National Cybersecurity R&D Laboratory

Funded under National Cybersecurity R&D (NCRD) Programme since Nov 2015

National Cybersecurity R&D Laboratory

NCL Objective

National Lab to support cybersecurity R&D in Singapore

- For industries, government agencies and academia

Long Term Mission

- Develop NCL into a hub that facilitates the growth of a vibrant Singapore cybersecurity ecosystem

Key Areas of Support

- R&D and it's translation
- Development, Testing and Evaluation of security solutions
- Training and Skills Assessment

Current Status

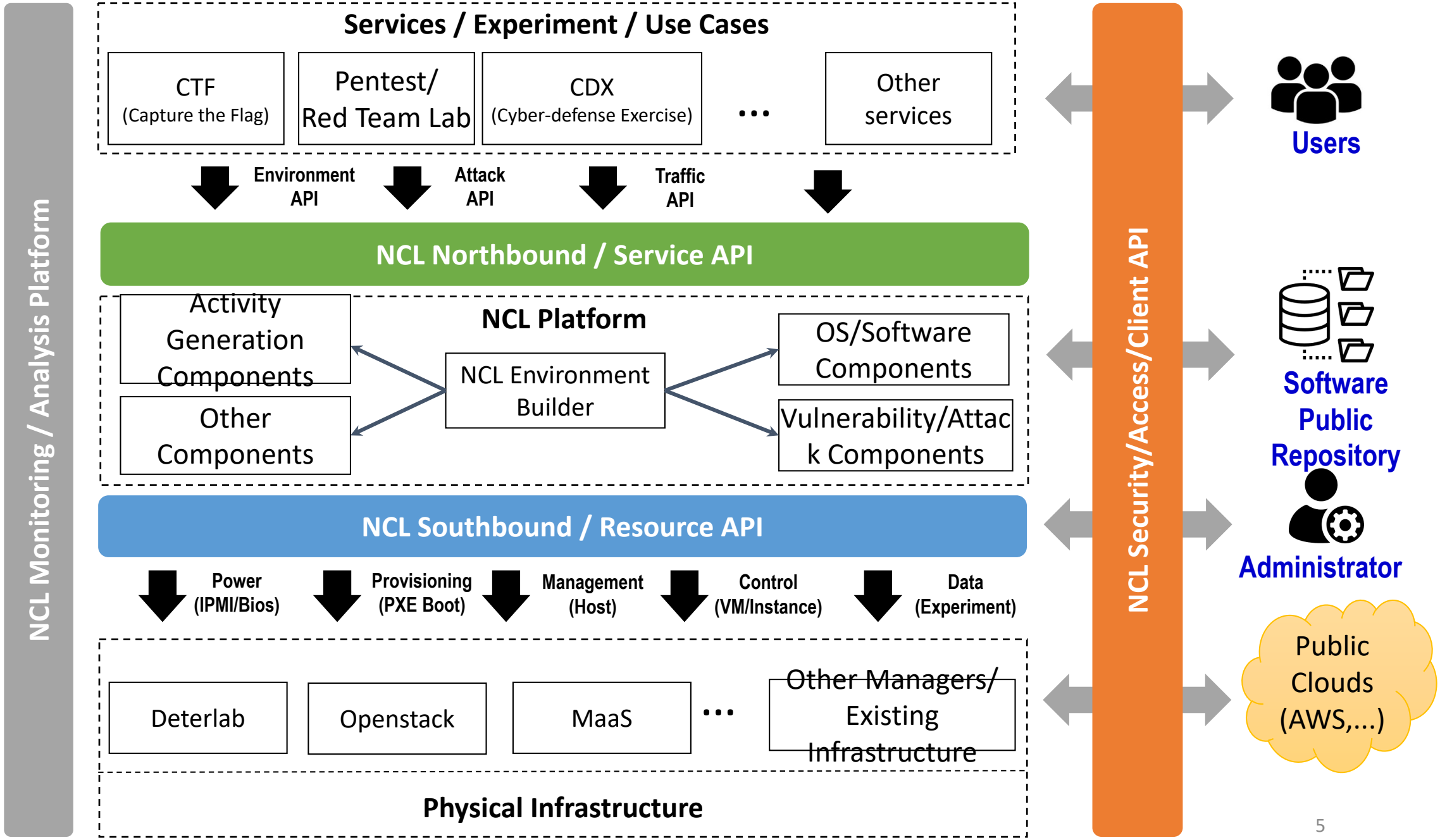
- Supported a wide range of projects since inception
- Over **100 projects** from industries, agencies and academia
- High utilization rate of testbed (~**96% utilized**)
- Growing an active community of users and collaborators
- Large number of academia and industry users
- Almost all Singapore education/ research institutes involved in the NCL projects as users, collaborators, interns, etc.

What We Offer

- **Provide environments for cybersecurity experimentation and testing**
  - ✓ Consists of virtual networks, vulnerability environments, attacking scripts, 50+ CVE's etc.
  - ✓ Hard to simulate and controlled environments
  - ✓ Common components supporting wide range of activities
  - ✓ Streamline/expedite R&D, translation, delivery of new solutions
  - ✓ Example of virtual environments : smart grid OT environment, Red Team environment, Healthcare environment

- **Add-on Services and Tools**
  - ✓ Applications/Services based on these environments
  - ✓ Example: Red Team/Pentest training labs for hands-on practice

- **Provide infrastructure**
  - ✓ Cloud service for cybersecurity activities
  - ✓ Facilitate support of risky environments & experiments
  - ✓ Support activities which do not need environment e.g. fuzzing experiments


NCL Monitoring / Analysis Platform
Services / Experiment / Use Cases
CTF
(Capture the Flag)
Pentest/
Red Team Lab
CDX
(Cyber-defense Exercise)
...
Other
services
Environment
API
Attack
API
Traffic
API
NCL Northbound / Service API
NCL Platform
Activity
Generation
Components
Other
Components
NCL Environment
Builder
OS/Software
Components
Vulnerability/Attac
k Components
NCL Southbound / Resource API
Power
(IPMI/Bios)
Provisioning
(PXE Boot)
Management
(Host)
Control
(VM/Instance)
Data
(Experiment)
Deterlab
Openstack
MaaS
...
Other Managers/
Existing
Infrastructure
Physical Infrastructure
NCL Security/Access/Client API
Users
Software
Public
Repository
Administrator
Public
Clouds
(AWS,...)

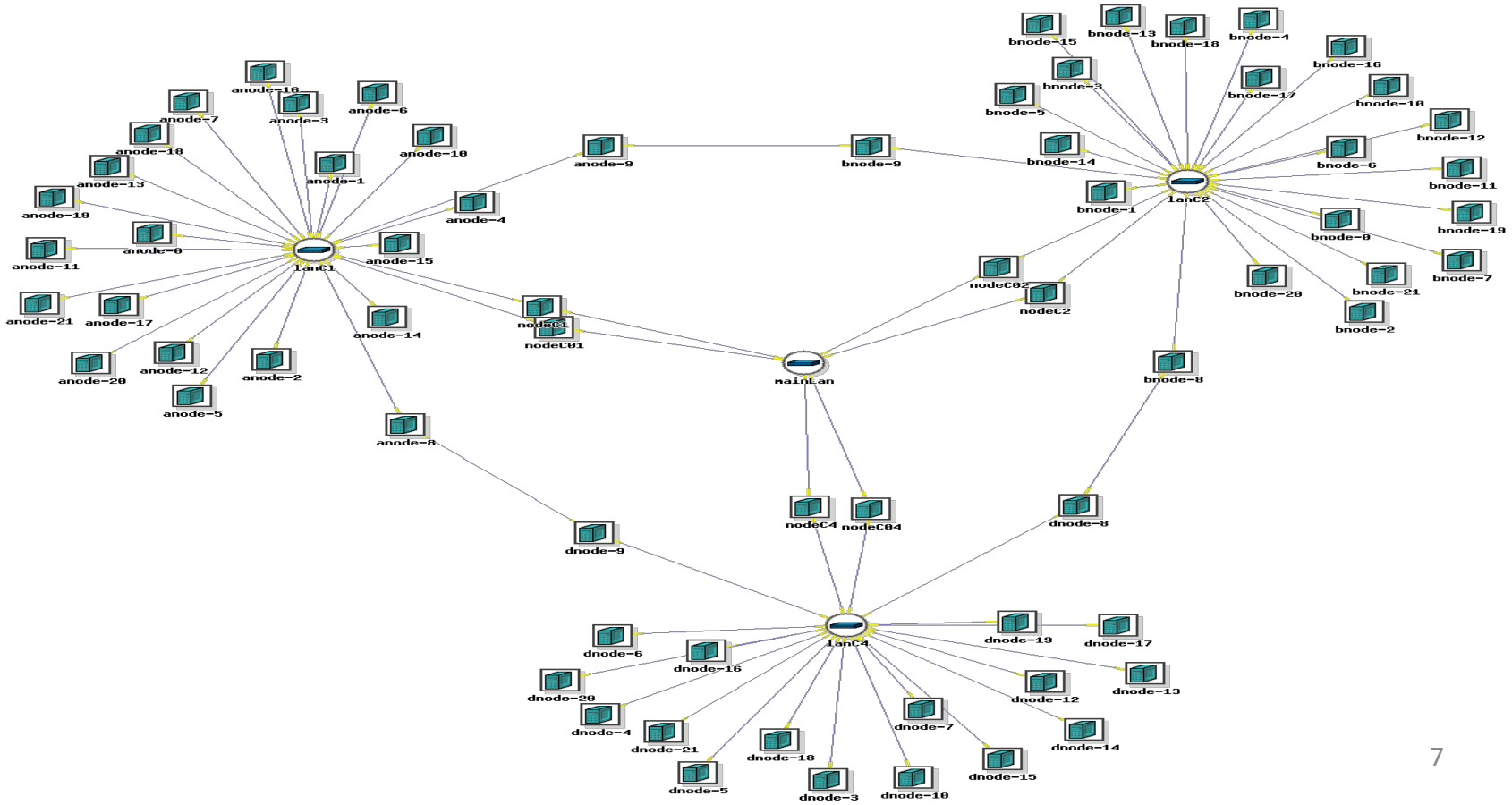
Computing Resources

- Cloud service with ~200 nodes, including GPU’s & high end servers

Services and Tools

- Customizable virtual networks & vulnerability environments

- Virtual enterprise IT networks ,OT Networks & Secure Data Processing Environment



Services and Tools

- Customizable virtual environments in different domains e.g. (IT, OT, Healthcare, Fintech)
- Red Team and Penetration Testing Lab
- Activity Traffic Generator
- Support for Capture-the-Flag (CTF) events
- Malware sandbox testing environment with samples

Example of Environments

Smart Grid OT Environment

- Operational Technology testbed in cloud
- Can be used to emulate Cyberattacks in SCADA systems (eg. 2015 Ukraine attack on Smart Grid)
- Leverage open-source software to facilitate development/usage
- Emulate all OT physical/embedded devices (e.g. sensor, PLC) into VM instances for safer & faster testing/development
- Uses publicly available power consumption data for power generation control

Example of Environments

Pentest and Red Team Lab (24*7 remotely accessible)

- Active Directory environment to practice and develop Red Team skills
- Comes with various red team activities like Lateral Movement, Obfuscation, Evasion
- Latest vulnerabilities like Zero Logon are included in the environment

Fintech Environment

- Common vulnerabilities in Web Applications based on OWASP Top 10
- Comes with vulnerabilities that occur in a real world Web Application
- Demonstrates how a successful kill-chain could be designed by chaining the vulnerabilities for remote code execution

Example of Environments

Hospital/Healthcare Environment

- A simulated Healthcare environment integrated with Windows Active Directory services to facilitate more realistic testing/training
- Provides dynamic and realistic environment with simultaneous access by attackers and users in various roles (e.g. Doctor, Patient) and simulated workflow
- Supports role-based access management with multiple level of authentication configured with predefined users account (more than 1000)
- Supports Data Anonymity to protect patient's information

Development, Testing & Evaluation of Security Solutions (DTE)

Environment to facilitate Development, Testing and Evaluation of security solutions

- Non Trivial Attack - obfuscation and avoiding detection
- Distributed Scanning- Perform scanning in a coordinated way to remain unnoticed
- Normal & Attack Traffic - an enhanced attack traffic by embedding the various attack techniques in the normal traffic
- Embedding the Malicious Traffic
- Activity Traffic Generator (OctoBot)

Thank you!

Any questions?

To find out more:

Website: https://ncl.sg

Email: support@ncl.sg

National Cybersecurity R&D Laboratory