(ICS) Cyber Range as a Service® (CRaaS)

Creating Infrastructure and workflows as a Service to implement
ICS Cyber Range Activities for the lifecycle of MOSAICS

Agenda – Sample from our webinar

Introductions

What is a Cyber Range

Challenges of delivering a Cyber Range

What is Cyber Range as a Service (CRaaS)

How do you deliver CRaaS

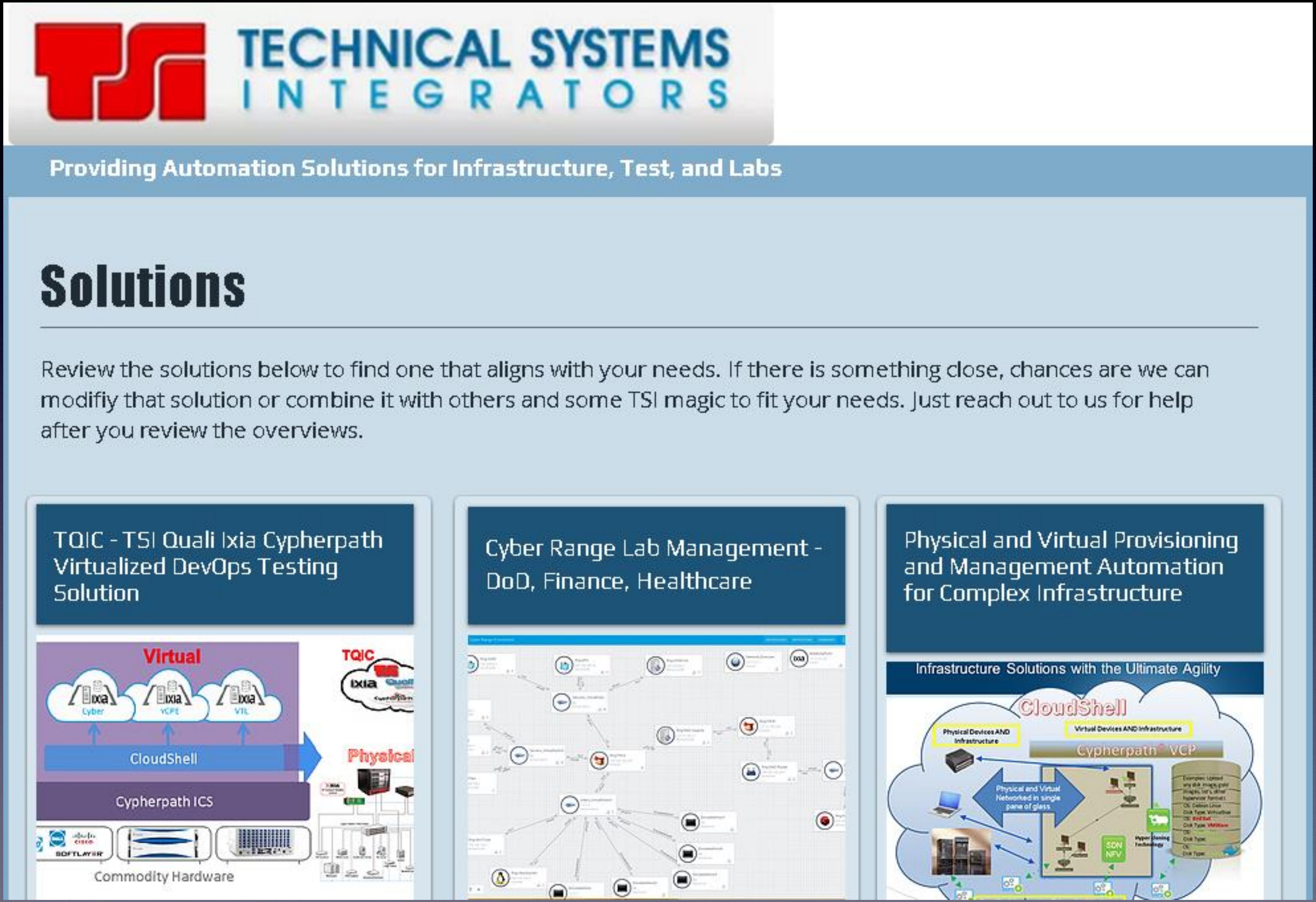
What is the value of CRaaS

Examples

TSI's Role

- SI/VAR Focused on LaaS, PaaS, IaaS, TaaS, CRaaS and Cloud Solutions for:
  - ❑ CyberRanges
  - ❑ Data Centers
  - ❑ Demo/POC
  - ❑ Test and QA Labs
  - ❑ NERC CIP
  - ❑ Clouds
  - ❑ Training

- DoD Focus
- Program Registration for Select Technologies
- Technology Discovery and Integration
- Cyber training and Exercise Content Libraries
- Cyber Range as a Service®



TECHNICAL SYSTEMS INTEGRATORS

Providing Automation Solutions for Infrastructure, Test, and Labs

Solutions

Review the solutions below to find one that aligns with your needs. If there is something close, chances are we can modifiy that solution or combine it with others and some TSI magic to fit your needs. Just reach out to us for help after you review the overviews.

TQIC - TSI Quali Ixia Cypherpath Virtualized DevOps Testing Solution

Cyber Range Lab Management - DoD, Finance, Healthcare

Physical and Virtual Provisioning and Management Automation for Complex Infrastructure

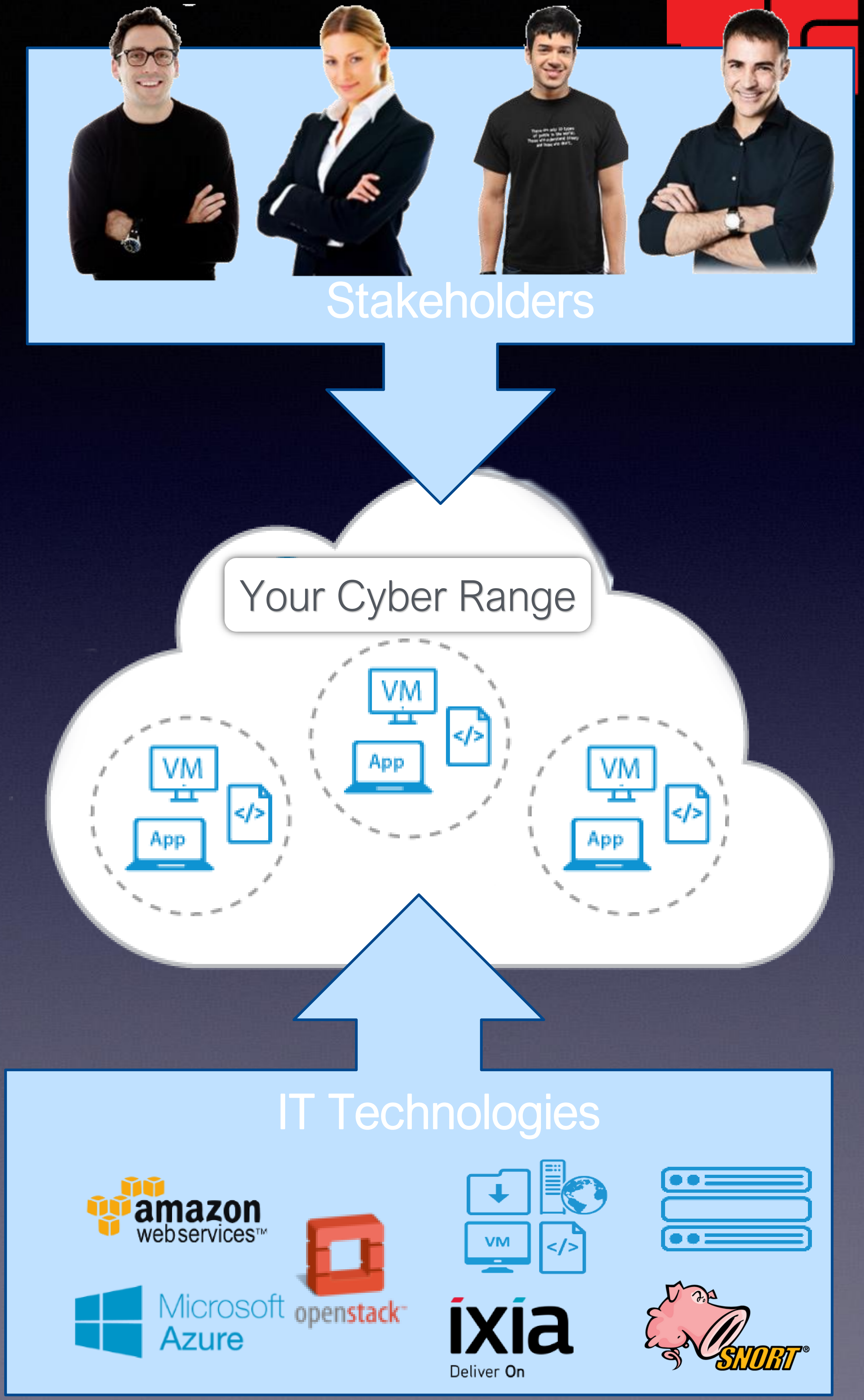
Virtual
ixia
Cyber
VCPE
VIL
TQIC
CloudShell
Cypherpath ICS
Physical
SOFTLAYER
Commodity Hardware
Infrastructure Solutions with the Ultimate Agility
CloudShell
Physical Devices AND Infrastructure
Virtual Devices AND Infrastructure
Cypherpath VCP
Physical and Virtual Networked in single pane of glass
SDN NFV

Established 1987

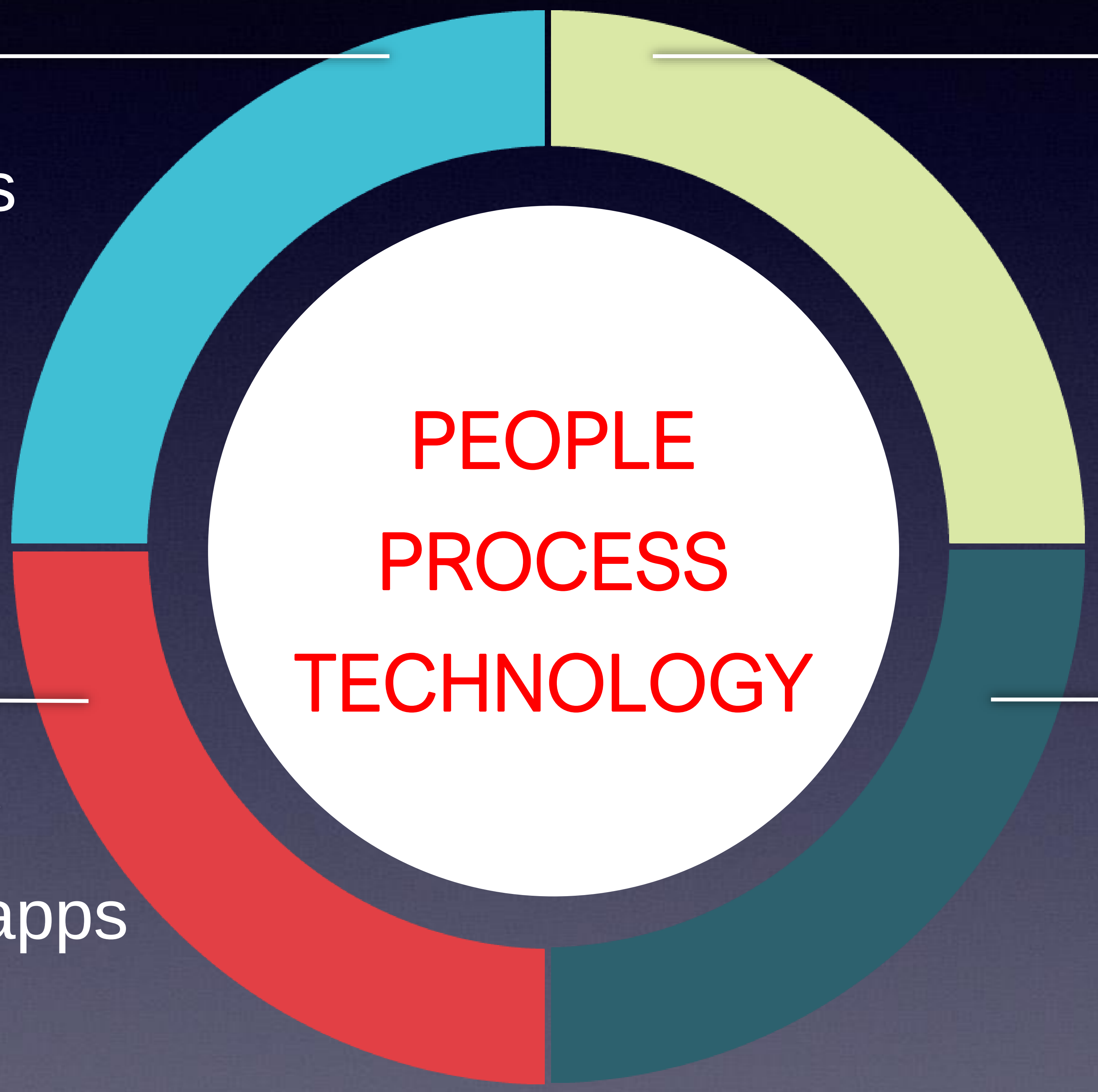
What is a Cyber Range?

Full Stack Automated Lab/Data Center for Hardening IT

- Replicate Production On-Demand
  - –**IT Infrastructure**: end to end network, data, storage, security/firewall, end point devices, IoT, ICS, including physical, virtual, and cloud resources
  - –**IT Applications**: mobile, middleware, back end, etc.
  - –**Test Equipment**: Traffic generators, physical layer switching
  - –**Test/Security Tools**: Attack scripts, security software, detection software, etc.
- Uses – Stakeholders
  - –**Training IT** – Cyber scenario games with Red Team, Blue Team, White Team, classroom training. online training
  - –**Test Configurations** - HW/SW/Firmware Updates, Network configurations
  - –**Simulate** new attacks and IT Outages
  - –**Cyber DevOps Support** for Security testing and design for security
  - –**PoCs** for new equipment, vendors, architectures
  - –**Application Compliance Assessment** for Security Reporting



Cyber Range Stakeholders/Tasks



PEOPLE

PROCESS

TECHNOLOGY

IT Cyber Range Admin

- Spin up virtual/physical resources
- Manage IT Infrastructure (Cloud)
- Deliver conflict free range
- Manage roles/users/domains
- Automation Scripts

Content Developers – Exercise/Train

- Sharing Cyber topologies
- Developing reusable content and training
- Application/Service Performance
- LMS support

End User

- Ease of access/availability
- Ease of use of resources/apps
- Real world replication
- Catalog of Cyber Ranges
- Integration into End User environment

Management

- Analysis of performance of Range
- Analysis of end user performance
- Cycle time for next deployment
- Personnel and Process Alignment
- Costs

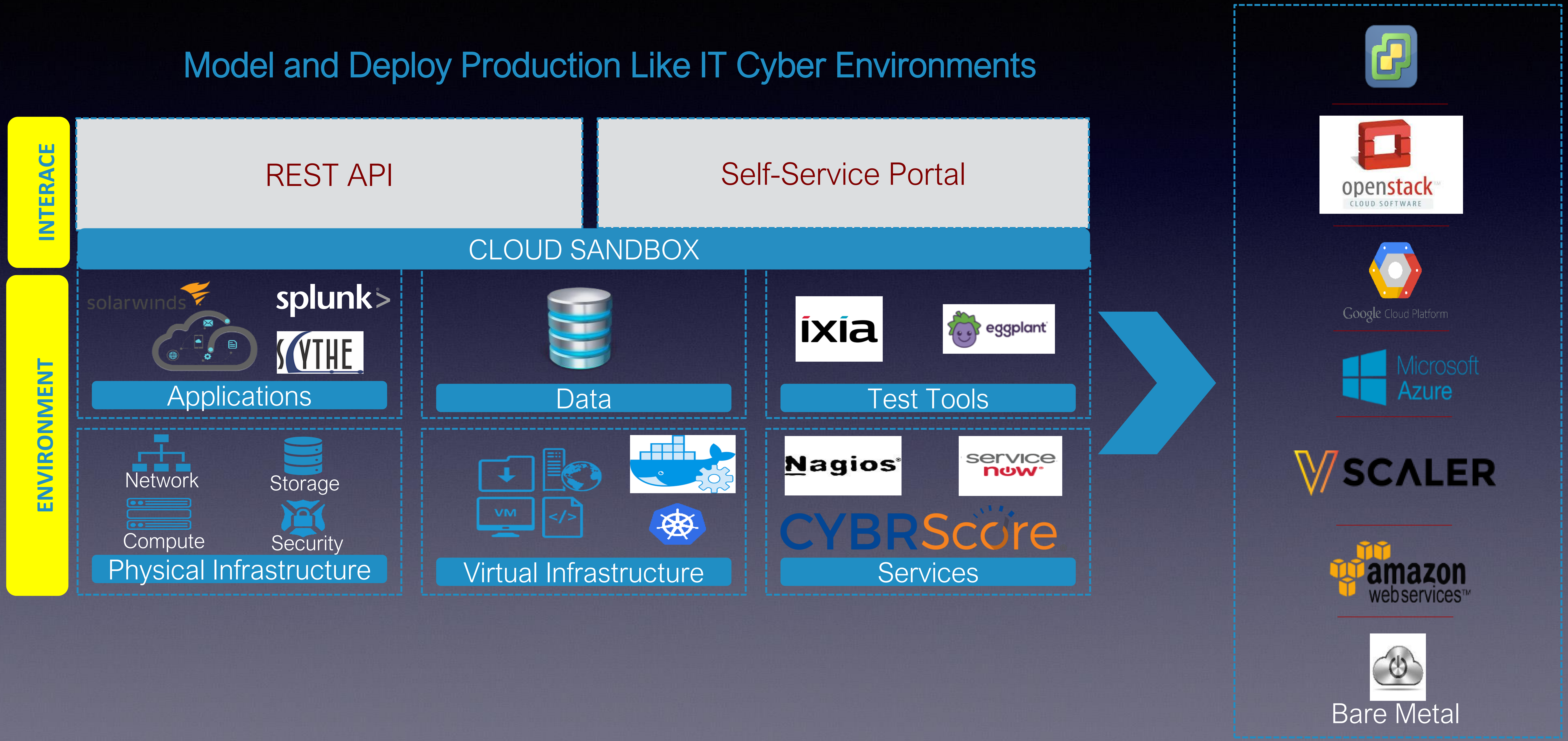
Challenges for Delivering Cyber Ranges

- Support multiple use cases
  - Training, Exercises, Virtual, Physical and Hybrid, DevOps, on-prem/off-prem, multiple clouds, public/private clouds
- Life Cycle Management of a Cyber Range is complex
  - Administration and IT Support is expensive and time consuming
  - IT Fulfillment is complex, End user content constantly changing
  - Support of new technologies and infrastructure (clouds)
  - Keeping your Cyber Range up to date (matching production)
  - Capturing Metrics on the usefulness of the range is difficult (CAPEX and OPEX)
- Fragmented Access and Users
  - Web portal, Scheduling/reserving, managing resource conflicts, accessing resources, no self service
- Reuse of Automation of complex setups and tasks in the Cyber Range
  - Save and Restore, higher quality/repeatability – performance
- Others?

Cyber Range as a Service®

Model and Deploy Production Like IT Cyber Environments

ANY CLOUD or DATA CENTER



INTERACE

REST API

Self-Service Portal

CLOUD SANDBOX

ENVIRONMENT

Applications

Data

Test Tools

Network

Storage

Compute

Security

Physical Infrastructure

Virtual Infrastructure

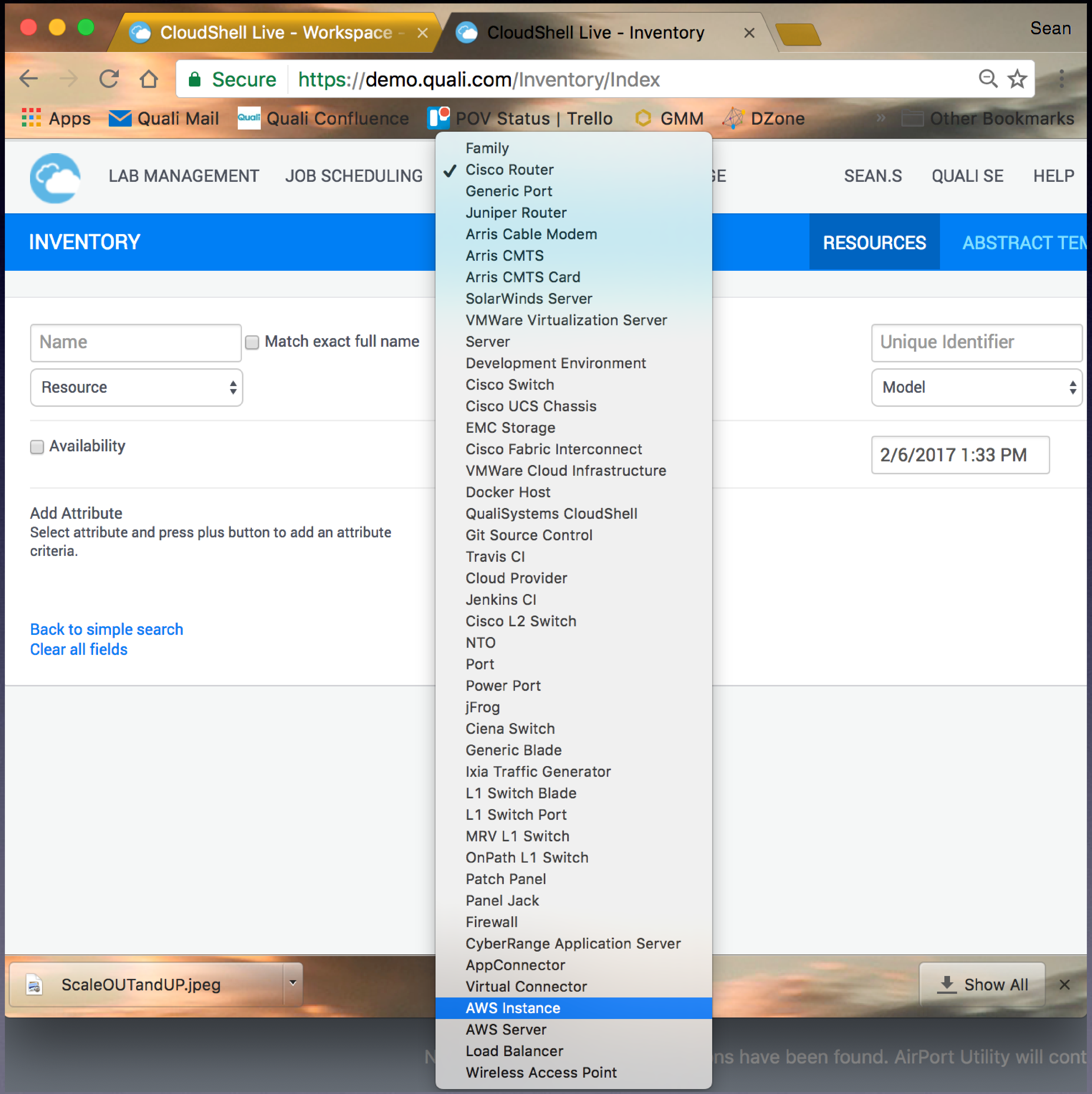
Services

Bare Metal

Manage the Inventory of your Range

Physical, Virtual, App, Service, Cloud(s)

- Autoload Shells, DCIM integration, asset DB synchronization, etc.
  - Typically fully automated
  - Integrated with business process workflows
- Physical & virtual resources, apps, services, connectivity
- Build your Cyber Range infrastructure from your lab assets (see CRaaS Library of Assets)



Name

□ Match exact full name

Resource

□ Availability

Unique Identifier

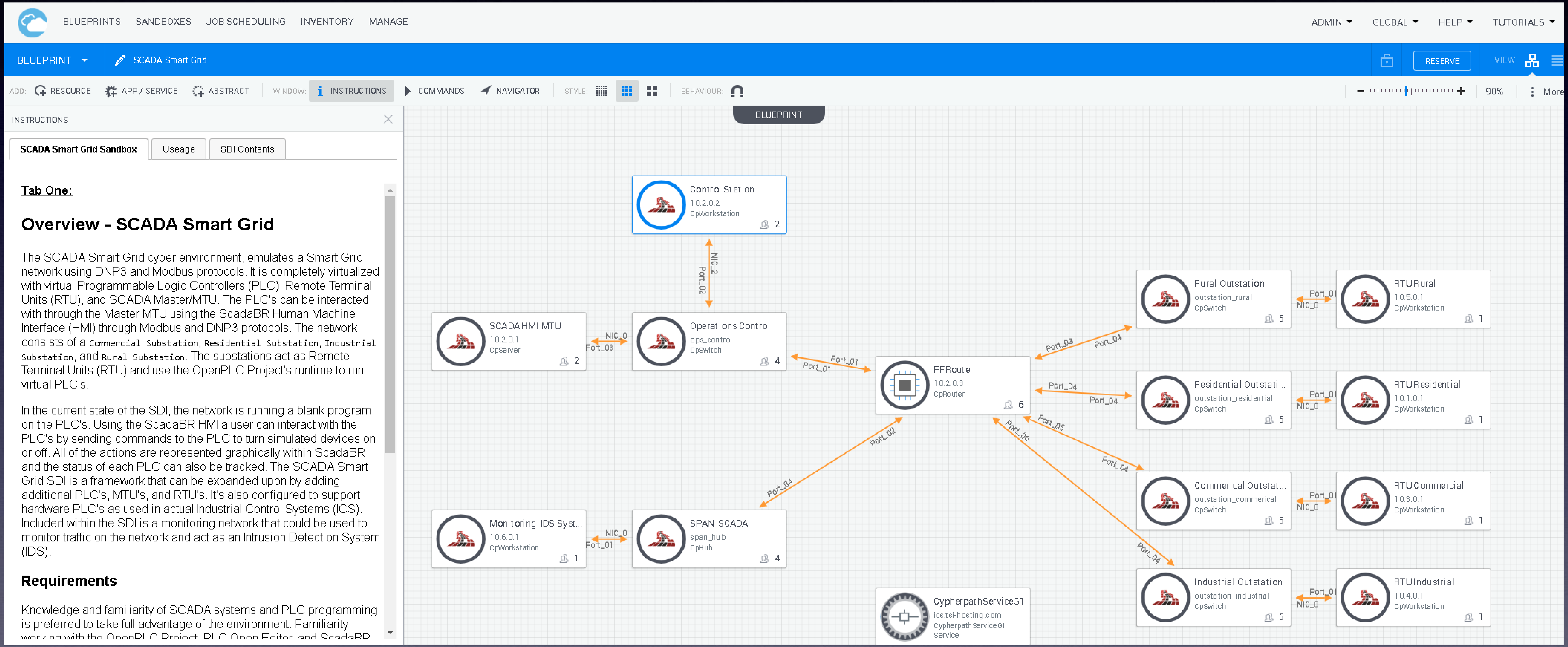
Model

2/6/2017 1:33 PM

Add Attribute
Select attribute and press plus button to add an attribute criteria.

Model IT Blueprints for Cyber Range

- Visual based Drag and drop directly from inventory
- Abstract complexity (pool support)
- Set connectivity based on infrastructure
- Any Physical, Virtual, Cloud(s), Apps
- Model is “Automation Ready”
- Replica of your Production IT Infrastructure with configuration management



Tab One:

Overview - SCADA Smart Grid

The SCADA Smart Grid cyber environment, emulates a Smart Grid network using DNP3 and Modbus protocols. It is completely virtualized with virtual Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), and SCADA Master/MTU. The PLC's can be interacted with through the Master MTU using the ScadaBR Human Machine Interface (HMI) through Modbus and DNP3 protocols. The network consists of a `Commercial Substation`, `Residential Substation`, `Industrial Substation`, and `Rural Substation`. The substations act as Remote Terminal Units (RTU) and use the OpenPLC Project's runtime to run virtual PLC's.

In the current state of the SDI, the network is running a blank program on the PLC's. Using the ScadaBR HMI a user can interact with the PLC's by sending commands to the PLC to turn simulated devices on or off. All of the actions are represented graphically within ScadaBR and the status of each PLC can also be tracked. The SCADA Smart Grid SDI is a framework that can be expanded upon by adding additional PLC's, MTU's, and RTU's. It's also configured to support hardware PLC's as used in actual Industrial Control Systems (ICS). Included within the SDI is a monitoring network that could be used to monitor traffic on the network and act as an Intrusion Detection System (IDS).

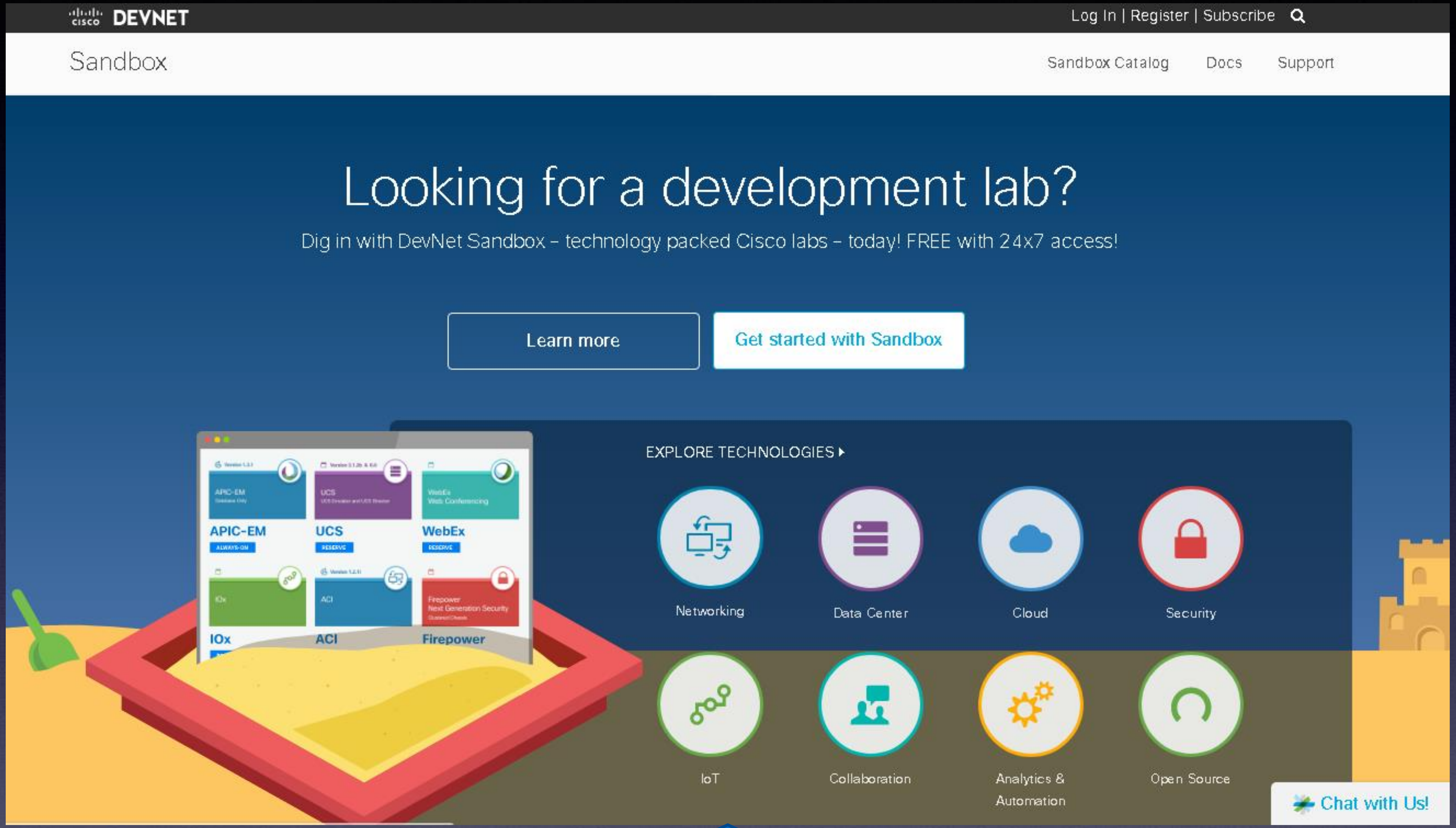
Requirements

Knowledge and familiarity of SCADA systems and PLC programming is preferred to take full advantage of the environment. Familiarity working with the OpenPLC Project, PLC Open Editor, and ScadaBR

Think Live Visio Diagram!

Publish Catalog of Cyber Range Blueprints

- Publish Blueprints Catalogs
  - Save environment as Blueprint, publish for others to use
  - Standardize Cyber Range test beds and cyber training environments as Blueprints for consistent results
- Self-service access to Cyber assets using Blueprints
- Define how Cyber blueprints are consumed by end users
  - Forms / inputs
  - User access / categories / domains

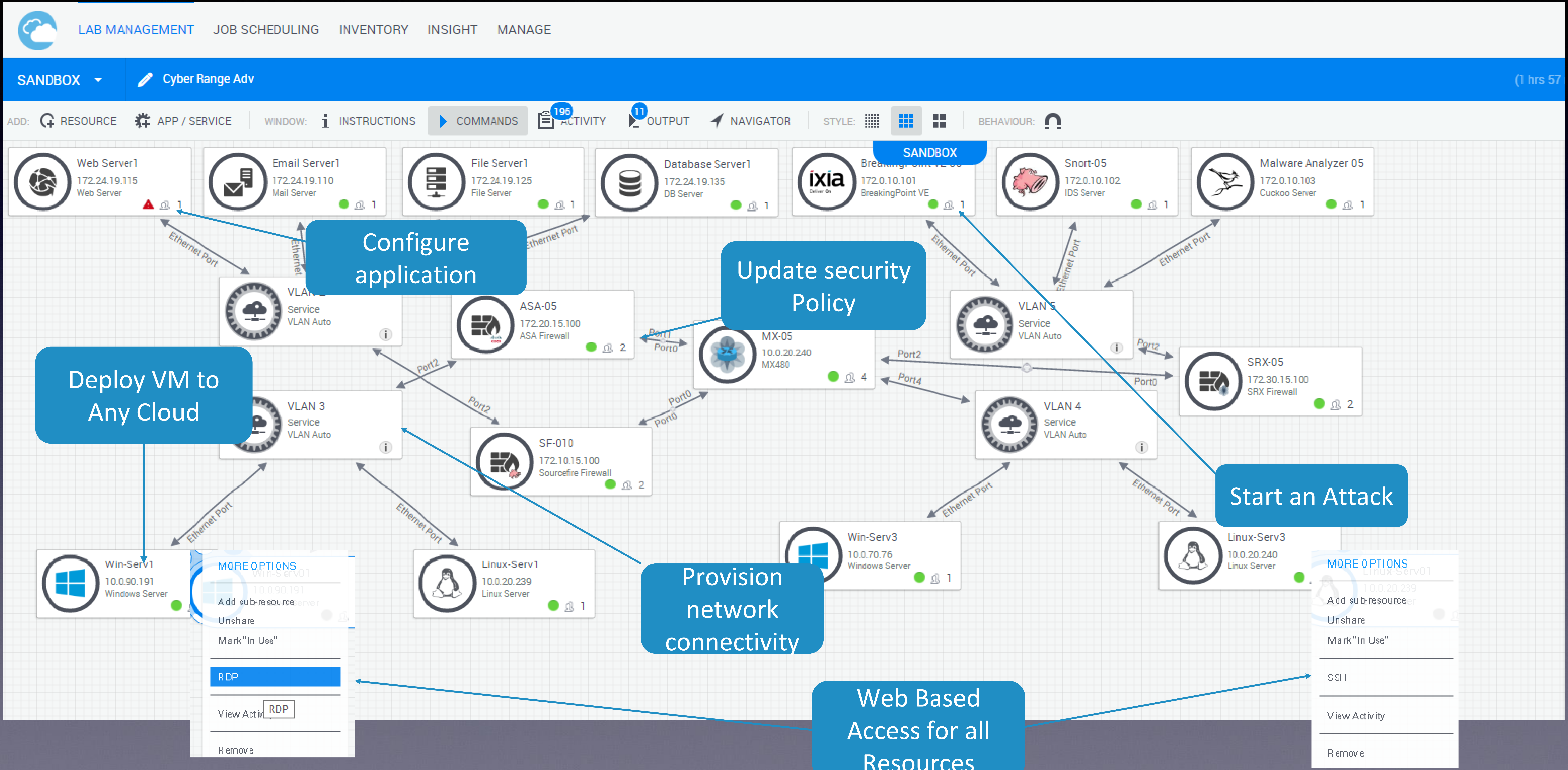


Looking for a development lab?

Dig in with DevNet Sandbox – technology packed Cisco labs – today! FREE with 24x7 access!

http://developer.cisco.com for a complete implementation of an Infrastructure Catalog – Over 700,000 registered users!

Cyber Range as a Service Sandbox


LAB MANAGEMENT
JOB SCHEDULING
INVENTORY
INSIGHT
MANAGE
SANDBOX
Cyber Range Adv
(1 hrs 57
ADD: RESOURCE
APP / SERVICE
WINDOW: INSTRUCTIONS
COMMANDS
196 ACTIVITY
11 OUTPUT
NAVIGATOR
STYLE:
BEHAVIOUR:
SANDBOX
Web Server1 172.24.19.115 Web Server
Email Server1 172.24.19.110 Mail Server
File Server1 172.24.19.125 File Server
Database Server1 172.24.19.135 DB Server
BreakingPoint VE 172.0.10.101 BreakingPoint VE
Snort-05 172.0.10.102 IDS Server
Malware Analyzer 05 172.0.10.103 Cuckoo Server
VLAN 2 Service VLAN Auto
ASA-05 172.20.15.100 ASA Firewall
MX-05 10.0.20.240 MX480
VLAN 5 Service VLAN Auto
SRX-05 172.30.15.100 SRX Firewall
VLAN 3 Service VLAN Auto
SF-010 172.10.15.100 Sourcefire Firewall
VLAN 4 Service VLAN Auto
Win-Serv1 10.0.90.191 Windows Server
Linux-Serv1 10.0.20.239 Linux Server
Win-Serv3 10.0.70.76 Windows Server
Linux-Serv3 10.0.20.240 Linux Server
Ethernet Port
Port0
Port1
Port2
Port4
MORE OPTIONS
Add sub-resource
Unshare
Mark "In Use"
RDP
View Activity
Remove
MORE OPTIONS
Add sub-resource
Unshare
Mark "In Use"
SSH
View Activity
Remove

Configure application

Update security Policy

Deploy VM to Any Cloud

Start an Attack

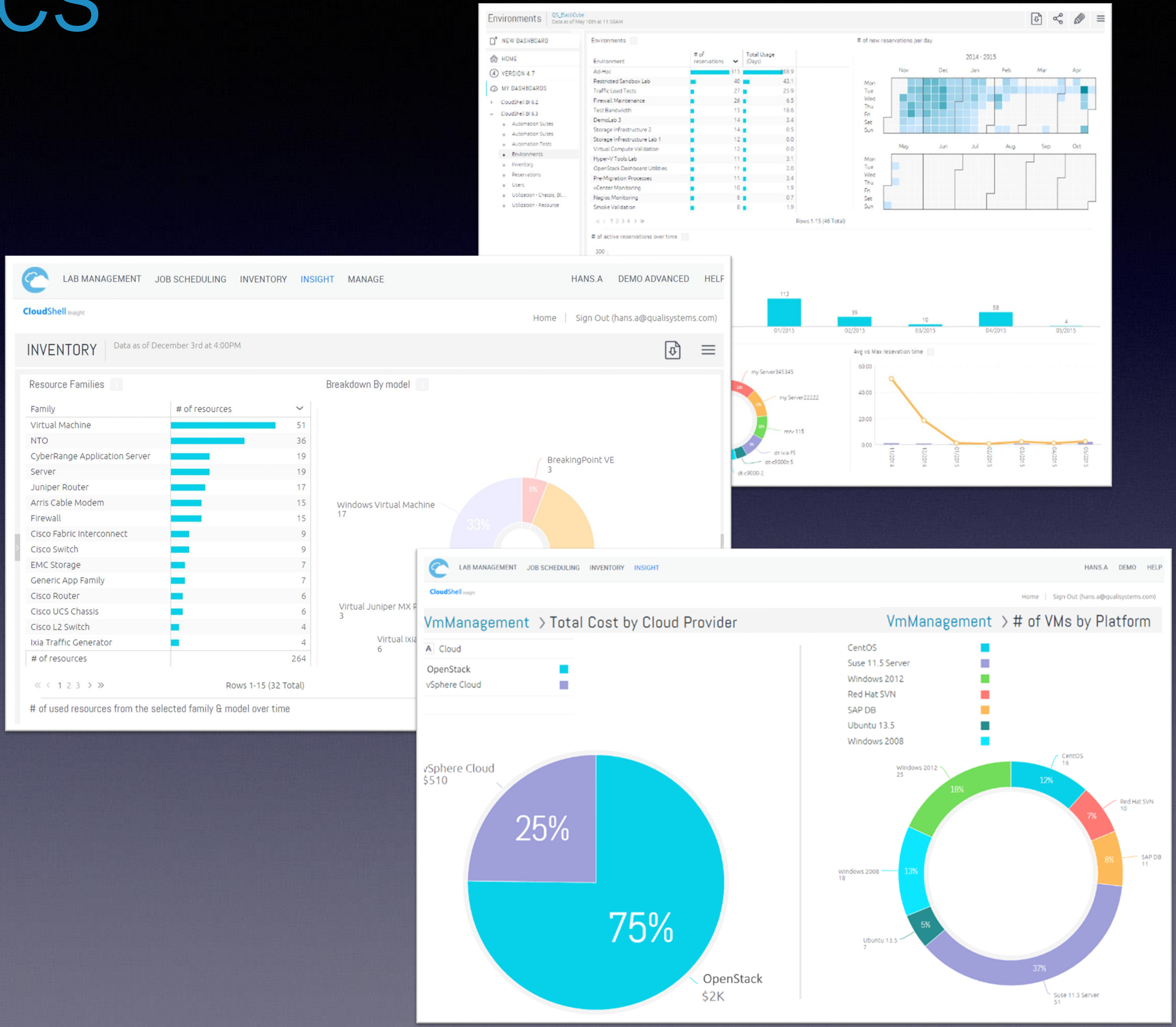
Provision network connectivity

Web Based Access for all Resources

BI & Analytics

Metrics on your Cyber Range

- Analysis for actionable decision making
  - capture usage trends
- Attributes - define meaningful data based on decisions needed
- Usage and utilization
- Capturing needed data and details
- Measure usage of resources



Environments | QS_ElastiCube Data as of May 10th at 11:58AM

NEW DASHBOARD
HOME
VERSION 4.7
MY DASHBOARDS
CloudShell BI 6.2
CloudShell BI 6.3
Automation Suites
Automation Suites
Automation Tests
Environments
Inventory
Reservations
Users
Utilization - Chassis, Bl...
Utilization - Resource

Environments

Environment	# of reservations	Total Usage (Days)
Ad-Hoc	315	68.9
Restricted Sandbox Lab	40	43.1
Traffic Load Tests	27	25.9
Firewall Maintenance	26	6.5
Test Bandwidth	15	18.6
DemoLab 3	14	3.4
Storage Infrastructure 2	14	0.5
Storage Infrastructure Lab 1	12	0.0
Virtual Compute Validation	12	0.0
Hyper-V Tools Lab	11	3.1
OpenStack Dashboard Utilities	11	2.0
Pre-Migration Processes	11	3.4
vCenter Monitoring	10	1.9
Negios Monitoring	8	0.7
Smoke Validation	8	1.9

« ‹ 1 2 3 4 › » Rows 1-15 (46 Total)

# of new reservations per day

# of active reservations over time

Avg vs Max reservation time

LAB MANAGEMENT JOB SCHEDULING INVENTORY INSIGHT MANAGE HANS.A DEMO ADVANCED HELP

CloudShell Insight

Home | Sign Out (hans.a@qualisystems.com)

INVENTORY | Data as of December 3rd at 4:00PM

Resource Families

Family	# of resources
Virtual Machine	51
NTO	36
CyberRange Application Server	19
Server	19
Juniper Router	17
Arris Cable Modem	15
Firewall	15
Cisco Fabric Interconnect	9
Cisco Switch	9
EMC Storage	7
Generic App Family	7
Cisco Router	6
Cisco UCS Chassis	6
Cisco L2 Switch	4
Ixia Traffic Generator	4
# of resources	264

« ‹ 1 2 3 › » Rows 1-15 (32 Total)

# of used resources from the selected family & model over time

Breakdown By model

LAB MANAGEMENT JOB SCHEDULING INVENTORY INSIGHT HANS.A DEMO HELP

CloudShell Insight

Home | Sign Out (hans.a@qualisystems.com)

VmManagement › Total Cost by Cloud Provider

Cloud	
OpenStack	🟦
vSphere Cloud	🟪

VmManagement › # of VMs by Platform

CentOS	🟦
Suse 11.5 Server	🟪
Windows 2012	🟩
Red Hat SVN	🟥
SAP DB	🟧
Ubuntu 13.5	🟦
Windows 2008	🟦

Cyber Range as a Service Workflow

Quickly And Effectively Build out and consume Cyber Ranges – Stepped Process

WORKFLOW

1 INVENTORY

- Discovery
- Configuration (P/V Infra., Applications)
- User to group mapping
- Reservable

2 MODEL

- P/V Infra.
- Applications
- Database
- Tools
- Service
- Drag-n-drop

3 CREATE BLUEPRINTS

- Publish self-service catalogs
- Workflows
- Standardized

4 AUTOMATE & ORCHESTRATE

- Reserve and Deploy
- Active Environments "CyberRange Sandboxes"
- Deploy on any cloud

5 CONSUME

- Single pane of glass
- One click RDP, SSH and Web
- API Access
- Tools

6 BI & ANALYTICS

- Measure
  - Visibility
  - Costing
  - Utilization
  - RoI

INFRA/APP OWNER | BLUEPRINT DESIGNER | BLUEPRINT CONSUMER | BLUEPRINT CONSUMER | INFRA/APP OWNER

Why Cyber Range as a Service®

- Increase agility, responsiveness and repeatability
  - Support of new technologies and infrastructure
    - Clouds, on-prem/off-prem, hybrid, apps, containers, services
  - Automation of provisioning and orchestration
  - Base lining of device/application/service/content
- Lessen administrative burden
  - Implement infrastructure/automation reuse to deliver Cyber Ranges Faster
- Broaden and control use case adoption
  - Easy to consume service catalogs
  - Support domains and roles
- Better utilization of the Cyber Range infrastructure
  - Scheduling and reserving to utilize the infrastructure more efficiently
  - Spin-up/spin-down of resources with scheduling and reserving (Saving power)
- Easier to implement Business Analytics

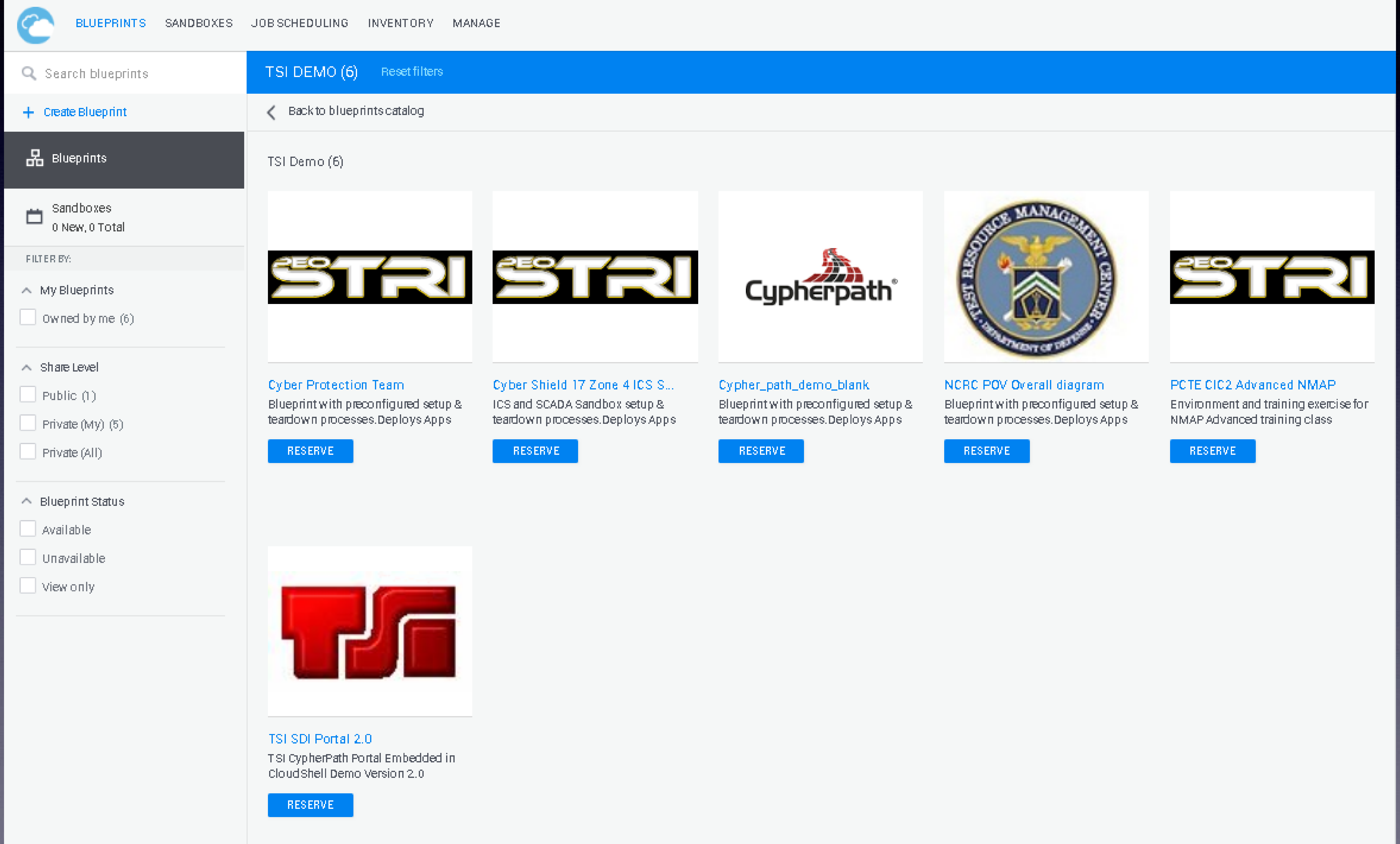
CyberRange as a Service® Advantage

ICS Cyber Range

Traditional Approach		CyberRange-as-a-Service	
Design Environment Manual: Visio, Powerpoint	Hours	Minutes	**Model & Publish Blueprint** Drag n' drop from asset inventory, connectivity, abstract blueprint
Request I.T. Dedicated P/V Infrastructure	Hours	Minutes	**Self-Service** On-demand equipment reservation and scheduling
I.T. Fulfillment Rack and Stack, Configure, Validation, Approval	Days/ Months	Minutes	**Automate & Orchestrate** Simplified configuration and provisioning, save and restore.
Fragmented Access Telnet, SSH, RDP, API, CLI	Complex	Simple	**Unified Access** Embedded Web-portal
Fragmented Users Single user access, conflicts, hoarding	Siloed	Shared/ Reused	**Multi-Tenant + Scalable** Consolidated labs, global shared user base, **Community**

VS

Examples



Search blueprints

+ Create Blueprint

Blueprints

Sandboxes
0 New, 0 Total

FILTER BY:

My Blueprints

□ Owned by me (6)

Share Level

□ Public (1)

□ Private (My) (5)

□ Private (All)

Blueprint Status

□ Available

□ Unavailable

□ View only

TSI DEMO (6) Reset filters

Back to blueprints catalog

TSI Demo (6)

Cyber Protection Team
Blueprint with preconfigured setup & teardown processes.Deploys Apps
RESERVE

Cyber Shield 17 Zone 4 ICS S...
ICS and SCADA Sandbox setup & teardown processes.Deploys Apps
RESERVE

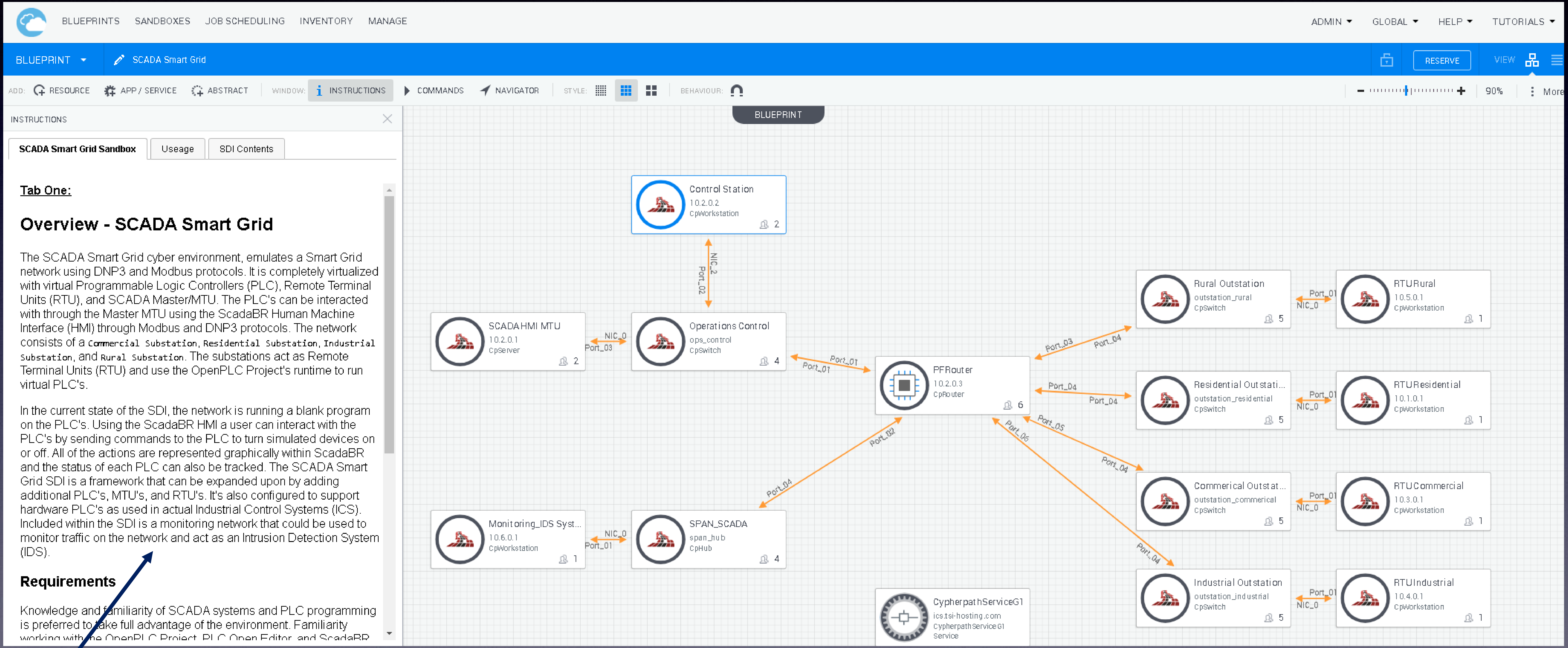
Cypher_path_demo_blank
Blueprint with preconfigured setup & teardown processes.Deploys Apps
RESERVE

NCRC POV Overall diagram
Blueprint with preconfigured setup & teardown processes.Deploys Apps
RESERVE

PCTE CIC2 Advanced NMAP
Environment and training exercise for NMAP Advanced training class
RESERVE

TSI SDI Portal 2.0
TSI CypherPath Portal Embedded in CloudShell Demo Version 2.0
RESERVE

ICS SCADA Smart Grid



Tab One:

Overview - SCADA Smart Grid

The SCADA Smart Grid cyber environment, emulates a Smart Grid network using DNP3 and Modbus protocols. It is completely virtualized with virtual Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), and SCADA Master/MTU. The PLC's can be interacted with through the Master MTU using the ScadaBR Human Machine Interface (HMI) through Modbus and DNP3 protocols. The network consists of a `Commercial Substation`, `Residential Substation`, `Industrial Substation`, and `Rural Substation`. The substations act as Remote Terminal Units (RTU) and use the OpenPLC Project's runtime to run virtual PLC's.

In the current state of the SDI, the network is running a blank program on the PLC's. Using the ScadaBR HMI a user can interact with the PLC's by sending commands to the PLC to turn simulated devices on or off. All of the actions are represented graphically within ScadaBR and the status of each PLC can also be tracked. The SCADA Smart Grid SDI is a framework that can be expanded upon by adding additional PLC's, MTU's, and RTU's. It's also configured to support hardware PLC's as used in actual Industrial Control Systems (ICS). Included within the SDI is a monitoring network that could be used to monitor traffic on the network and act as an Intrusion Detection System (IDS).

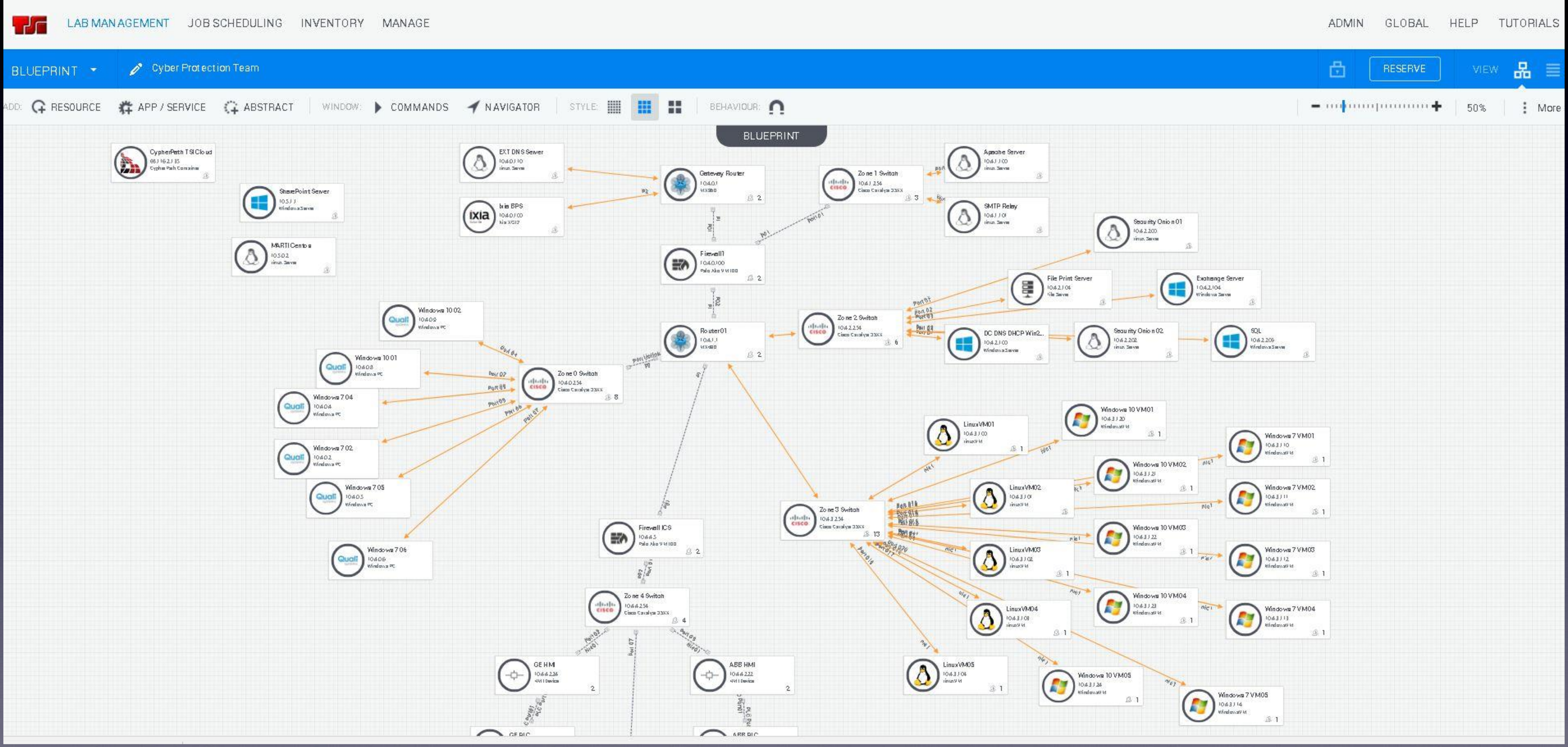
Requirements

Knowledge and familiarity of SCADA systems and PLC programming is preferred to take full advantage of the environment. Familiarity working with the OpenPLC Project, PLC Open Editor, and ScadaBR

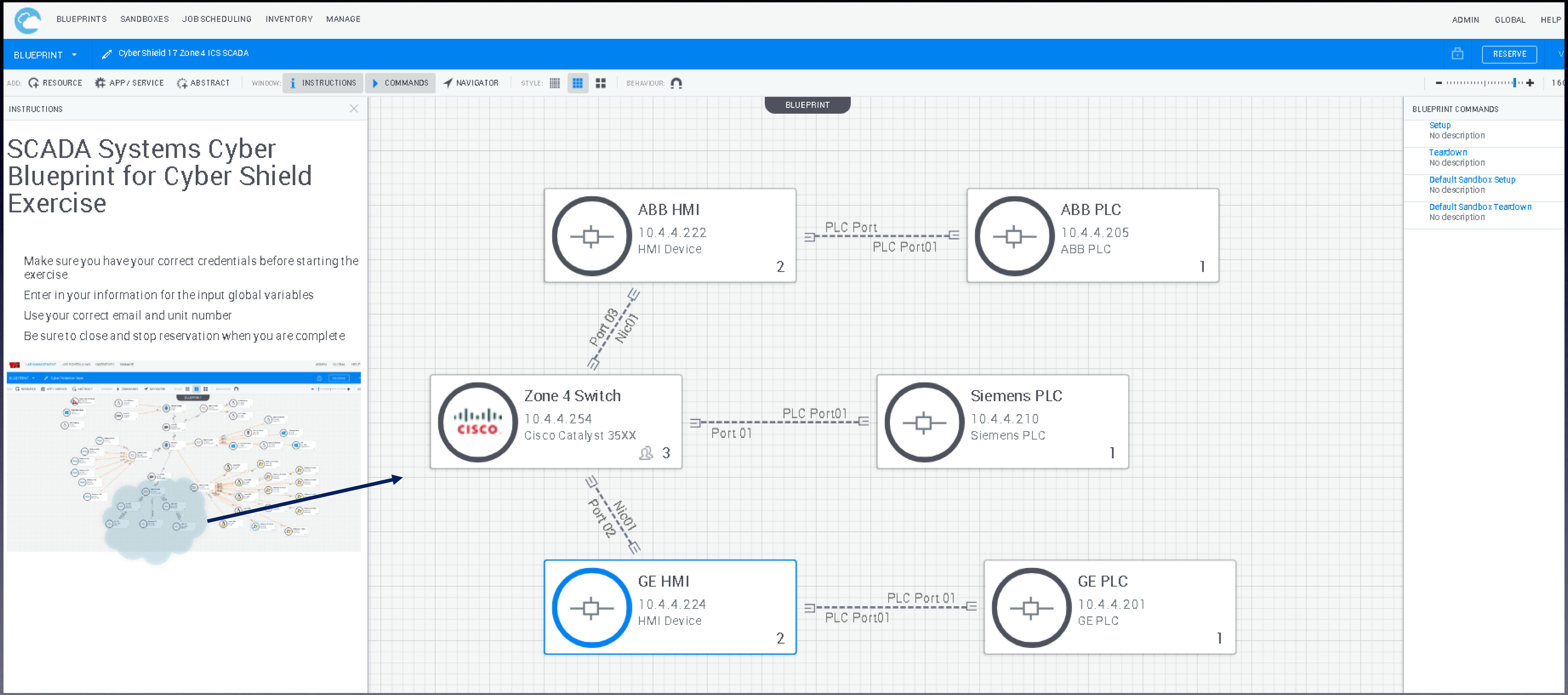
LMS – Instructions
HTML5
Easy to build

Your Cyber Range or Training Environment – Deploy to Any Cloud and/or Physical

Cyber Exercise Full View



Cyber Exercise ICS SCADA Only View



SCADA Systems Cyber Blueprint for Cyber Shield Exercise

Make sure you have your correct credentials before starting the exercise

Enter in your information for the input global variables

Use your correct email and unit number

Be sure to close and stop reservation when you are complete

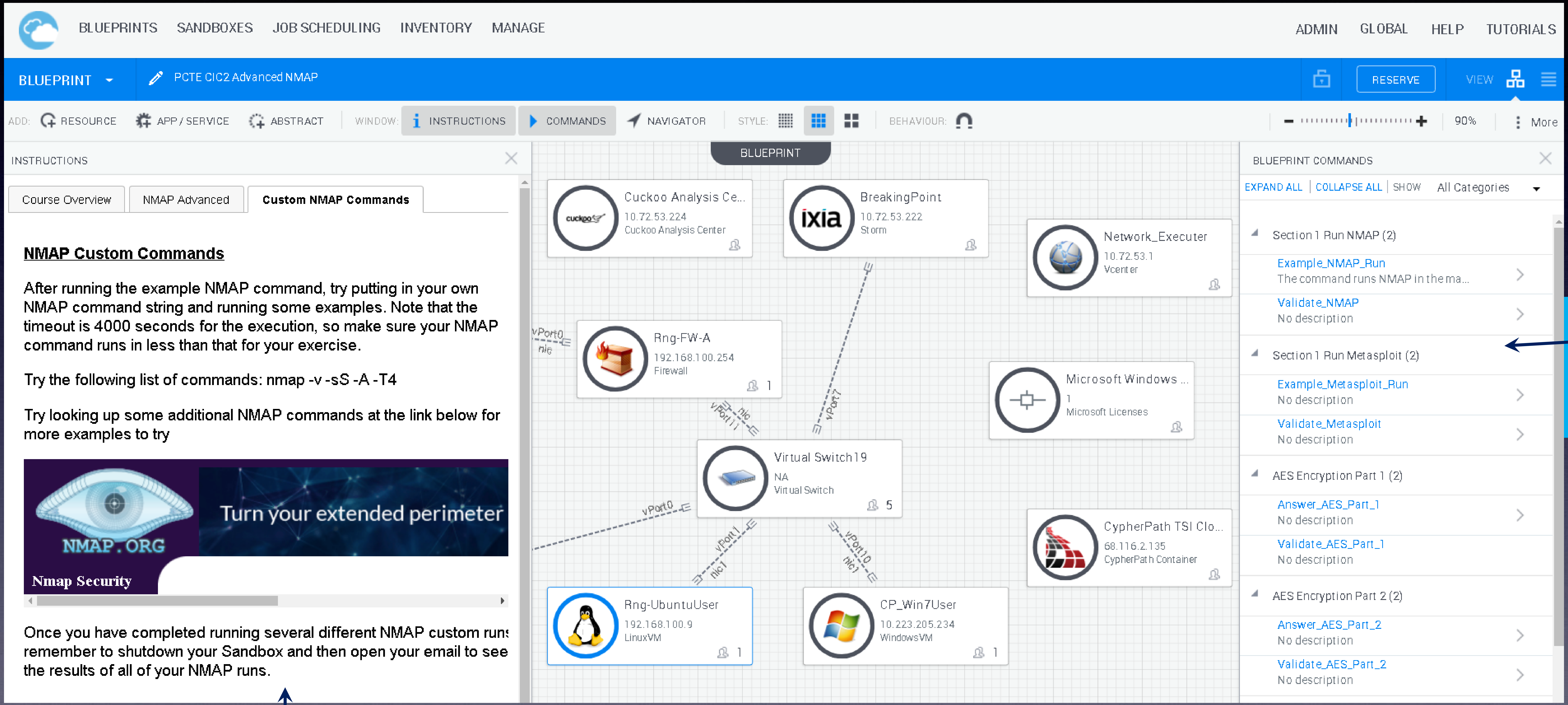
Setup
No description

Teardown
No description

Default Sandbox Setup
No description

Default Sandbox Teardown
No description

Physical and Virtual Training Exercise/Range



NMAP Custom Commands

After running the example NMAP command, try putting in your own NMAP command string and running some examples. Note that the timeout is 4000 seconds for the execution, so make sure your NMAP command runs in less than that for your exercise.

Try the following list of commands: nmap -v -sS -A -T4

Try looking up some additional NMAP commands at the link below for more examples to try

Once you have completed running several different NMAP custom runs remember to shutdown your Sandbox and then open your email to see the results of all of your NMAP runs.

Section 1 Run NMAP (2)
- Example_NMAP_Run
  The command runs NMAP in the ma...
- Validate_NMAP
  No description

Section 1 Run Metasploit (2)
- Example_Metasploit_Run
  No description
- Validate_Metasploit
  No description

AES Encryption Part 1 (2)
- Answer_AES_Part_1
  No description
- Validate_AES_Part_1
  No description

AES Encryption Part 2 (2)
- Answer_AES_Part_2
  No description
- Validate_AES_Part_2
  No description

Automation
For provisioning, training, grading and response monitoring

LMS embedded – HTML5
Easy to build – drag N Drop embed Videos, links, PPTX, PDF, Web, etc.

Supports online or classroom training or exercise environments

Full Production Replica with Automated Configuration Management Deploying to any Cloud

BLUEPRINT
NCRC POV Overall diagram
ADD: RESOURCE
APP / SERVICE
ABSTRACT
WINDOW: COMMANDS
NAVIGATOR
STYLE:
BEHAVIOUR:
BLUEPRINT
Microsoft Windows ...
1
Microsoft Licenses
lariat-is1
Application
DNS-NTP
Application
spb-wks01
Application
spb-mail01
Application
spb-wks02
Application
Internet-rtr
Application
Core 01
Application
spb-web02
Application
spb-wks03
Application
VLAN
VLAN
Service
Core 04
Application
spb-web01
Application
spb-wks04
Application
Core 03
Application
spb-dc02
Application
spb-wks05
Application
spb-dc01
Application
vCenter Clone VM From VM
vCenter VM From Template
vCenter Deploy VM From Linked Clone
vCenter VM From Image
AWS EC2 Instance
Azure VM From Marketplace
Azure VM From Custom Image
General
Deployment Paths (1)
Configuration Management
App Resource
Add New Deployment Path
Done
Cancel
General
Deployment Paths
Configuration Management
App Resource
Done
Cancel

CORE 03

VCenter - VCenter Deploy V

DEPLOYMENT	VCenter Deploy VM From Linked Clone
CLOUD PROVIDER	VCenter
VCENTER VM	Vyos
VCENTER VM SNAPSHOT	Enter Value

SPB-DC01

SELECT TOOL	Script
CONNECTION METHOD	Windows Remote Management

Script Location

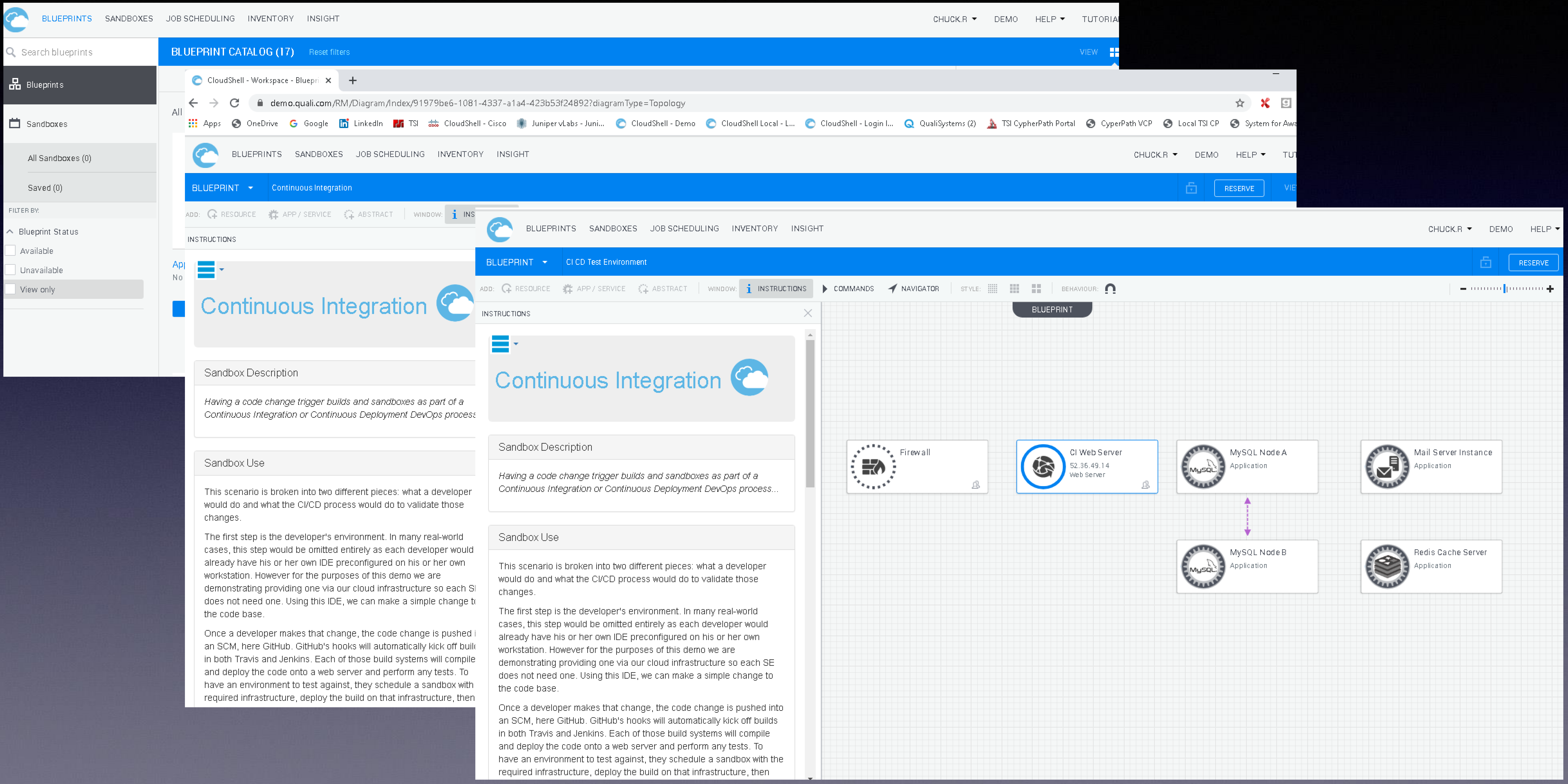
URL	http://ftp.tsieda.com
USER	admin
PASSWORD	••••••••

Parameters

EHT2	20.169.82.2
OU1	spbclients

CM support - Ansible, Puppet, Chef, PS, Bash, Scripts etc.

DevSecOps - CI/CD Flow Automation and Self Service



Continuous Integration

Sandbox Description

Having a code change trigger builds and sandboxes as part of a Continuous Integration or Continuous Deployment DevOps process

Sandbox Use

This scenario is broken into two different pieces: what a developer would do and what the CI/CD process would do to validate those changes.

The first step is the developer's environment. In many real-world cases, this step would be omitted entirely as each developer would already have his or her own IDE preconfigured on his or her own workstation. However for the purposes of this demo we are demonstrating providing one via our cloud infrastructure so each SI does not need one. Using this IDE, we can make a simple change t the code base.

Once a developer makes that change, the code change is pushed i an SCM, here GitHub. GitHub's hooks will automatically kick off buil in both Travis and Jenkins. Each of those build systems will compile and deploy the code onto a web server and perform any tests. To have an environment to test against, they schedule a sandbox with required infrastructure, deploy the build on that infrastructure, then

Continuous Integration

Sandbox Description

Having a code change trigger builds and sandboxes as part of a Continuous Integration or Continuous Deployment DevOps process...

Sandbox Use

This scenario is broken into two different pieces: what a developer would do and what the CI/CD process would do to validate those changes.

The first step is the developer's environment. In many real-world cases, this step would be omitted entirely as each developer would already have his or her own IDE preconfigured on his or her own workstation. However for the purposes of this demo we are demonstrating providing one via our cloud infrastructure so each SE does not need one. Using this IDE, we can make a simple change to the code base.

Once a developer makes that change, the code change is pushed into an SCM, here GitHub. GitHub's hooks will automatically kick off builds in both Travis and Jenkins. Each of those build systems will compile and deploy the code onto a web server and perform any tests. To have an environment to test against, they schedule a sandbox with the required infrastructure, deploy the build on that infrastructure, then

Rebranded Catalogs – Multi-tenancy

BLUEPRINTS
SANDBOXES
JOB SCHEDULING
INVENTORY
MANAGE
ADMIN
GLOBAL
HELP
TUTORIALS
Search blueprints
Create Blueprint
Blueprints
Sandboxes
All Sandboxes (0)
Saved (0)
FILTER BY:
My Blueprints
Owned by me (8)
Share Level
Private (All)
Blueprint Status
Available
Unavailable
DHS HIRT (8)
Reset filters
VIEW
Back to blueprints catalog
RESERVE
Back to top
DIGIFLIGHT
Accelerate Mission Success

DHS HIRT (8)

Banking Financial HIRT Fly...
Blueprint with preconfigured setup & teardown processes. Deploys Apps

Healthcare HIRT Flyaway Kit
Blueprint with preconfigured setup & teardown processes. Deploys Apps

HIRT Base System
Blueprint with preconfigured setup & teardown processes. Deploys Apps

HIRT Base System w Targe...
Blueprint with preconfigured setup & teardown processes. Deploys Apps

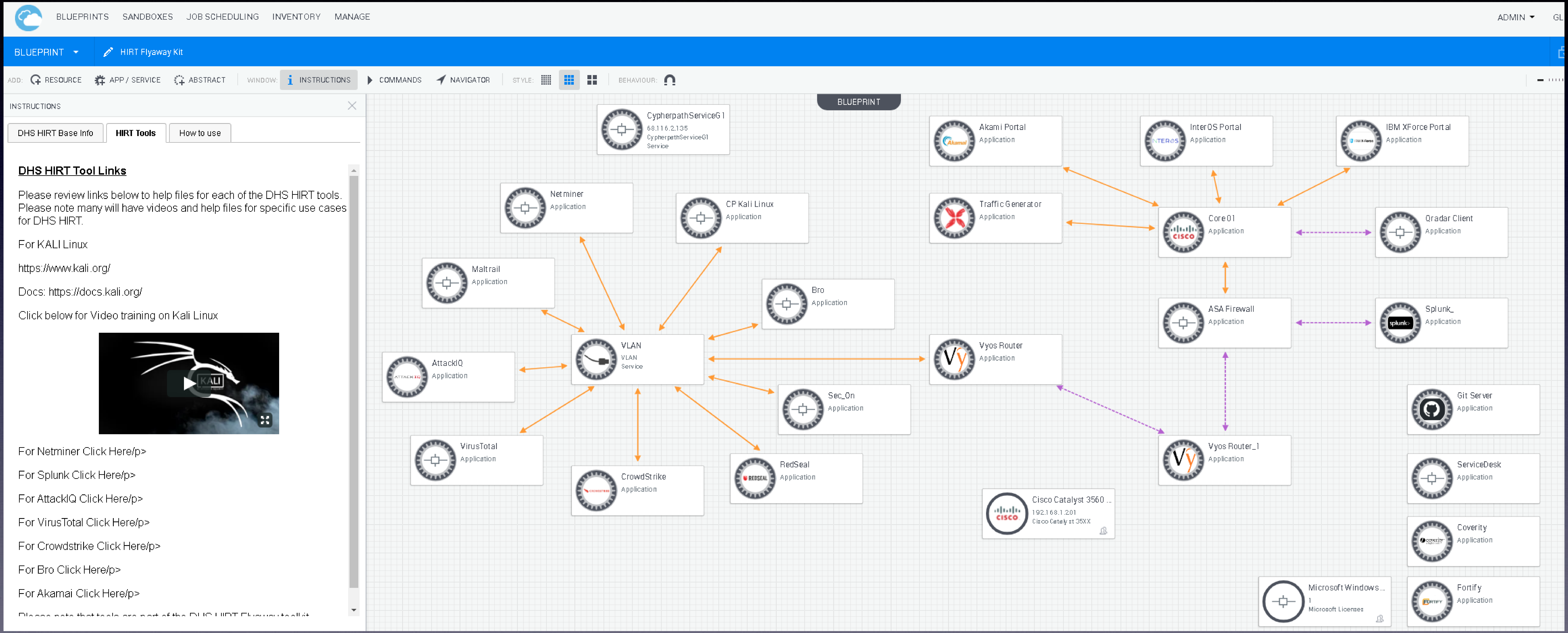
HIRT Flyaway Kit
Blueprint with preconfigured setup & teardown processes. Deploys Apps

DHS HIRT
No description

ALL CATEGORIES

- CypherPath
- LaaS
- Aberdeen Proving Grounds
- JITC/DISA Test Sandboxes

HIRT Flyaway Kit – Self service with Instructions Cyber Range as a Service® in a box



DHS HIRT Tool Links

Please review links below to help files for each of the DHS HIRT tools. Please note many will have videos and help files for specific use cases for DHS HIRT.

For KALI Linux

https://www.kali.org/

Docs: https://docs.kali.org/

Click below for Video training on Kali Linux

For Netminer Click Here/p>

For Splunk Click Here/p>

For AttackIQ Click Here/p>

For VirusTotal Click Here/p>

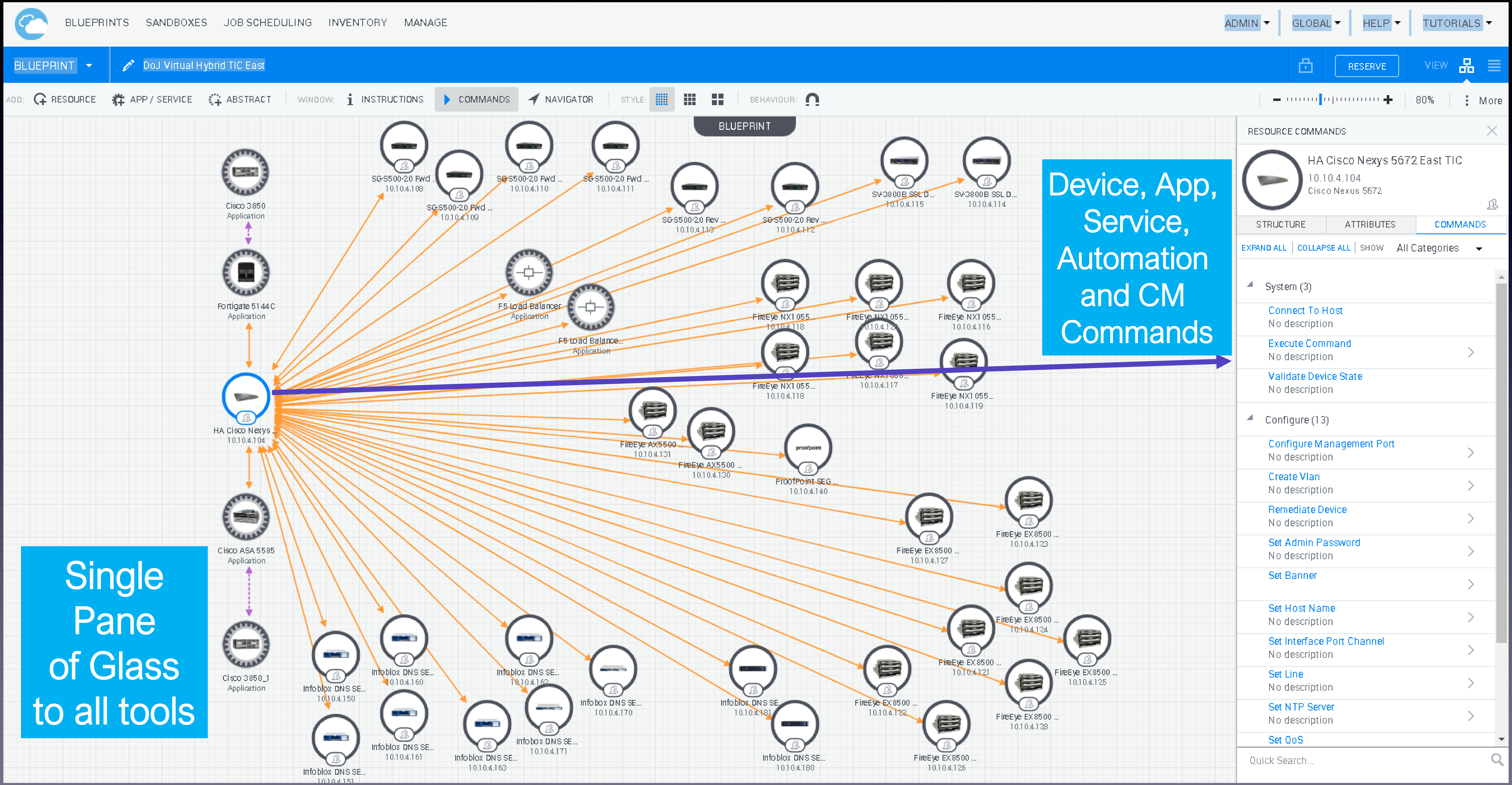
For Crowdstrike Click Here/p>

For Bro Click Here/p>

For Akamai Click Here/p>

Please note that tools are part of the DHS HIRT Flyaway toolkit

Automated OT Dashboard – NOC/SOC



BLUEPRINTS
SANDBOXES
JOB SCHEDULING
INVENTORY
MANAGE
ADMIN
GLOBAL
HELP
TUTORIALS
BLUEPRINT
DoJ Virtual Hybrid TIC East
RESERVE
VIEW
ADD: RESOURCE
APP / SERVICE
ABSTRACT
WINDOW: INSTRUCTIONS
COMMANDS
NAVIGATOR
STYLE:
BEHAVIOUR:
80%
More
BLUEPRINT
Cisco 3850 Application
Fortigate 5144C Application
HA Cisco Nexys ... 10.10.4.104
Cisco ASA 5585 Application
Cisco 3850_1 Application
SG-S500-20 Fwd ... 10.10.4.108
SG-S500-20 Fwd ... 10.10.4.109
SG-S500-20 Fwd ... 10.10.4.110
SG-S500-20 Fwd ... 10.10.4.111
SG-S500-20 Rev ... 10.10.4.113
SG-S500-20 Rev ... 10.10.4.112
SV-3800B SSL D... 10.10.4.115
SV-3800B SSL D... 10.10.4.114
F5 Load Balancer Application
F5 Load Balance... Application
FireEye NX1055... 10.10.4.118
FireEye NX1055... 10.10.4.12
FireEye NX1055... 10.10.4.116
FireEye NX1055... 10.10.4.118
10.10.4.117
FireEye NX1055... 10.10.4.119
FireEye AX5500 ... 10.10.4.131
FireEye AX5500 ... 10.10.4.130
ProofPoint SEG ... 10.10.4.140
FireEye EX8500 ... 10.10.4.127
FireEye EX8500 ... 10.10.4.123
FireEye EX8500 ... 10.10.4.124
FireEye EX8500 ... 10.10.4.121
FireEye EX8500 ... 10.10.4.125
FireEye EX8500 ... 10.10.4.122
FireEye EX8500 ... 10.10.4.128
FireEye EX8500 ... 10.10.4.126
Infoblox DNS SE... 10.10.4.150
Infoblox DNS SE... 10.10.4.151
Infoblox DNS SE... 10.10.4.160
Infoblox DNS SE... 10.10.4.161
Infoblox DNS SE... 10.10.4.162
Infoblox DNS SE... 10.10.4.163
Infoblox DNS SE... 10.10.4.170
Infoblox DNS SE... 10.10.4.171
Infoblox DNS SE... 10.10.4.181
Infoblox DNS SE... 10.10.4.180

RESOURCE COMMANDS

HA Cisco Nexys 5672 East TIC
10.10.4.104
Cisco Nexus 5672

STRUCTURE | ATTRIBUTES | COMMANDS

EXPAND ALL | COLLAPSE ALL | SHOW All Categories

System (3)

- Connect To Host
  No description
- Execute Command
  No description
- Validate Device State
  No description

Configure (13)

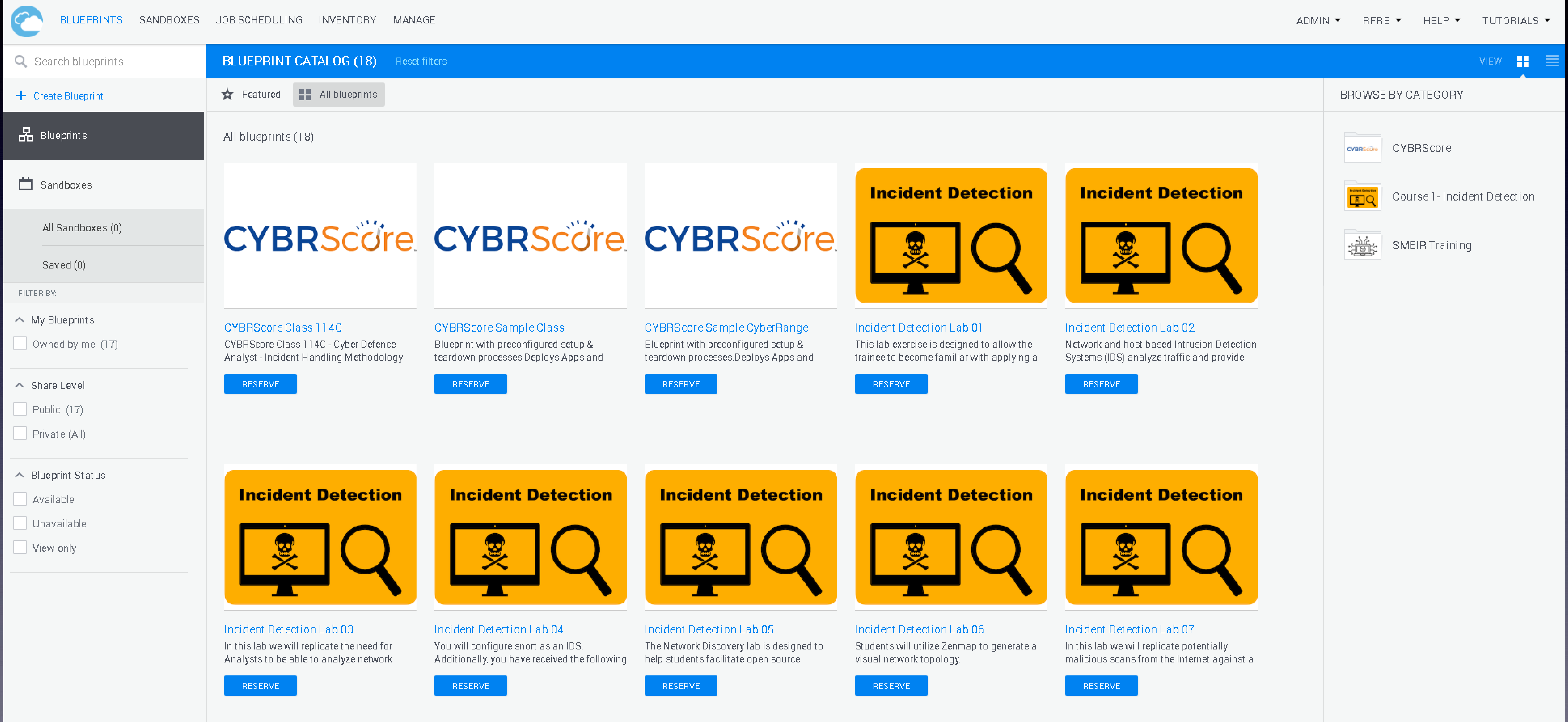
- Configure Management Port
  No description
- Create Vlan
  No description
- Remediate Device
  No description
- Set Admin Password
  No description
- Set Banner
- Set Host Name
  No description
- Set Interface Port Channel
  No description
- Set Line
  No description
- Set NTP Server
  No description
- Set QoS

Quick Search...

Device, App, Service, Automation and CM Commands

Single Pane of Glass to all tools

Cyber Range as a Service® – Online Cyber Catalog



All blueprints (18)

CYBRScore Class 114C
CYBRScore Class 114C - Cyber Defence Analyst - Incident Handling Methodology

CYBRScore Sample Class
Blueprint with preconfigured setup & teardown processes.Deploys Apps and

CYBRScore Sample CyberRange
Blueprint with preconfigured setup & teardown processes.Deploys Apps and

Incident Detection Lab 01
This lab exercise is designed to allow the trainee to become familiar with applying a

Incident Detection Lab 02
Network and host based Intrusion Detection Systems (IDS) analyze traffic and provide

Incident Detection Lab 03
In this lab we will replicate the need for Analysts to be able to analyze network

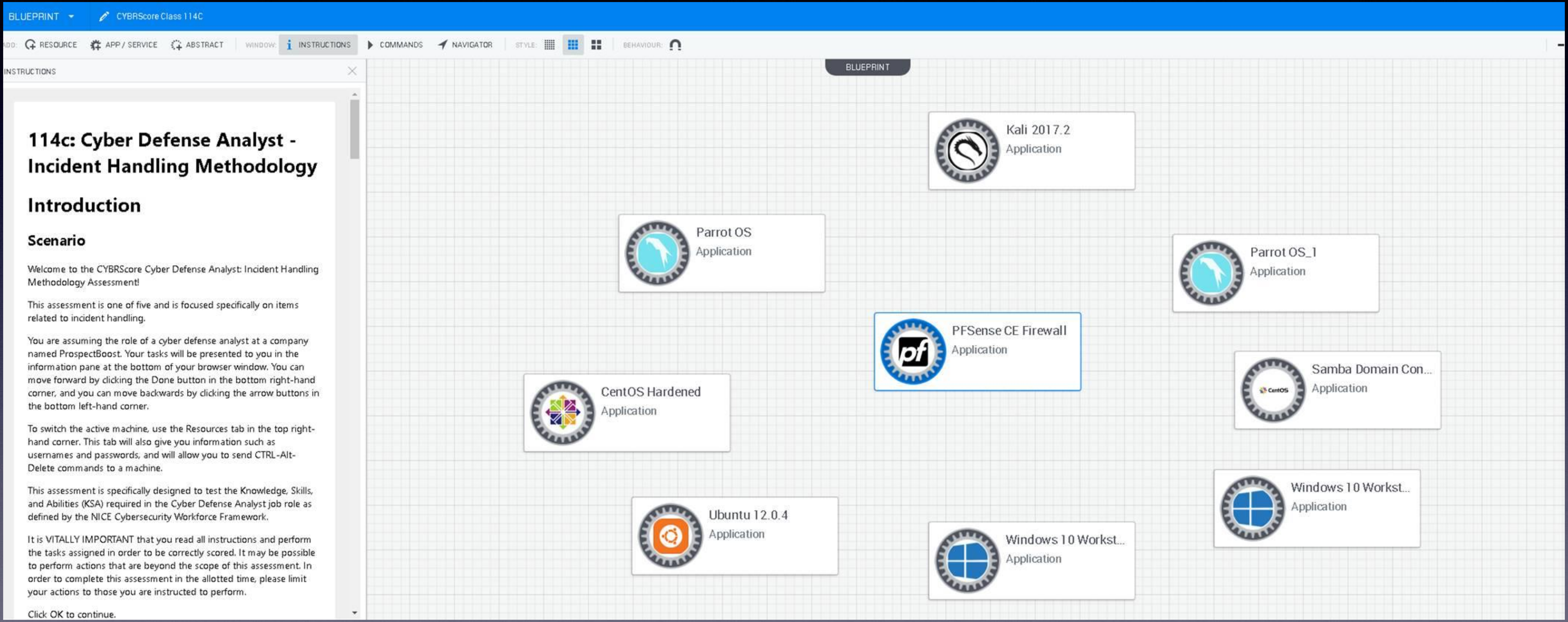
Incident Detection Lab 04
You will configure snort as an IDS. Additionally, you have received the following

Incident Detection Lab 05
The Network Discovery lab is designed to help students facilitate open source

Incident Detection Lab 06
Students will utilize Zenmap to generate a visual network topology.

Incident Detection Lab 07
In this lab we will replicate potentially malicious scans from the Internet against a

Cyber Range as a Service® – Online Cyber Training



114c: Cyber Defense Analyst - Incident Handling Methodology

Introduction

Scenario

Welcome to the CYBRScore Cyber Defense Analyst: Incident Handling Methodology Assessment!

This assessment is one of five and is focused specifically on items related to incident handling.

You are assuming the role of a cyber defense analyst at a company named ProspectBoost. Your tasks will be presented to you in the information pane at the bottom of your browser window. You can move forward by clicking the Done button in the bottom right-hand corner, and you can move backwards by clicking the arrow buttons in the bottom left-hand corner.

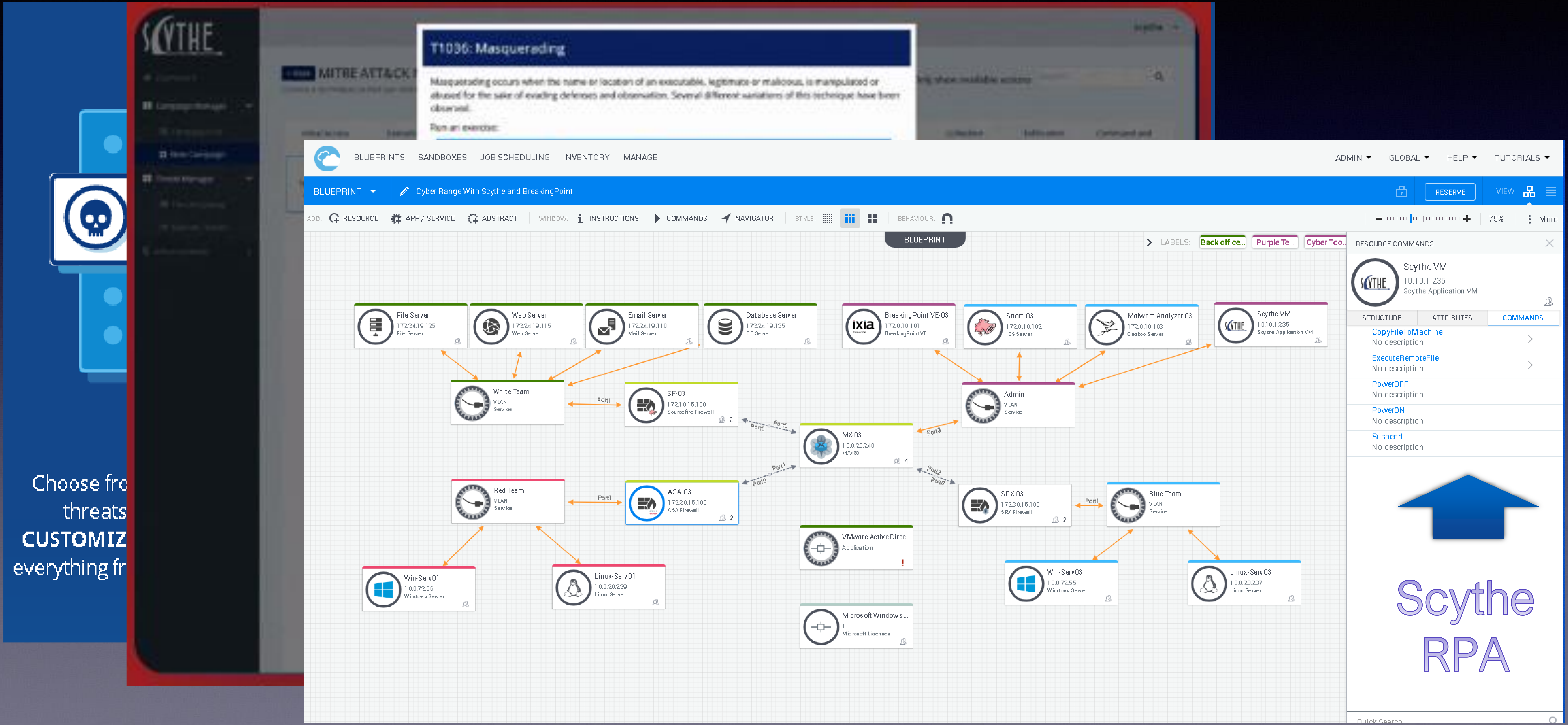
To switch the active machine, use the Resources tab in the top right-hand corner. This tab will also give you information such as usernames and passwords, and will allow you to send CTRL-Alt-Delete commands to a machine.

This assessment is specifically designed to test the Knowledge, Skills, and Abilities (KSA) required in the Cyber Defense Analyst job role as defined by the NICE Cybersecurity Workforce Framework.

It is VITALLY IMPORTANT that you read all instructions and perform the tasks assigned in order to be correctly scored. It may be possible to perform actions that are beyond the scope of this assessment. In order to complete this assessment in the allotted time, please limit your actions to those you are instructed to perform.

Click OK to continue.

Cyber Range as a Service®
– RBP Teams with Scythe Embedded



Choose fro
threats
CUSTOMIZ
everything fr

T1036: Masquerading

Masquerading occurs when the name or location of an executable, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. Several different variations of this technique have been observed.

Run an exercise:

RESOURCE COMMANDS

Scythe VM
10.10.1.235
Scythe Application VM

STRUCTURE | ATTRIBUTES | COMMANDS

CopyFileToMachine
No description

ExecuteRemoteFile
No description

PowerOFF
No description

PowerON
No description

Suspend
No description

Scythe RPA

Thank you

Chuck Reynolds

info@tsieda.com

www.tsieda.com

www.tsieda.com/craas