Operationalizing Automation Standards for Cheaper/Better/Faster Cybersecurity

Borderless Cyber USA 2018

Michael Stair
Lead Member of Technical Staff
AT&T Chief Security Office
Operationalizing Automation Standards for Cheaper/Better/Faster Cybersecurity

Cyber Defense Automation

- OpenC2
- Cyber Events
- Sensors/Actuators
- Threat Intelligence
- Context Enrichment
- Enterprise Inventory
- Sense-Making Services
- Threat Analytics
- CoA Workflows
- Reversibility
- Open-loop
- Case Management
- Workflows
- Context Enrichment
- Open-loop
- Reversibility
Malware Containment Workflow

START

OpenC2

Enterprise Inventory

Context Enrichment

OpenC2

Decision

Workstation Contain

CoA

END
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
Philip Royer
Security Analyst
Phantom
MISSION
To use Lean Security to automate the orchestration, governance and protection of critical infrastructure

VISION
Keeping the connected world safe

NEW CONTEXT
New Context protects data and the movement of data in highly regulated industries
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.
- **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
{  
"id": "05c58f9-07b0-40a0-b0dc-0b0e9f2e09e4",  
"action": "query",  
"target": {  
  "property": {  
    "name": "battery_percentage"  
  }  
},  
"actuator": {  
  "endpoint_smart_meter": {}  
}  
}
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
Code

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

Curl  Node.js  Python

```python
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-Control":null}
response = requests.request("POST", url, data=payload, headers=headers)
print(response.text)
```
Questions?