APIs are critical to security

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?
Types of APIs

- Libraries
- Operating systems
- Remote APIs
- Web APIs

Windows API Index

The following is a list of the reference content for the Windows application programming interface (API) for desktop and server applications.

Using the Windows API, you can develop applications that run successfully on all versions of Windows while taking advantage of the features and capabilities unique to each version. (Note that this was formerly called the Win32 API. The name Windows API more accurately reflects its roots in 16-bit Windows and its support on 64-bit Windows.)
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)
What is a good API?
Availability of API / interfaces
Documentation

IN NEED OF TECHNICAL SUPPORT
PLEASE CALL 6203429
Versioned API

Nothing bugs more than an API endpoint change that breaks scripts / workflows
Sample data so people can play
Reference implementation

**README**

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

FACETIME

FACEBOOK

CONTROVERSY

हिंदी में

Cambridge Analytica
Pyramid of API

- Versions
- Documentation
- Availability of an 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


Index

- Online
- Tools
- SIEM
- Various

Online

<table>
<thead>
<tr>
<th>API</th>
<th>Description</th>
<th>Auth</th>
<th>HTTPS</th>
<th>Link</th>
<th>Free / Commercial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apility.IO API</td>
<td>Threat Intelligence Anti-Abuse API</td>
<td>apikey</td>
<td>Yes</td>
<td>Link!</td>
<td>Free</td>
</tr>
<tr>
<td>Alexa</td>
<td>Alexa Top Sites</td>
<td>apikey</td>
<td>Yes</td>
<td>Link!</td>
<td>?</td>
</tr>
<tr>
<td>Blucoat Site Review</td>
<td>URL Analysis</td>
<td>none</td>
<td>Yes</td>
<td>Link!</td>
<td>Free</td>
</tr>
<tr>
<td>bgpmon.net</td>
<td>Bgp monitoring</td>
<td></td>
<td>Yes</td>
<td>Link!</td>
<td>?</td>
</tr>
<tr>
<td>censys.io</td>
<td>Free for Researchers Threat Intel</td>
<td>apikey</td>
<td>Yes</td>
<td>Link!</td>
<td>?</td>
</tr>
</tbody>
</table>
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
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 capabilities as well as requirements for future security tools to
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