MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

AUTOMATED EXERCISE DEVELOPMENT FOR IMPROVED CYBER TRAINING

Carnegie Mellon University
Software Engineering Institute

Matt Kaar

Team Lead, Cyber Workforce Dev

mkaar@cert.org | @mattkaar

John G. Bush

Cyber Exercise Developer

jbush@cert.org

BECAUSE… LAWYERS

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM18-0246

WHAT ARE CYBER EXERCISES?

CYBER EXERCISE

Definition: A planned event during which an organization simulates a cyber disruption to develop or test capabilities such as preventing, detecting, mitigating, responding to or recovering from the disruption.

Source: US-CERT

Cyber Exercise Playbook

Jason Kick

November 2014

MP140714

Wiesbaden, Germany

MITRE

Practice makes perfect.

PRACTICING CYBER DEFENSE

Real-life provides plenty of practice scenarios.


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
About bitcoin
How to buy bitcoins?
Contact Us
Check Payment
Decrypt

WANNACRY RANSOMWARE (2017)

- **300,000+** computers infected.
- **98% running Windows 7** operating system
- Used **ExernalBlue** exploit released by Shadow Brokers in April 2017

CYBERSECURITY

Why the OPM Hack Is Far Worse Than You Imagine

By **Michael Adams** Friday, March 11, 2016, 10:00 AM

The Office of Personnel Management ("OPM") data breach involves the greatest theft of sensitive personnel data in history. But, to date, neither the scope nor scale of the breach, nor its significance, nor the inadequate and even self-defeating response has been fully aired.

The scale of the OPM breach is larger and more harmful than appreciated, the response to it has worsened the data security of affected individuals, and the government has inadequately addressed the breach's counterintelligence consequences. While we can never know for sure exactly what the government is doing in secret to address the breach and mitigate its consequences, based on

Michael Adams is currently Global Director for Information Security with a Swiss-based company. He is a recognized professional in information security and privacy protections with an extensive history of advising and assisting both the private and public sectors globally, including the U.S. Government. Adams is an ex-United States Special Operations Command Sergeant Major with over 20 years direct experience leading and executing classified combat and intelligence operations. He has held USG security clearances for over three decades.

mla1396

MORE ARTICLES ›

OFFICE OF PERSONNEL MANAGEMENT BREACH (2015)

- One of the largest breaches of government data in the history of the U.S.
- **21.5 million** personnel records stolen
- **5.6 million** fingerprints stolen
- Discovered during forensic tool demonstration on OPM's network

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	*	
	*	CRIMINAL NO.
v.	*	
	*	(18 U.S.C. §§ 2, 371, 1349, 1028A)
INTERNET RESEARCH AGENCY LLC A/K/A MEDIASINTEZ LLC A/K/A GLAVSET LLC A/K/A MIXINFO LLC A/K/A AZIMUT LLC A/K/A NOVINFO LLC,	*	
CONCORD MANAGEMENT AND CONSULTING LLC,	*	
CONCORD CATERING,	*	
YEVGENIY VIKTOROVICH PRIGOZHIN,	*	
MIKHAIL IVANOVICH BYSTROV,	*	
MIKHAIL LEONIDOVICH BURCHIK A/K/A MIKHAIL ABRAMOV,	*	
ALEKSANDRA YURYEVNA KRYLOVA,	*	
ANNA VLADISLAVOVNA BOGACHEVA,	*	
SERGEY PAVLOVICH POLOZOV,	*	

INDICTMENT

The Grand Jury for the District of Columbia charges:

Introduction

1. The United States of America, through its departments and agencies, regulates the activities of foreign individuals and entities in and affecting the United States in order to prevent, disclose, and counteract improper foreign influence on U.S. elections and on the U.S. political system. U.S. law bans foreign nationals from making certain expenditures or financial disbursements for the purpose of influencing federal elections. U.S. law also bars agents of any foreign entity from engaging in political activities within the United States without first registering with the Attorney General. And U.S. law requires certain foreign nationals seeking entry to the United States to obtain a visa by providing truthful and accurate information to the government. Various federal agencies, including the Federal Election Commission, the U.S. Department of Justice, and the U.S. Department of State, are charged with enforcing these laws.

2016 U.S. ELECTION HACKING

- “…engaged in operations to interfere with elections and political processes.”
- Registered social media accounts using VPNs to mask origin and control of their activity.
- Controlled hundreds of web-based email accounts under false names to give the appearance of U.S. persons.
- Used stolen identities to register for PayPal accounts used to purchase social media advertisements.

Examples provide
adversary tactics, techniques and **procedures**.

CREATING REALISTIC TRAINING

Who are we?

SOFTWARE ENGINEERING INSTITUTE

SEI founded in 1984 at CMU as Department of Defense **Federally Funded Research and Development Center** (FFRDC):

- Only DoD R&D center focused on software engineering and cybersecurity
- **~700** employees
- **CERT Division** founded in 1988

Carnegie Mellon University
Software Engineering Institute

CERT CYBER WORKFORCE DEVELOPMENT

CWD Directorate Mission

Provide force-multiplying solutions to rapidly grow and strengthen DoD's cybersecurity workforce--addressing the problems of time, scale, and cost.

- We empower DoD's Cyber Mission Force to **"Train as You Fight"**
- We develop and transition cutting-edge Prototypes and Content:
  - Training and Exercise Platforms
  - Modeling and Simulation Tools
  - Gamified, on-demand training

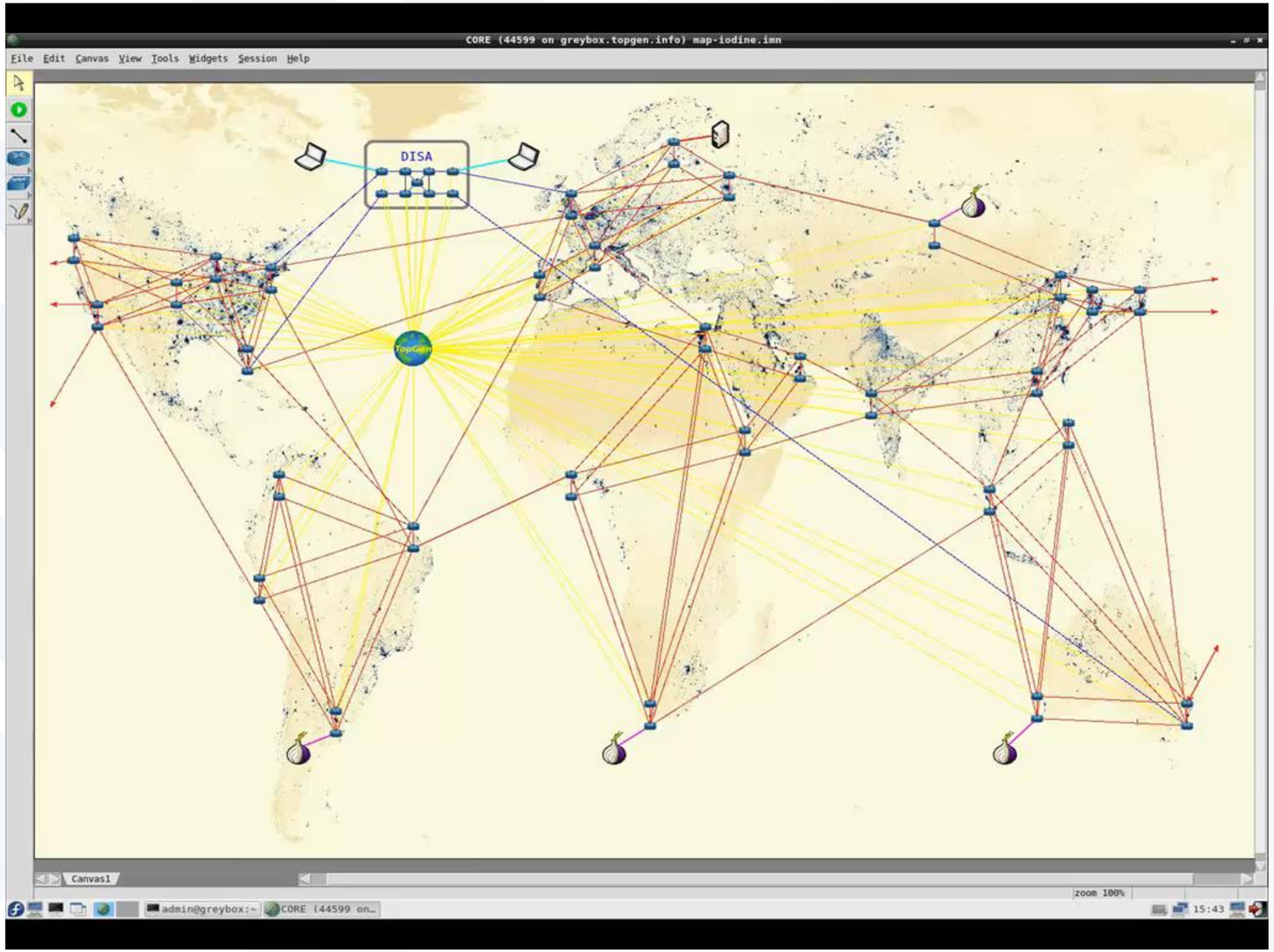
Training Prototypes

GREYBOX

Simulates complex Internet topology in a single virtual machine

- Built using NRL's Common Open Research Emulator (CORE)
- Core routing infrastructure with accurate geospatial delays
- Domain Name System with all root servers plus .com, .net, .edu, .mil, etc.
- Email services like Gmail, Yahoo, Outlook.com, etc.

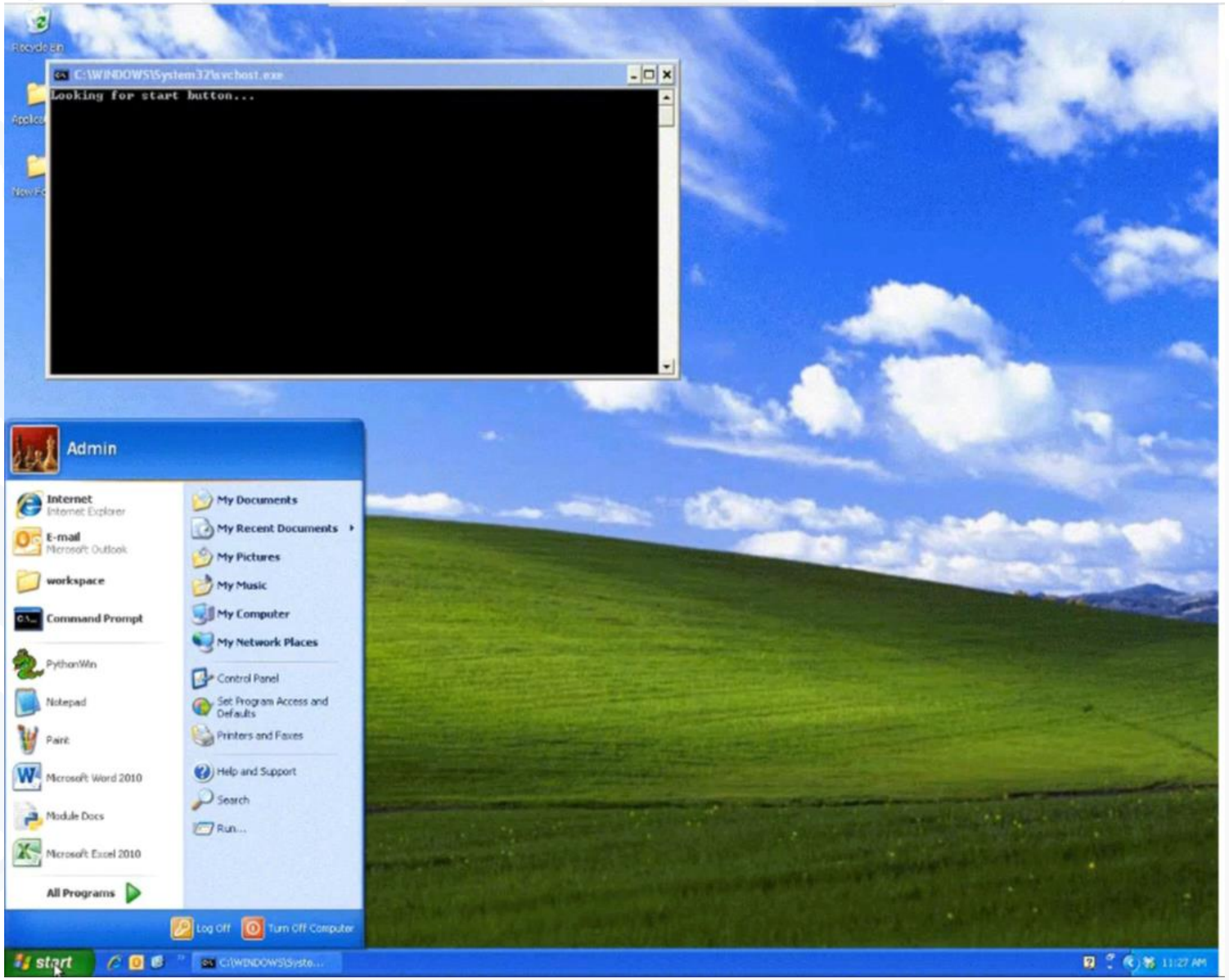
github.com/cmu-sei/greybox



USERSIM

- Agent that simulates user activities like:
  - Web surfing
  - Email
  - Typing documents in Word
  - Chat
- Can be taught to use any Windows application
- Users generate trouble tickets when they have issues (bounced email, Web site down, etc.)

github.com/cmu-sei/usersim



WELLE-D

Enables wireless training within a virtualized environment without transmission of radio frequencies

- **Cost effective** – no hardware
- **Portable** – brings wireless inside secure facilities
- **Scalable and repeatable** - No interference
- **Realistic** - Functions like a real wireless device

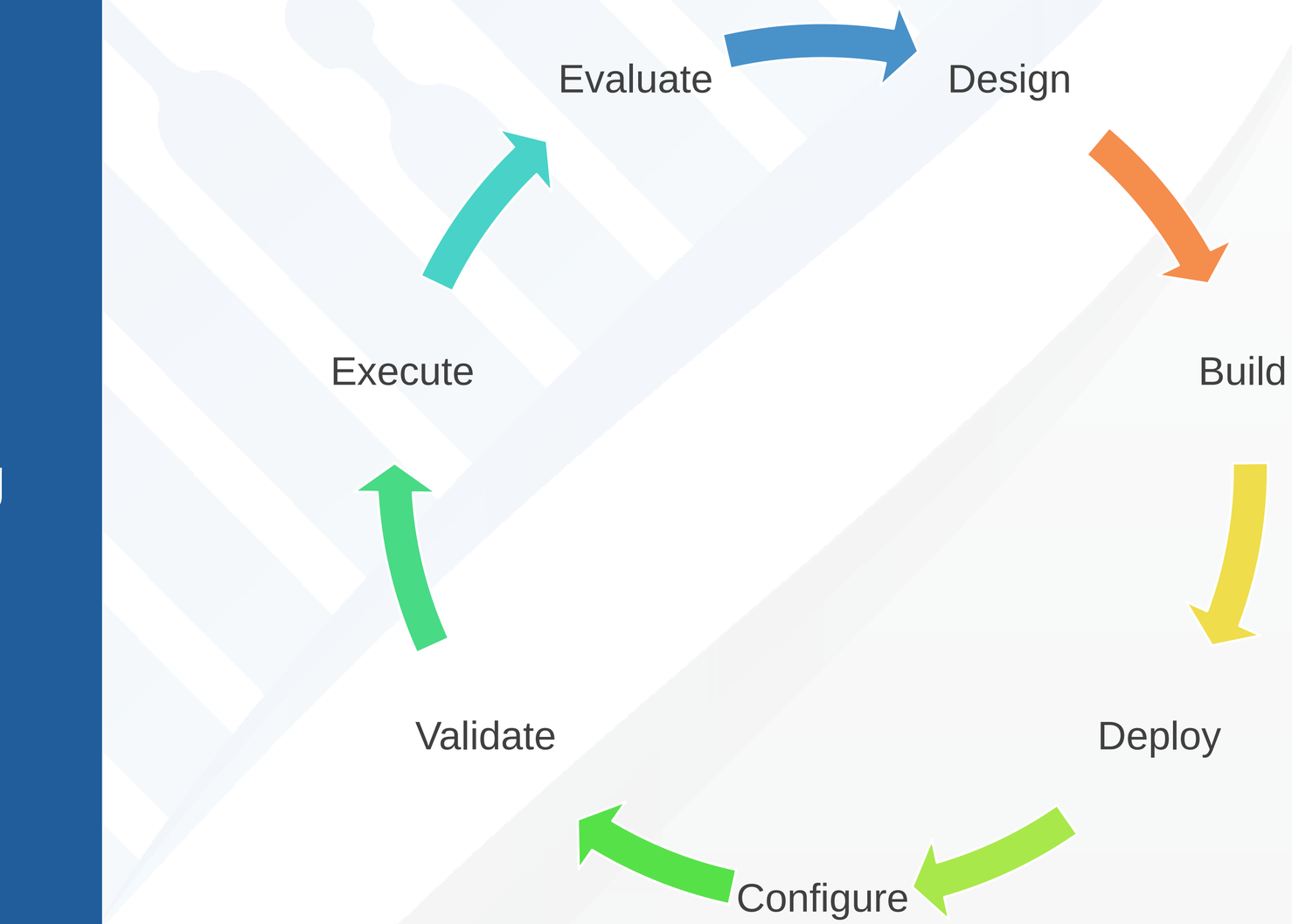
Open source coming soon.

How can this training scale?

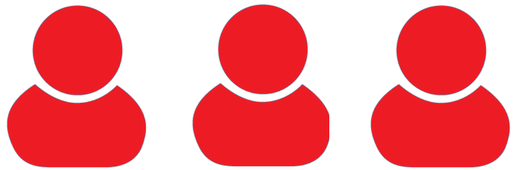
BUILDING CYBER EXERCISES

EXERCISE LIFECYCLE

- “Time to market” – Time from exercise inception to execution
- Reducing time at any phase results in being able to execute training faster
- Phases currently last on the order of weeks or months at a time



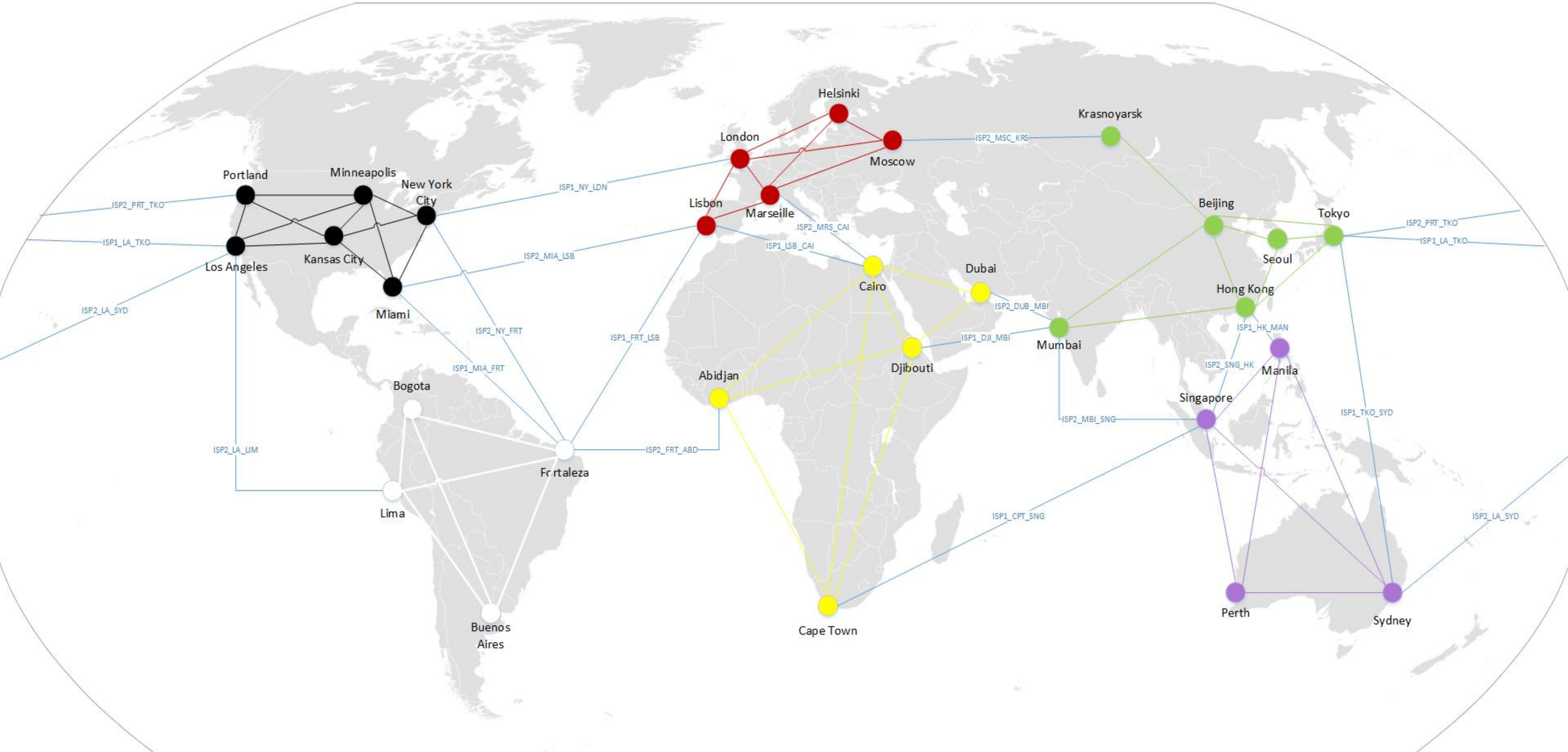
RED VS. BLUE



OPFOR

Blue Teams

PSEUDO INTERNET



SERVICES

- **Protocols**
  - HTTP/S
  - DNS
  - NTP
  - BGP
  - OSPF
- **Internet Services**
  - Websites
  - Package repositories
  - Certification authorities
  - Cloud services
- **Team networks**
  - Active Directory
  - Microsoft Exchange
  - File servers
  - Simulated users
  - Management workstations
  - DNS servers
  - Web servers
  - Security monitoring
  - Firewalls
- **And much more...**

QUESTIONS

How do you scale to handle a growing number of participants?

QUESTIONS

How do you avoid costly mistakes?

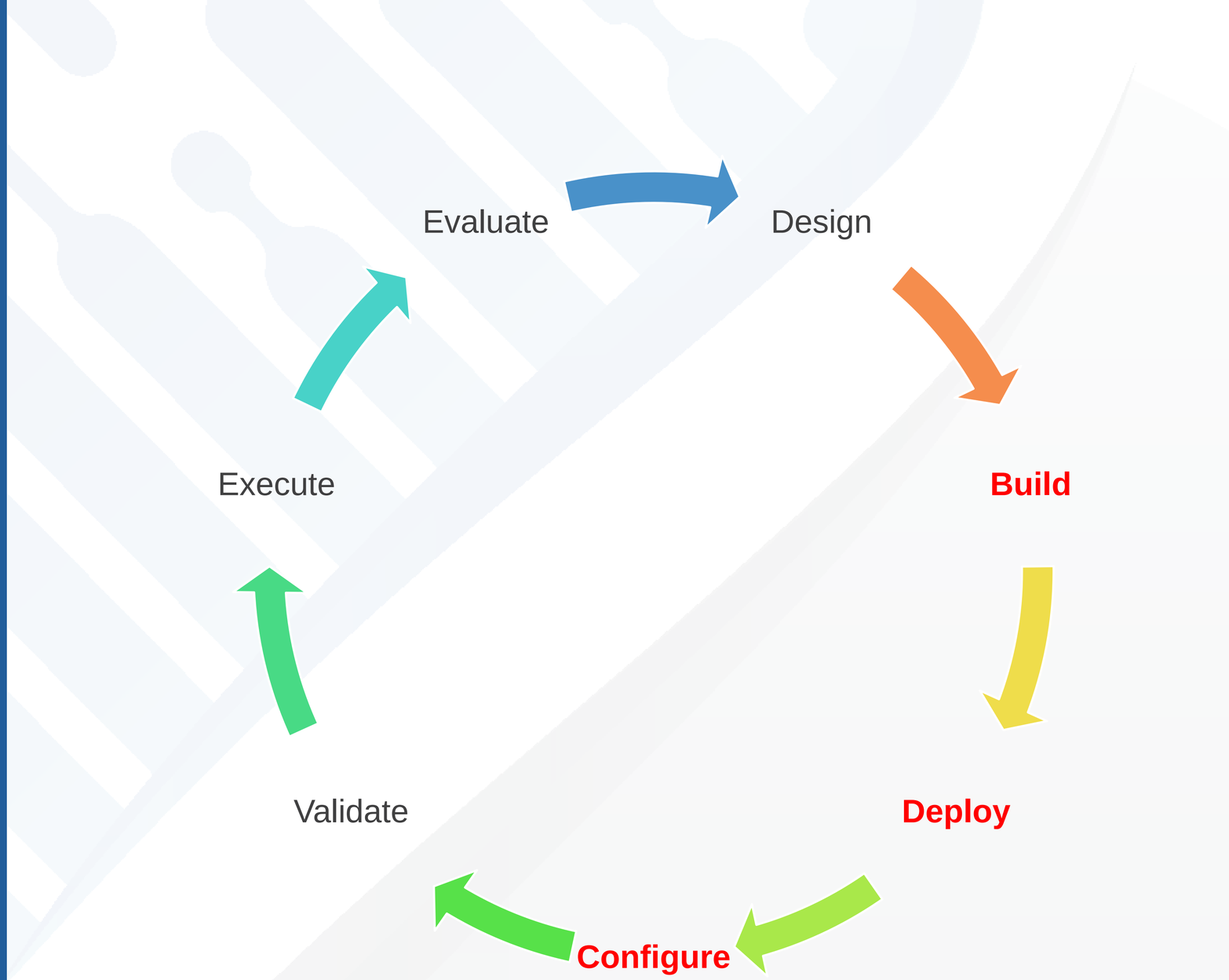
QUESTIONS

How do you adapt to changing customer requirements?

ANSWER

Automate!
Automate!
Automate!

AUTOMATING THE EXERCISE LIFECYCLE

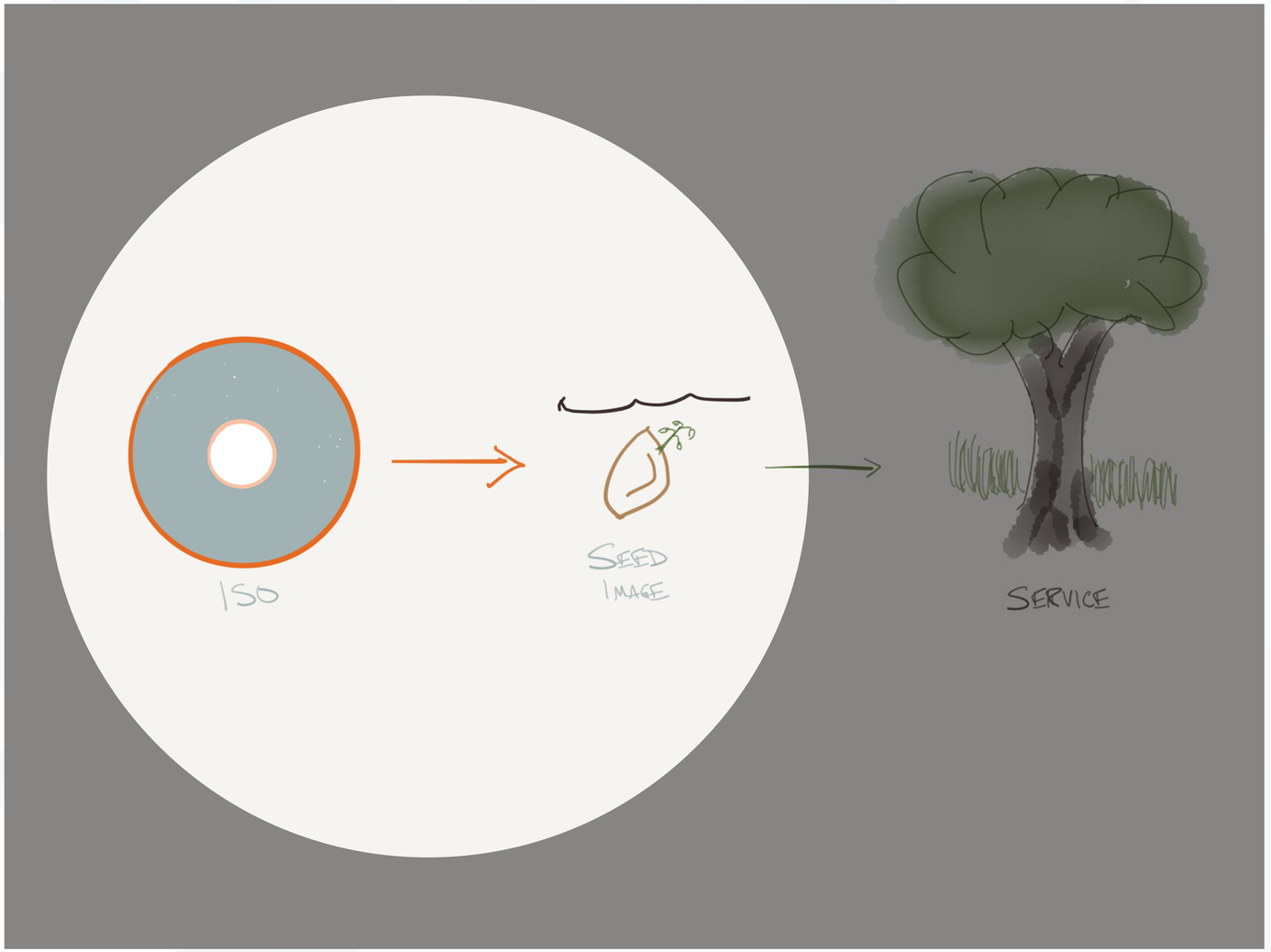


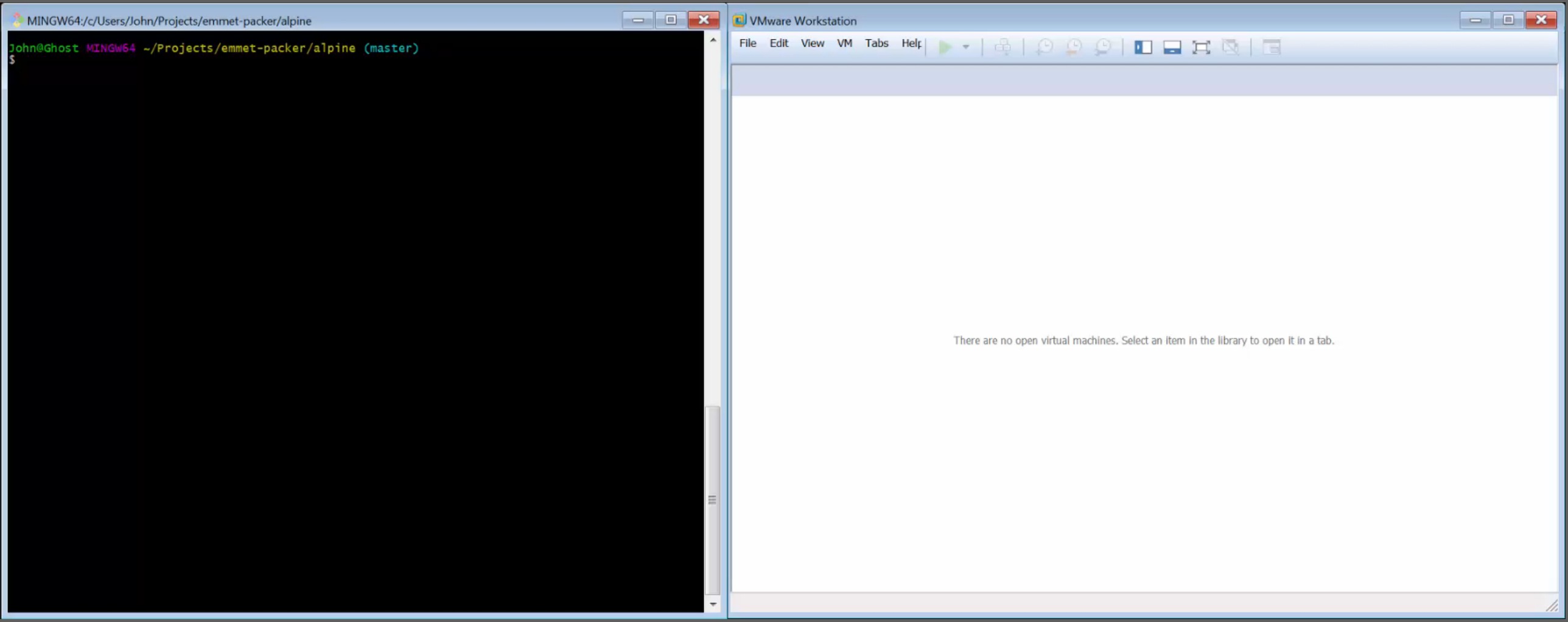
PACKER (BUILD)

Open-source tool for building virtual machine disks:

- Used to create “seed” images as starting points for each build.
- Allows for easy software upgrades between iterations.
- Couple with continuous integration for automated builds.

github.com/hashicorp/packer



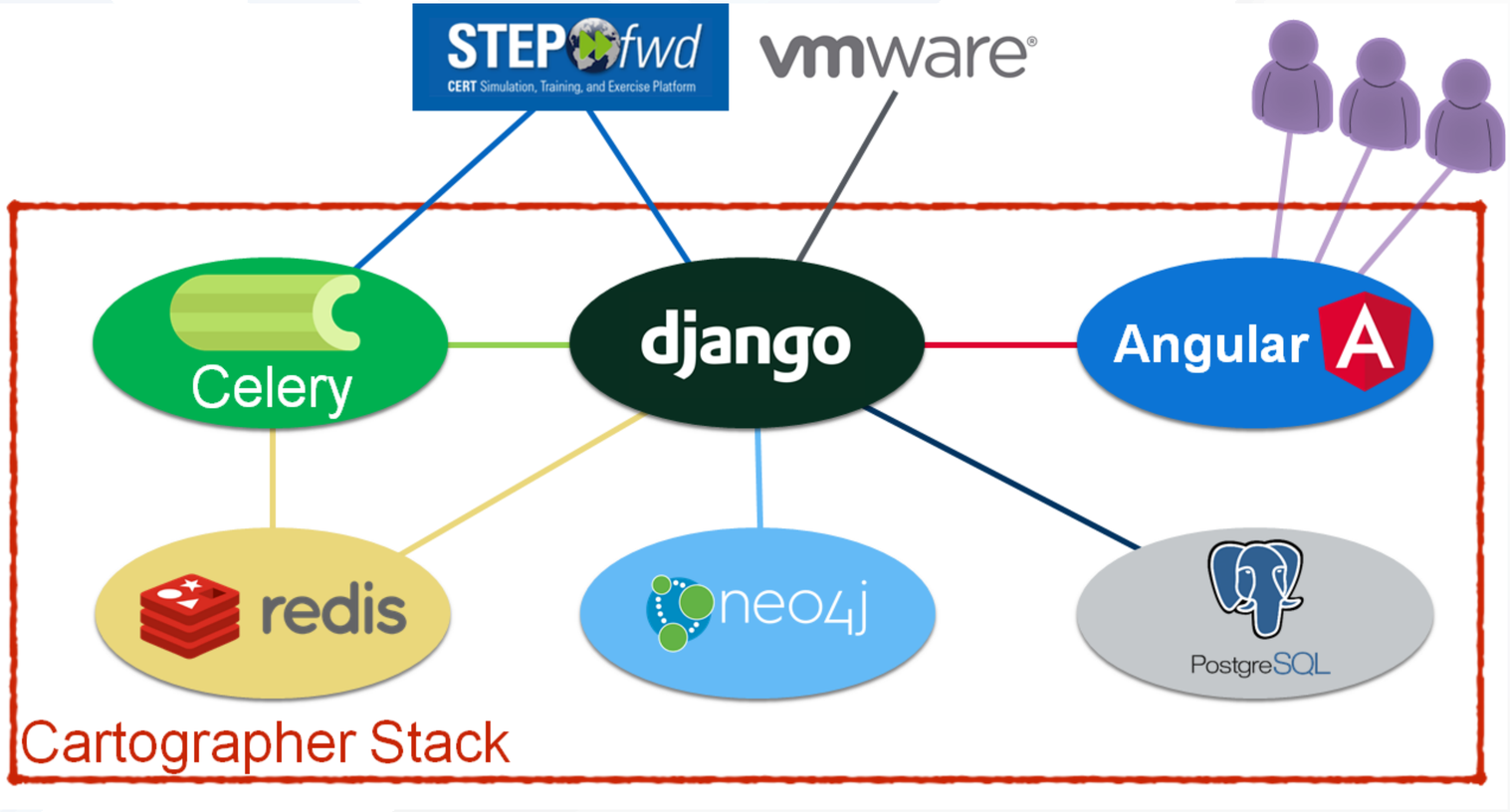

MINGW64:/c/Users/John/Projects/emmet-packer/alpine
John@Ghost MINGW64 ~/Projects/emmet-packer/alpine (master)
$
VMware Workstation
File Edit View VM Tabs Help
There are no open virtual machines. Select an item in the library to open it in a tab.

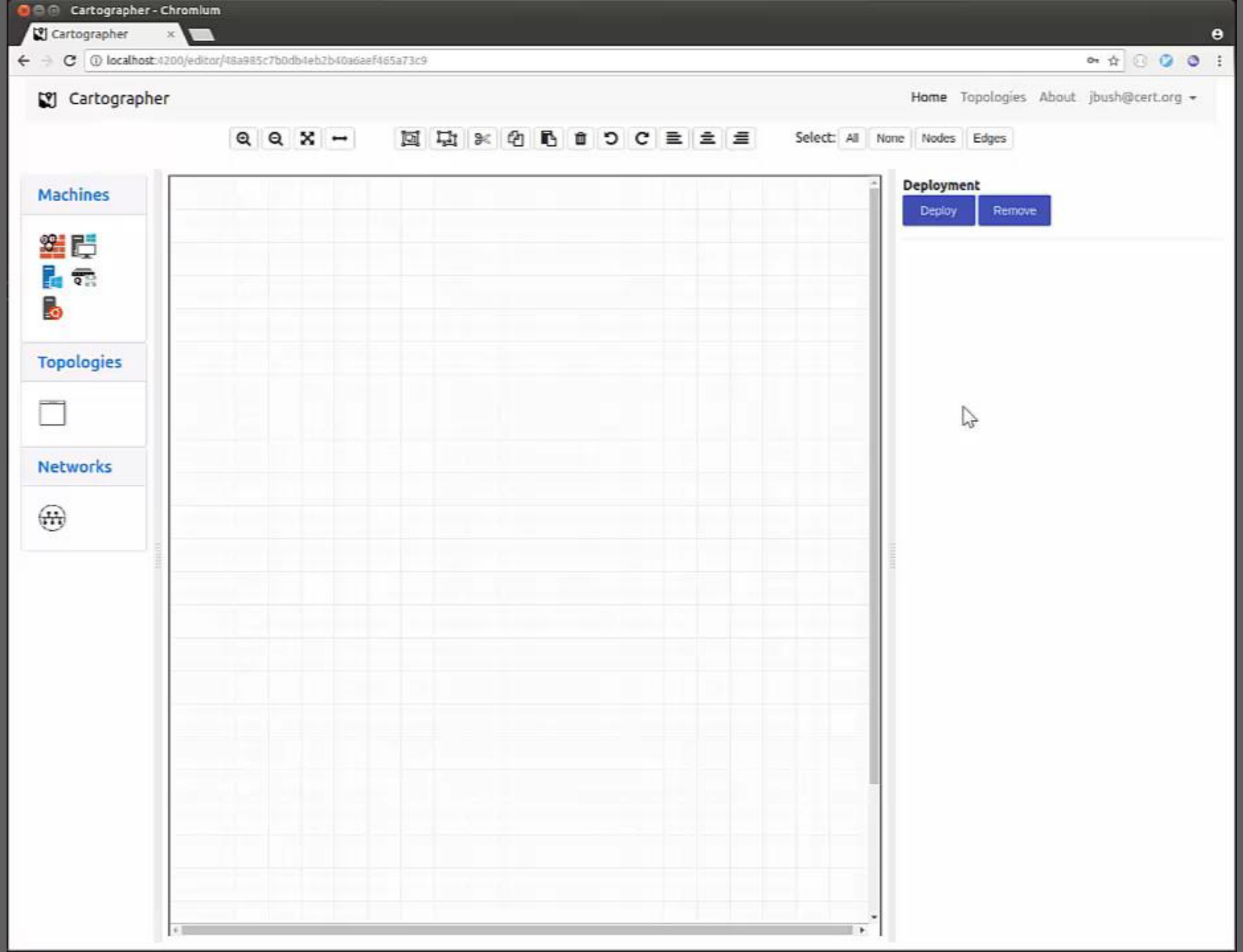
CARTOGRAPHER (DEPLOY)

Topology construction tool currently being developed by the SEI:

- Web-based diagramming tool for designing networks and validating configurations
- Deploy machines directly from diagrams.
- Don’t Repeat Yourself. (DRY)

Open source coming soon.



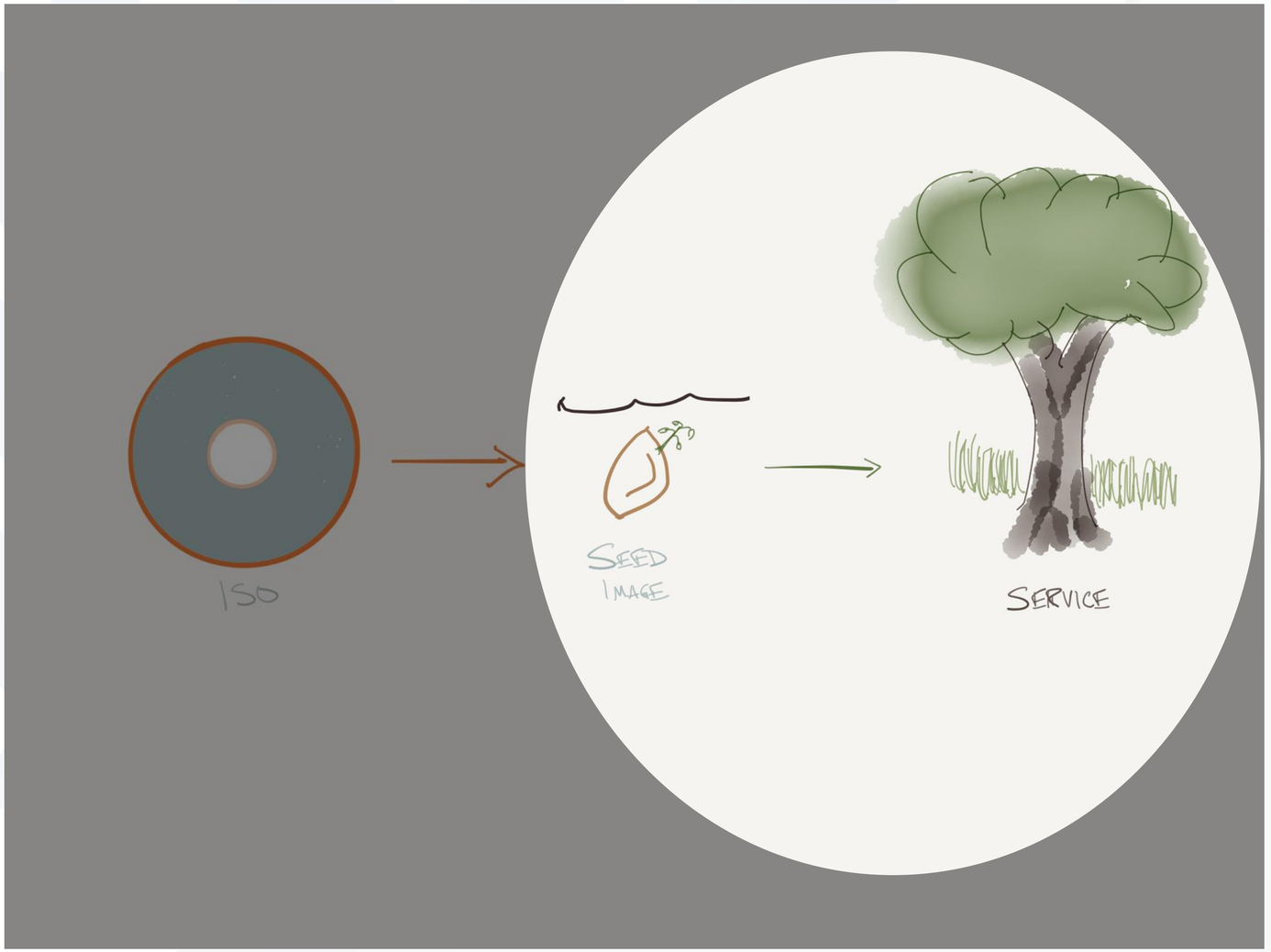

Cartographer - Chromium
Cartographer
localhost:4200/editor/48a985c7b0db4eb2b40a6aef465a73c9
Cartographer
Home
Topologies
About
jbush@cert.org
Select:
All
None
Nodes
Edges
Machines
Topologies
Networks
Deployment
Deploy
Remove

ANSIBLE (CONFIGURE)

Open-source configuration management tool:

- Grow “seed” images into full-blown services
- Idempotent – successive runs do not leave machine in a bad state
- Agentless – minimize footprint on deployed VMs
- Playbooks/roles written in readable YAML

github.com/ansible/ansible



Root A
DNS Server

AUTOMATION BENEFITS

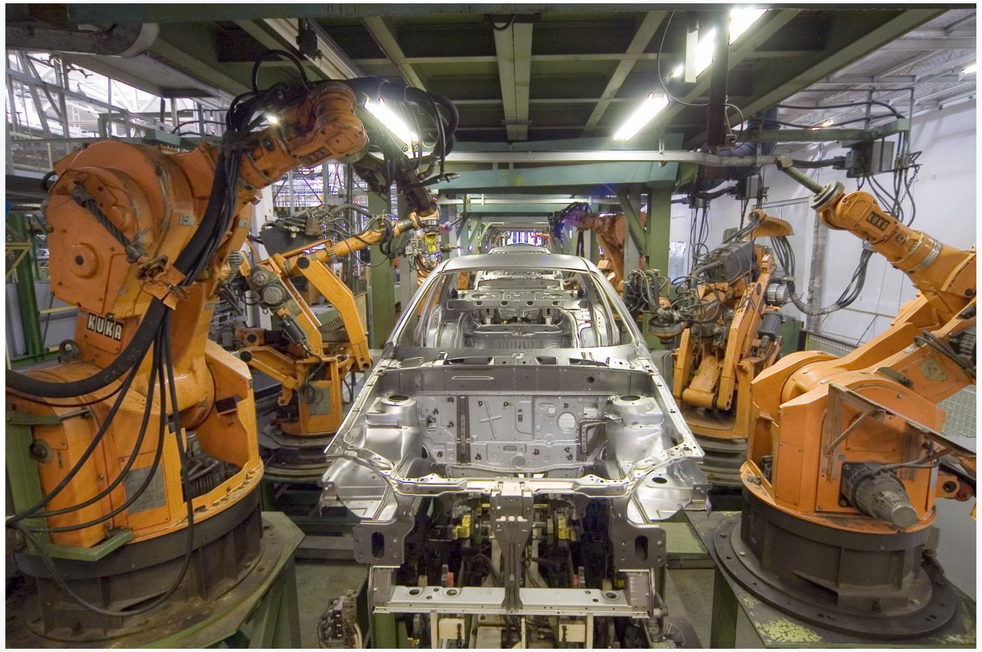
- Environments can scale as new participants join:
  - Most teams have similar setups
  - Easy to roll out a new instance

- Reduced troubleshooting time by avoiding common errors:
  - Fat-fingering
  - Skipping steps
  - Invalid input

- Tool idempotency ensures machines are left in a known state

- Self-documenting build processes

- Parallel provisioning



MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Carnegie Mellon University
Software Engineering Institute

Matt Kaar
Team Lead, Cyber Workforce Dev
mkaar@cert.org | @mattkaar

John G. Bush
Cyber Exercise Developer
jbush@cert.org