KubeCon | CloudNativeCon

Europe 2022

WELCOME TO VALENCIA

KubeCon CloudNativeCon Europe 2022

Scaling and Orchestrating “Good Bot” with Kubernetes

Aris Cahyadi Risdianto
National University of Singapore (NUS)

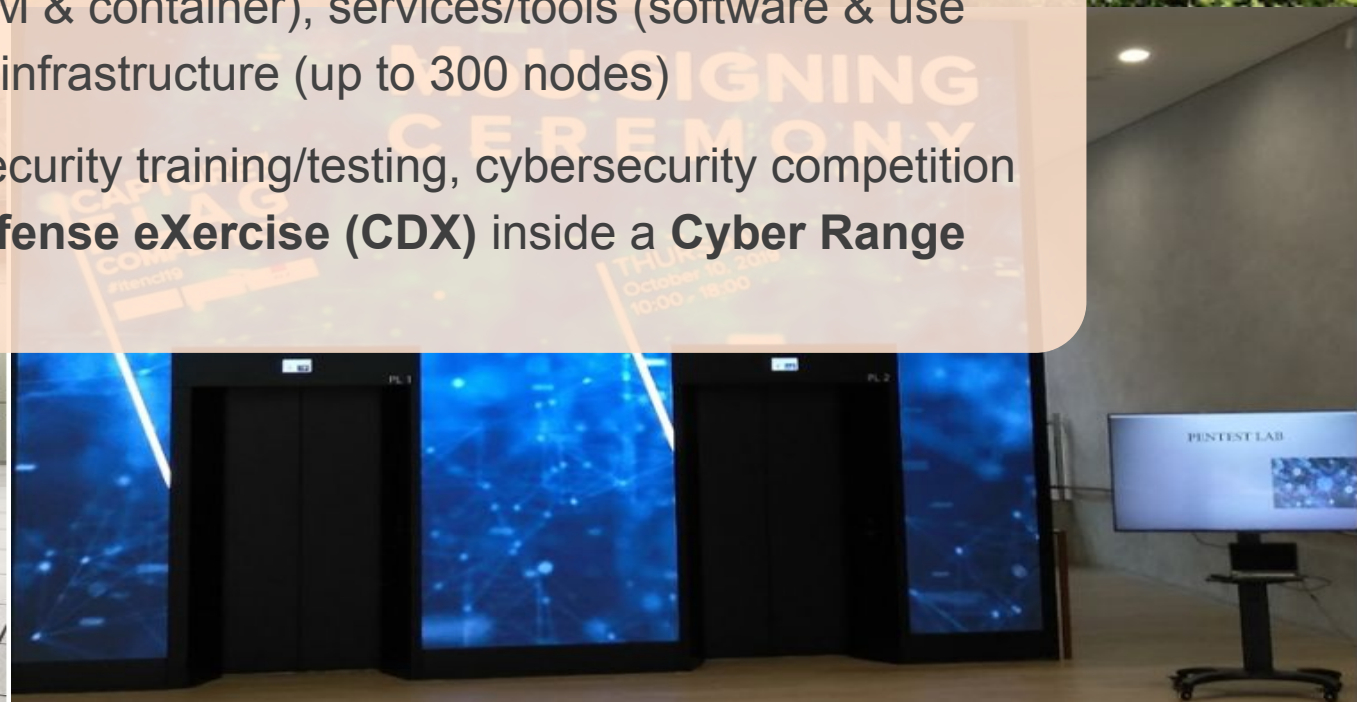
Thursday, May 19th 2022
Feria Valencia - Spain

National Cybersecurity Research and Development Lab (NCL)

National Lab funded by Singapore NRF followed by CSA since 2015 to support industries, government agencies and academia

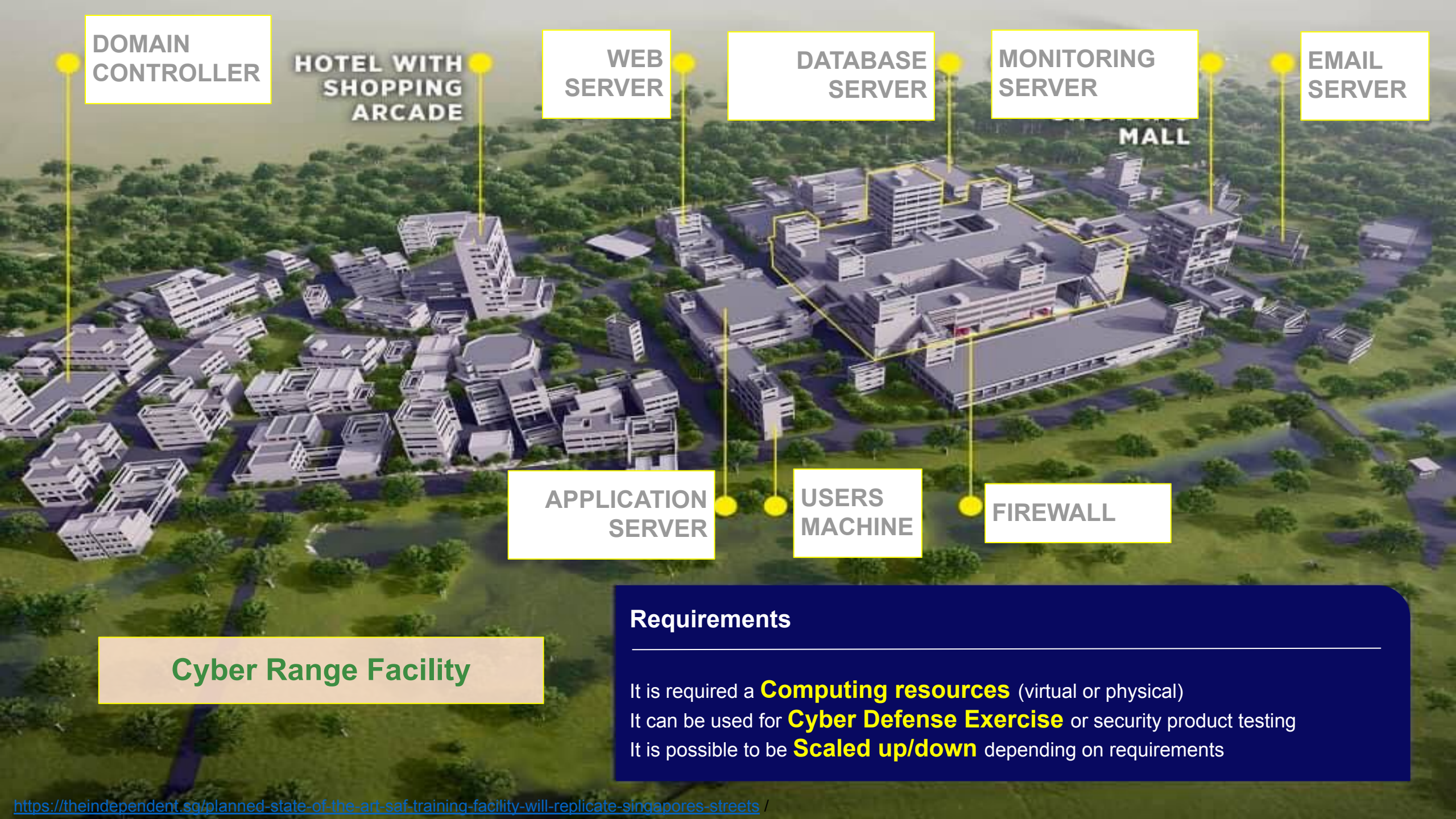
NCL provides virtual environment (VM & container), services/tools (software & use cases) and computing infrastructure (up to 300 nodes)

NCL support multiple activities: cybersecurity training/testing, cybersecurity competition (CTF) and plan to support **Cyber Defense eXercise (CDX)** inside a **Cyber Range**



SAFTI (SAF Training Facility)

https://theindependent.sg/planned-state-of-the-art-saf-training-facility-will-replicate-singapores-streets /



Cyber Range Facility

Requirements

It is required a **Computing resources** (virtual or physical)
It can be used for **Cyber Defense Exercise** or security product testing
It is possible to be **Scaled up/down** depending on requirements

https://theindependent.sg/planned-state-of-the-art-saf-training-facility-will-replicate-singapores-streets /

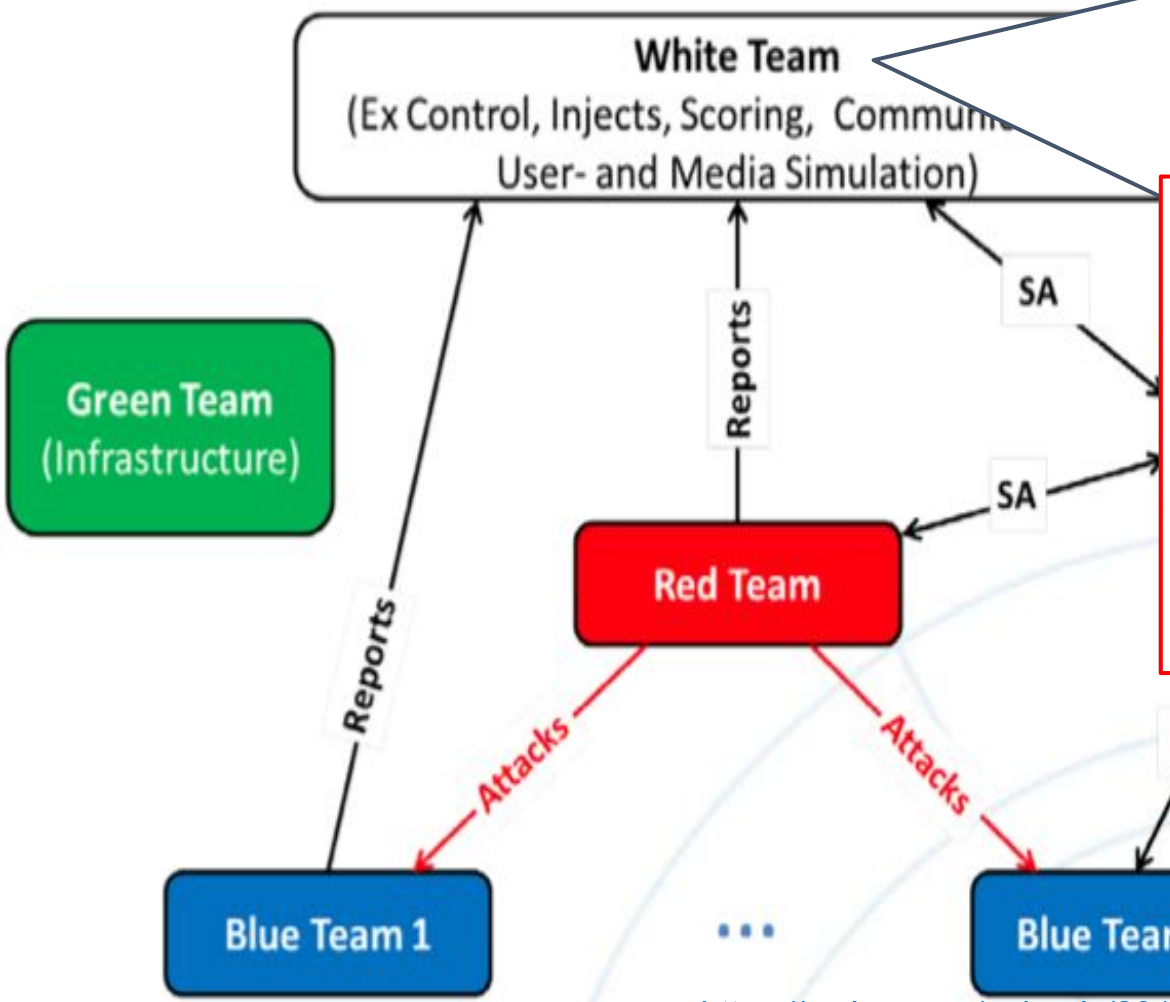
Military Defense Exercise

https://www.chinadailyhk.com/article/164117

Cyber Defense Exercise (CDX)

https://www.chinadailyhk.com/article/164117

CDX Team Roles



1. **Controlling** the exercise and Red Team campaign. White Team must have a close cooperation with the Red Team. White Team decides when different phases start and stop, when the Red Teams have to wait or slow down their activities.
2. **Evaluating** the progress of the Blue and Red Teams and assigning manual scores. White Team has to evaluate the reports about successful compromises issued by the Red Team which will result in negative score. Successful detection of attacks described in incident reports, ability to respond to business injects, new creative ideas how to defend and collaborate with other Blue teams will give positive score.
3. Liaisoning with the Blue Teams.
4. Simulating the activities of Blue Team organization's **clients**. For instance, clients could request to get new services or complain over the quality of the services.
5. Simulating the **management** and the **users** of the organizations which networks the Blue Teams are defending.
   - Firstly, White Team will inject the Blue's different **business tasks** such as install new application to user's desktops, set up a new public service or provide the boss remote access to the file server.
   - Secondly, White Team members simulate the actions of **ordinary users** of Blue Team organizations by browsing the (game) internet, opening e-mail attachments, sending complaints. The also have to do selective checks on Blue Team systems to detect changes in functionality that may be not detected by the automatic scoring system.
6. Simulating the **Media**. For instance, injecting news stories and acting as contacting the Blue Teams as journalist.

https://ccdcoe.org/uploads/2018/10/LockedShields13_AAR.pdf

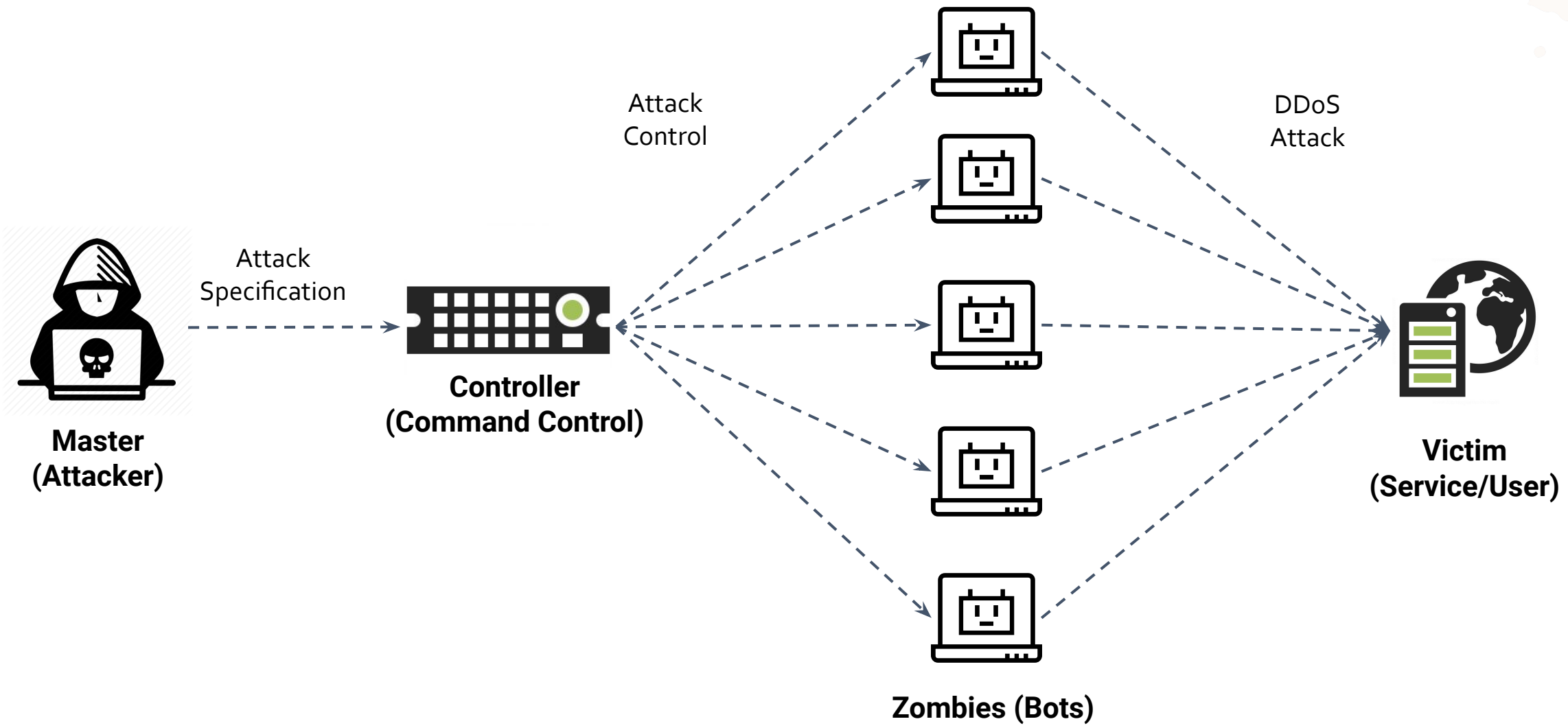
Background and Motivation

Normal traffic is required to hide the attacking traffic during exercise, so that is not too trivial for intrusion detection systems to detect attacks and exploitation

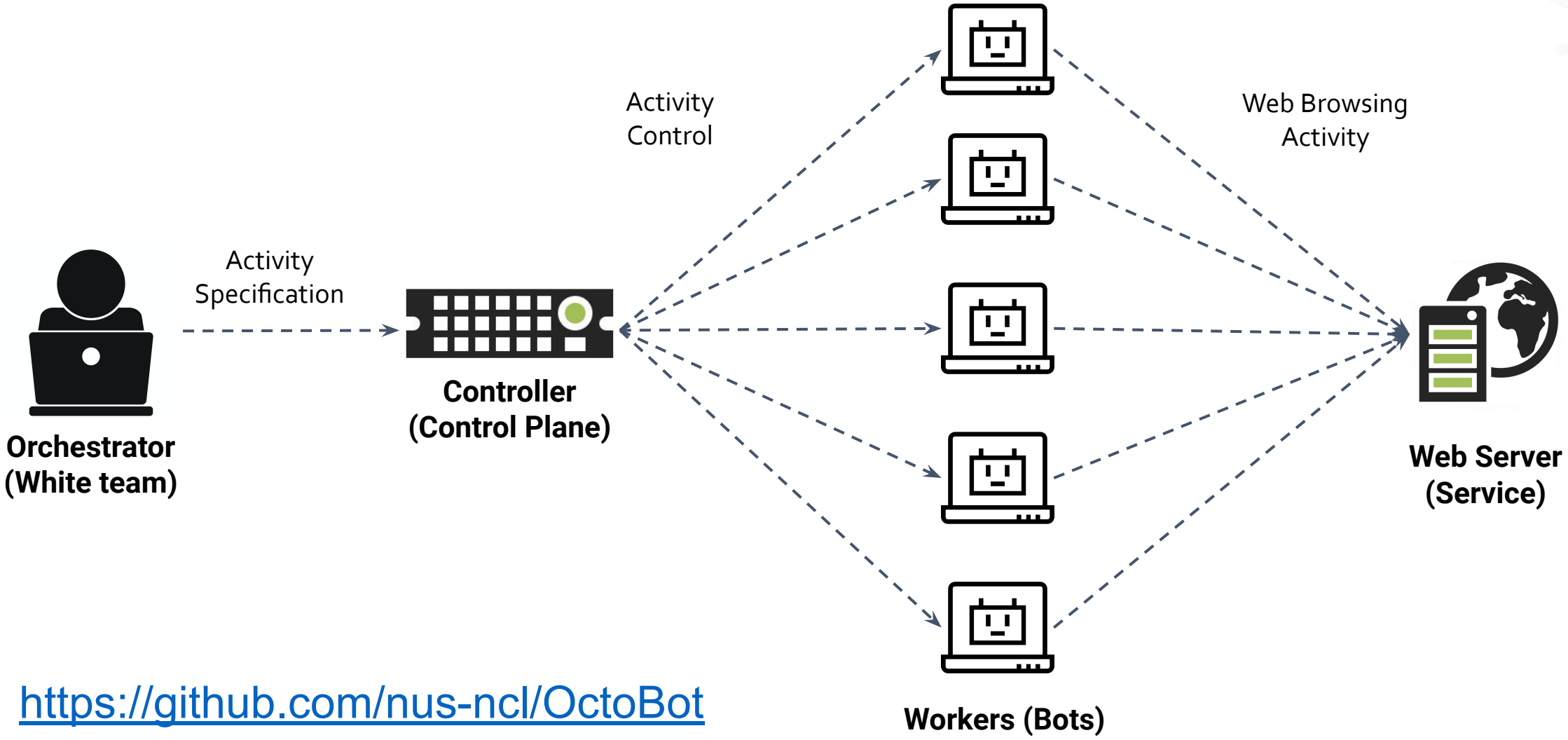
Traffic generation by human is not scalable and efficient as the scenarios may change continuously or the size of the exercise needs to be scaled up/down very quickly

It is required to generate realistic traffic incorporating a varsity of user behavior models to mimic complex user activities, but it should be easy-to-control to generate scalable and high-quality normal traffic based on the specification

BotNet = Bad Bot



OctoBot = Good Bot



https://github.com/nus-ncl/OctoBot

Requirements and Solutions

Modular implementation: independents components for different system users/purposes.

Automated provisioning and orchestration: faster and efficient centralized controller/worker provisioning and bot orchestration

Scaling and mobility: scheduled or interactive process to change bot's number and task and to move bot across nodes.

Open integration: users, developers, or researchers can contribute to the verification and development of the bot or orchestrator

- Multiple component in a **single software repository** with containerized bot in different programming languages
- **Ansible** used to provision controller and worker of Kubernetes cluster, and **Kubernetes API (deployment, pod, ...)** for bot orchestration
- Simple **interactive CLI prompt** and **customized API server** to scale bots /activities and to move them around based on the experiment scenarios
- All components **leverage open-source software** and the codes are available **online in GitHub**, and the bot can be **developed independently** by different users

Supported Type of Activities

Generic web browsing activity

Javascript-enabled web browsing activity

Customized web browsing activity for Healthcare informatics application (e.g., authentication, medical record submission, …)

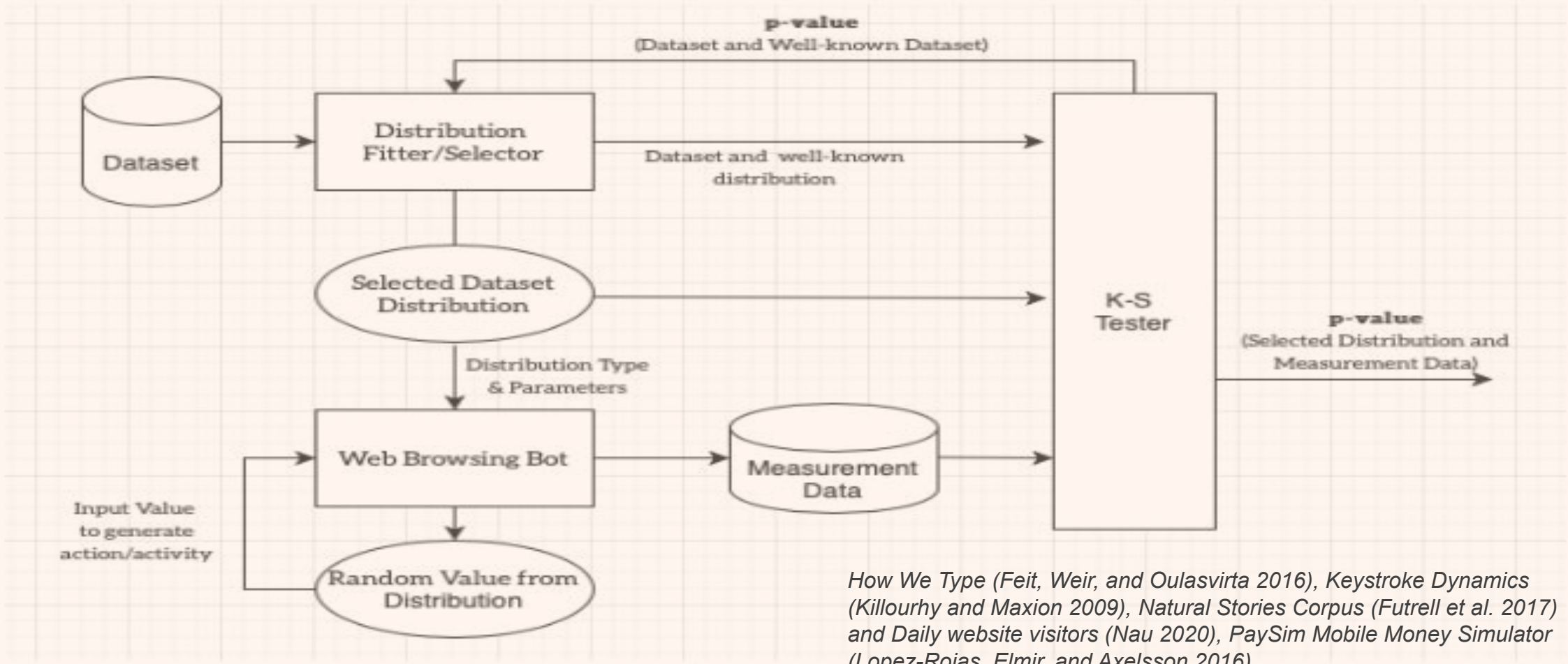
Customized registration activity for Healthcare informatics application

Customized packet-based activity generation

File transfer activity using secure shell

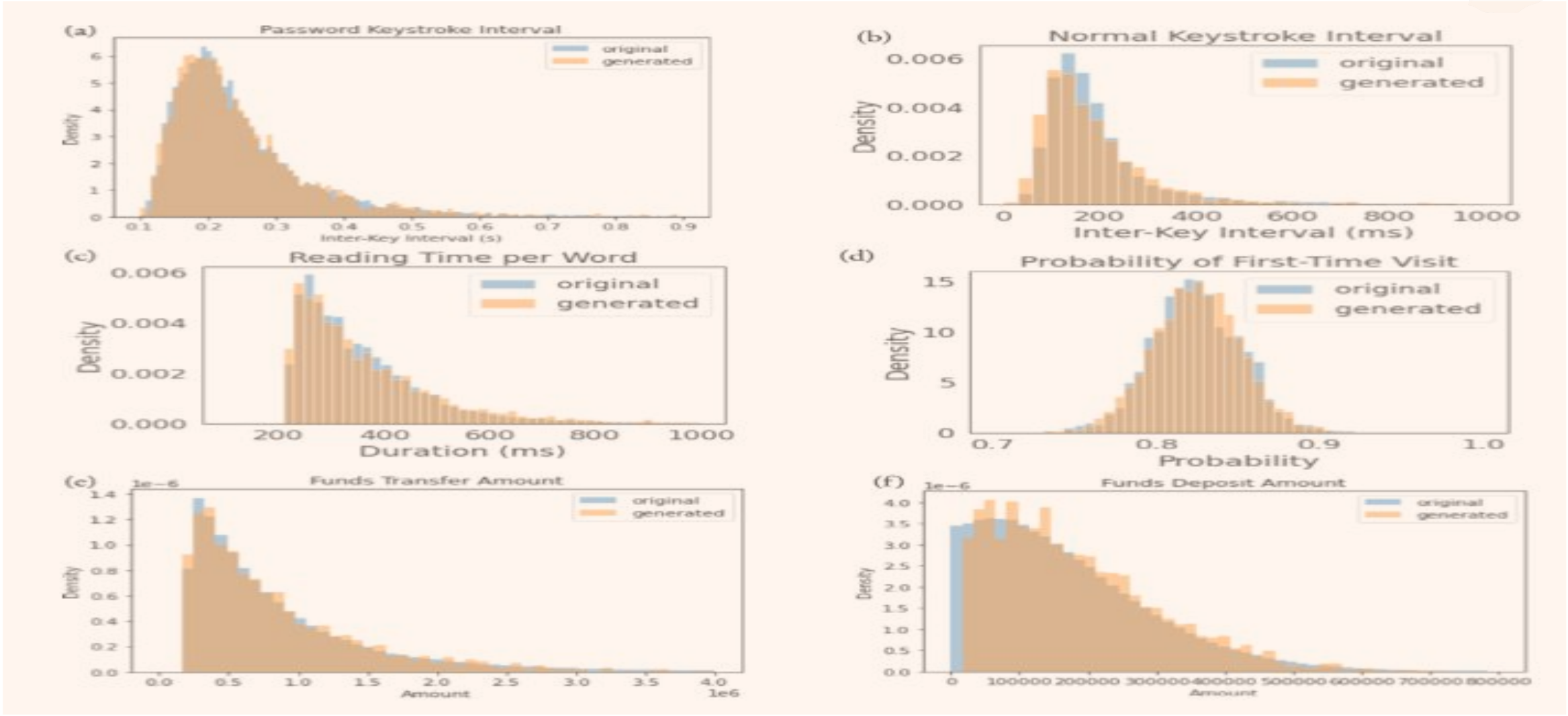
Customized web browsing activity for banking web application

Human-behave Bot Development



How We Type (Feit, Weir, and Oulasvirta 2016), Keystroke Dynamics (Killourhy and Maxion 2009), Natural Stories Corpus (Futrell et al. 2017) and Daily website visitors (Nau 2020), PaySim Mobile Money Simulator (Lopez-Rojas, Elmir, and Axelsson 2016).

Human-behave Bot Development



Testing and Deployment

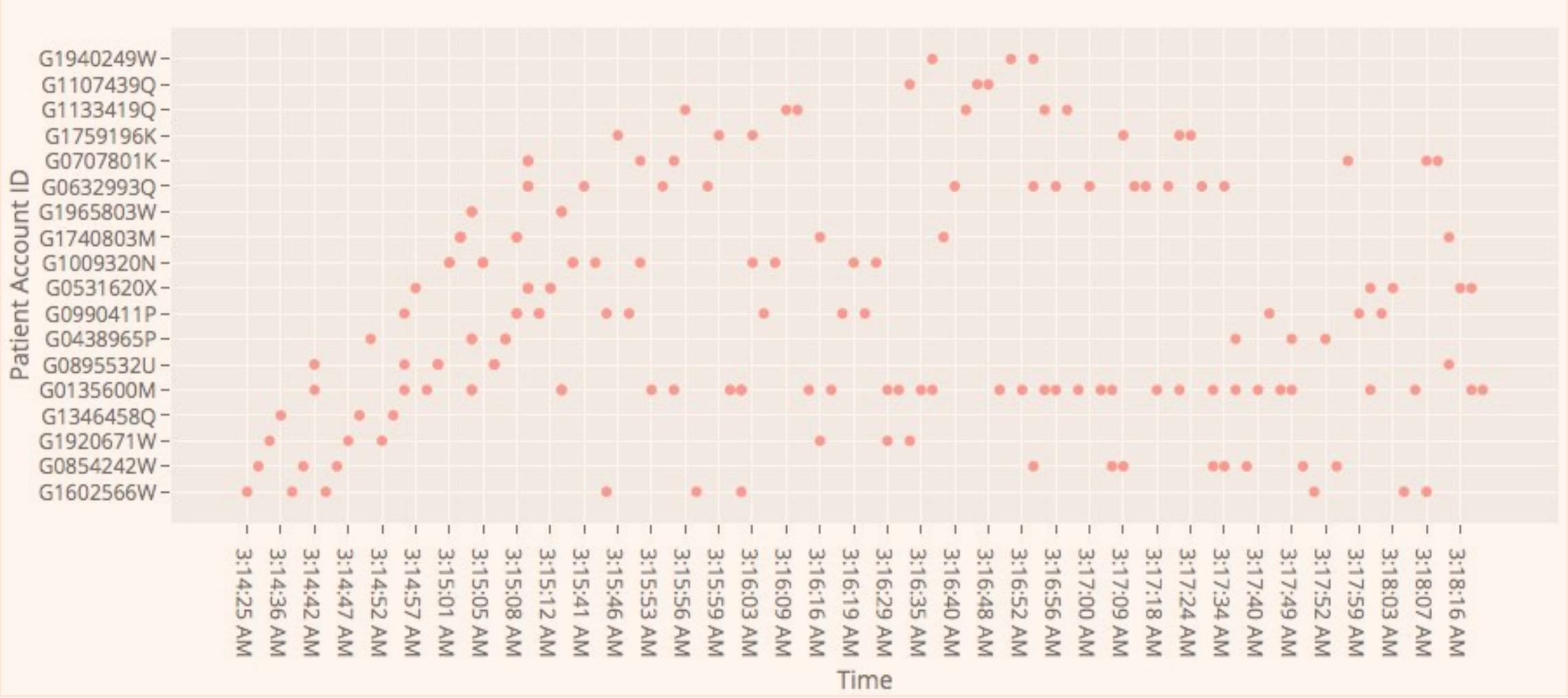
OctoBot is deployed inside physical and virtual computing resources over NCL (National Cybersecurity R&D Laboratory) production testbed

Kubernetes cluster on several VMs over multiple baremetal high-performance server with this specification

Able to deploy up to 1080 bots with a tiny Linux image (i.e., Busybox) in 10 worker nodes within 5 minutes

It is used healthcare informatics web application to verify the randomness of the bot

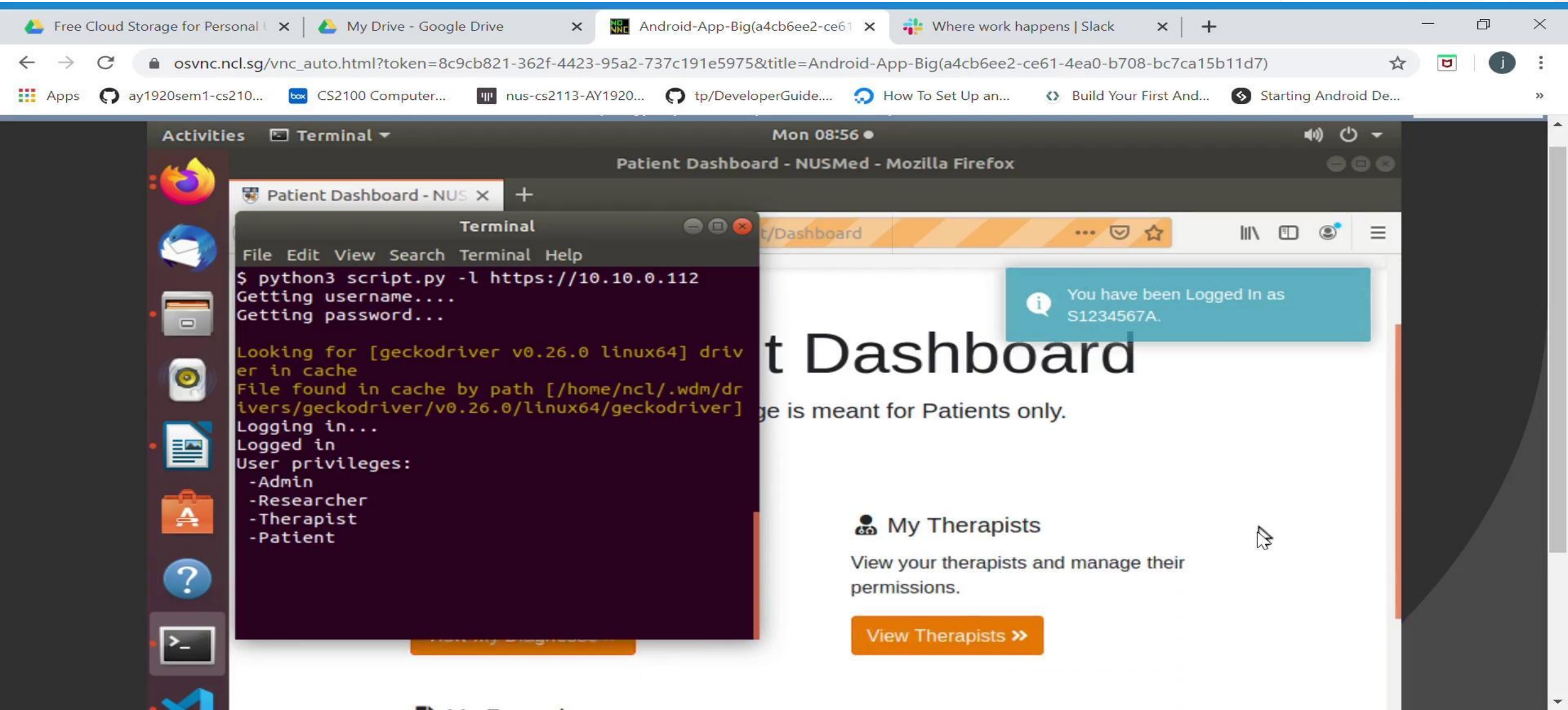
Verification



Demo

Octo-Bot Demo: Healthcare Informatics Web Application Bot

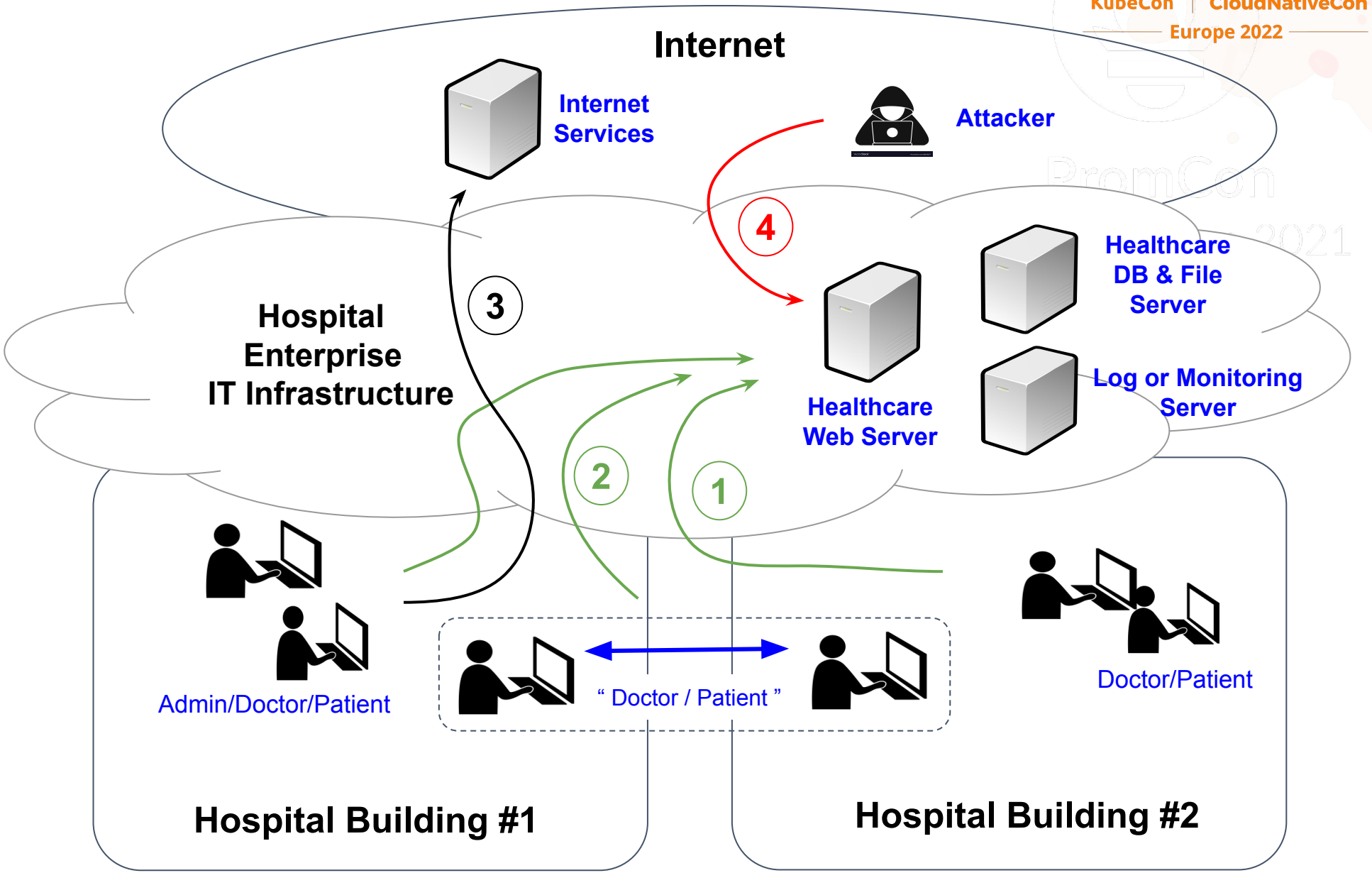
KubeCon CloudNativeCon Europe 2022



Octo-Play Demo: Healthcare Informatics in Hospital

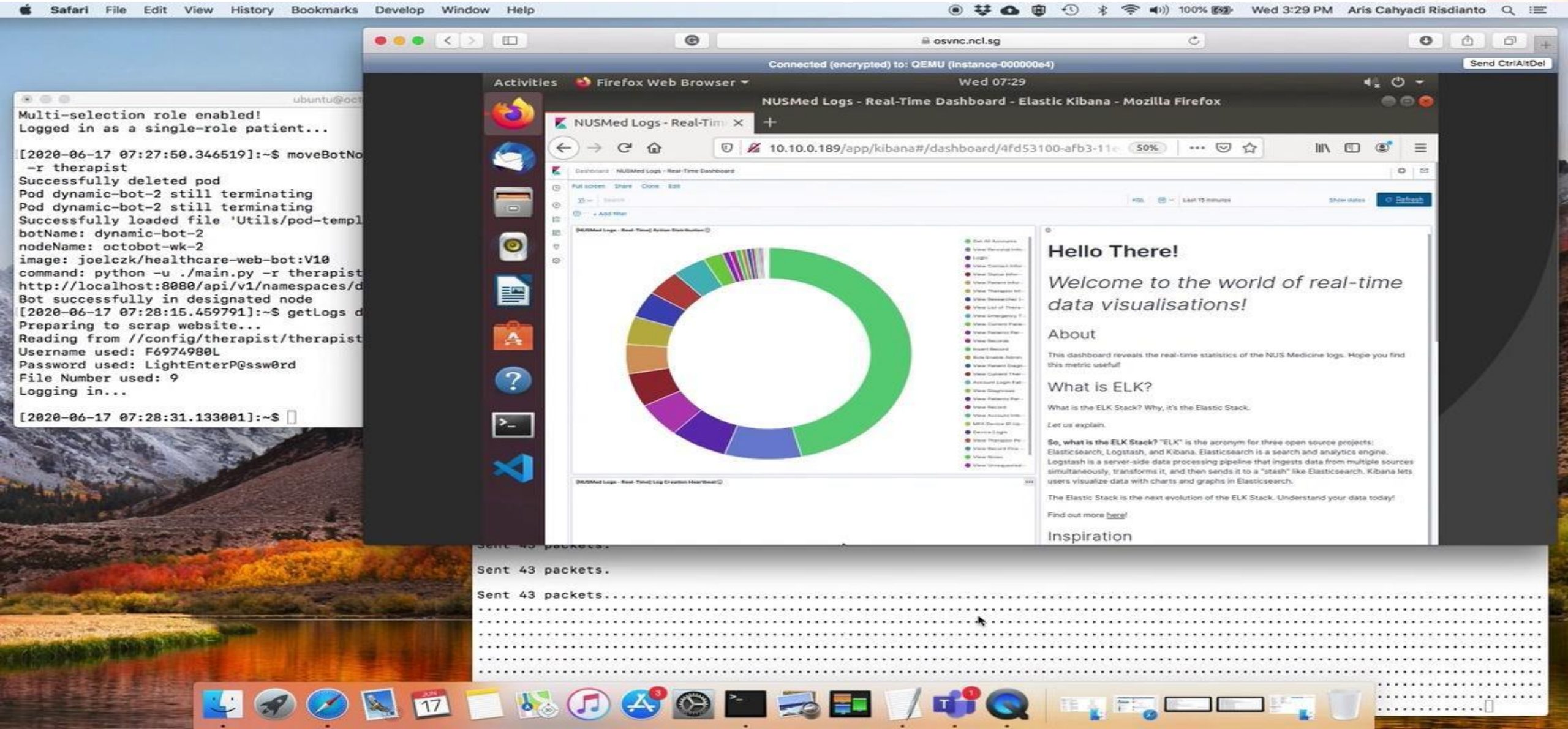
Orchestrator

- Admin: 2
- Doctor: 5
- Patient: 10
- "Doctor/Patient": 5
  - Role/login
  - Job
- Internet Users: 10
  - Internet URL/IP
  - Type of traffic
  - Rate
- Attacker: 100
  - Source IPs
  - Rate
  - Type of attack



Octo-Play Demo: Healthcare Informatics in Hospital

KubeCon CloudNativeCon Europe 2022



Summary

It is only used Kubernetes **Deployment Object** with customizable **replicas, image, command**, so it is easier to be understand by researcher or scientist

Node Selector and **Persistent Volume Claim** are used to support bot migration to mimic user movement

Kubectl exec CLI is used to interactively control the bot to do specific task

Lightweight OctoBot API is developed to hide the complexity of Kubernetes API

Contributors

Prof. Ee-Chien Chang (NCL/NUS) - changec@comp.nus.edu.sg

Aris Cahyadi Risdianto (NCL/NUS) - ariscahyadi

DeZhang Lee (NUS) - dezhanglee

Lai Yong Rong (Singapore Polytechnic) - WhyAre

Joel Chang Zhi Kai (NUS) - joelczk

Ang Chin Guan, Melvin (NUS) - krusagiz

Huang Kang (NUS) - hkwany

Akhil Vuputuri (NUS) - akhilvuputuri

Thank You!

aris@comp.nus.edu.sg
ariscr@ncl.sg