October 3, 2018

Operationalizing Automation Standards for Cheaper/Better/Faster Cybersecurity

Borderless Cyber USA 2018

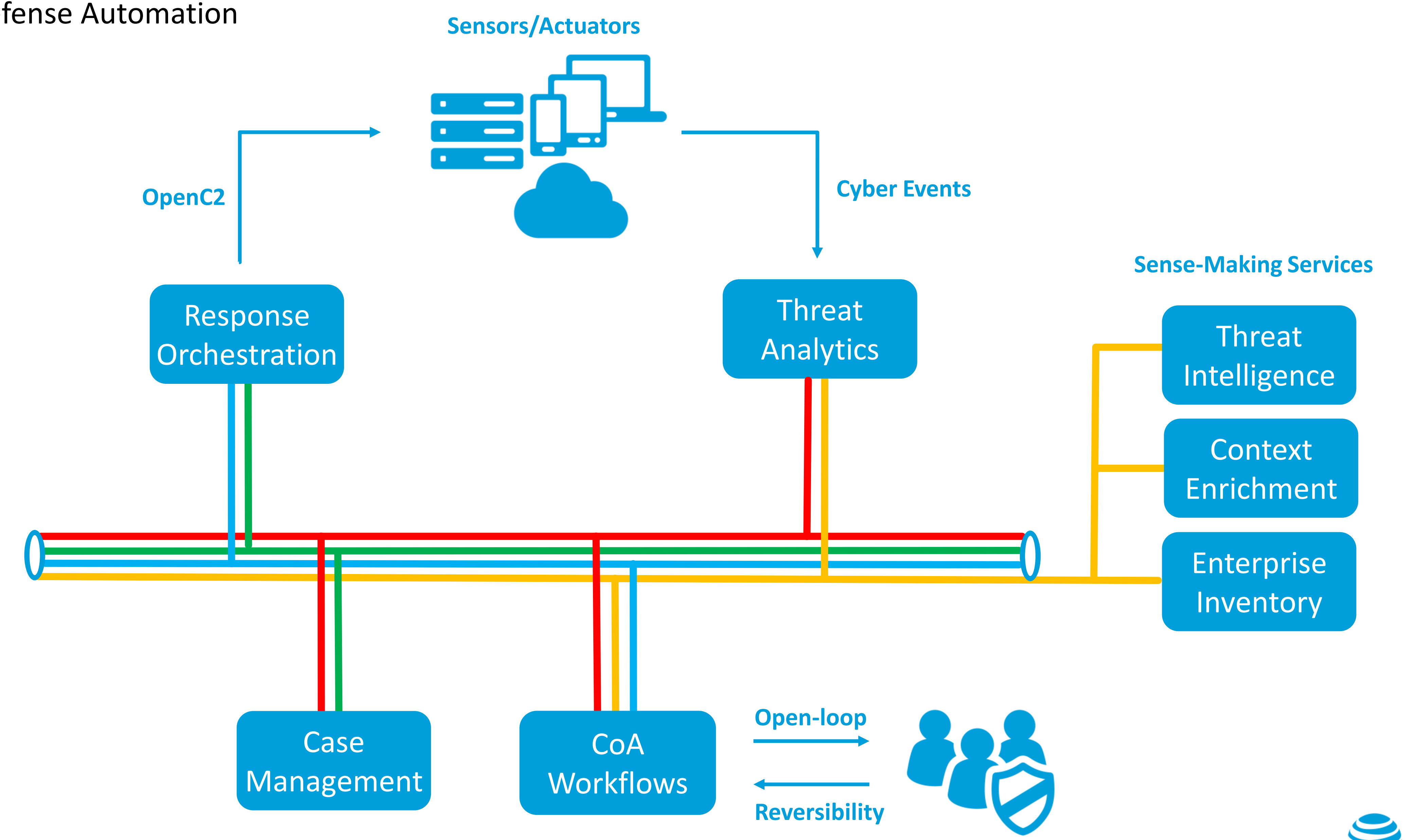
Michael Stair

Lead Member of Technical Staff

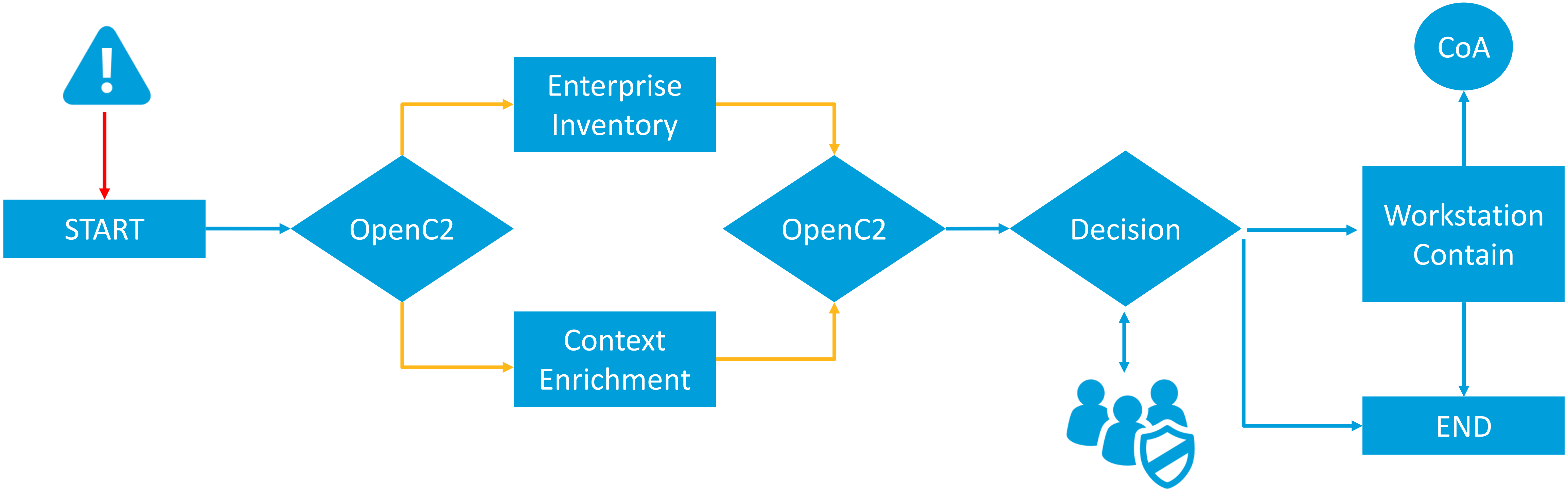
AT&T Chief Security Office

© 2018 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.

Cyber Defense Automation



Malware Containment Workflow



AT&T OpenC2 Open Source

OpenC2-Lycan

- Python/Java libraries to translate OpenC2 messages to/from language objects
- Currently supports OpenC2 CSD04 Language specification
- MIT license
- OASIS Github
    - https://github.com/oasis-open/openc2-lycan-python
    - https://github.com/oasis-open/openc2-lycan-java

OpenC2-AWS

- Manage AWS NACL/Security Groups over OpenC2
- BSD license
- AT&T Github
    - https://github.com/att/openc2-aws

ybersecurity

Philip Royer

Security Analyst

Phantom

NEW CONTEXT

New Context protects data and the movement of data in highly regulated industries

VISION

Keeping the connected world **safe**

MISSION

To use Lean Security to automate the orchestration, governance and protection of critical infrastructure

CALIFORNIA ENERGY SYSTEMS FOR THE 21ST CENTURY

Research program to explore machine to machine automated response for Industrial Control Systems (ICS) cybersecurity.

New Context task was to deliver a normalized standard/language for machines and humans.

U.S. DEPARTMENT OF ENERGY

Lawrence Livermore National Laboratory

PG&E Pacific Gas and Electric Company®

NEW CONTEXT

SDGE A Sempra Energy utility®

SOUTHERN CALIFORNIA EDISON®
An EDISON INTERNATIONAL® Company

INL Idaho National Laboratory

OpenC2

STIX™

CLOSING THE RESPONSE GAP WITH OpenC2

- Provide immediate action

  Change control approval can be too long or manual

  Manual may also be inaccurate, e.g. typos, or mistaken target

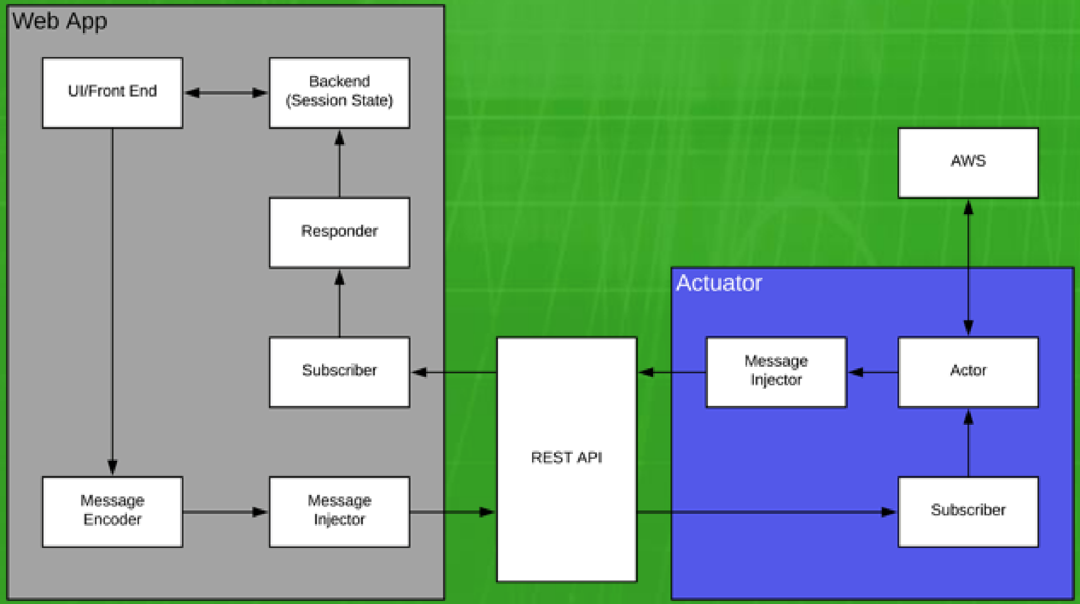
- Standardize among vendors

  Same command for all products in a class

  Environments with different devices can respond to same command

- Integration into SOC

  Leverage existing Cyber Threat Intel for smarter response



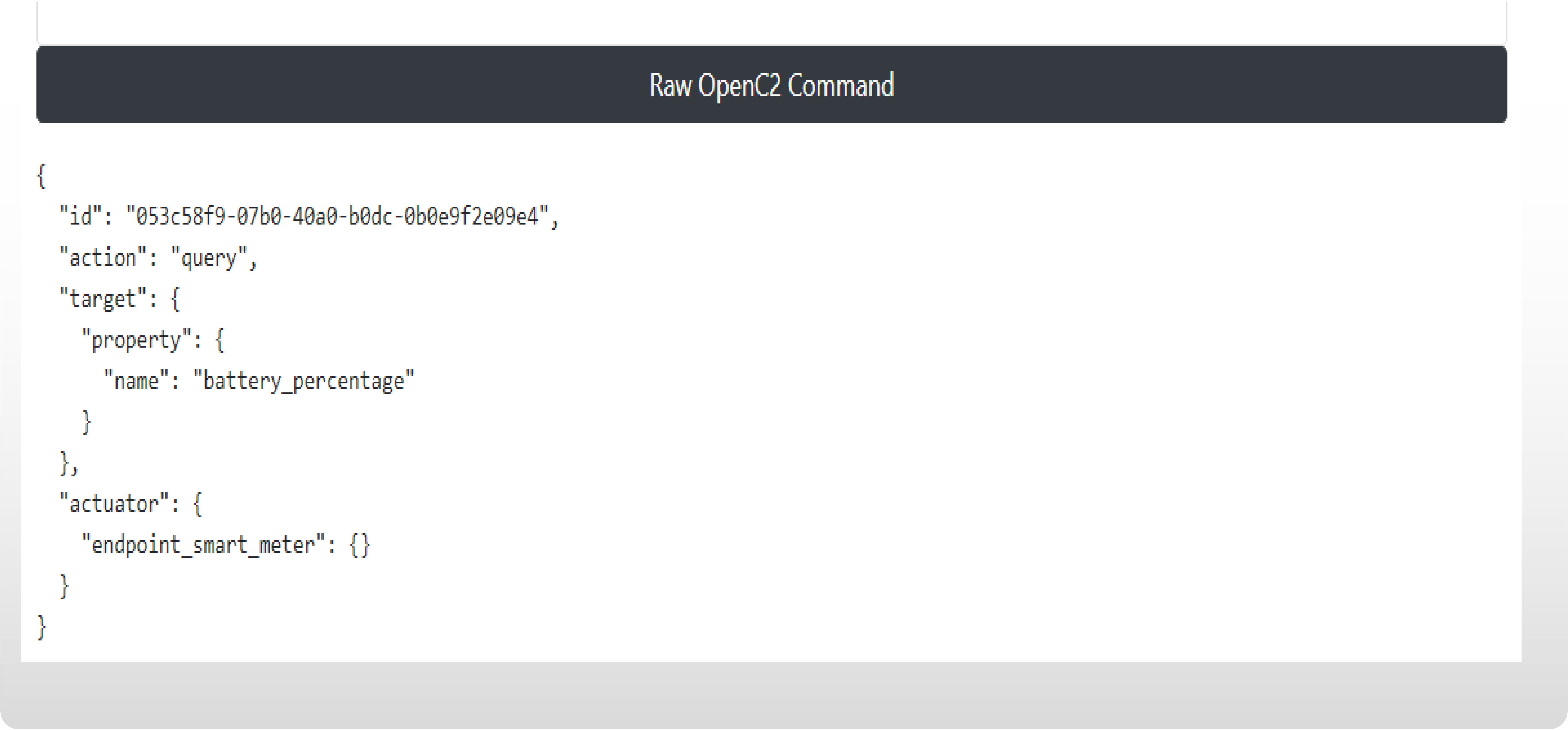
Openc2 Command Generator

By Efrain Ortiz, CISSP

Director, CTO Office

Symantec

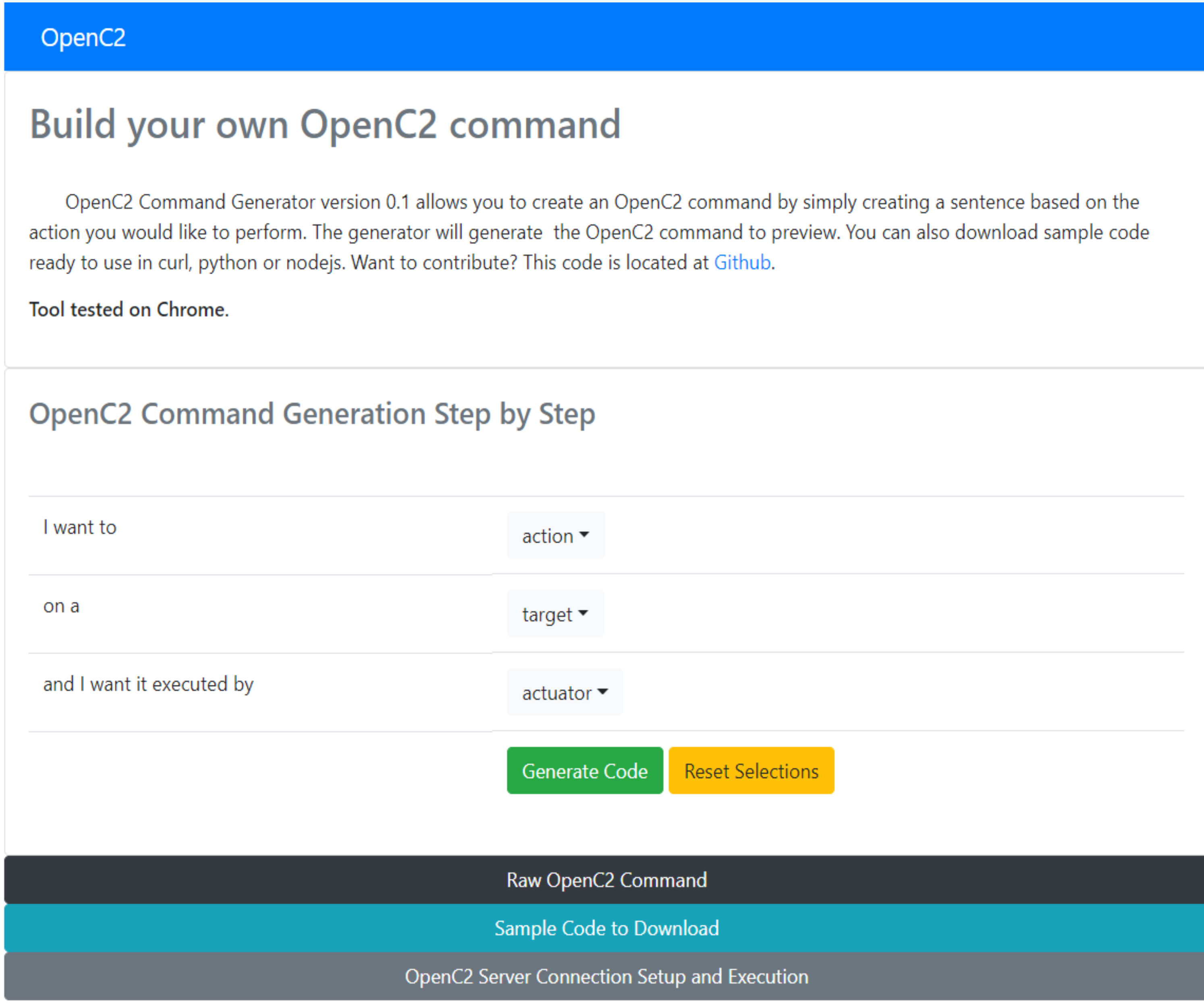
Raw OpenC2 Command Dropdown



```
{
  "id": "053c58f9-07b0-40a0-b0dc-0b0e9f2e09e4",
  "action": "query",
  "target": {
    "property": {
      "name": "battery_percentage"
    }
  },
  "actuator": {
    "endpoint_smart_meter": {}
  }
}
```

Openc2-universal-frontend

- Responsive Web Design
- Located at https://www.github.com/netcoredor/openc2-universal-frontend
- Uses Javascript, Jquery, Bootstrap, Popper, Font awesome on client side
- Used NodeJs on backend



Build your own OpenC2 command

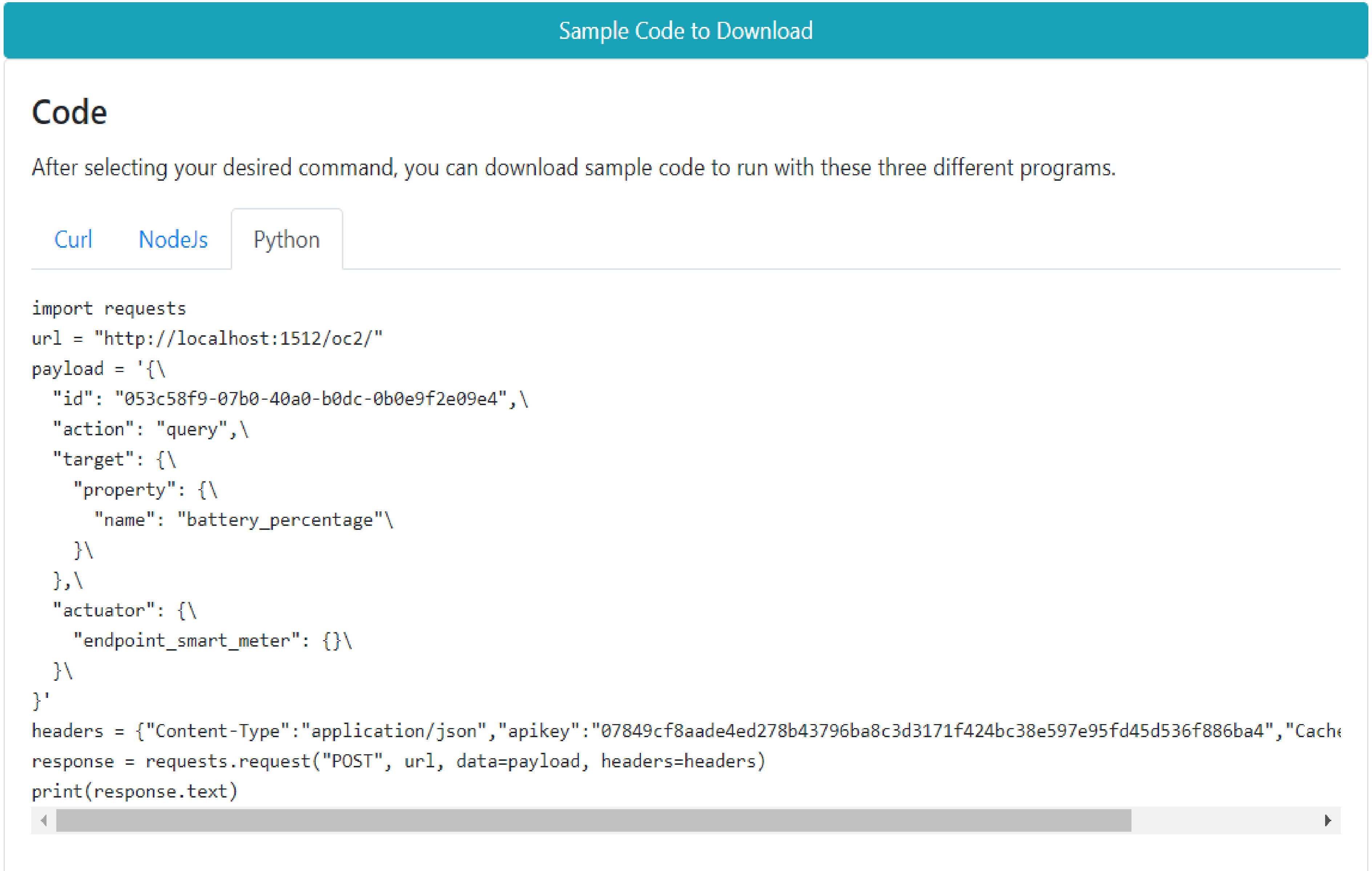
OpenC2 Command Generator version 0.1 allows you to create an OpenC2 command by simply creating a sentence based on the action you would like to perform. The generator will generate the OpenC2 command to preview. You can also download sample code ready to use in curl, python or nodejs. Want to contribute? This code is located at Github.

Tool tested on Chrome.

OpenC2 Command Generation Step by Step

I want to	action ▾
on a	target ▾
and I want it executed by	actuator ▾

“Sample Code to Download” Button



Code

After selecting your desired command, you can download sample code to run with these three different programs.

```
import requests
url = "http://localhost:1512/oc2/"
payload = '{\
  "id": "053c58f9-07b0-40a0-b0dc-0b0e9f2e09e4",\
  "action": "query",\
  "target": {\
    "property": {\
      "name": "battery_percentage"\
    }\
  },\
  "actuator": {\
    "endpoint_smart_meter": {}\
  }\
}'
headers = {"Content-Type":"application/json","apikey":"07849cf8aade4ed278b43796ba8c3d3171f424bc38e597e95fd45d536f886ba4","Cache
response = requests.request("POST", url, data=payload, headers=headers)
print(response.text)
```

Questions?

Copyright © 2017 Symantec Corporation