Cyber Range as a Service™ (CRaaS)

Creating Lab & Infrastructure as a Service to implement Cyber Range Activities

Agenda

What is a Cyber Range

Challenges of delivering a Cyber Range

What is Cyber Range as a Service (CRaaS)

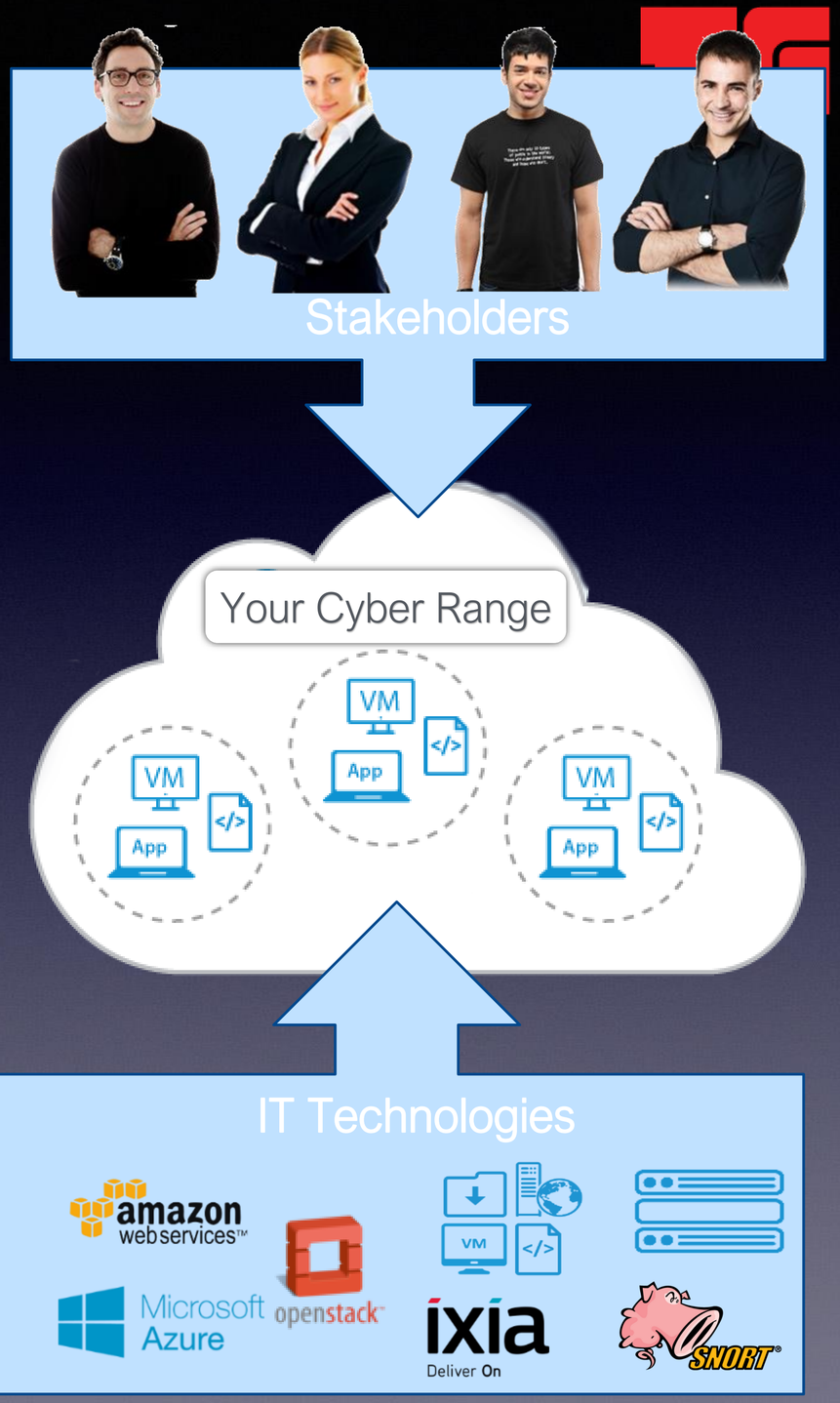
How do you deliver CRaaS

What is the value of CRaaS

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, 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



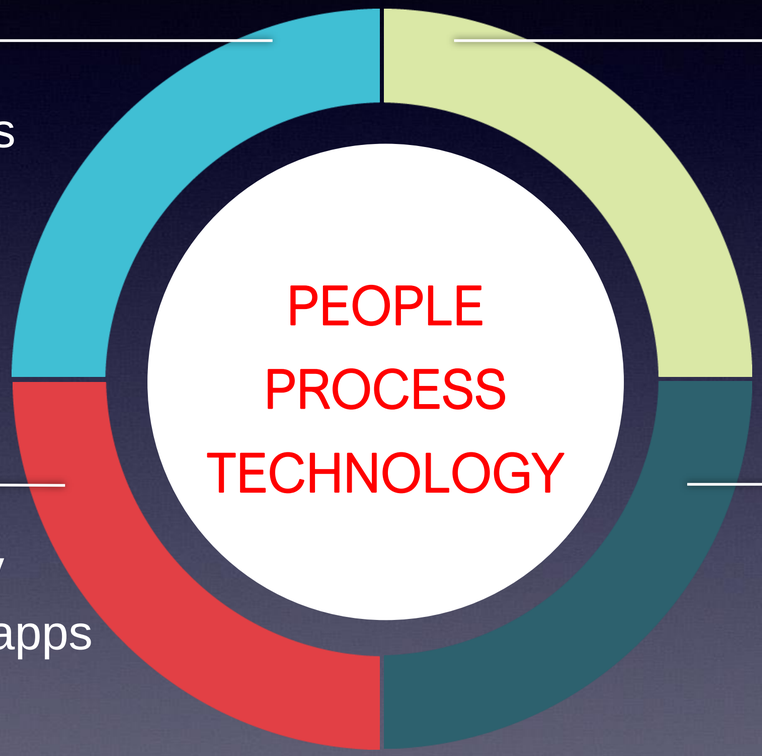
Cyber Range Stakeholders/Tasks

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

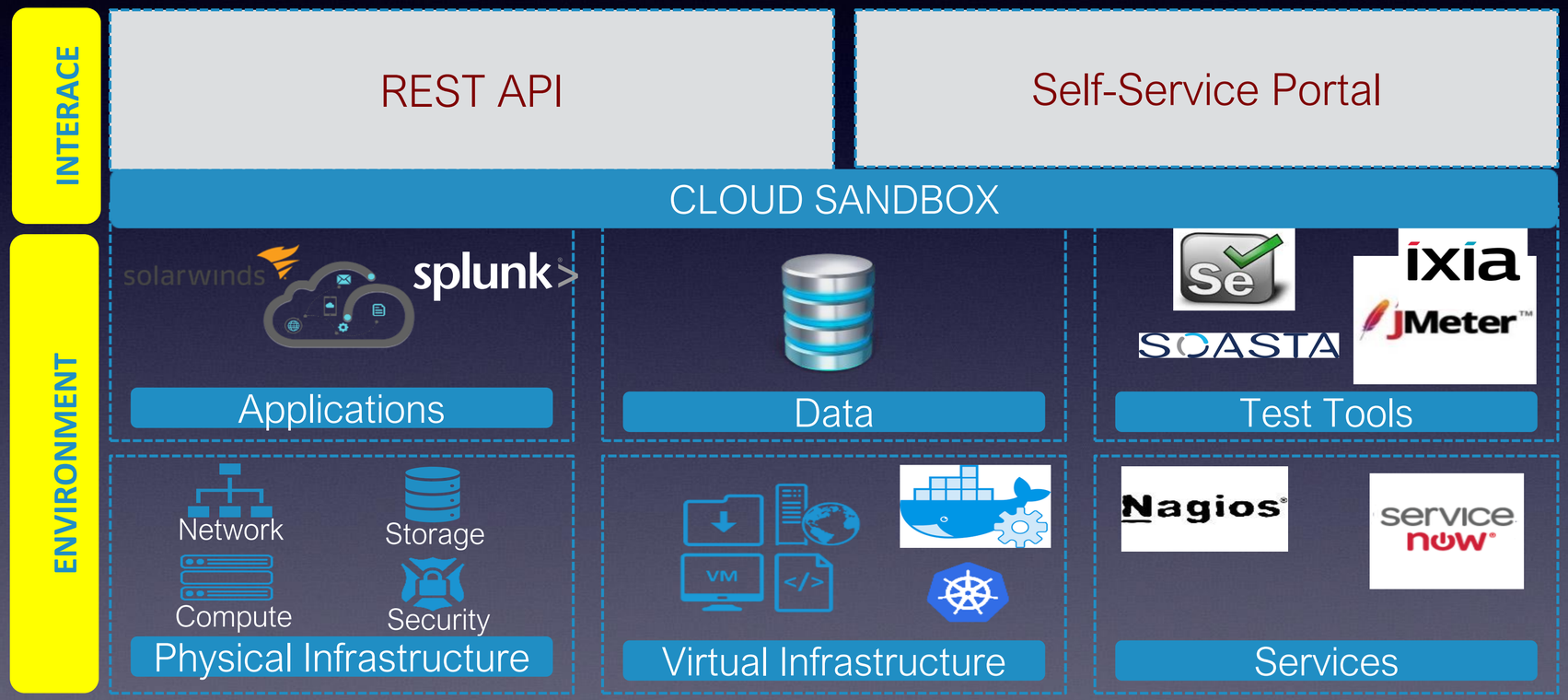
- Analysis of performance of Range
- Analysis of end user performance
- Cycle time for next deployment
- Personnel and Process Alignment
- Costs

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

openstack CLOUD SOFTWARE

Cypherpath Are You CyberReady?

Microsoft Azure

Google Cloud Platform

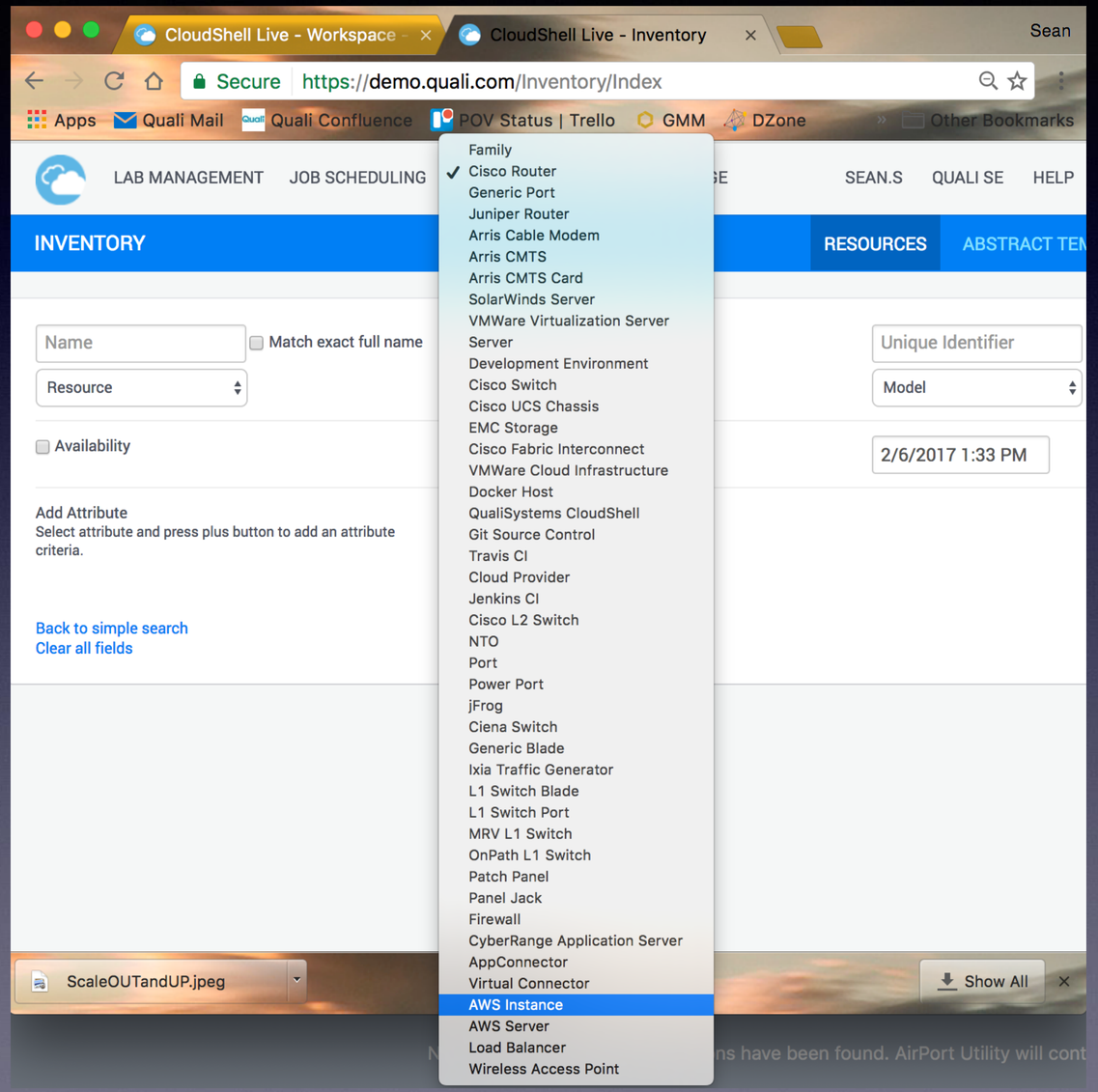
amazon web services™

Bare Metal

Manage the Inventory of your Range

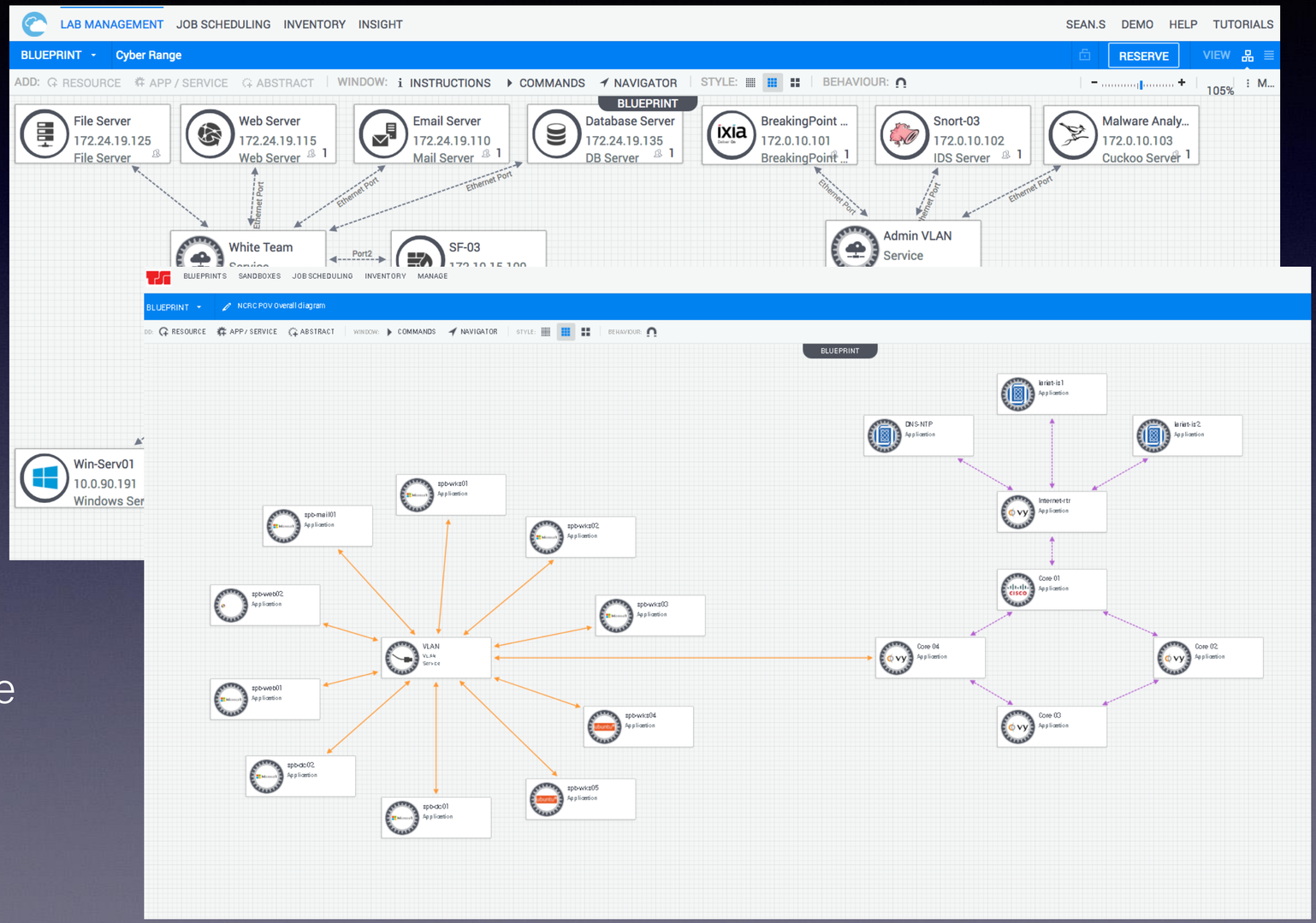
Physical, Virtual, App, Service, Cloud(s)

- 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



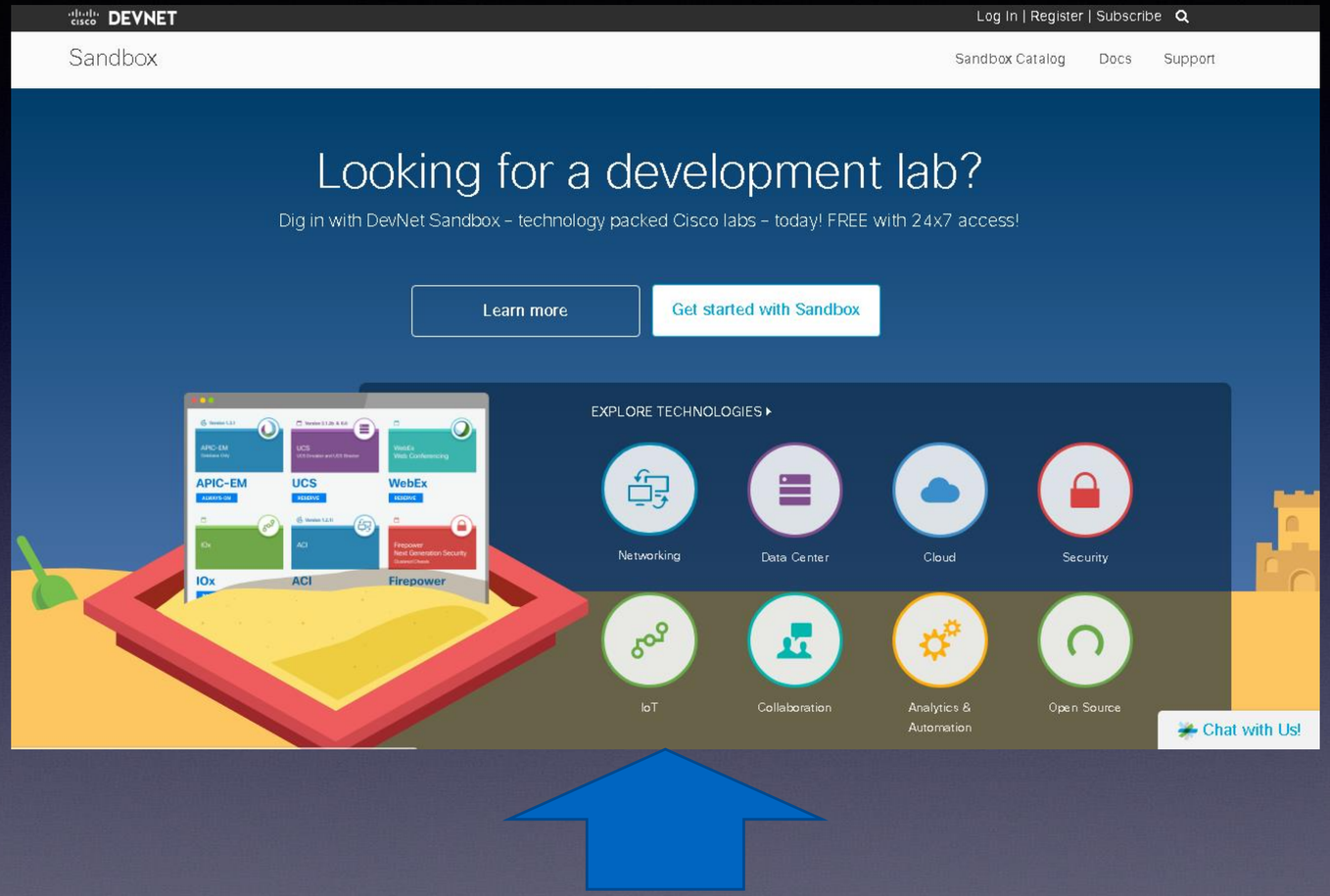
Model IT Blueprints for Cyber Range

- 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
- Think Live Visio Diagram!



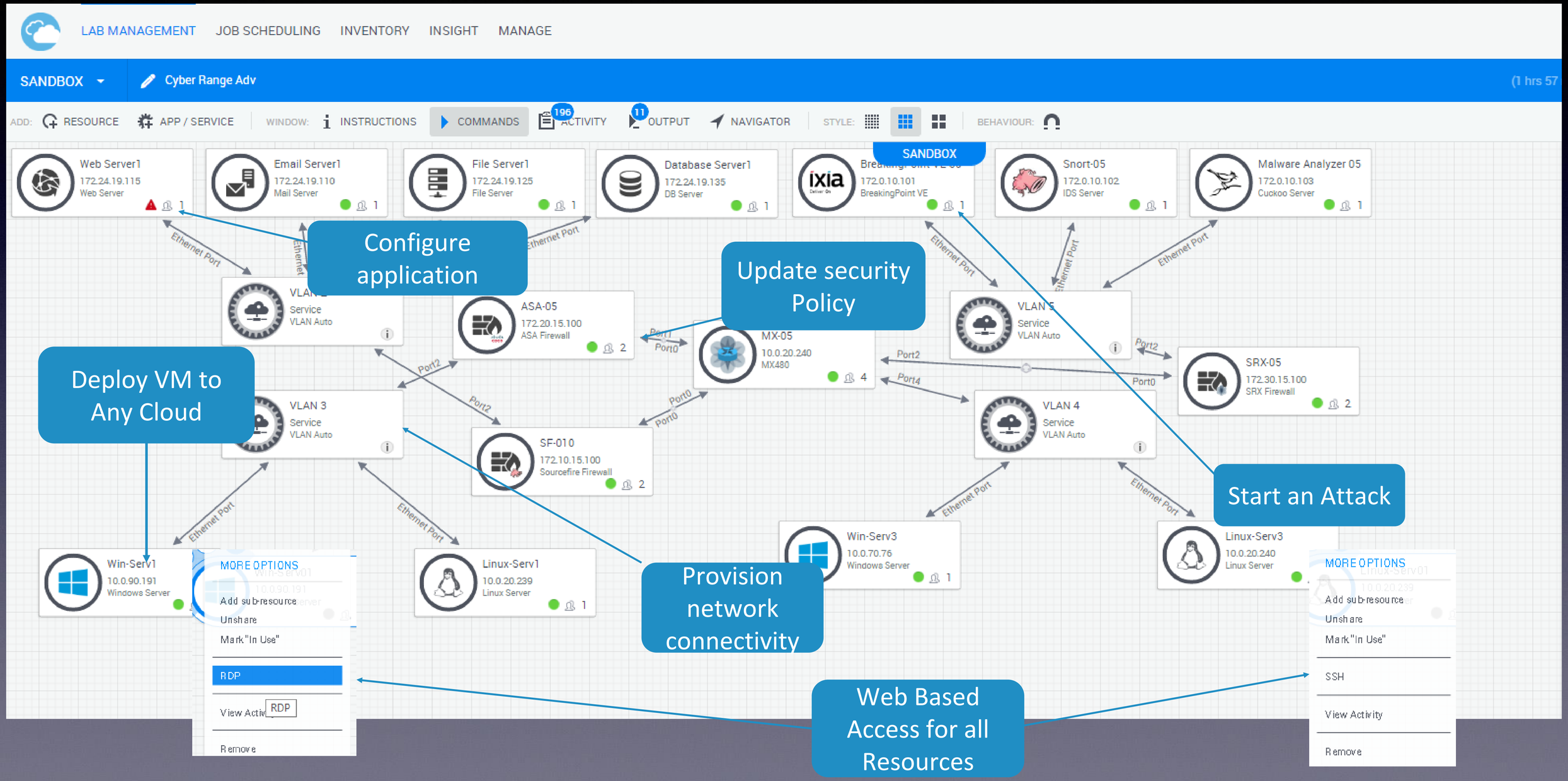
Publish Catalog of Cyber Range Blueprints

- 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



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

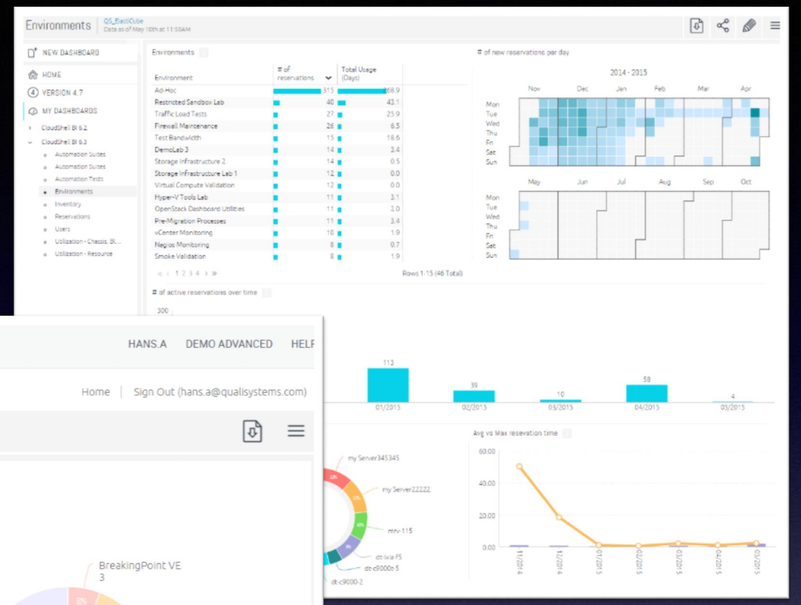
Cyber Range as a Service Sandbox

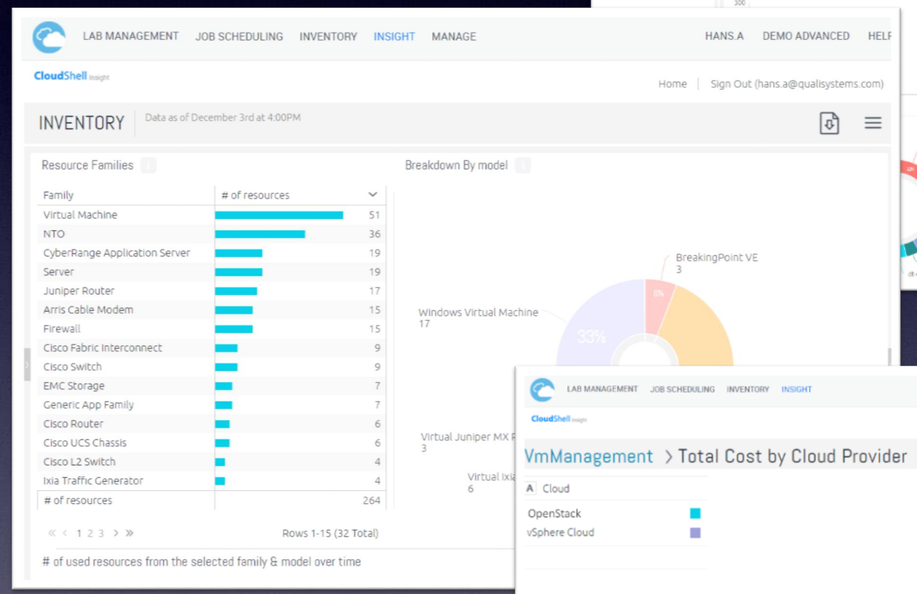


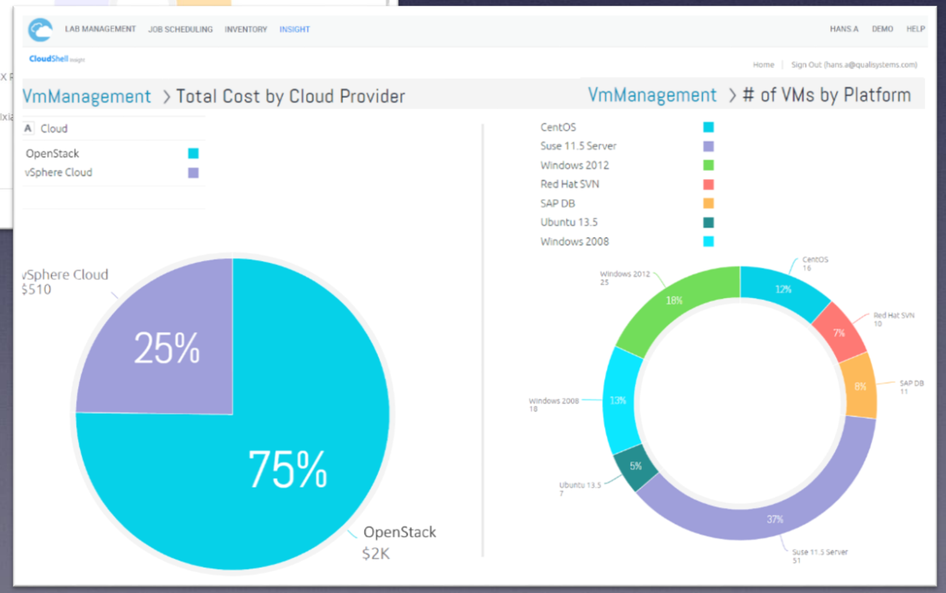
BI & Analytics

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







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

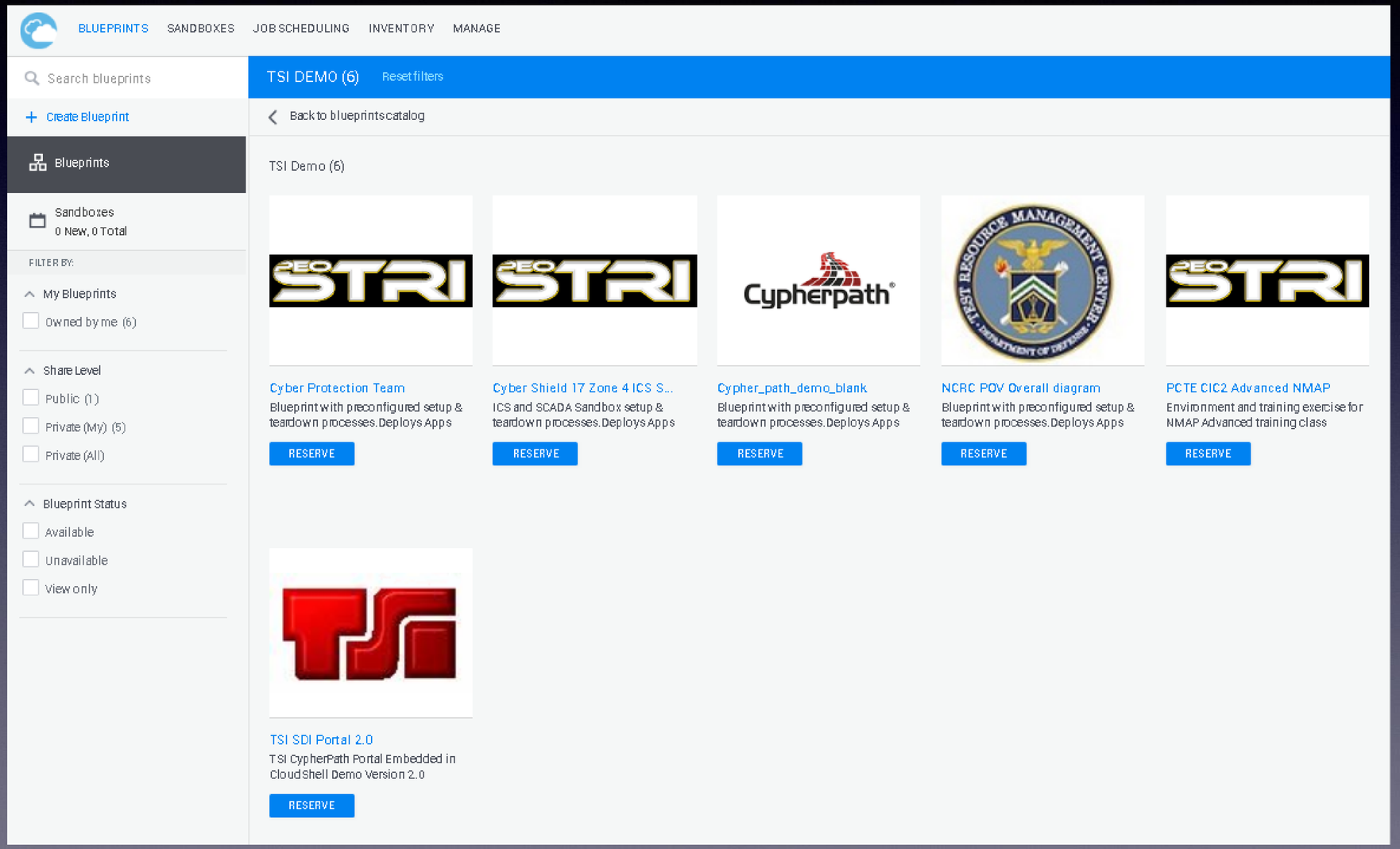
CyberRange as a Service Advantage

	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**

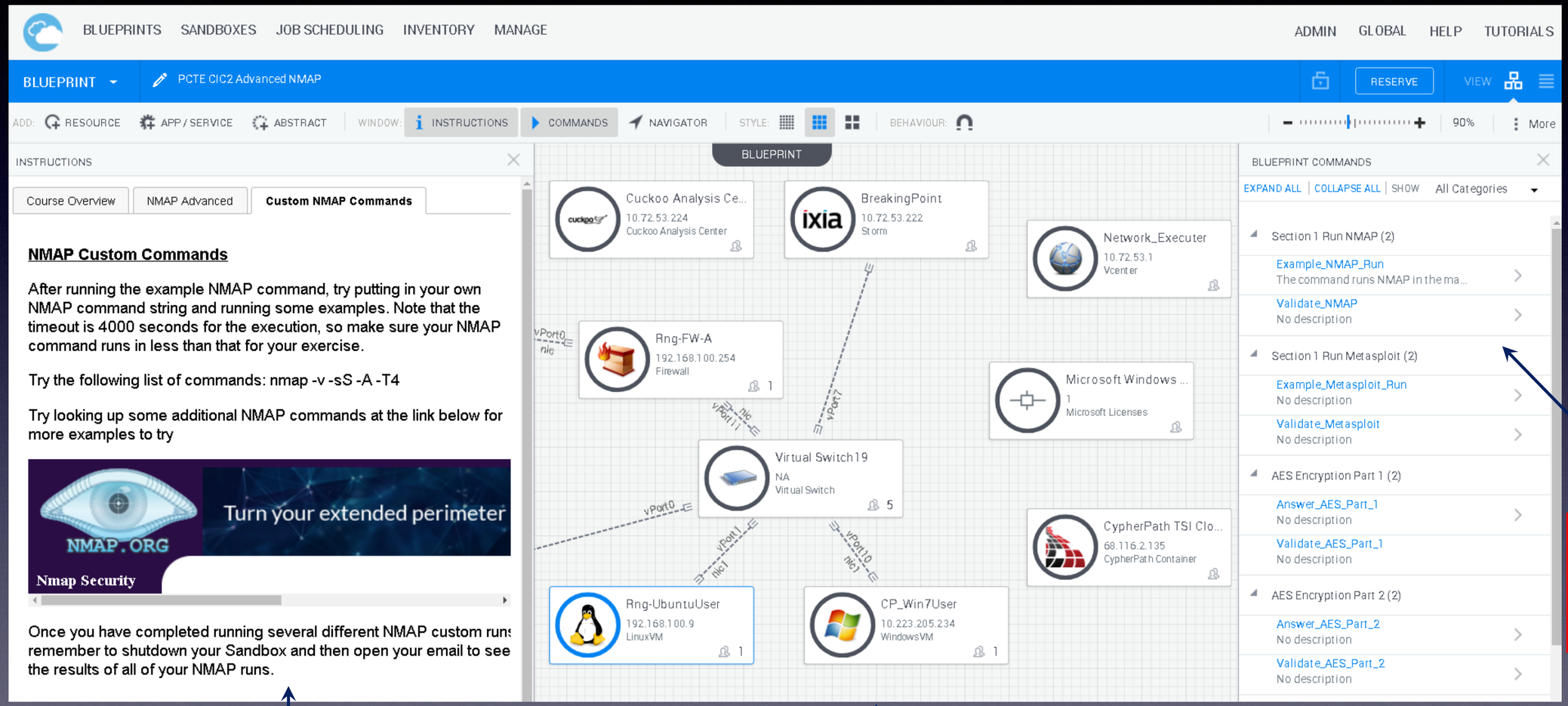
VS

Cyber Range

Examples


BLUEPRINTS
SANDBOXES
JOB SCHEDULING
INVENTORY
MANAGE
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

Physical and Virtual Training Exercise/Range



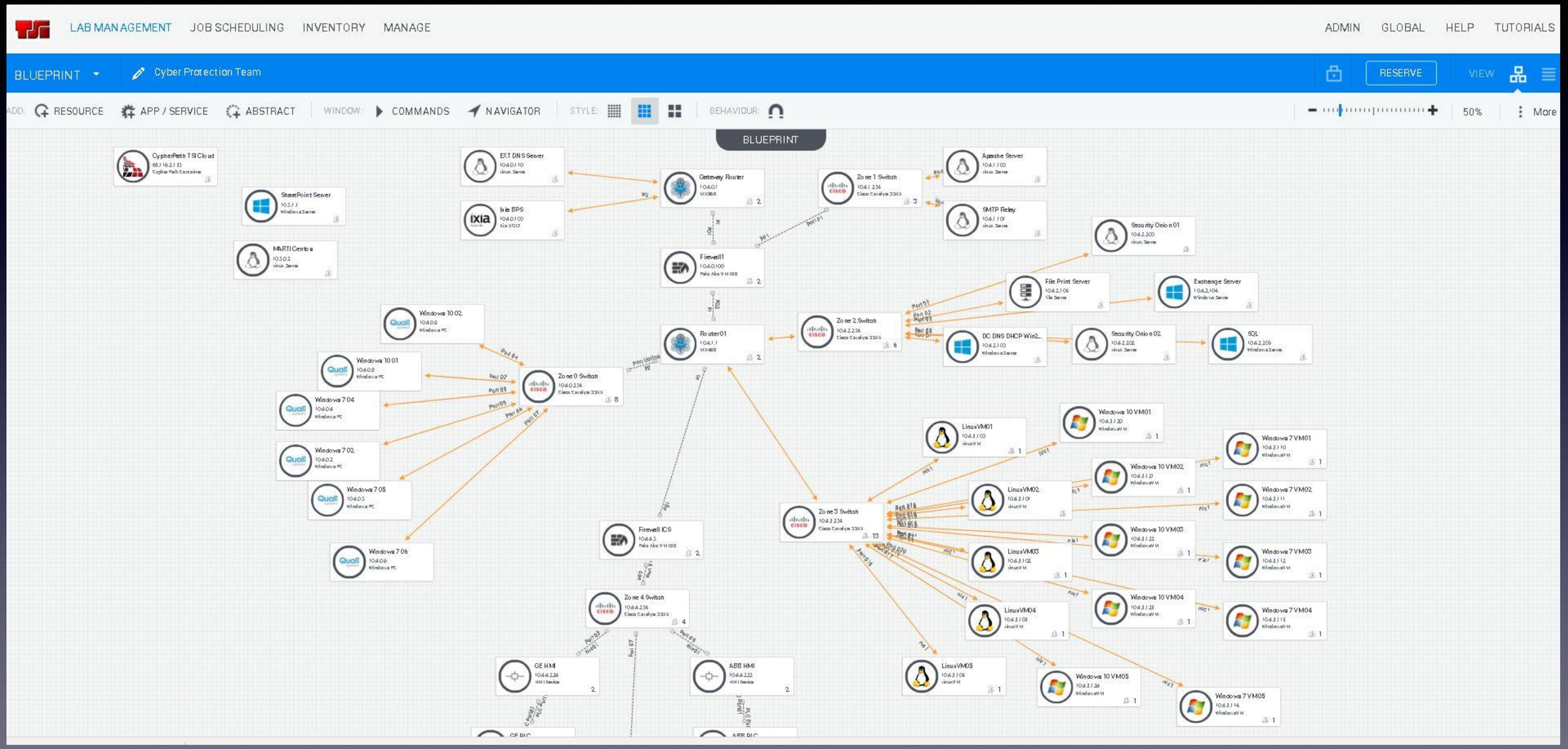
Automation
For provisioning, training, grading and response monitoring

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

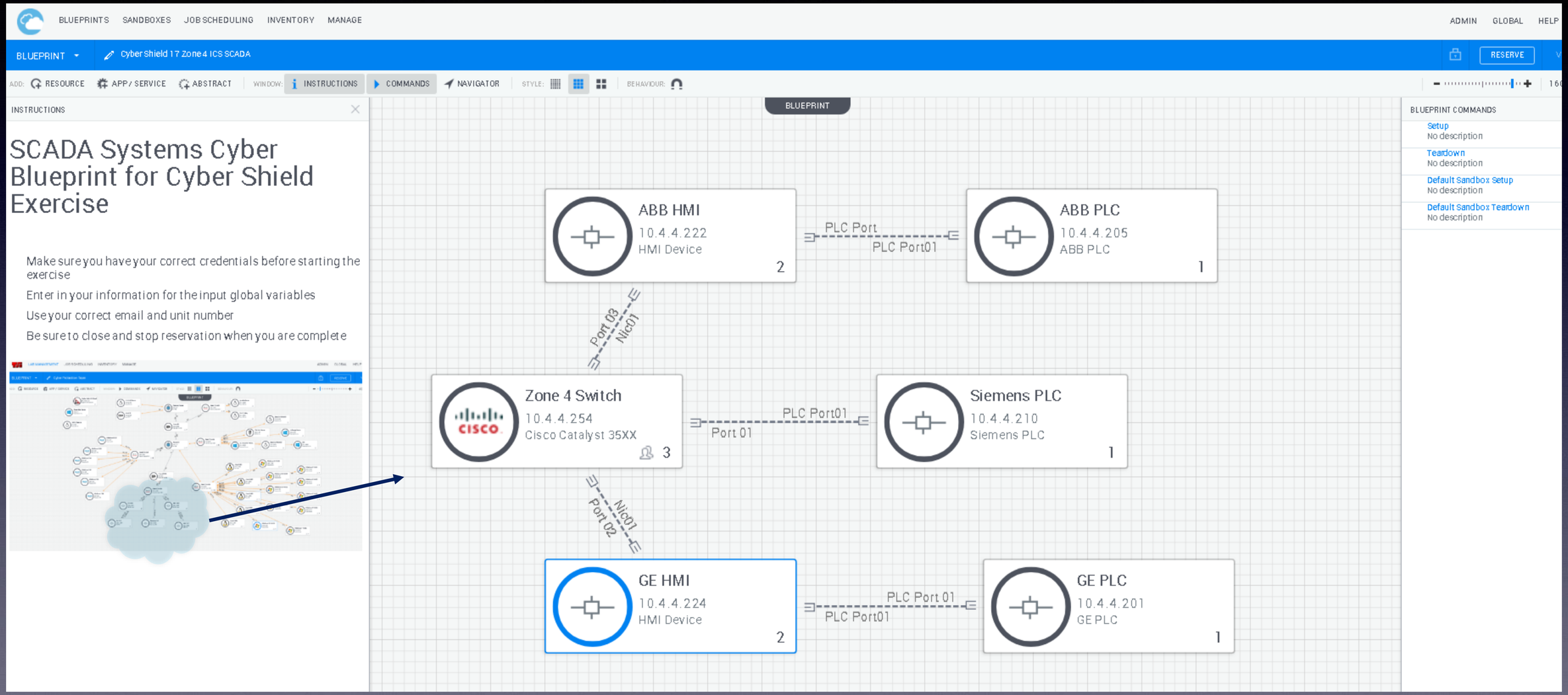
Your Cyber Range or Training Environment - AWS and/or Physical

Supports online or classroom training or exercise environments

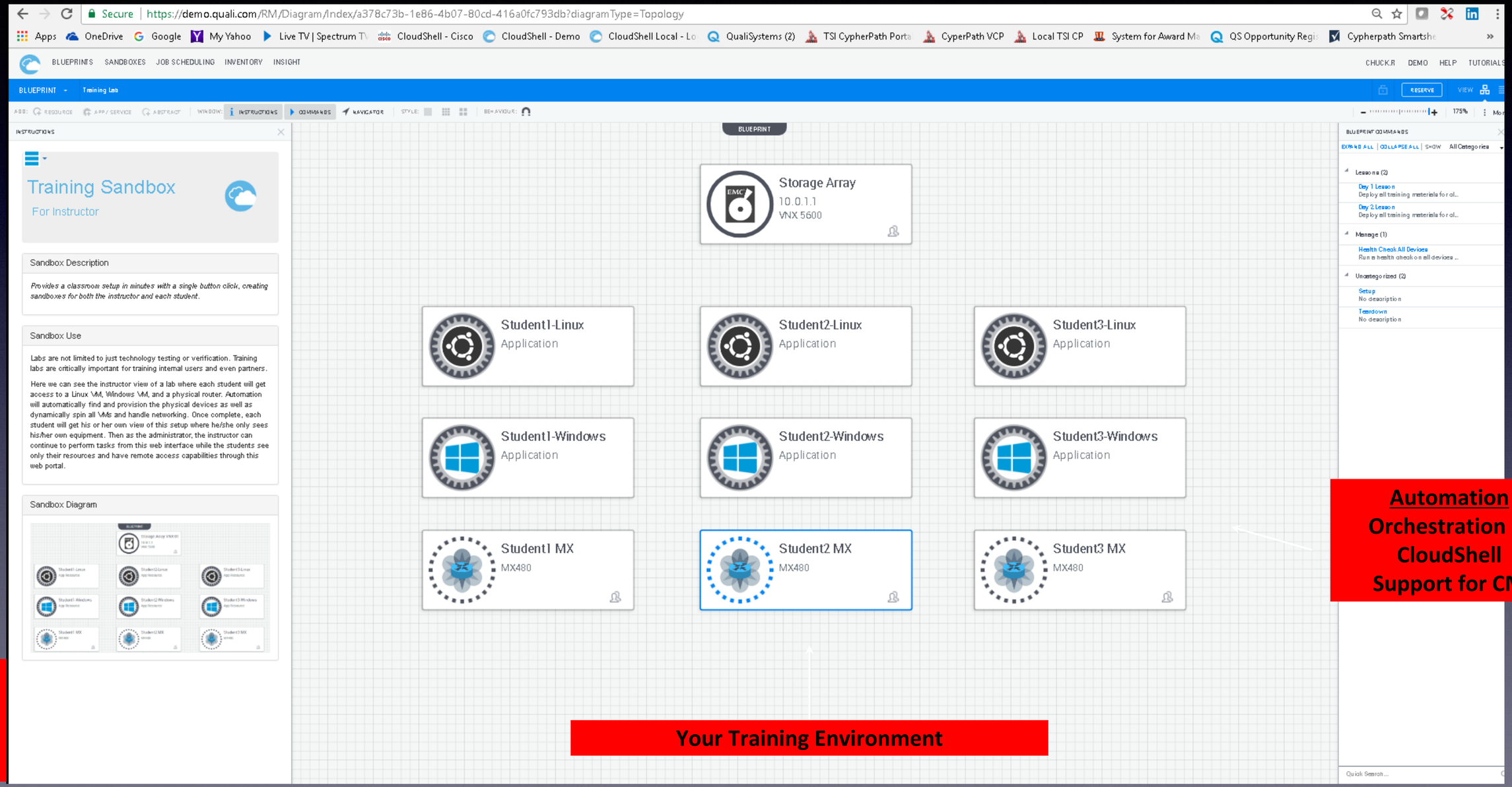
Cyber Exercise Full View



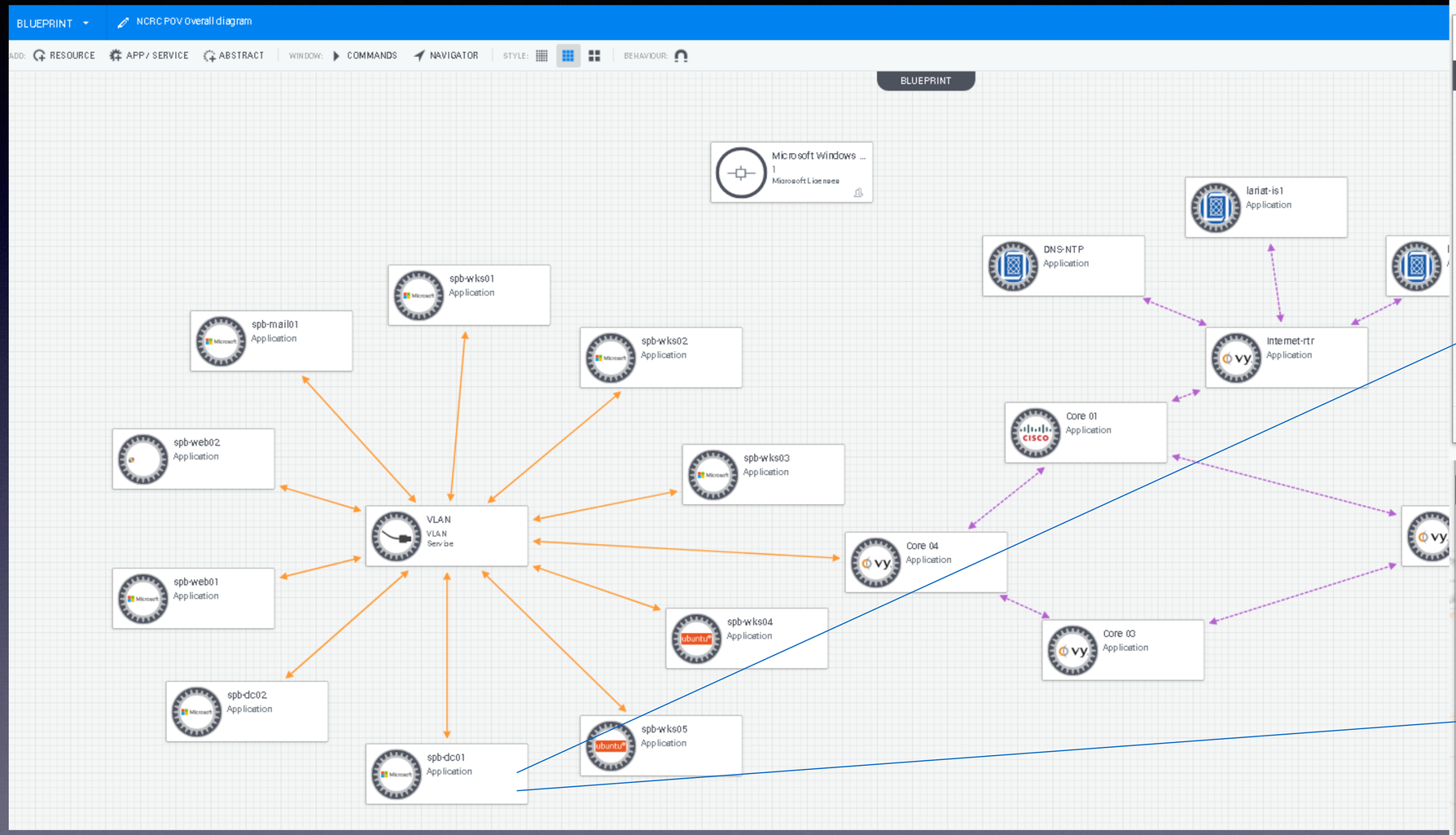
Cyber Exercise SCADA Only View

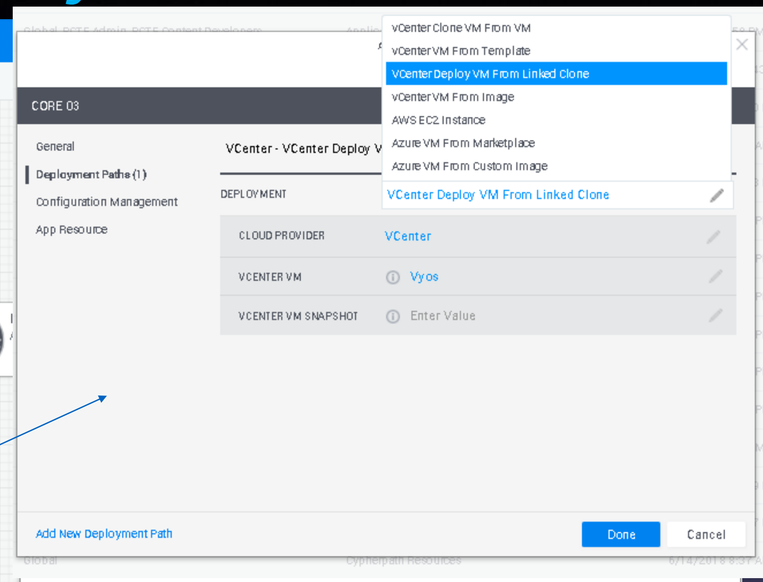


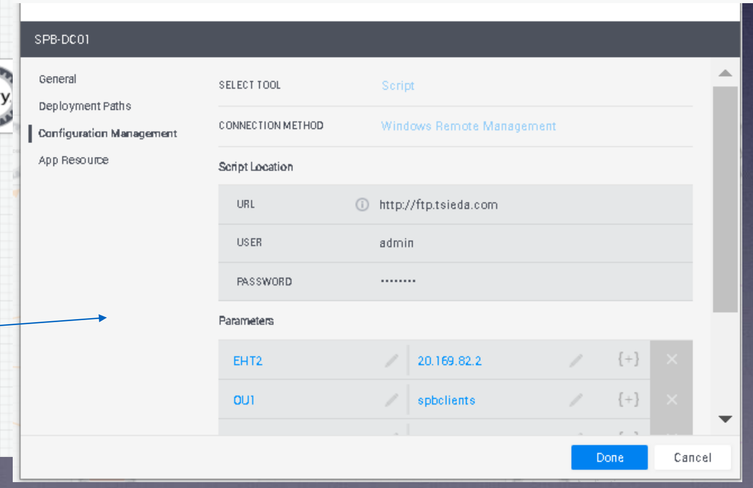
Full Training and LMS embedded Training



Full Production Replica for Cyber Use with Automated Configuration Management targeting any cloud

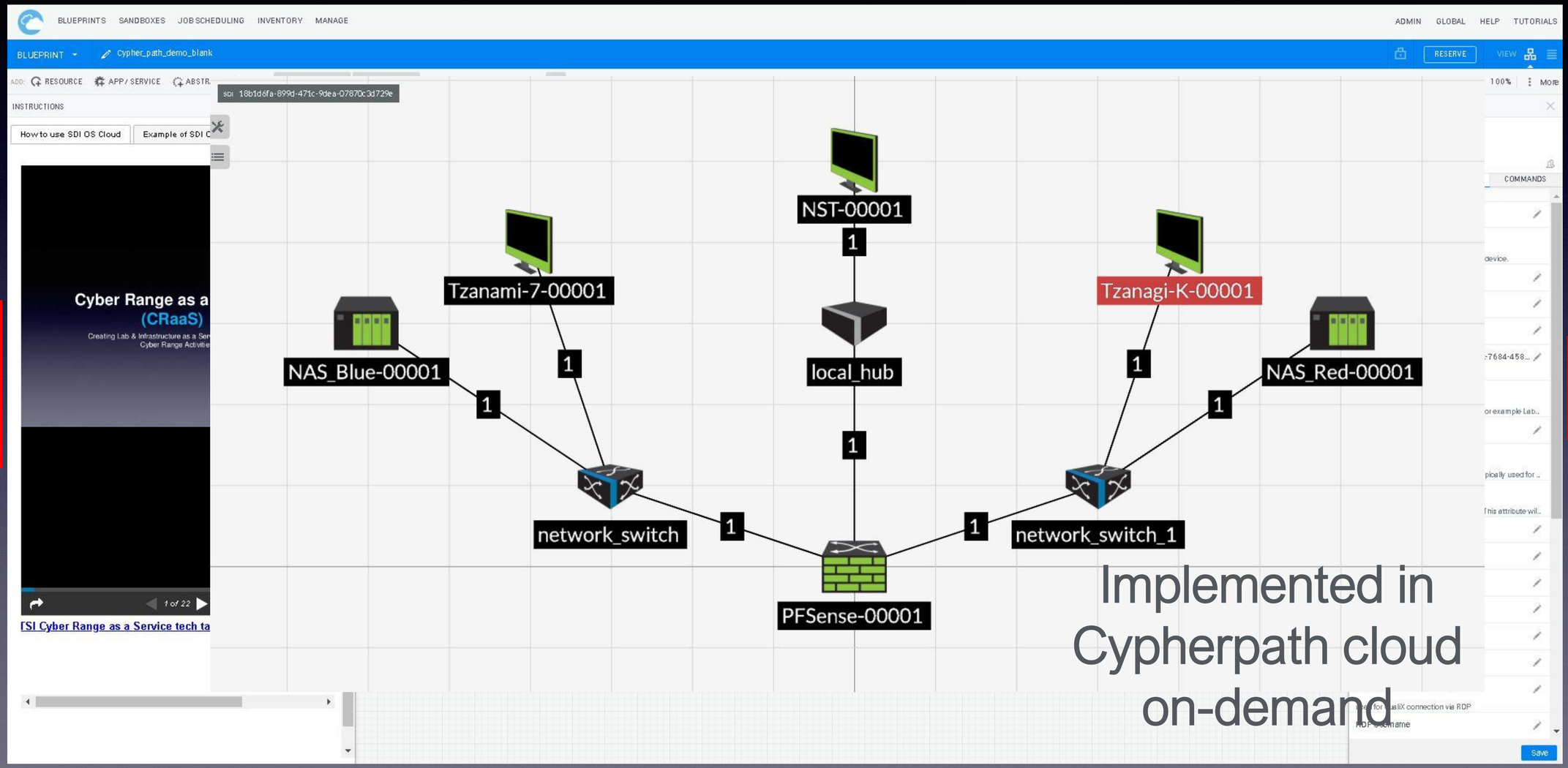






TSI SDI OS Cloud Support

Embedded training and Exercise Content

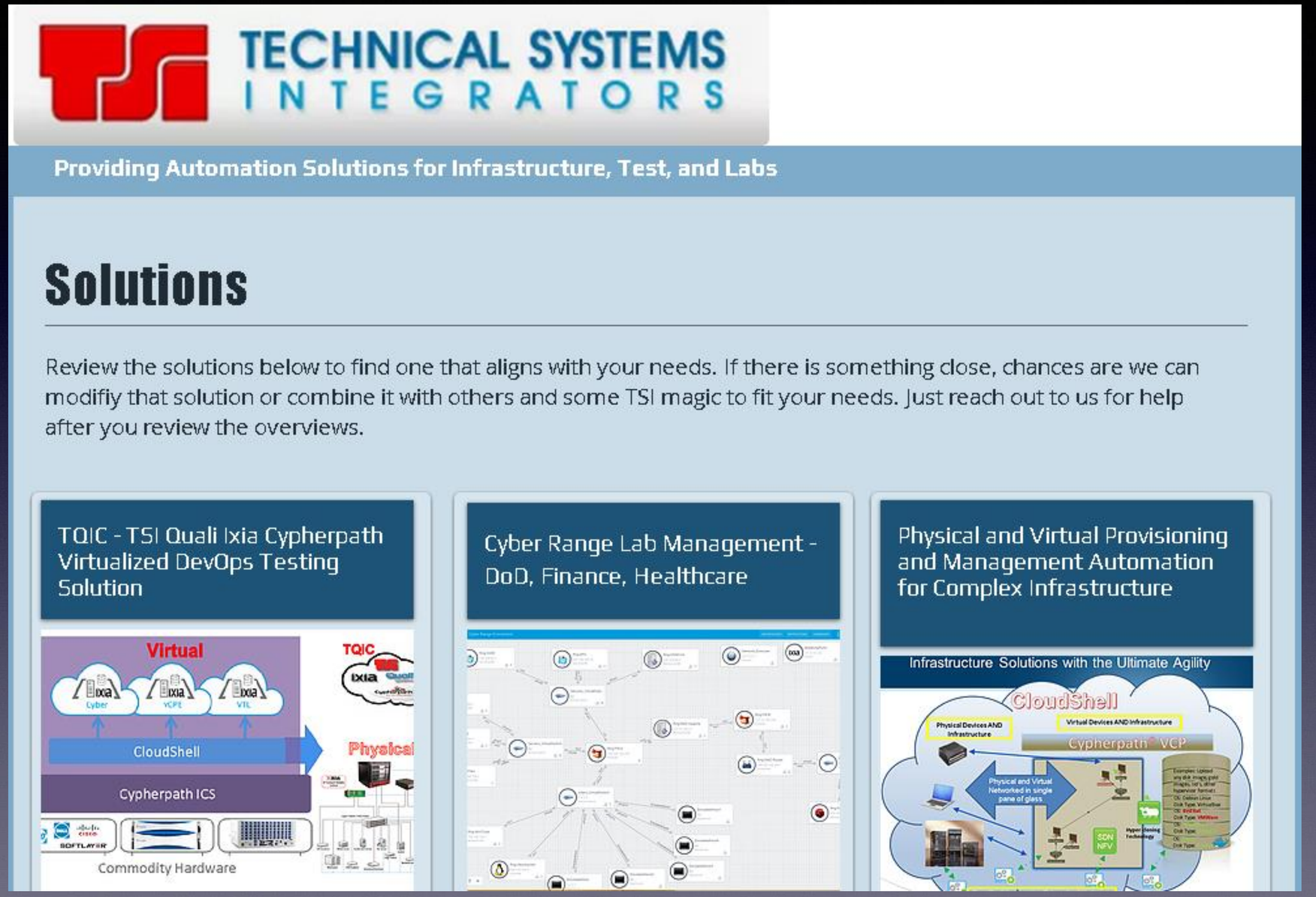


Custom Cloud Attributes

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



Established 1987

Thank you

Chuck Reynolds
info@tsieda.com
www.tsieda.com

www.tsieda.com/blog for
the white paper on CRaaS