OSTrICa – Open Source Threat Intelligence Collector

Roberto Sponchioni

Senior Threat Analysis Engineer

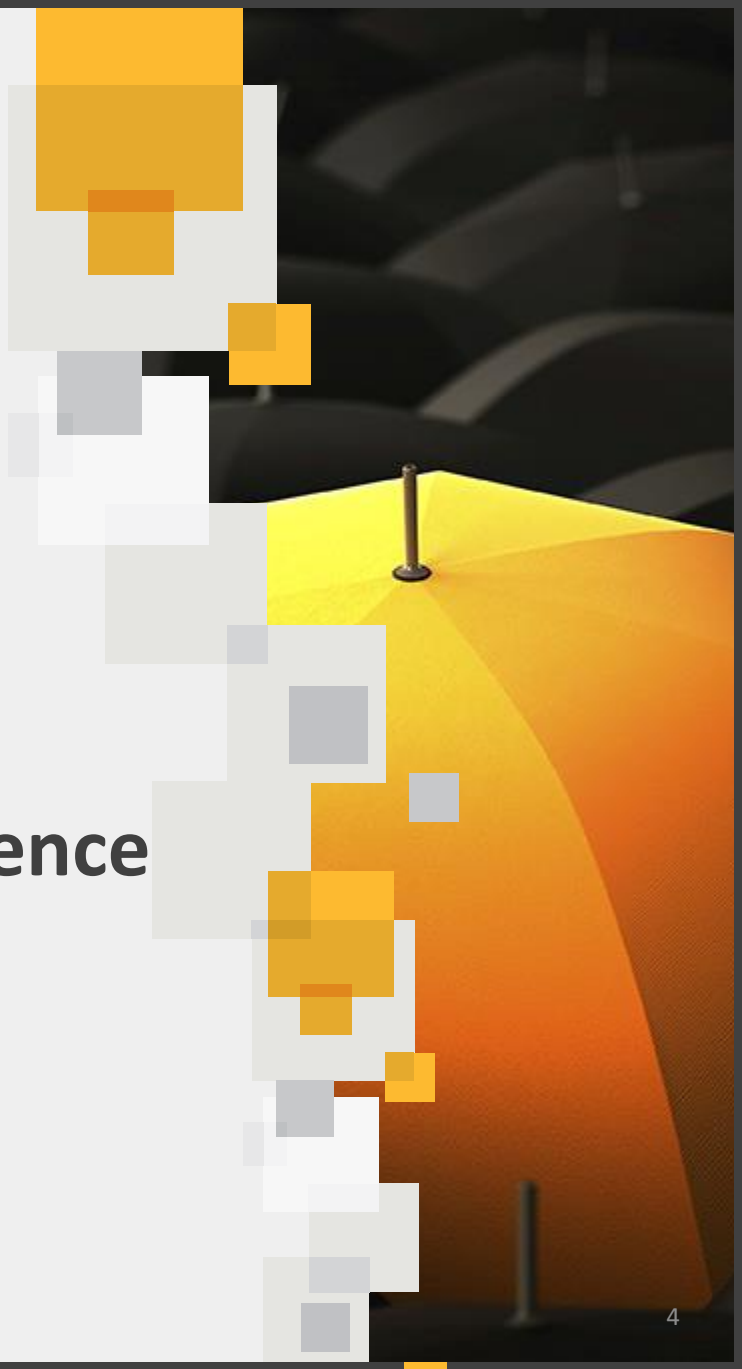
Agenda

- Introduction to Threat Intelligence
- Scenarios where to use TI
- What is OSTrICa?
- Demo
- How to develop OSTrICa Plugins

Who am I?

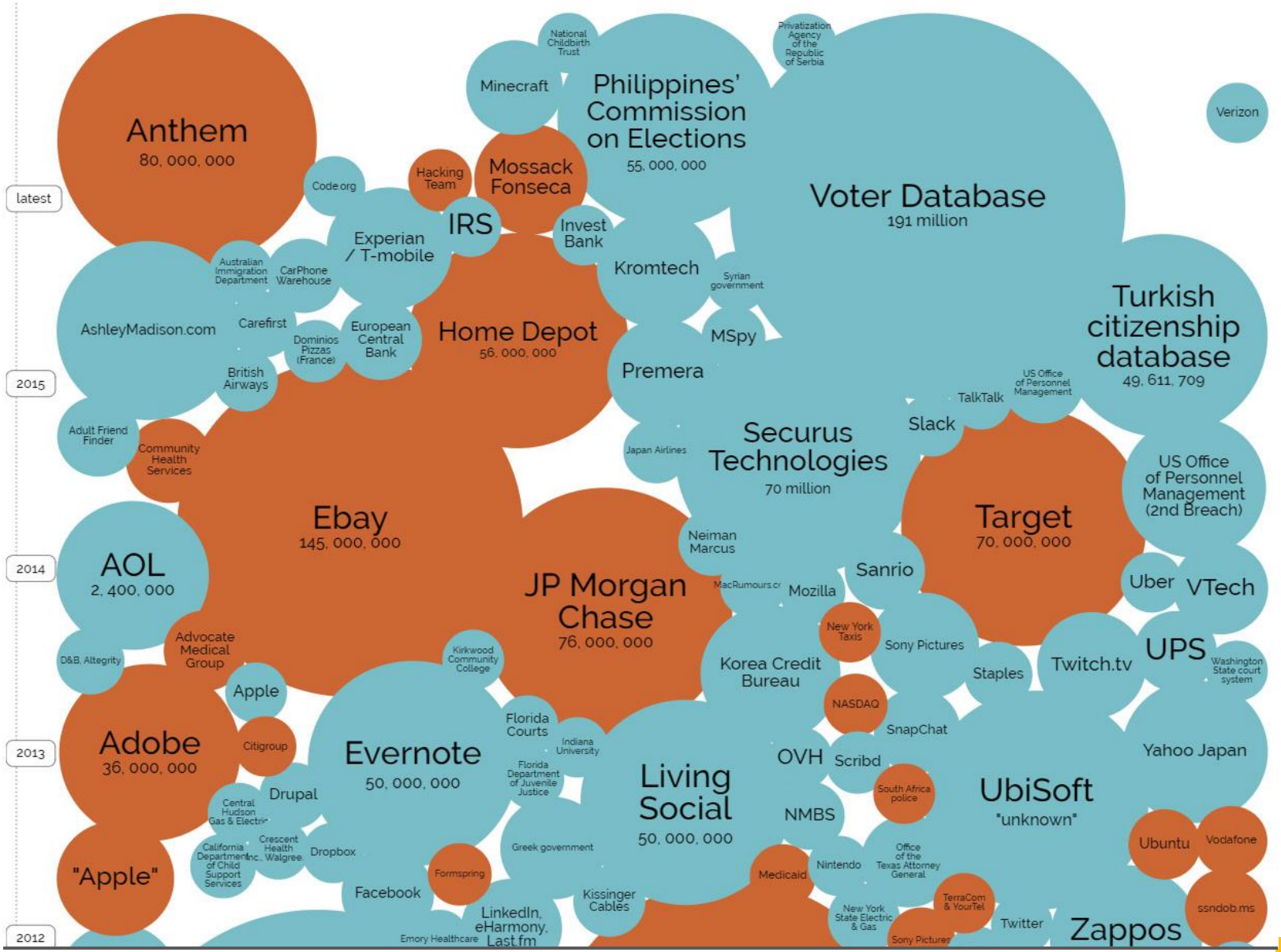
- Working as a Senior Threat Analysis Engineer @ Symantec
- Working as an Independent Security Researcher (Development, Malware Analysis, etc)
- Worked as a Security Consultant (PT/VA, Incident Response)

- Contacts:
  - @Ptr32Void on Twitter
  - https://github.com/Ptr32Void/ - GitHub Page
  - Roberto_Sponchioni@symantec.com
  - rsponchioni@yahoo.it



Introduction to Threat Intelligence

Data breaches are a big issue…



Ref.: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

What is Threat Intelligence & Why we have to use it

According to Gartner:

"Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."

What can we do with Threat Intelligence?

- Tracking cyber criminals, hacktivists
- Provide "context" to reconstruct attacks quickly
- Proactively block new attacks
- Validate and prioritize indicators and alerts
- Provide priorities to C-Levels (based on business risks)

Scenarios where to use TI

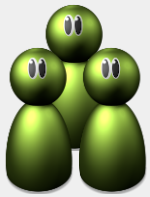
Current solutions that most companies use are…

- Anti-Virus products
- Firewall
- IDS/IPS
- Log collectors / SIEMs
- …

PDF

```
unescape("%u33dd%u3030%u33dd%u3030....")
pointerSled = unescape("<Contents>");
while (pointerSled.length < chunk_size)
        pointerSled += pointerSled;
pointerSled_len = chunk_size - (....
```

Attacker



Victims

TI can help to proactively protect your network

Ref.: http://www.bloomberg.com/graphics/2014-data-breaches/

Collecting Threat Intelligence Information

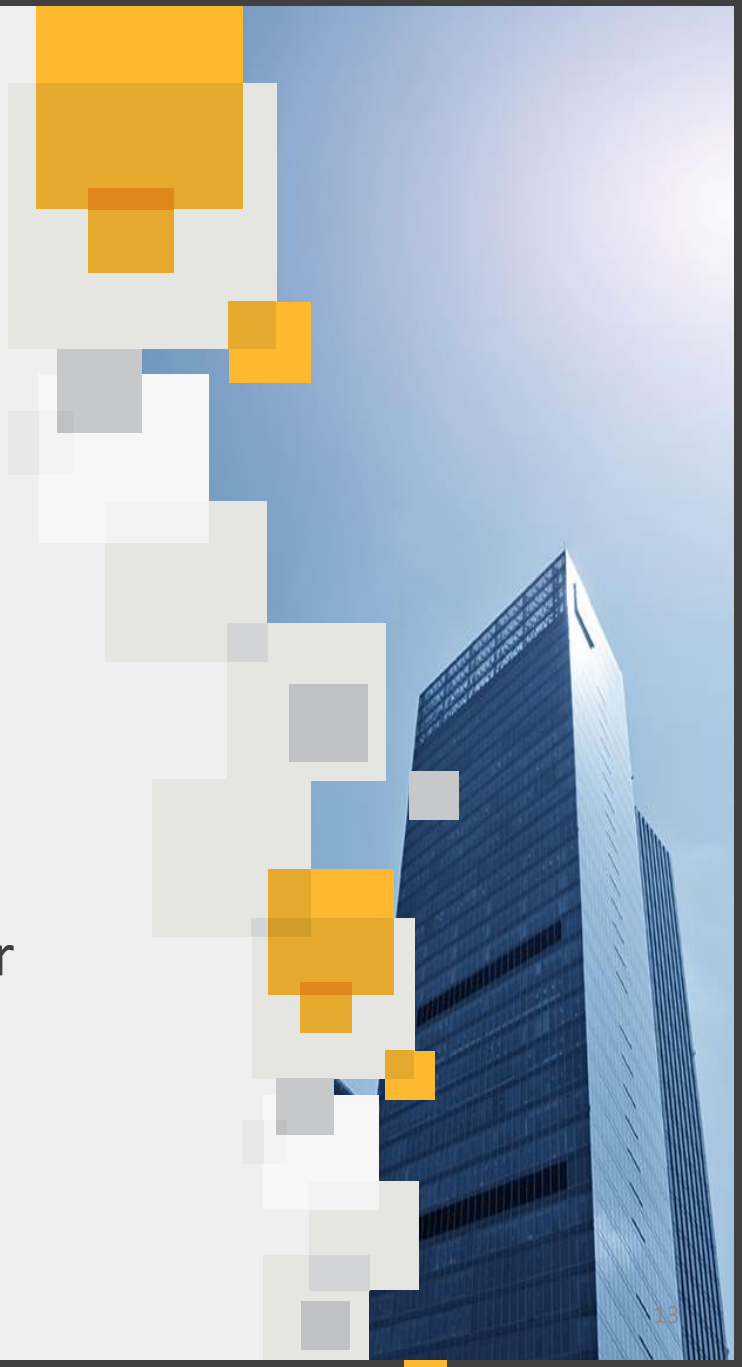
Threat Indicators (IoCs)

- File hashes (MD5, SHA256, …)
- C&C Server (Domain & IP Address)
- URL Reputation
- AV Detections
- Mutex
- File names
- ….

Threat Intelligence Sources…

	Free	Community	Commercial	Internal
Costs	Free	Free / $	$$$	-
Typology	Generic Intelligence	Generic / Specific Intelligence	Generic / Specific Intelligence	Very specific intelligence
Where do you get it	Public Systems, Honeypots, Scanners on network	Public/Private Systems (Sandboxing products...)	Public/Private Systems (Sandboxing products, surveys, underground market places...)	Internal Appliances, Logs, Analysis systems, SIEMS

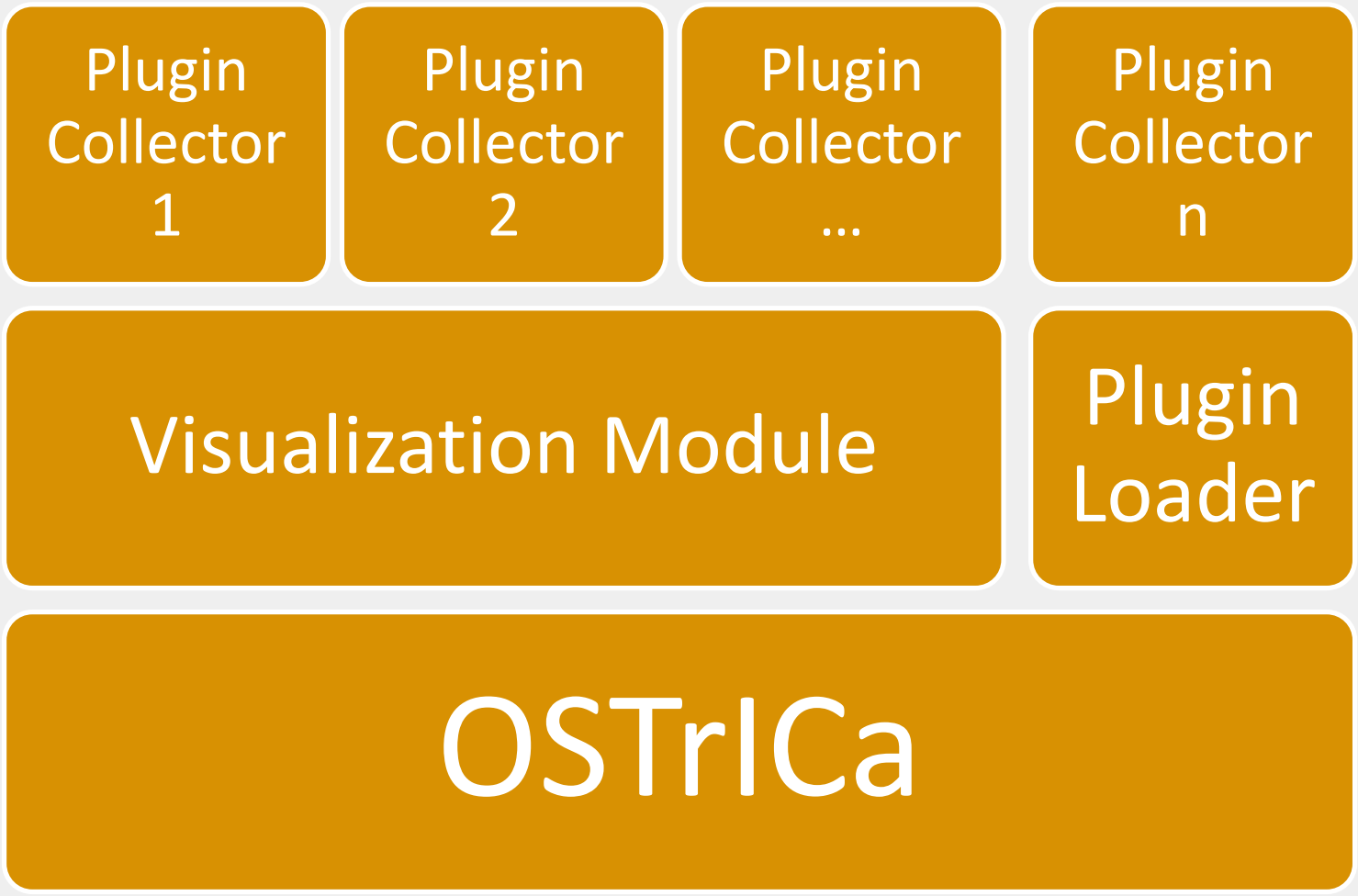
OSTrICa – Open Source Threat Intelligence Collector



What is OSTrICa?

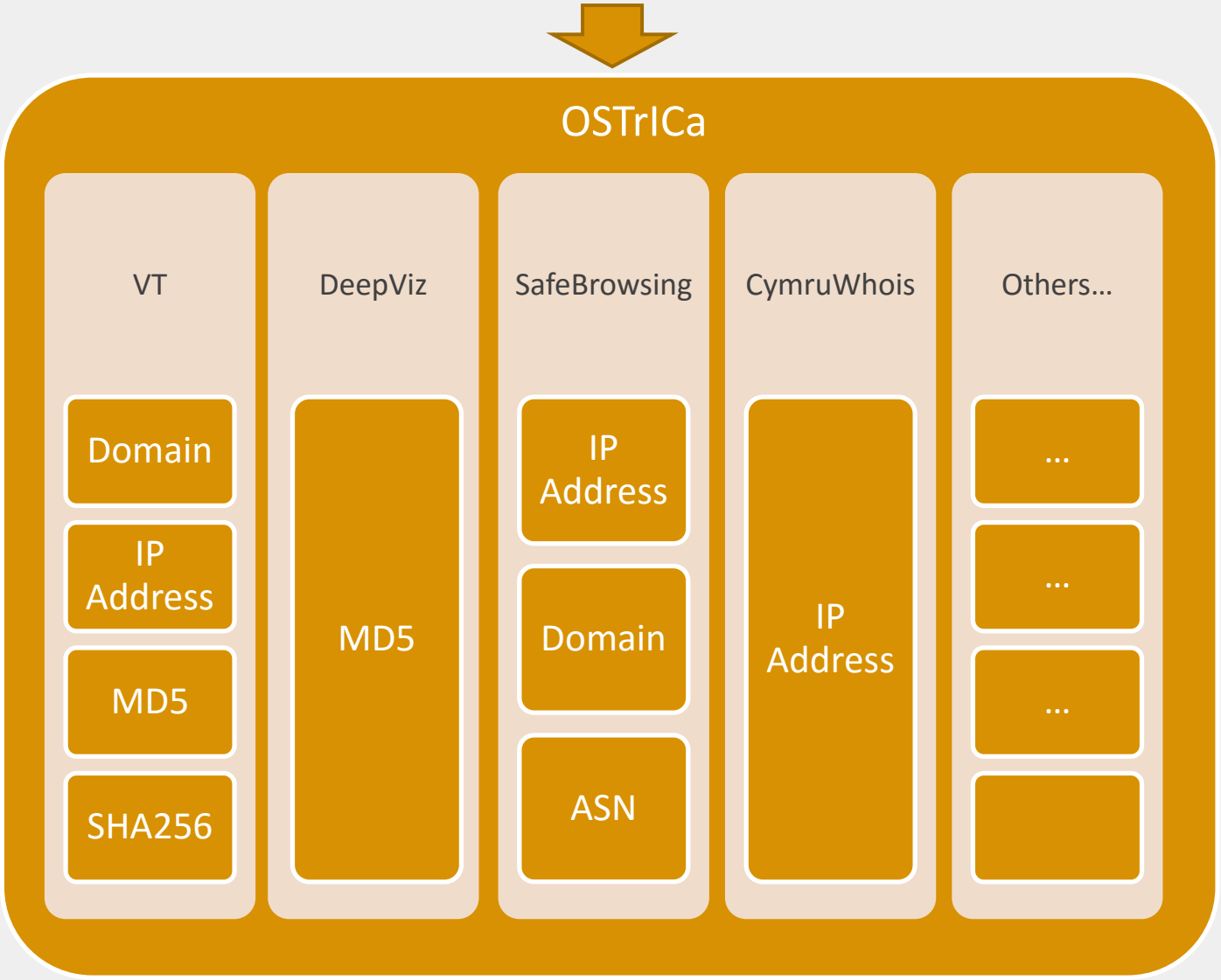
Open Source Threat Intelligence Collector

What is OSTrICa?

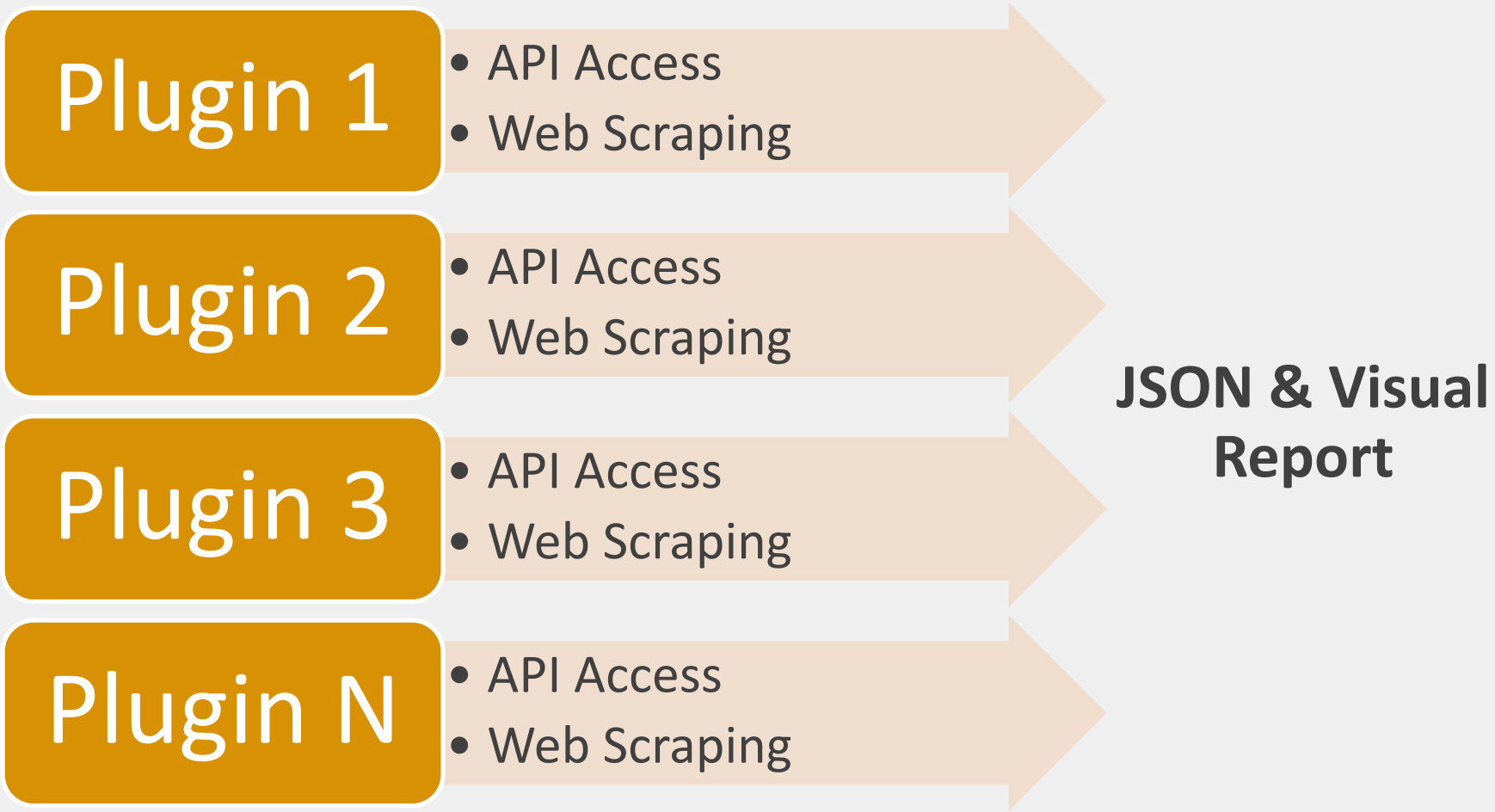


How does OSTrICa work?

747b3fd525de1af0a56985aa29779b86



How do plugins work?



Why OSTrICa?

- It is Free & Open Source (will be released soon on my GitHub page)
- It has a plugin architecture. You can include Free, Commercial and Internal intelligence data
- It allows anyone to create a relevant and accurate threat profile
- It can be used to proactively protect company's information
- It automatically generates:
  - A report in JSON format containing all the collected information
  - A graph allowing the users to link together the information, filter out, hide and search IoCs. End goal is to help SOC Analysts, IR, Attack Investigators

Note: all the collected IoCs have been collected from publicly available sources like VirusTotal, Google SafeBrowsing, etc.

Demo

How to develop OSTrICa Plugins

A quick overview…

Conclusion & Future Works

- It’s Open Source: you can add new features and add new plugins (to extract intelligence from your internal systems). You can download it soon from my GitHub page… Follow me @Ptr32Void for updates
- Add a Timeline
- Weights intelligence and links based on how malicious the collected information could be
- Improve graphic interface
- Add a interactive map containing the location of the threats

Thank you!

Q&A

Roberto Sponchioni
@Ptr32Void