Open Source Intelligence Aggregation

TF-CSIRT MAY 15TH, 2017

Rogier Spoor
Sjors Haanen

SURF NET

Why?

- Nowadays a working IT infrastructure is critical
- Services are interconnected and reachable
- Security often not on par:
  - Bugs in outdated software;
  - Wrong configuration;
  - Default/weak passwords;
  - Password reuse.

Data leaks in the news

COMPUTERWORLD
FROM IDG

Home > Security

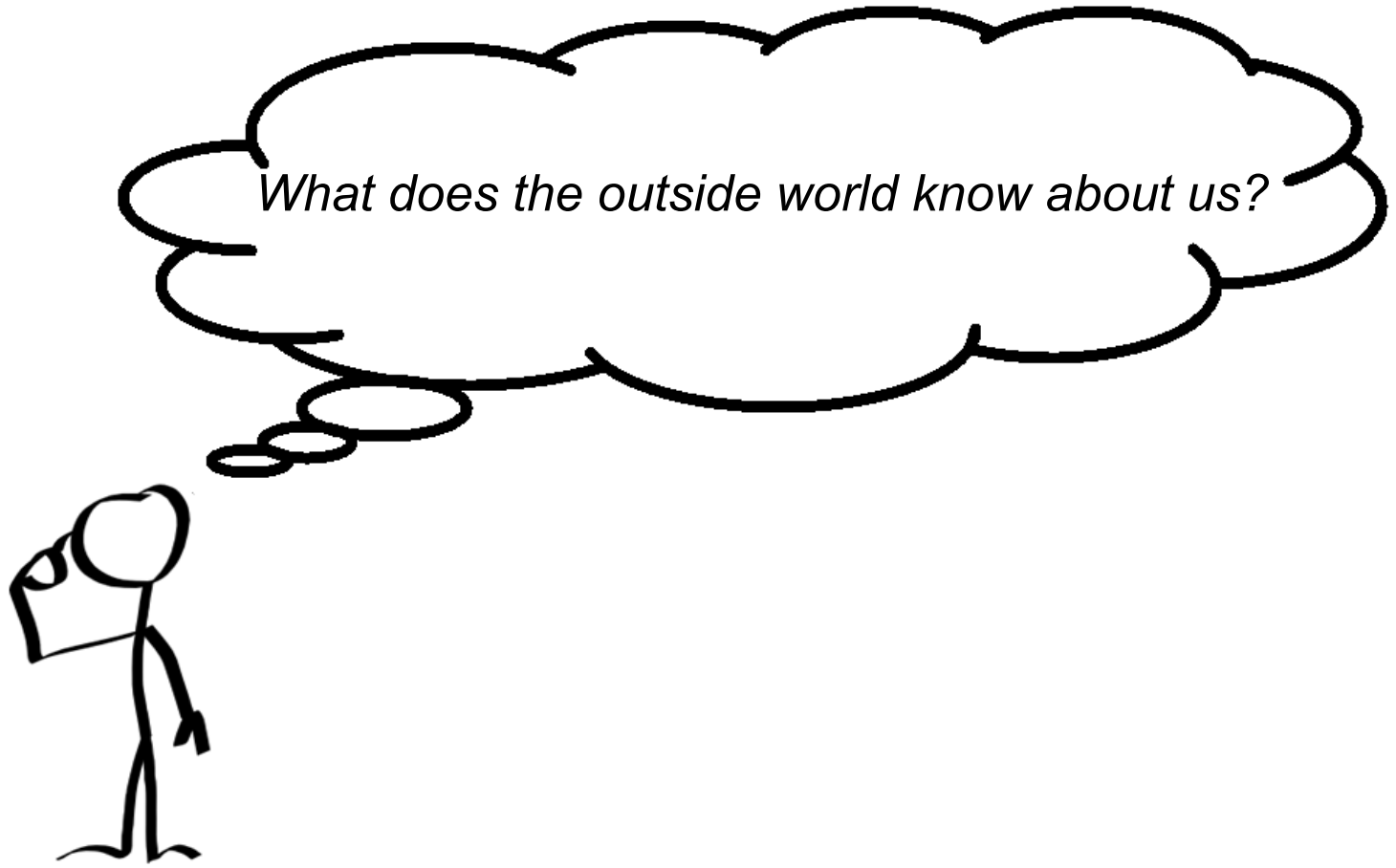
NEWS

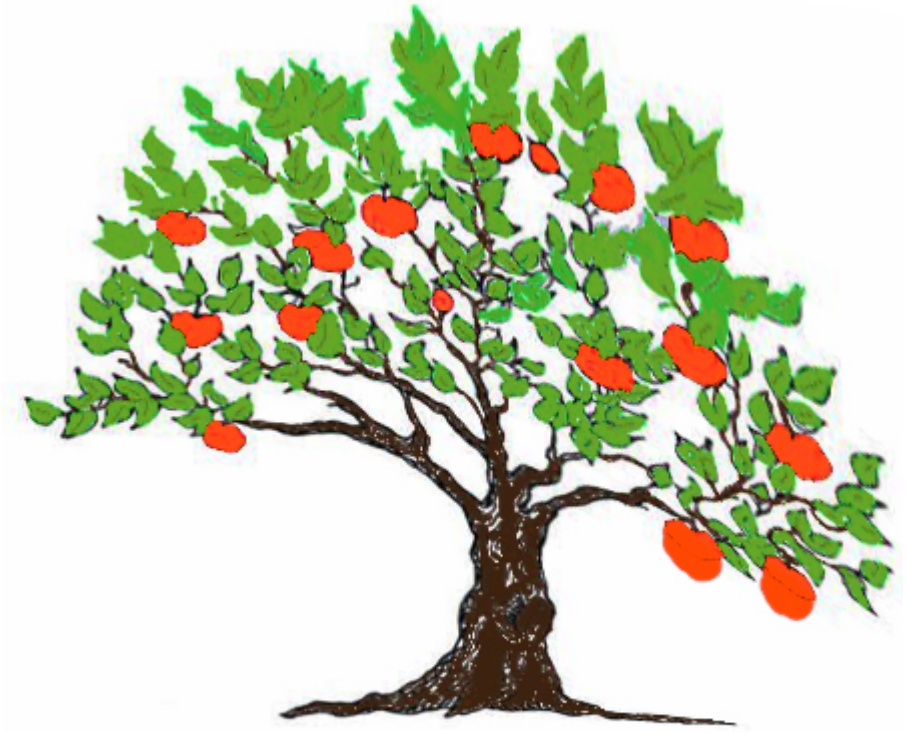
After MongoDB attack, ransomware groups hit exposed Elasticsearch clusters

Over 600 Elasticsearch instances had their data wiped and replaced with a ransom message

SURF NET

Raising question





Lots of vulnerabilities are like low hanging fruit

Problem

- Missing aggregation of Open Source Security Intelligence (OSINT)
  - Missing overview;
  - False positives;
  - Awareness of exploitable vulnerabilities;
  - The bad guys are often quicker.

Goals

- Give CSIRTS insights in vulnerabilities/services exposed to the world;
- Let users share and discuss search queries to make it a collaborate project;
- Reducing the cyber crime possibilities;
- Reducing the time to "fix“;
- Doing the right things (focus on high risk).

Source: IOT-scanners

Star IFBD-HE07/08
Network Utility

Contents | System Access | Network Configuration | Display Status | | Contact us

- Network Configuration
  - IP Parameters
  - System Configuration
  - Change Password
  - Save
  - Set Default
- Display Status
  - Network Card Info.
  - Network Status
  - Device Info.
  - Device Status
- System Access
  - Logout
- Contact us
  - Star Web Site
  - E-Mail

Device Model: FVP10 (STR_T-001)
MAC Address: 00:11:62:06:4B:63

IP Parameters

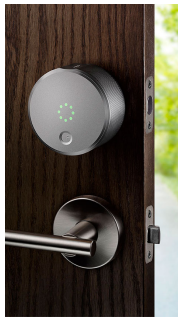
○ **Static //following addresses are used.**

IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0

◉ **Dynamic //Addresses are obtained from network.**

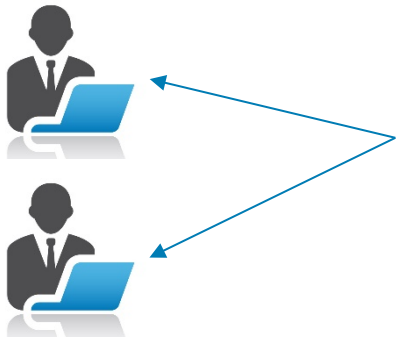
DHCP/BOOTP	ENABLE
RARP	ENABLE

Submit Cancel

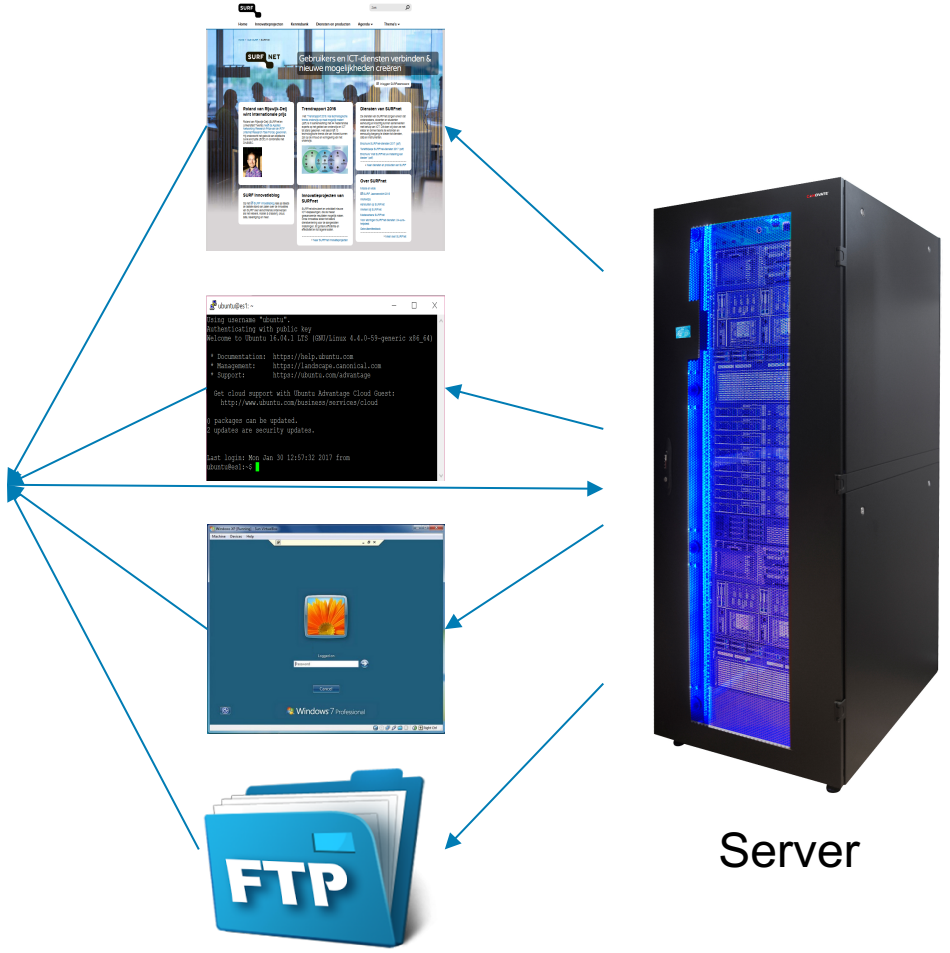


Workings of IOT-scanner

1. Scan device for services
2. Store service banners
3. End users can search on banners



IOT-scanner



Server

Source: IOT-scanners

SHODAN

censys

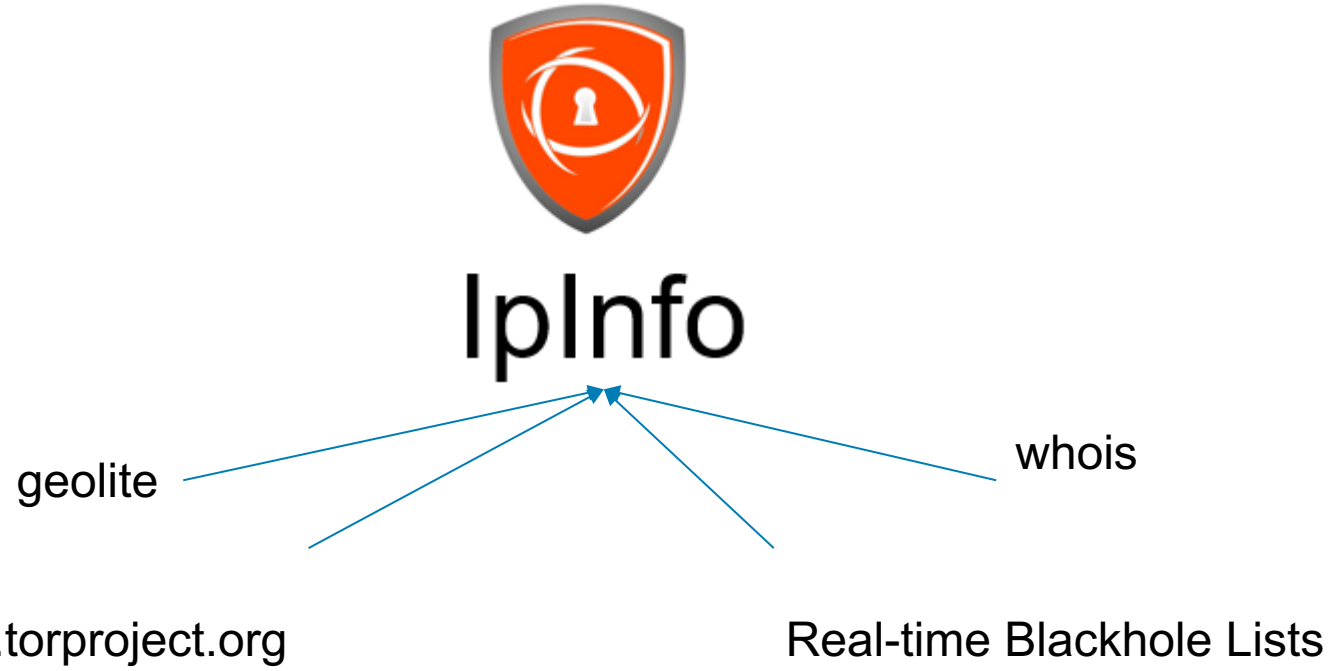
Source: IpInfo

REMCO VERHOEF

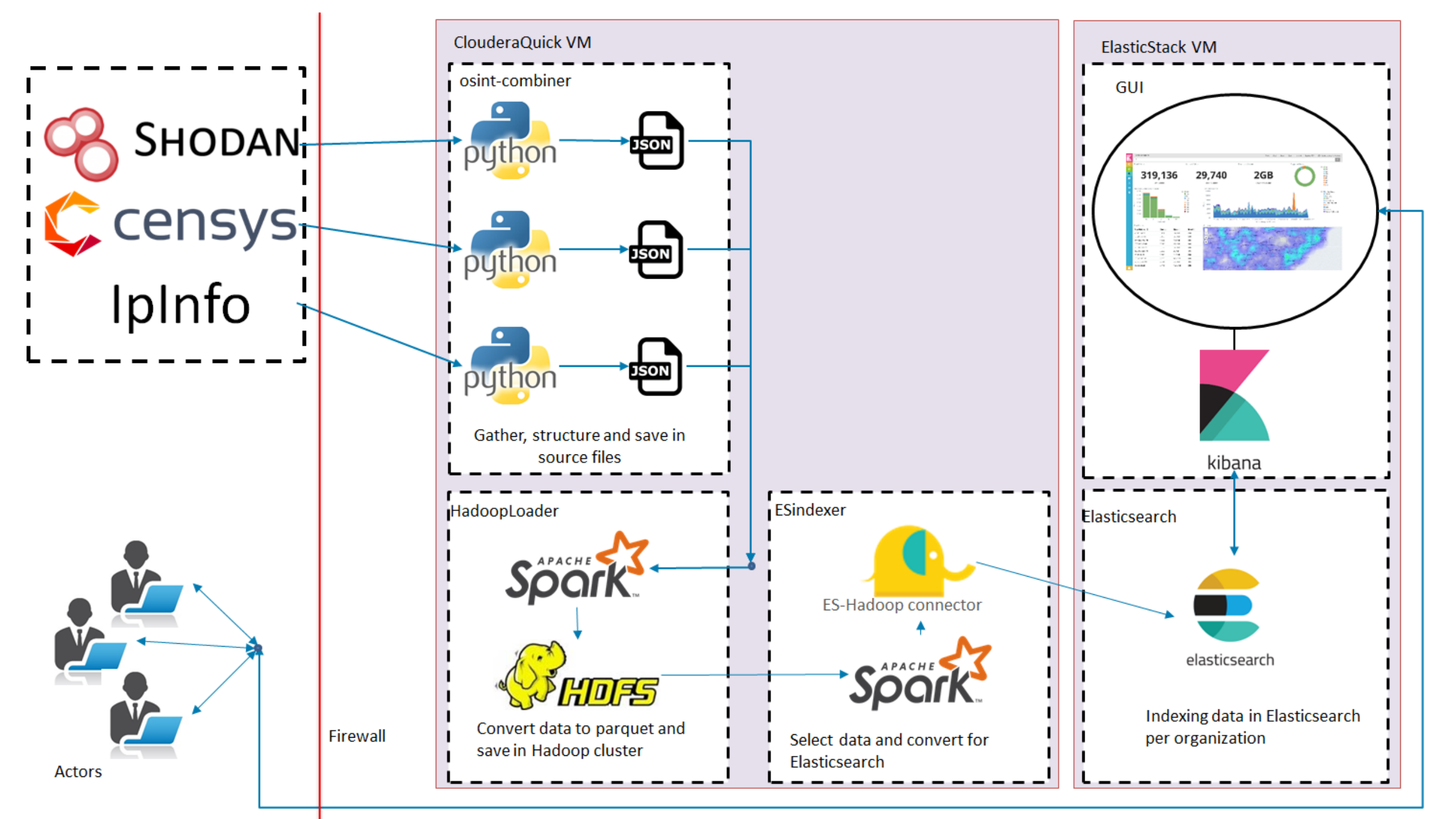
Founder of Honeycast.io

@remco_verhoef hackerone

- Enriching found data about IP-addresses
- Online blacklists



Proof of Concept


SHODAN
censys
IpInfo
Actors
Firewall
ClouderaQuick VM
osint-combiner
python
JSON
python
JSON
python
JSON
Gather, structure and save in source files
HadoopLoader
APACHE Spark
HDFS
Convert data to parquet and save in Hadoop cluster
ESindexer
ES-Hadoop connector
APACHE Spark
Select data and convert for Elasticsearch
ElasticStack VM
GUI
319,136
29,740
2GB
kibana
Elasticsearch
elasticsearch
Indexing data in Elasticsearch per organization

Collaboration with GDI Foundation

Tool is used at GDI Foundation

Scope: worldwide

GDI.Foundation

A safer Internet for everybody & everywhere

Project "***Internet & Cyber Security Health Check***"

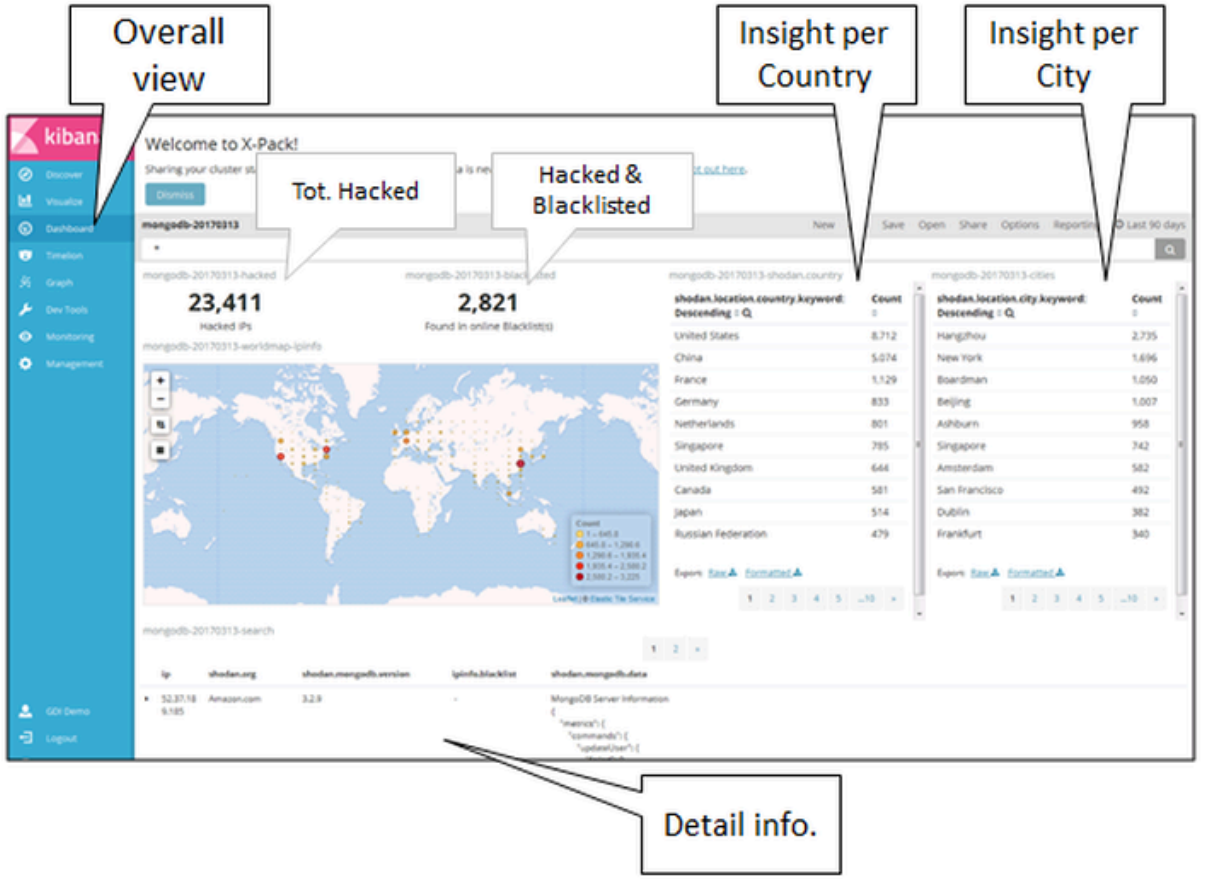
Victor Gevers
@0xDUDE

Vincent Toms
(IT) Security Specialist & co founder GDI.Foundation
The Hague Area, Netherlands | Information Technology and Services

In the future…

Future:

- Additional OSINT sources
- GDI: upscale



Demo

Demo

- Visualisations with Kibana
- Datasets: + as-surfnet (123K IPs);
  + GDI: Dahua IP cameras