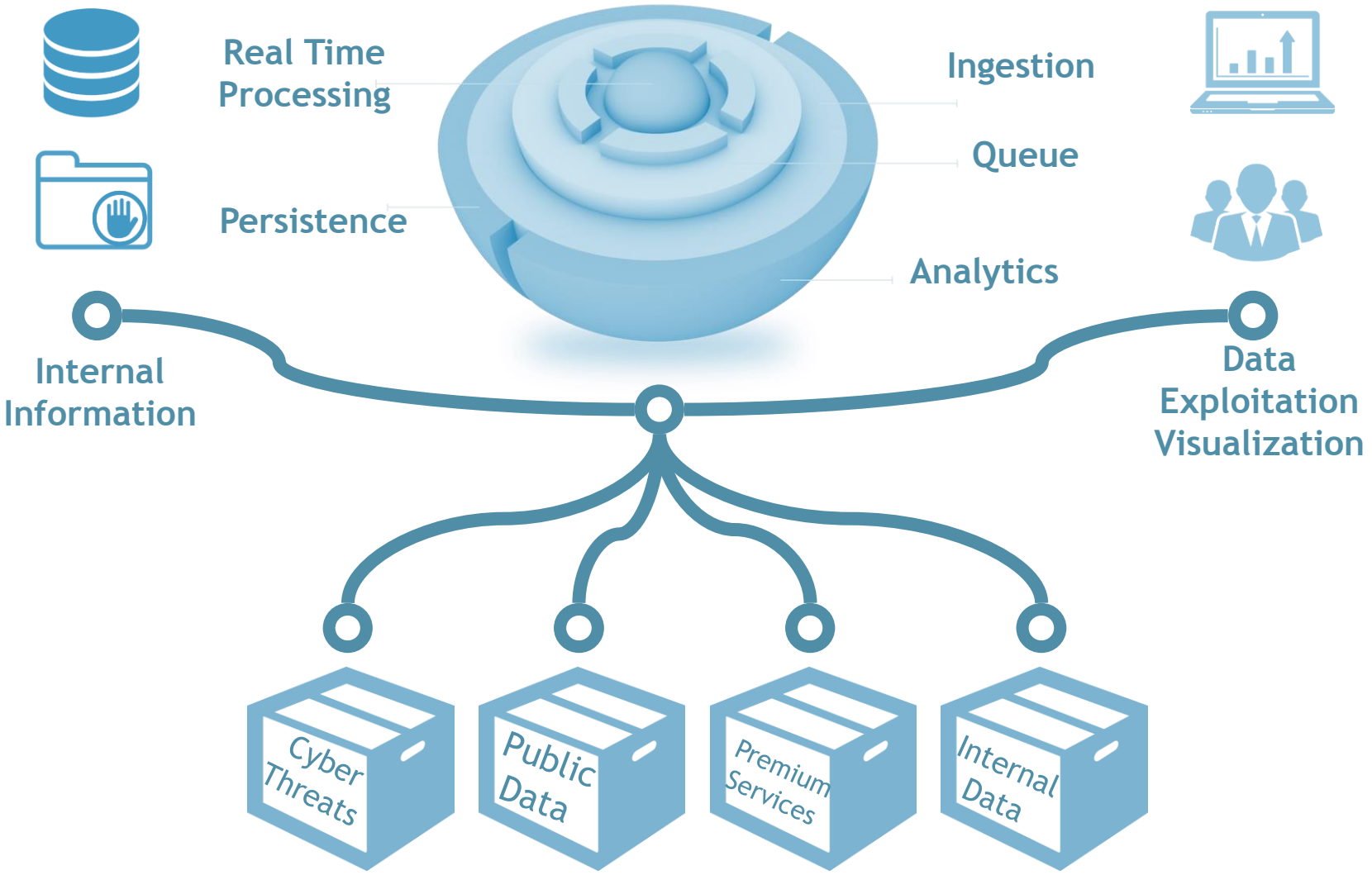
Saqqara Dashboard

3 Produce Results



Ticket Type: Incident
Service: RISK MONITORING
Product type: INCIDENT NOTIFICATION
Problem type: MALICIOUS CODE
Status: Resolved
Priority: MEDIA
Detection date: 2015-03-24 14:48:03
Opening Date: 2015-03-24 14:53:09
Resolution date: 2015-03-24 16:42:41

Duration (min): 109
Location: Spain
Updates:
24/03/2015 15:42:42 IU_SOC Resolved - Incident, we will closed the case with a massive disinfection in all affected computers.


Real Time Processing
Persistence
Ingestion
Queue
Analytics
Internal Information
Data Exploitation Visualization
Cyber Threats
Public Data
Premium Services
Internal Data


FI-WARE

Join us

Join us:
sinfonier-project.net

@e_Sinfonier

@ffranz @LeoAmorV

Sinfonier

"All knowledge is connected to all other knowledge. The fun is in making the connections"

Arthur Aufderheide

Telefónica