APIs are critical to security people

what I learned trying to discover useful APIs

Motivation for that talk

- Working on Incident Response on a daily base
- Wide variety of tools in use
- Very important data is processed by Security people
- Developing / contribute some open source tools

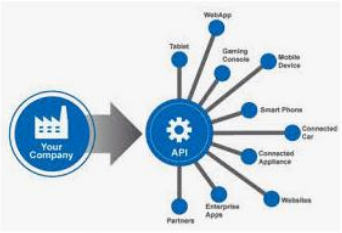
Agenda

- What is an API?
- Why do IR teams need APIs?
- Requirements to an API?
- How I approached it?
- The Good
- The Bad
- The Ugly
- What can you do?

Google api

All Images News Videos Maps More Settings Tools View saved SafeSearch

ancient egypt | integration | machine learning | I ♥ APIs love | digital | honey bee | insect | apis mellifera | arthropoda



API Economy ...
developer.ibm.com

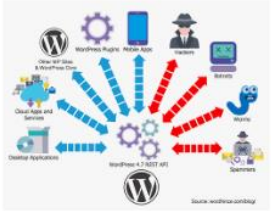
An API-First Development App...
blog.restcase.com

Application Programming Interface ...
goodfirms.co

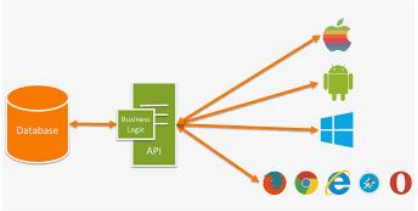
The Problem with APIs – Hac...
hackernoon.com

What is an API? In English, please ...
medium.freecodecamp.org

Google Awareness API | G...
developers.google.com



Wordfence Blocks Username Harve...
wordfence.com

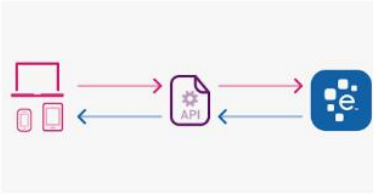


Intro + Easy Integration Tutorials ...
snipcart.com

What is a realtime API? - Realtime API ...
realtimeapi.io

VisibleThread API | Document & Web ...
visiblethread.com

What Is an API?- Prosyscom ...



API | Business Information | Experian UK

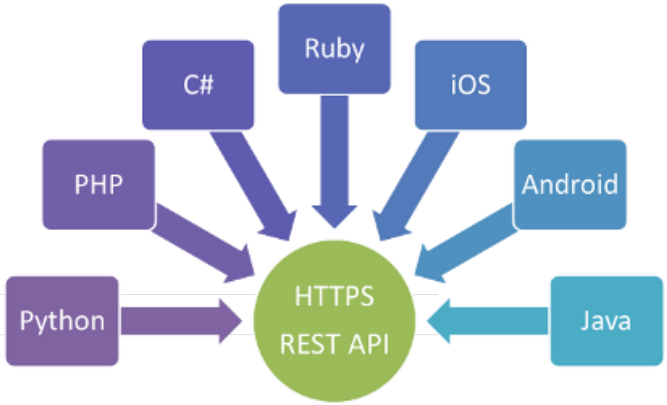
Application Programming I...

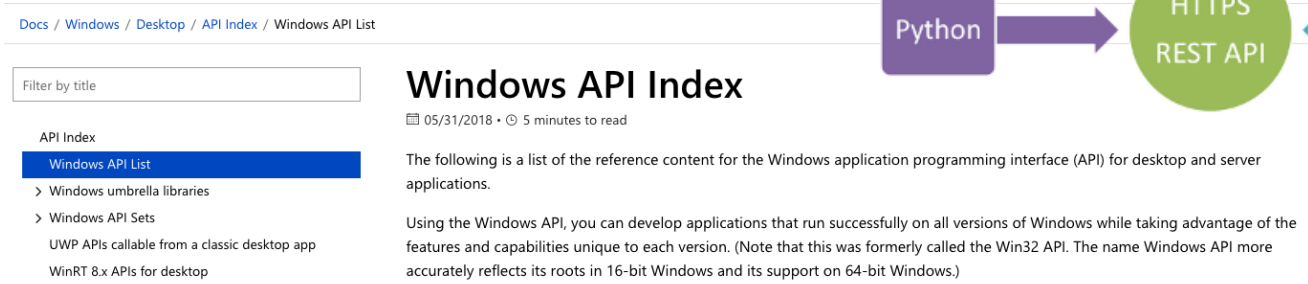
What are Web APIs – Hacker Noon

SDKs | Intel® Software

Types of APIs

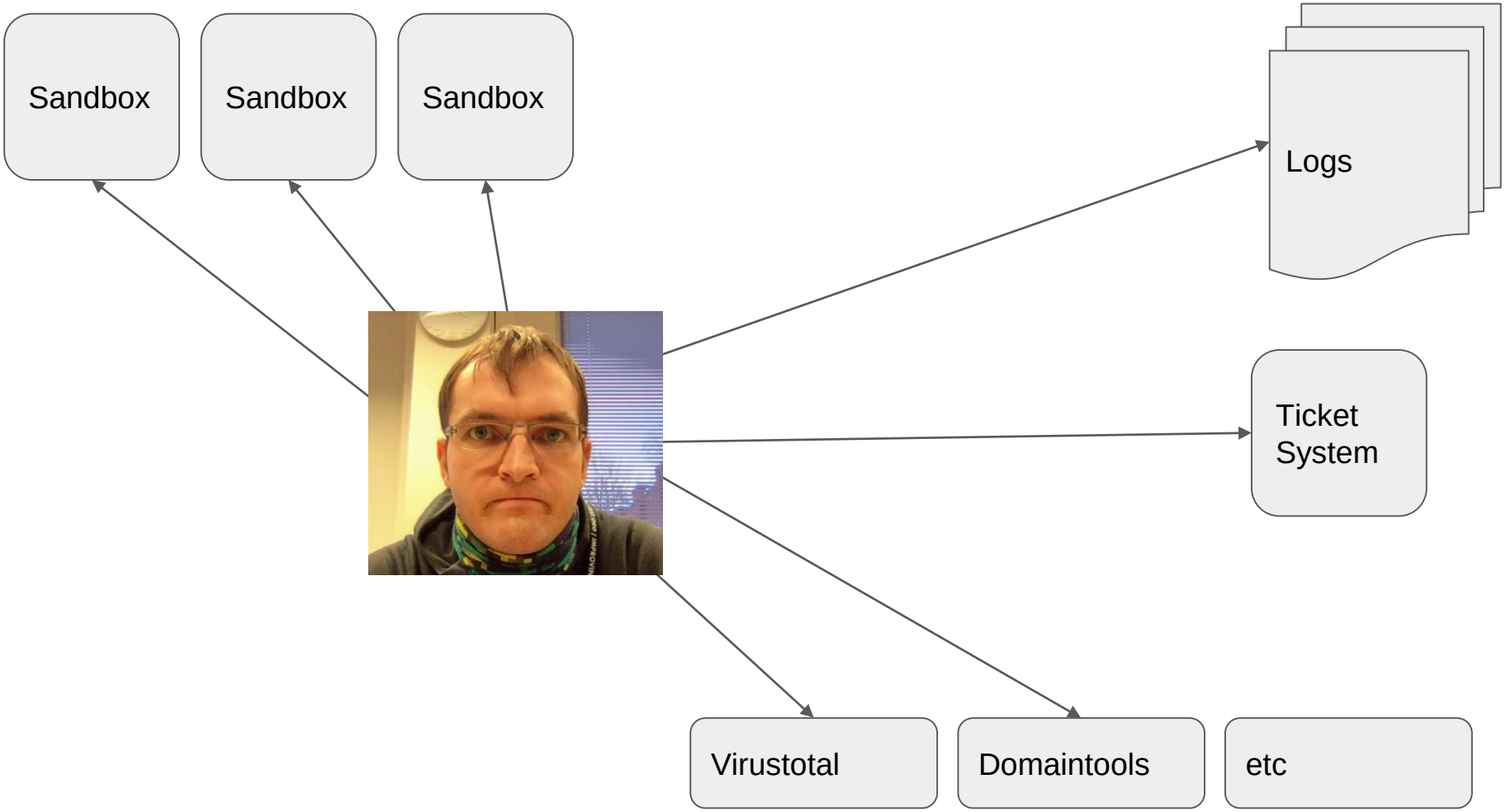
- Libraries
- Operating systems
- Remote APIs
- Web APIs

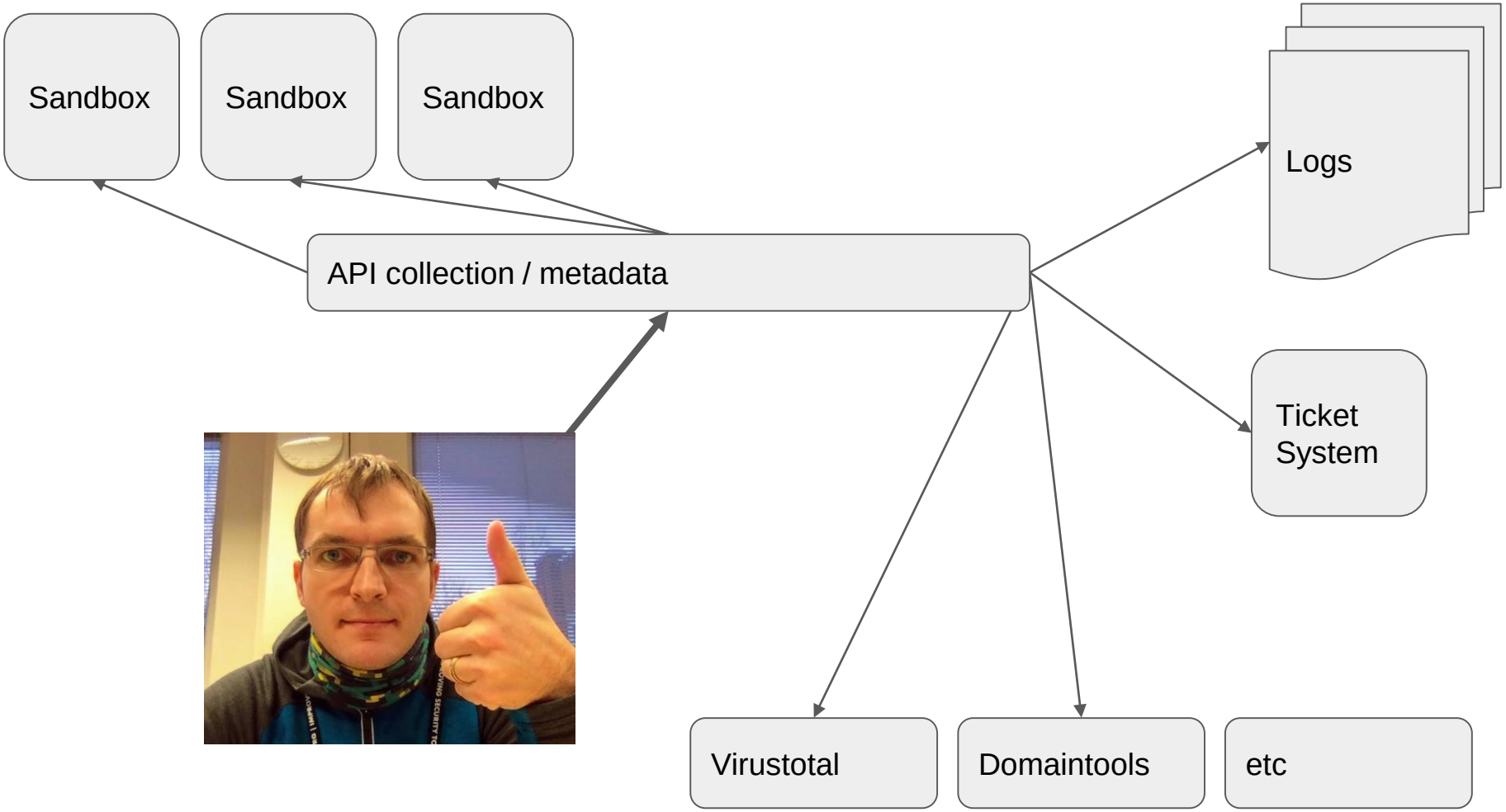




Why do Security people need APIs

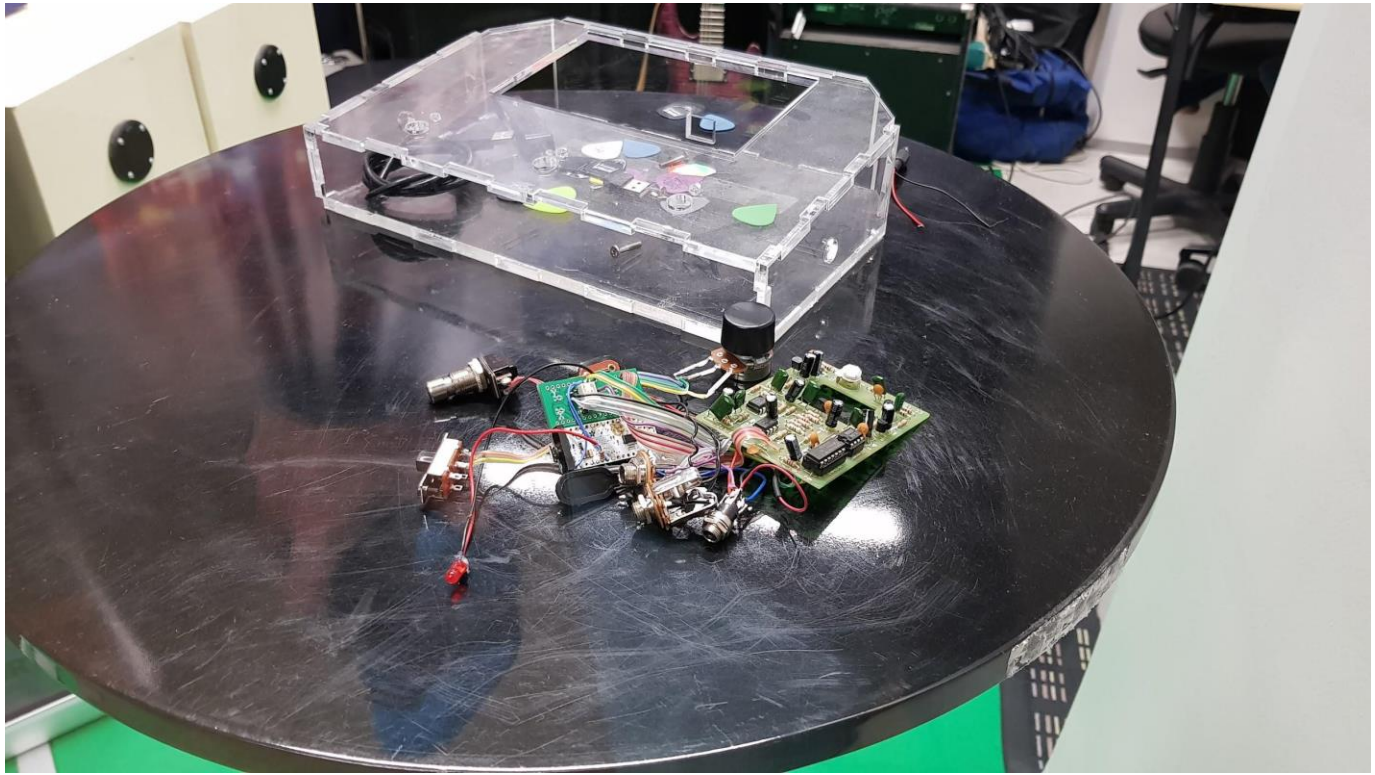
- Cyber requires different sources of information to ...
- Not one tool to rule them all
- Different destinations to prevent badness
- (Interact with Systems / devices)


Sandbox
Sandbox
Sandbox
Logs
Ticket System
Virustotal
Domaintools
etc

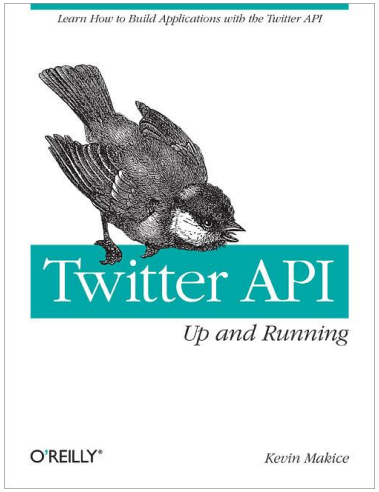

Sandbox
Sandbox
Sandbox
Logs
API collection / metadata
Ticket System
Virustotal
Domaintools
etc

What is a good API?

Availability of API / interfaces

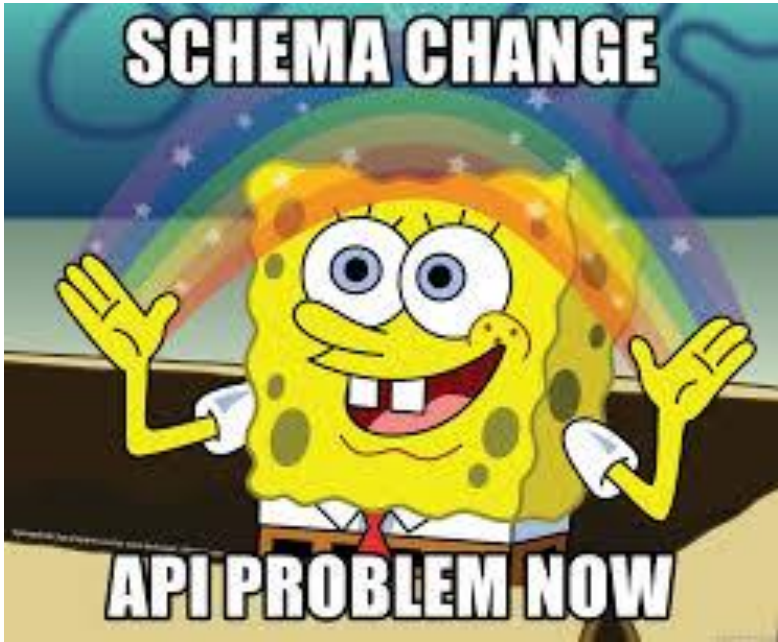


Documentation



Versioned API

Nothing bugs more than an API endpoint change that breaks scripts / workflows



Sample data so people can play

Reference implementation

README

docs passing | build passing | coverage 49%

PyMISP - Python Library to access MISP

PyMISP is a Python library to access MISP platforms via their REST API.

PyMISP allows you to fetch events, add or update events/attributes, add or update samples or search for attributes.

Requirements

- requests

Install from pip

```
pip3 install pymisp
```

Install the latest version from repo

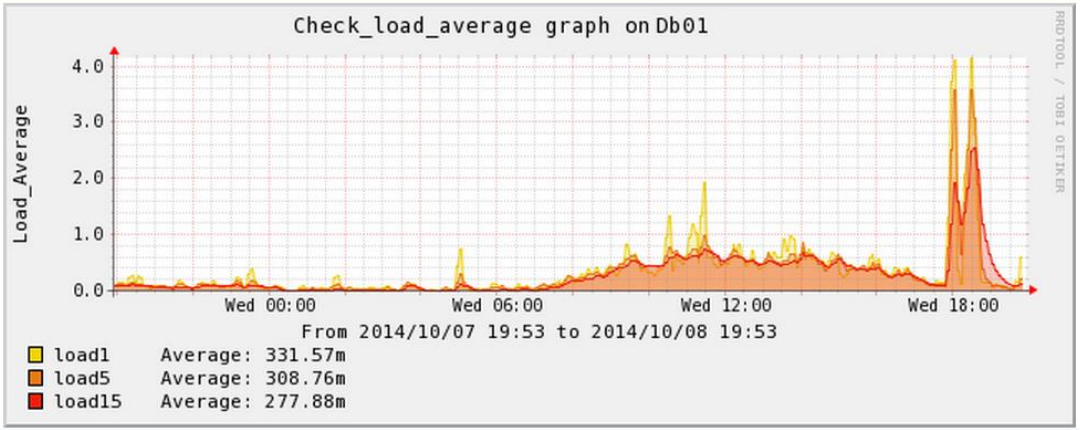
```
git clone https://github.com/MISP/PyMISP.git && cd PyMISP
git submodule update --init
pip3 install -I .[fileobjects,neo,openioc,virustotal]
```

RESTful

Makes it easier for everyone involved

scalable

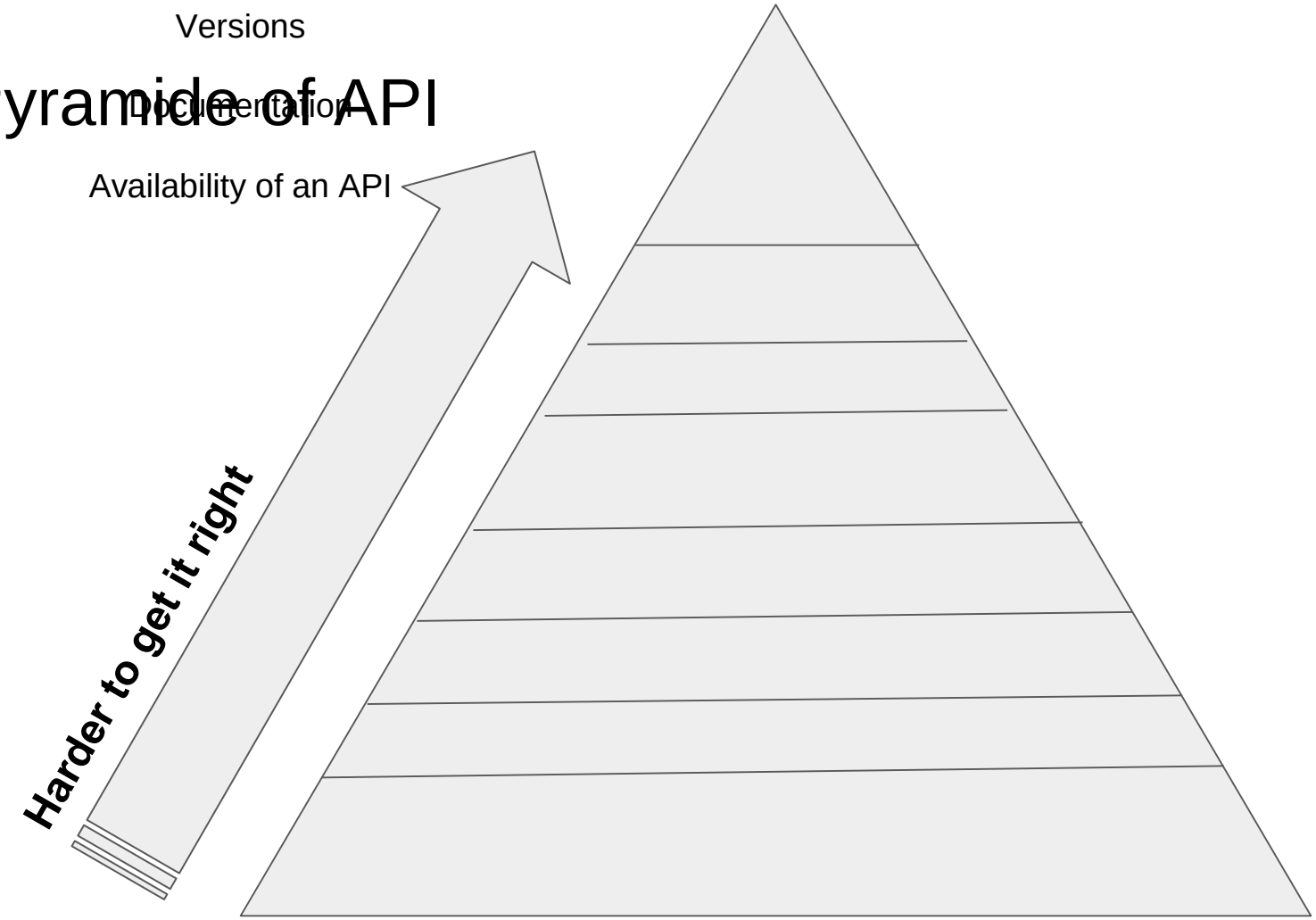
- API needs to grow
- give feedback of implemented rate limiting



Security built in

- encryption
- logging
- authentication

Pyramide of API



How I approached it

- Wrote down every tool I used during a day
- Answered following questions
  - Am I the only one using the tool / database?
  - Does the tool has an API?
  - Where is the API documentation?

The Good

- Virustotal
- Cuckoo
- New Misp API

The Bad (with reasons)

- MISP (old Api)
  - API documented, but not 100 % accurate
  - manual effort to keep it updated
  - no samples for every endpoint available
- Timesketch
  - Api.py available
  - No documentation
  - No examples
  - But: python api wrapper

The Ugly

- Proxy provider had a public facing site
- Used an public facing API
- was discovered and documented
- was used among security people
- silently very hard rate limiting

https://github.com/deralexxx/security-apis

security-apis

A collective list of public JSON APIs for use in security. https://alexanderjaeger.de Learn about REST: https://github.com/marmelab/awesome-rest

Index

Online

API	Description	Auth	HTTPS	Link	Free / Commercial
Apility.IO API	Threat Intelligence Anti-Abuse API	`apiKey`	Yes	Link!	Free
Alexa	Alexa Top Sites	`apiKey`	Yes	Link!	?
Bluecoat Site Review	URL Analysis	`none`	Yes	Link!	Free
bgpmon.net	Bgp monitoring	`?`	Yes	Link!	?
censys.io	Free for Researchers Threat Intel	`apiKey`	Yes	Link!	?

What can you do?

- make it a hard requirement for
  - every commercial security tool you buy
  - every security tool you develop inhouse
  - every security tool you contribute to
- contribute to the github repository
  - tools you developed
  - tools you use
  - other tools
- Open issues for tools you use with the vendor / developer

Q&A

Description

More and more Security tools are introduced in the cyber eco system which increases the complexity dramatically. To combat that - there are basically two ways to scale:

a) go for a “one tool to rule them all” approach
b) make use of APIs and connect them

For the option b the first step is to collect all tools that are available and discover if and what APIs these tools have. During a period of several months, I did that and open sources that list to github (https://github.com/deralexxx/security-apis).

Weaponized with that list, it is easier for security folks to do an inventory of their

Requirements to an API

- documented
  - (available for everyone)
- Examples
  - sample files so it is not mandatory to install tool xyz to write an integration
  - sample implementations to interact with the API
- security built in
  - encryption
  - access control
  - logging what was accessed
  - ...

TODO

API memes