



KYPO Cyber Range Platform

Daniel Tovarňák

CSIRT-MU



KYPO History

- 1st Gen, since ~2014
 - Funded by Ministry of Interior, Czech Republic
 - Minister of the Interior Award for Excellent Results (2016)
 - First national cyber-exercise with Czech NCISA
 - OpenNebula
 - 2nd Gen, since ~2016
 - Funded by Ministry of Interior, Czech Republic
 - Additional (~8) national and international exercises
 - Exercises and trainings for partners managing critical infrastructures
 - OpenNebula
-

KYPO CRP Today

- 3rd Gen, since ~2018
 - Funded by Ministry of Interior, Czech Republic
 - Planned to be released as open-source
 - Lectures and courses at MUNI
 - OpenStack

 - CONCORDIA
 - Helps to speed up the open-sourcing process
 - Open-sourcing Topology Definition to promote tools interoperability (Federation/Integration)
 - Provides platform for EU-wide dissemination
-

Technologies

- **OpenStack** (cloud provider, network emulation)
 - Python, **Django Rest Framework**; Java, **Spring Boot** (backend – micro-services)
 - **Angular 10** (frontend)
 - **Ansible** (sandbox provisioning)
 - **Docker** (deployment, complex async tasks)
 - **Redis** (task queue)
 - **OpenID Connect** – OIDC (authentication)
 - **Elasticsearch** (event store)
-

Sandbox Service (Core Service)

1. Network topology instantiation
2. Network configuration provisioning
3. Sandbox provisioning

```
1 name: small-sandbox
2
3 provider: OpenStack
4
5 hosts:
6   - name: server
7     base_box:
8       image: debian-9-x86_64
9       man_user: debian
10      flavor: csirtmu.tiny1x2
11      hidden: True
12
13   - name: home
14     base_box:
15       image: debian-9-x86_64
16       man_user: debian
17     flavor: csirtmu.tiny1x2
```

```
75 - name: install MySQL
76   become: yes
77   hosts:
78     - routers
79   tasks:
80     - include_role:
81       name: mysql
82     vars:
83       mysql_database_scripts: files/tables.sql
84       mysql_user_name: cowrie
85       mysql_user_password: PASSWORD HERE
86       mysql_database_name: cowrie
87       mysql_user_privileges:
88         - cowrie.*:ALL
89       mysql_remote_host_ip: '%'
90
91 - name: install DefenceStrategy
92   become: yes
93   hosts:
94     - routers
95   tasks:
96     - include_role:
97       name: DefenceStrategy
```

Demo

- *Training Run*
 - Sandbox Definition Details
 - Pool Creation
 - Sandbox Allocation
 - Import/Creation of Training Definition
 - Training Instance Creation
 - Post-training Analysis
-

Summary

- KYPO uses OpenStack and it is a 3rd generation of CRP at MUNI
 - KYPO CRP is used during courses and lectures at MUNI
 - Public release of open-source is planned for Q4/2020
 - It is possible to create trainings and CTF games (and Sandboxes)
 - The potenial is in the CONTENT and ECOSYSTEM
 - Do you want to join early adopters? Let us know at info@kypo.cz
-

Contact

Research Institute CODE
Carl-Wery-Straße 22
81739 Munich
Germany

contact@concordia-h2020.eu

Follow us



www.concordia-h2020.eu



www.twitter.com/concordiah2020



www.facebook.com/concordia.eu



www.linkedin.com/in/concordia-h2020
