Sinfonier Storm Builder for Security Intelligence

Fran Gomez  @ffranz
Leonardo Amor  @LeoAmorV
Storm Builder for Security Intelligence

"Connecting information, delivering intelligence"
Our Employees

- Mostly:
  - Telco engineers
  - Computer Science Engineers
  - Science or Scientist people
But there also space to:

- Lawyers
- Business administration
- Economist
- Psychologist
- Philologist
Diversity
Ideas explosion
Unfortunately yet not everyone knows to code
Fortunately everyday schools are getting it should be one more basic class
But... Why we need to code?

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/
- 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 =

Telefonica

Sinfonier
public static void main(String[] args) throws Exception {
    TopologyBuilder builder = new TopologyBuilder();
    builder.setSpout("word", new TestWordSpout(), 10);
    builder.setBolt("exclam1", new ExclamationBolt(), 3).shuffleGrouping("word");
    builder.setBolt("exclam2", new ExclamationBolt(), 2).shuffleGrouping("exclam1");
    Config conf = new Config();
    conf.setDebug(true);
    if (args != null && args.length > 0) {
        conf.setNumWorkers(3);
        StormSubmitter.submitTopologyWithProgressBar("test", conf, builder); 
    } else {
        LocalCluster cluster = new LocalCluster();
        cluster.submitTopology("test", conf, builder);
        Util.sleep(10000);
        cluster.killTopology("test");
        cluster.shutdown();
    }
}
Topology life cycle

Canvas

User Tools

Context Info
Topology Wordpressrss

Wordpressrss

Description:
No description yet

Sharing:
private

Tag:
undefined

Updated:
26 days ago

Last Execution:
ever

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

Delete  Stop  Edit  Update  Use as template
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 cybersecurity data output normalization
KEEP CALM AND SHARE IT
<table>
<thead>
<tr>
<th>Module</th>
<th>Type</th>
<th>Entity</th>
<th>Status</th>
<th>Language</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebThumbnail</td>
<td>bolt</td>
<td>url</td>
<td>published</td>
<td>Java</td>
<td>Code URL: <a href="https://gist.githubusercontent.com/ff4nzo/b01d7dcd0a45f9b9bc">https://gist.githubusercontent.com/ff4nzo/b01d7dcd0a45f9b9bc</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Description: Offers a simple tool to generate website screenshots on demand.</td>
</tr>
<tr>
<td>ShodanSearch</td>
<td>spout</td>
<td>ip</td>
<td>published</td>
<td>Java</td>
<td>Code URL: <a href="https://gist.githubusercontent.com/ff4nzo/6194d69fda732c964f">https://gist.githubusercontent.com/ff4nzo/6194d69fda732c964f</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Description: Searches Shodan using the same query syntax as the website and use facets to get summary information for different properties. Emit each new match term.</td>
</tr>
<tr>
<td>LinkedInUserParser</td>
<td>bolt</td>
<td>user</td>
<td>published</td>
<td>Java</td>
<td>Code URL: <a href="https://gist.githubusercontent.com/ff4nzo/2c751a335ce791003a8">https://gist.githubusercontent.com/ff4nzo/2c751a335ce791003a8</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Description: Gets user info from public profile URL.</td>
</tr>
<tr>
<td>CSV</td>
<td>spout</td>
<td>unknown</td>
<td>private</td>
<td>Java</td>
<td>Code URL: <a href="https://gist.githubusercontent.com/ff4nzo/a999e61e00600f03e314">https://gist.githubusercontent.com/ff4nzo/a999e61e00600f03e314</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Description: Get CSV file and emit each line into a JSON object. Key list are key names for common separated values.</td>
</tr>
<tr>
<td>DucksBoardStatus</td>
<td>drain</td>
<td>unknown</td>
<td>published</td>
<td>Java</td>
<td>Code URL: <a href="https://gist.githubusercontent.com/ff4nzo/932afa7cd30065c2609">https://gist.githubusercontent.com/ff4nzo/932afa7cd30065c2609</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Description: Display the status of an item in your Ducksboard.</td>
</tr>
<tr>
<td>TwitterUser</td>
<td>spout</td>
<td>tweet</td>
<td>published</td>
<td>Java</td>
<td>Code URL: <a href="https://gist.githubusercontent.com/ff4nzo/627cadcf018969f911d">https://gist.githubusercontent.com/ff4nzo/627cadcf018969f911d</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Description: Real-time updates of all data from user timeline.</td>
</tr>
<tr>
<td>InstaPush</td>
<td>drain</td>
<td>unknown</td>
<td>published</td>
<td>Java</td>
<td>Code URL: <a href="https://gist.githubusercontent.com/ff4nzo/19e374a5d716550f9a5">https://gist.githubusercontent.com/ff4nzo/19e374a5d716550f9a5</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Description: Send push using instapush.im events. Needs a trackers list, each element match with a json received fields and an event title.</td>
</tr>
<tr>
<td>VirusTotalIP</td>
<td>bolt</td>
<td>ip</td>
<td>published</td>
<td>Java</td>
<td>Code URL: <a href="https://gist.githubusercontent.com/ff4nzo/8538194a9e778394b9a9">https://gist.githubusercontent.com/ff4nzo/8538194a9e778394b9a9</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Description: Retrieve a report on a given IP address (including the information recorded by VirusTotal's Passive DNS infrastructure).</td>
</tr>
<tr>
<td>Module</td>
<td>Type</td>
<td>Entity</td>
<td>Status</td>
<td>Language</td>
<td>Code URL</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------</td>
<td>--------</td>
<td>--------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DomainTLD</td>
<td>bolt</td>
<td>domain</td>
<td>published</td>
<td>Java</td>
<td><a href="https://gist.github.com/ffr4nz/45edc9e39309ff13c55b">https://gist.github.com/ffr4nz/45edc9e39309ff13c55b</a></td>
</tr>
<tr>
<td>HibpwnedAccount</td>
<td>bolt</td>
<td>user</td>
<td>published</td>
<td>Java</td>
<td><a href="https://gist.github.com/ffr4nz/3c934492c20d00d17f8">https://gist.github.com/ffr4nz/3c934492c20d00d17f8</a></td>
</tr>
<tr>
<td>FreeGeoIP</td>
<td>bolt</td>
<td>ip</td>
<td>published</td>
<td>Java</td>
<td><a href="https://gist.github.com/ffr4nz/1b9491155b5ef7e16702">https://gist.github.com/ffr4nz/1b9491155b5ef7e16702</a></td>
</tr>
<tr>
<td>PeerReach</td>
<td>bolt</td>
<td>user</td>
<td>published</td>
<td>Java</td>
<td><a href="https://gist.github.com/ffr4nz/1b9491155b5ef7e16702">https://gist.github.com/ffr4nz/1b9491155b5ef7e16702</a></td>
</tr>
<tr>
<td>JSONArray</td>
<td>spout</td>
<td>unknown</td>
<td>published</td>
<td>Java</td>
<td><a href="https://gist.github.com/ffr4nz/54445455d76d42c592a6">https://gist.github.com/ffr4nz/54445455d76d42c592a6</a></td>
</tr>
<tr>
<td>RdataDNSDB</td>
<td>bolt</td>
<td>domain</td>
<td>published</td>
<td>Java</td>
<td><a href="https://gist.github.com/ffr4nz/6686d104518e63fc6da">https://gist.github.com/ffr4nz/6686d104518e63fc6da</a></td>
</tr>
</tbody>
</table>
Adding Knowledge: Modules

New module

- 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.

Fields

Name         Label
apikey       API Key

Allows Variables

Ticktupel

Libraries
/*
 * 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 FirstComModule extends BaseSinfonierSpout {
    private File file;
    private Scanner sc;

    public FirstComModule(String spoutName, String xmlPath) {
        super(spoutName, xmlPath);
    }

    public void useropen(){
        // TO-DO: Init values. Code here runs once.
        // Iterate to use it in userNextTuple()
        File file = new File(String) this.getPara("file");
        try {
            sc = new Scanner(file);
        } catch (FileNotFoundException e) {
            e.printStackTrace();
        } // end try
    }
}
Sharing information - The need of standards
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
My Topologies

DetectingEmbeddedAPKs
- **Description:**
  - eCrime 2015 Keynote: Join the phishing dots to detect suspicious mobile apps
- **Sharing:**
  - private
- **Tag:**
  - undefined
- **Updated:**
  - a day ago
- **Last Execution:**
  - never
- **Created by cironio at Sun May 10 2015 17:26:59 GMT+0200 (CEST)**

EmailInjectorTacyct
- **Description:**
  - No description yet
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 Play services is used to update Google apps and apps from Google Play. This component provides core functionality 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+ is a free app where you can explore your interests, connect with people, and share things you’re into. Follow interesting people, experts and influencers to start getting great content in your home stream. You can also find content using the search box, trending hashtags, What’s Hot, and...
MATCH(n:Apk{url:"http://d.guomob.com/1142/2.apk"}) RETURN n
EAT OUR OWN DOG FOOD (AND I LIKE IT TOO)
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

**BIG DATA**
- Security Analytics
- Sinfonier

**Saqqara Broker**

**Saqqara RA**

**Security Web Portals**
- Threats
- Antifraud
- Vulnerabilities

**Cybersecurity Services**
- Threats
- Antifraud
- Vulnerabilities

**OB Ticketing Tool**
- Ticketing Information

**Supervision Tool**
- Health Supervision Alerts
- Availability Information

**SIEM**
- Security Alerts

**Managed Security Services**

**GRC**
- Legal and regulatory compliance management
- Risk management
- Business process modeling
- Business continuity management
- Configurable dashboards with management metrics and indicators

**Tools, Processes and People**
- Different Presentations
- Real Time Processing
- Cybersecurity Services
- Telefonica’s Proprietary Technology

**Information**
**Technology**

Global
Local
1. Select Data Source

2. Process data

- Match Alarm_id in real time
- Kafka
- saqq-ticket
- saqq-security-alarm
- saqq-avail
- saqq-health-alarm
- Alarm_id
- Detection date
- Notification date
- Notification Time = Notification date - Detection date
- Ticket_id
- Alarm_id

3. Produce Results

- Big Data
- Cassandra
Cyber Security

- Real Time Processing
- Persistence
- Ingestion
- Queue
- Analytics
- Internal Information

Data Exploitation Visualization

- Cyber Threats
- Public Data
- Premium Services
- Internal Data
Join us
Join us:
sinfonier-project.net

@e_Sinfonier
@ffranz
@LeoAmorV
All knowledge is connected to all other knowledge.

The fun is in making the connections

Arthur Aufderheide