SIMSPACE CORPORATION

Emerging Cyber Topics

IARIA Cyber 2016

Presented by: Dr. Thomas J. Klemas, Principal Engineer

Cybersecurity through
PEOPLE, PROCESS & TECHNOLOGY

SimSpace

BOSTON (HQ)
320 Congress St.
Boston, MA 02210
www.simspace.com

SimSpace

Cybersecurity through PEOPLE, PROCESS & TECHNOLOGY

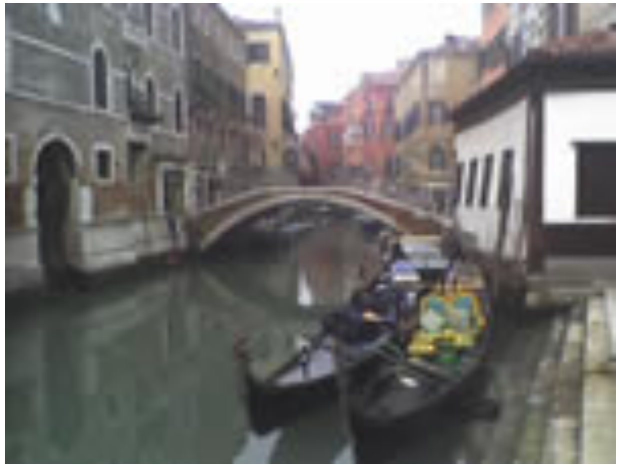
9 October 2016

Emerging Cyber Topics

- Establishing a definition for cyber is not so easy.
- The term cyber relates to computers, networks, and virtual reality
- Definition is evolving over time.

IARIA Cyber 2016

- Security (defense and offense)
- Resilience
- Crime
- Assessment and Risk Management
- Training and Technology



IARIA Cyber 2016: Security

- Defense and offense
- Internet of Things (IoT) is underway!
- Security for IoT follows
- IoT Topic Research
  - Security Threats facing IoT
  - Authentication for IoT
  - Privacy in an IoT World

IARIA Cyber 2016: Resilience

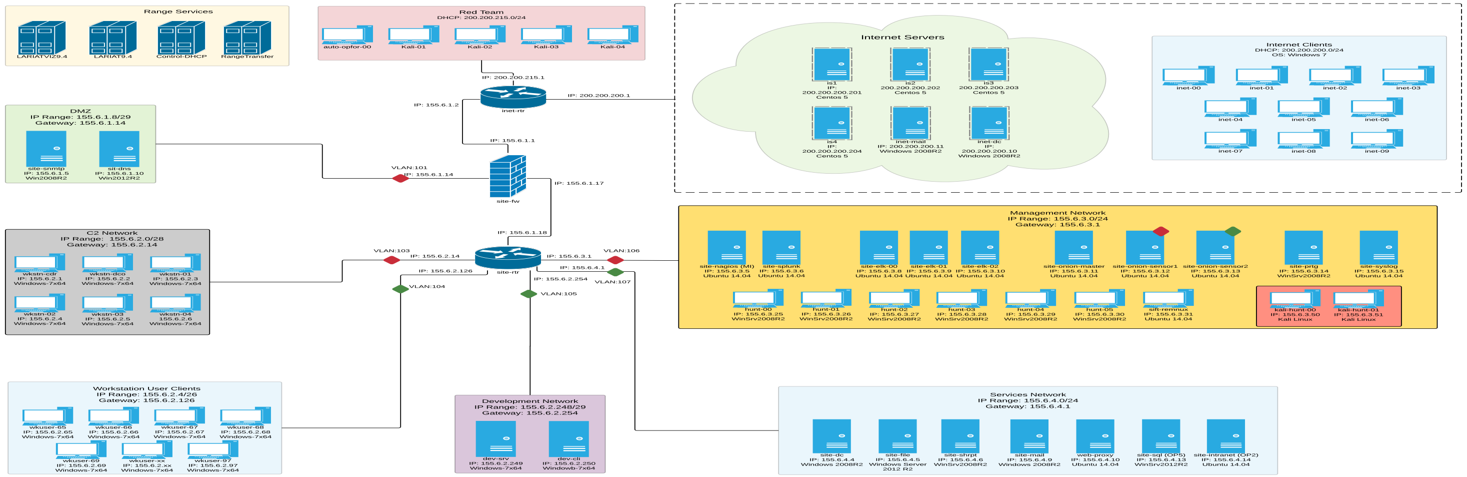
- Infrastructure and utilities
- Database access security
- Cyber-physical research
  - security
  - fault tolerance

IARIA Cyber 2016: Crime

- Vulnerability measurement
- Detecting data leaks
- Authentication research
- Forensic analysis
- Recovery

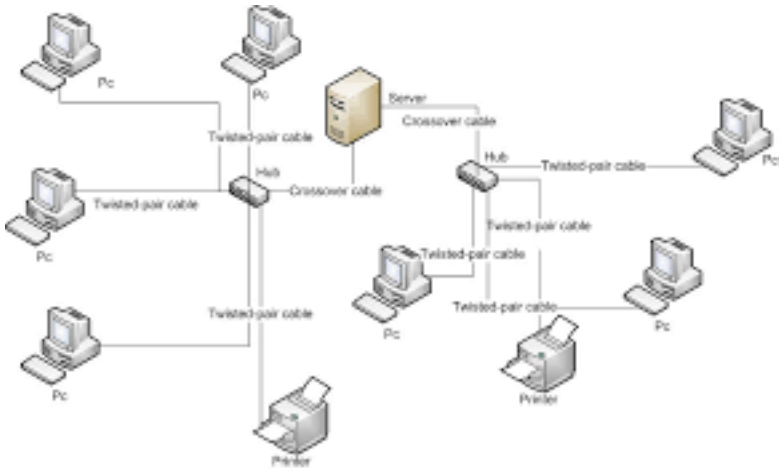
Assessment, Management, Training, Technology

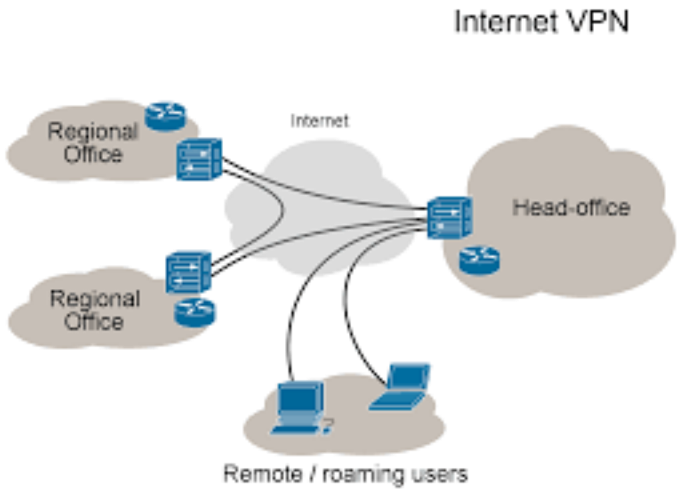
- Risk Management
  - Approaches for Assessment and Training
- Cyber Security Technologies

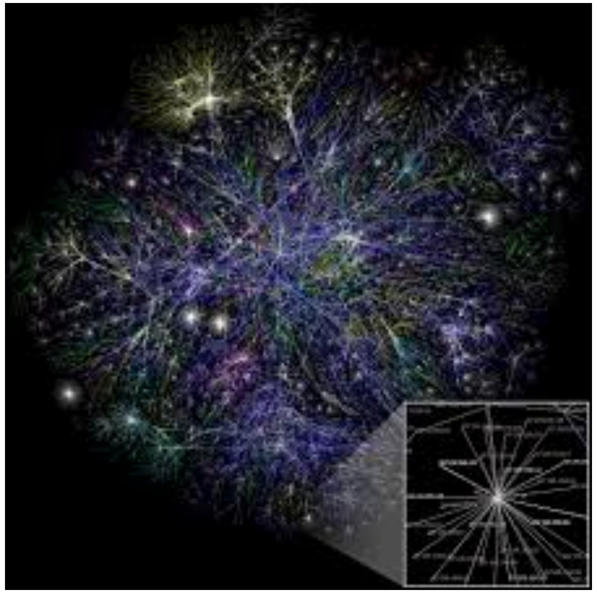


Evolution of Computers and the Internet

- The decades since the advent of computers have mainly focused on maximizing connectivity & access to resources







- The bottom line is that for a variety of reasons, our use of the term <u>cyber</u> has shifted - now almost synonymous with **<u>cybersecurity</u>**

The future: Coming Soon

- Internet of Things and Smart Cities

Cyber Crime Payoff

- US DoJ FBI Internet Crime Complaint Center (IC3) “2015 Internet Crime Report”
  - $1,070,711,522 reported losses
  - $8,421 average loss per complaint reporting a loss , $3718 average loss, $560 median loss
  - Past 5 years, IC3 has received ~300,000 complaints per year
- Forbes
  - Cyber crimes quadrupled between 2013 and 2015
  - Global cyber crime losses are projected $2.1 trillion by 2019
- Mounting frequency and magnitude of cyber incidents
- Nation states activity increasing

THE GREAT TRAIN ROBBERY
SENSATIONAL AND STARTLING HOLD UP OF THE GOLD EXPRESS BY FAMOUS WESTERN OUTLAWS.

Current State of Cyber Security

- Cyber and cyberspace grew from a vision of complete connectivity
- Computers were not conceived with security in mind

- Cyber field in "react" mode
  - Security not keeping pace with accelerating cyber growth
  - Always responding, not developed from 1st principles
- Serious challenges facing cybersecurity

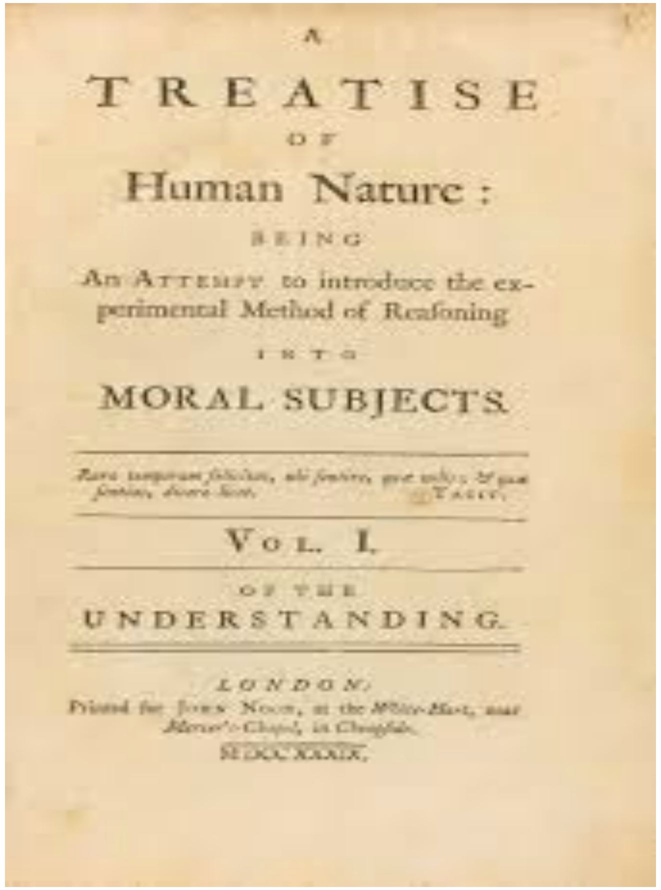
Some Key Issues for Cyber Security

- Education
  - Shortages of cyber professionals
  - User ignorance and human nature
- Offense
  - Significant tactical advantages for hostile actors
  - Cyber crime seems to pay
- Defense
  - Restoring “privacy” is almost impossible
  - Defending networks is much harder

“Sho, I wanna vote . . . where do ye vote? . . . ’n’ whut fer?”

Human Nature

- Many people are “programmed”
- Choose path of least resistance
- Focus on productivity vs security-driven
- Listen to curiosity before patience
- Heed authority and challenge authority



A
TREATISE
OF
Human Nature:
BEING
An ATTEMPT to introduce the experimental Method of Reaſoning
INTO
MORAL SUBJECTS.

Rara temporum felicitas, ubi ſentire, quæ velis; & quæ ſentias, dicere licet. TACIT.

VOL. I.

OF THE
UNDERSTANDING.

LONDON:
Printed for JOHN NOON, at the *White-Hart*, near *Mercer's-Chapel*, in *Cheapſide*.
MDCCXXXIX.

Pandora's Box

- Once open, very difficult to stuff released contents back inside
- Once privacy data is released it cannot be "fixed"
- We have become accustomed, even dependent on constant and complete connectivity
- Now organizations are trying to "dial it back"
  - Restrict employee internet access

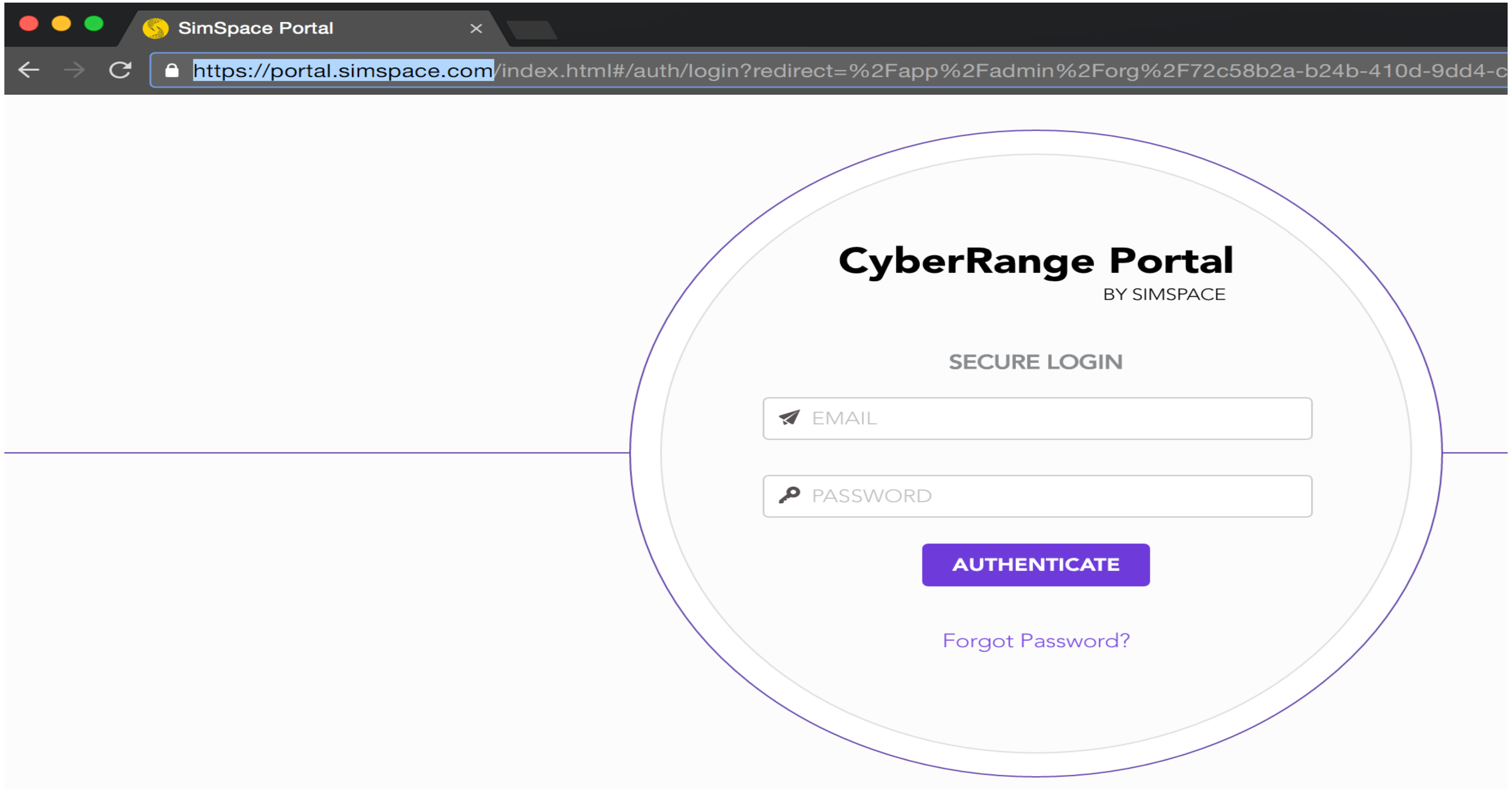
Call to Action

- Cyber threat is very real.
- Cybersecurity has urgent needs
- Opportunity abounds
  - Get more deeply involved in topics that will matter
  - Grow the field – severe shortages of skilled people AND data!
    - Education
    - Recruiting
    - New technologies

Personal Response to the Call

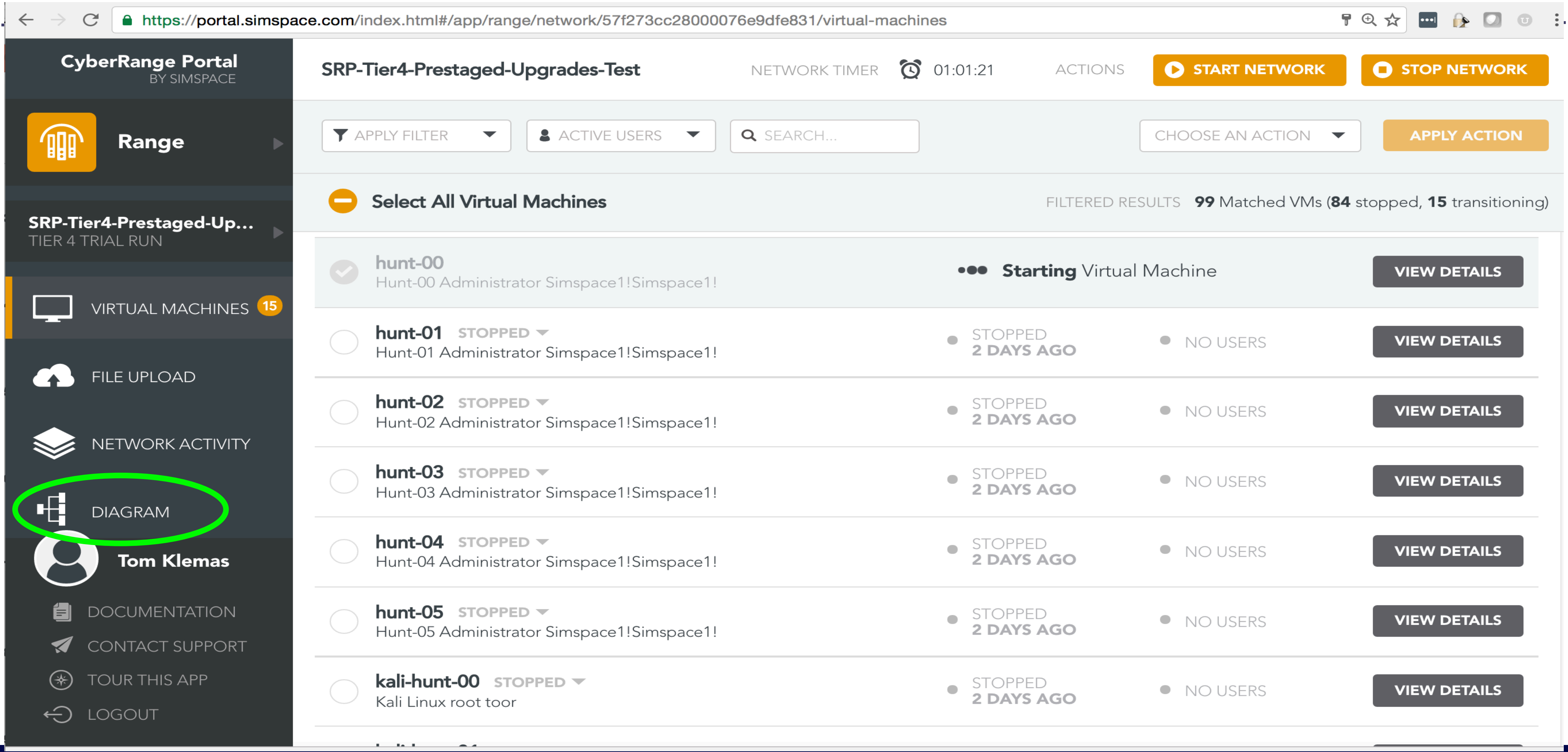
- Assessment & training
  - Teams
  - Individuals
  - Organizations
  - Tools
- Virtual Cyber Range
  - Example: Approximately 100 machines
  - Model customer networks
  - Features user emulator
- Cyber Assessor

SimSpace Portal to Cyber Range



https://portal.simspace.com/index.html#/auth/login?redirect=%2Fapp%2Fadmin%2Forg%2F72c58b2a-b24b-410d-9dd4-c

Virtual Machine Console Interfaces



https://portal.simspace.com/index.html#/app/range/network/57f273cc28000076e9dfe831/virtual-machines

SRP-Tier4-Prestaged-Upgrades-Test — NETWORK TIMER 01:01:21

FILTERED RESULTS **99** Matched VMs (**84** stopped, **15** transitioning)

hunt-00
Hunt-00 Administrator Simspace1!Simspace1!
Starting Virtual Machine — VIEW DETAILS

hunt-01 STOPPED
Hunt-01 Administrator Simspace1!Simspace1!
STOPPED 2 DAYS AGO — NO USERS — VIEW DETAILS

hunt-02 STOPPED
Hunt-02 Administrator Simspace1!Simspace1!
STOPPED 2 DAYS AGO — NO USERS — VIEW DETAILS

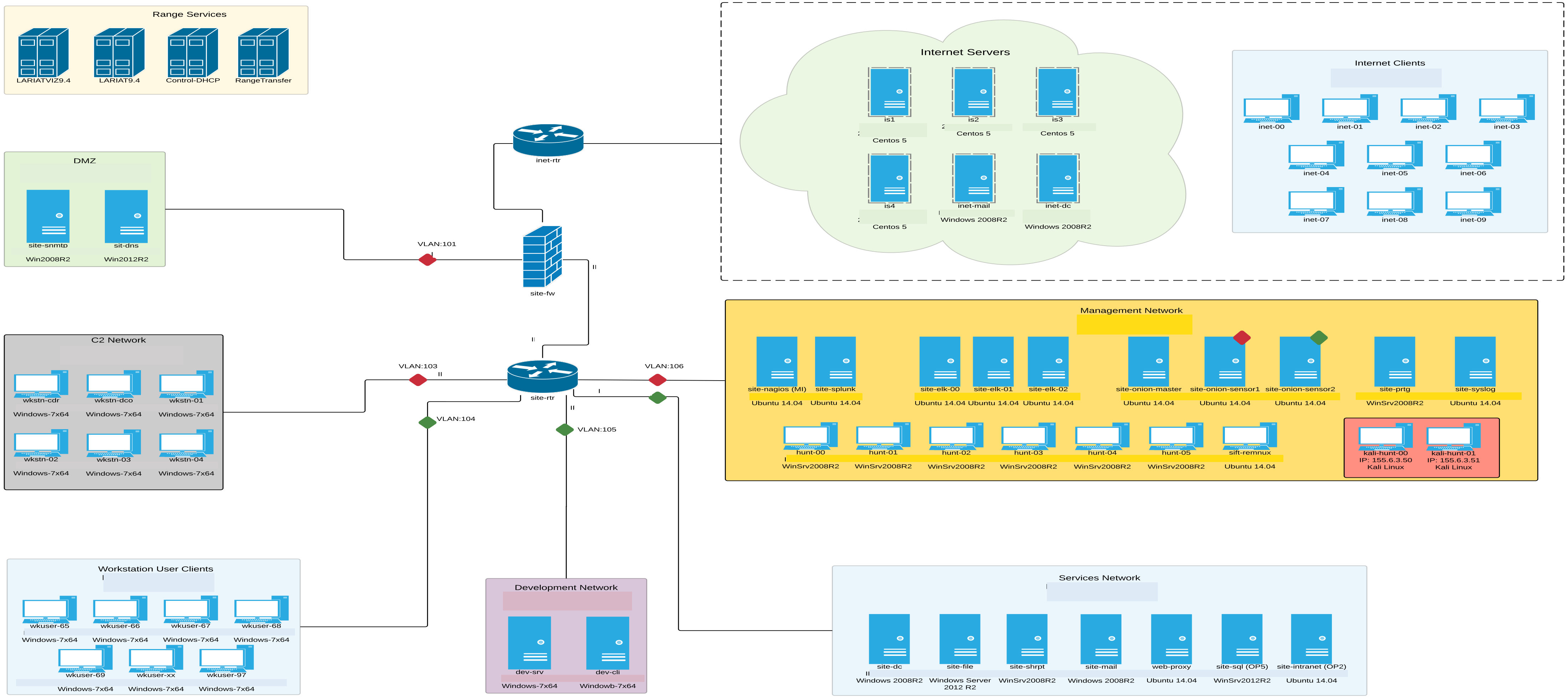
hunt-03 STOPPED
Hunt-03 Administrator Simspace1!Simspace1!
STOPPED 2 DAYS AGO — NO USERS — VIEW DETAILS

hunt-04 STOPPED
Hunt-04 Administrator Simspace1!Simspace1!
STOPPED 2 DAYS AGO — NO USERS — VIEW DETAILS

hunt-05 STOPPED
Hunt-05 Administrator Simspace1!Simspace1!
STOPPED 2 DAYS AGO — NO USERS — VIEW DETAILS

kali-hunt-00 STOPPED
Kali Linux root toor
STOPPED 2 DAYS AGO — NO USERS — VIEW DETAILS

Network Diagram



Range Services

LARIATVIZ9.4 | LARIAT9.4 | Control-DHCP | RangeTransfer

DMZ

site-snmtp Win2008R2

sit-dns Win2012R2

C2 Network

wkstn-cdr Windows-7x64

wkstn-dco Windows-7x64

wkstn-01 Windows-7x64

wkstn-02 Windows-7x64

wkstn-03 Windows-7x64

wkstn-04 Windows-7x64

Workstation User Clients

wkuser-65 Windows-7x64

wkuser-66 Windows-7x64

wkuser-67 Windows-7x64

wkuser-68 Windows-7x64

wkuser-69 Windows-7x64

wkuser-xx Windows-7x64

wkuser-97 Windows-7x64

Development Network

dev-srv Windows-7x64

dev-cli Windowb-7x64

inet-rtr

site-fw

site-rtr

VLAN:101

VLAN:103

VLAN:104

VLAN:105

VLAN:106

Internet Servers

is1 Centos 5

is2 Centos 5

is3 Centos 5

is4 Centos 5

inet-mail Windows 2008R2

inet-dc Windows 2008R2

Internet Clients

inet-00 | inet-01 | inet-02 | inet-03

inet-04 | inet-05 | inet-06

inet-07 | inet-08 | inet-09

Management Network

site-nagios (MI) Ubuntu 14.04

site-splunk Ubuntu 14.04

site-elk-00 Ubuntu 14.04

site-elk-01 Ubuntu 14.04

site-elk-02 Ubuntu 14.04

site-onion-master Ubuntu 14.04

site-onion-sensor1 Ubuntu 14.04

site-onion-sensor2 Ubuntu 14.04

site-prtg WinSrv2008R2

site-syslog Ubuntu 14.04

hunt-00 WinSrv2008R2

hunt-01 WinSrv2008R2

hunt-02 WinSrv2008R2

hunt-03 WinSrv2008R2

hunt-04 WinSrv2008R2

hunt-05 WinSrv2008R2

sift-remnux Ubuntu 14.04

kali-hunt-00
IP: 155.6.3.50
Kali Linux

kali-hunt-01
IP: 155.6.3.51
Kali Linux

Services Network

site-dc Windows 2008R2

site-file Windows Server 2012 R2

site-shrpt WinSrv2008R2

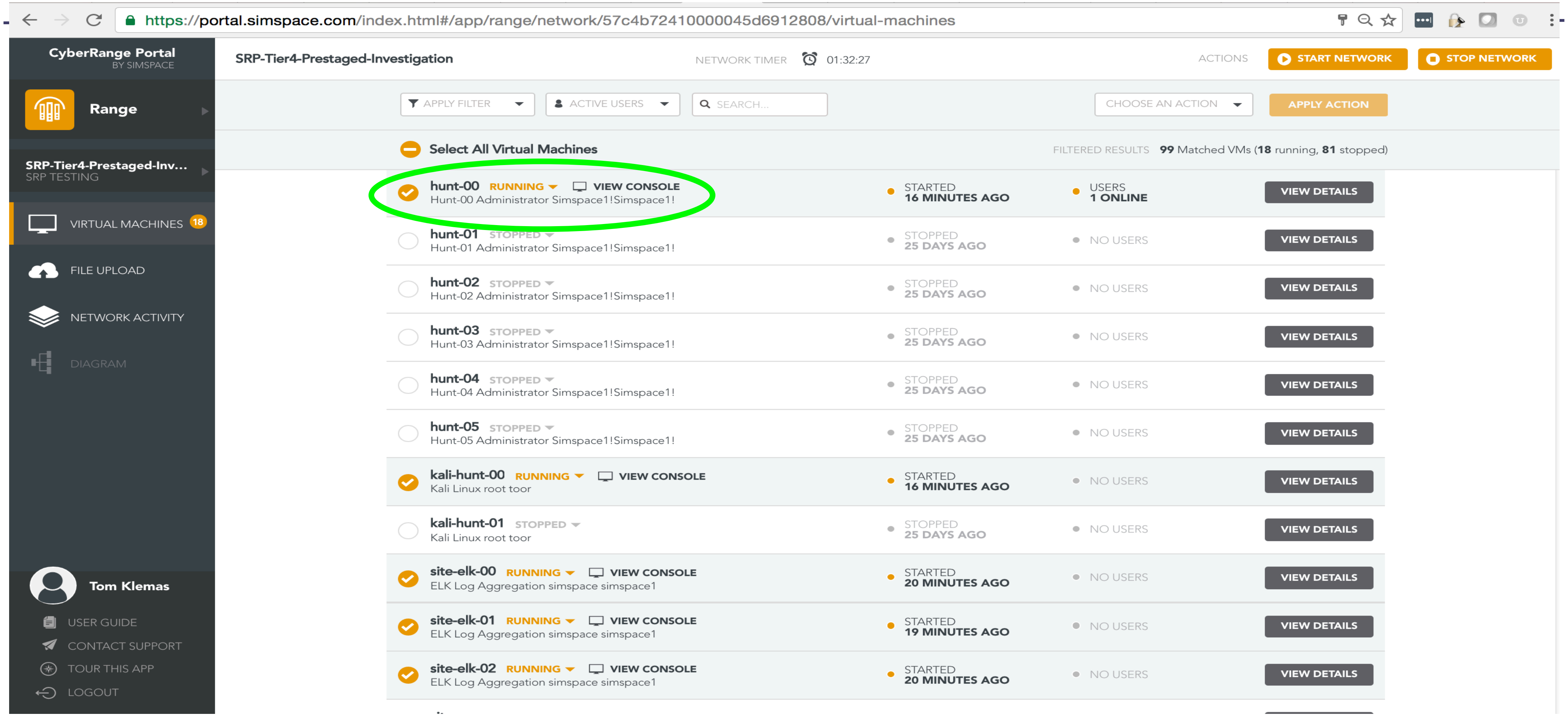
site-mail Windows 2008R2

web-proxy Ubuntu 14.04

site-sql (OP5) WinSrv2012R2

site-intranet (OP2) Ubuntu 14.04

Portal Console Access to Virtual Machines



https://portal.simspace.com/index.html#/app/range/network/57c4b72410000045d6912808/virtual-machines

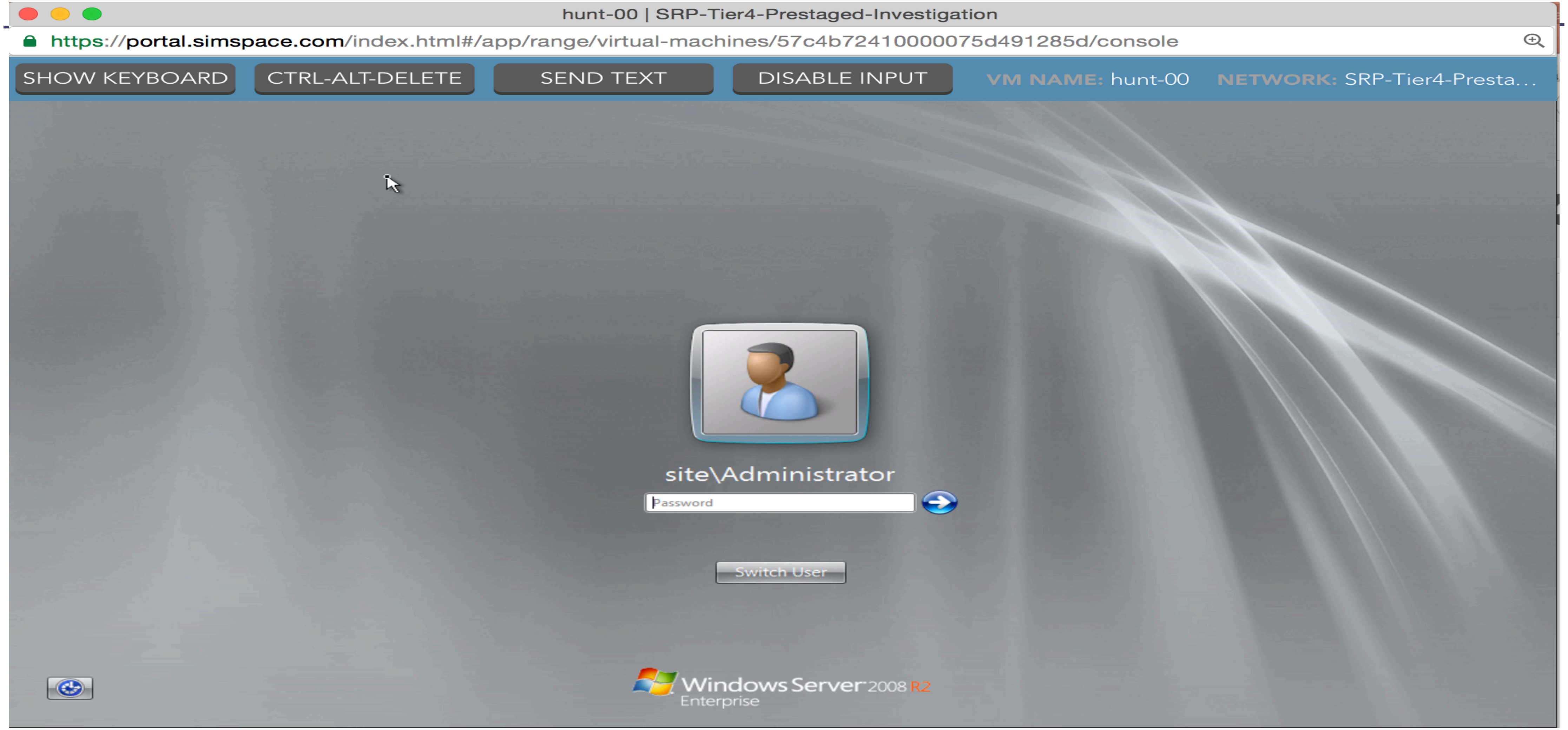
SRP-Tier4-Prestaged-Investigation

NETWORK TIMER 01:32:27

FILTERED RESULTS **99** Matched VMs (**18** running, **81** stopped)

hunt-00	RUNNING	VIEW CONSOLE	Hunt-00 Administrator Simspace1!Simspace1!	STARTED 16 MINUTES AGO	USERS 1 ONLINE	VIEW DETAILS
hunt-01	STOPPED		Hunt-01 Administrator Simspace1!Simspace1!	STOPPED 25 DAYS AGO	NO USERS	VIEW DETAILS
hunt-02	STOPPED		Hunt-02 Administrator Simspace1!Simspace1!	STOPPED 25 DAYS AGO	NO USERS	VIEW DETAILS
hunt-03	STOPPED		Hunt-03 Administrator Simspace1!Simspace1!	STOPPED 25 DAYS AGO	NO USERS	VIEW DETAILS
hunt-04	STOPPED		Hunt-04 Administrator Simspace1!Simspace1!	STOPPED 25 DAYS AGO	NO USERS	VIEW DETAILS
hunt-05	STOPPED		Hunt-05 Administrator Simspace1!Simspace1!	STOPPED 25 DAYS AGO	NO USERS	VIEW DETAILS
kali-hunt-00	RUNNING	VIEW CONSOLE	Kali Linux root toor	STARTED 16 MINUTES AGO	NO USERS	VIEW DETAILS
kali-hunt-01	STOPPED		Kali Linux root toor	STOPPED 25 DAYS AGO	NO USERS	VIEW DETAILS
site-elk-00	RUNNING	VIEW CONSOLE	ELK Log Aggregation simspace simspace1	STARTED 20 MINUTES AGO	NO USERS	VIEW DETAILS
site-elk-01	RUNNING	VIEW CONSOLE	ELK Log Aggregation simspace simspace1	STARTED 19 MINUTES AGO	NO USERS	VIEW DETAILS
site-elk-02	RUNNING	VIEW CONSOLE	ELK Log Aggregation simspace simspace1	STARTED 20 MINUTES AGO	NO USERS	VIEW DETAILS

Example: Loggin into hunt-00 Console



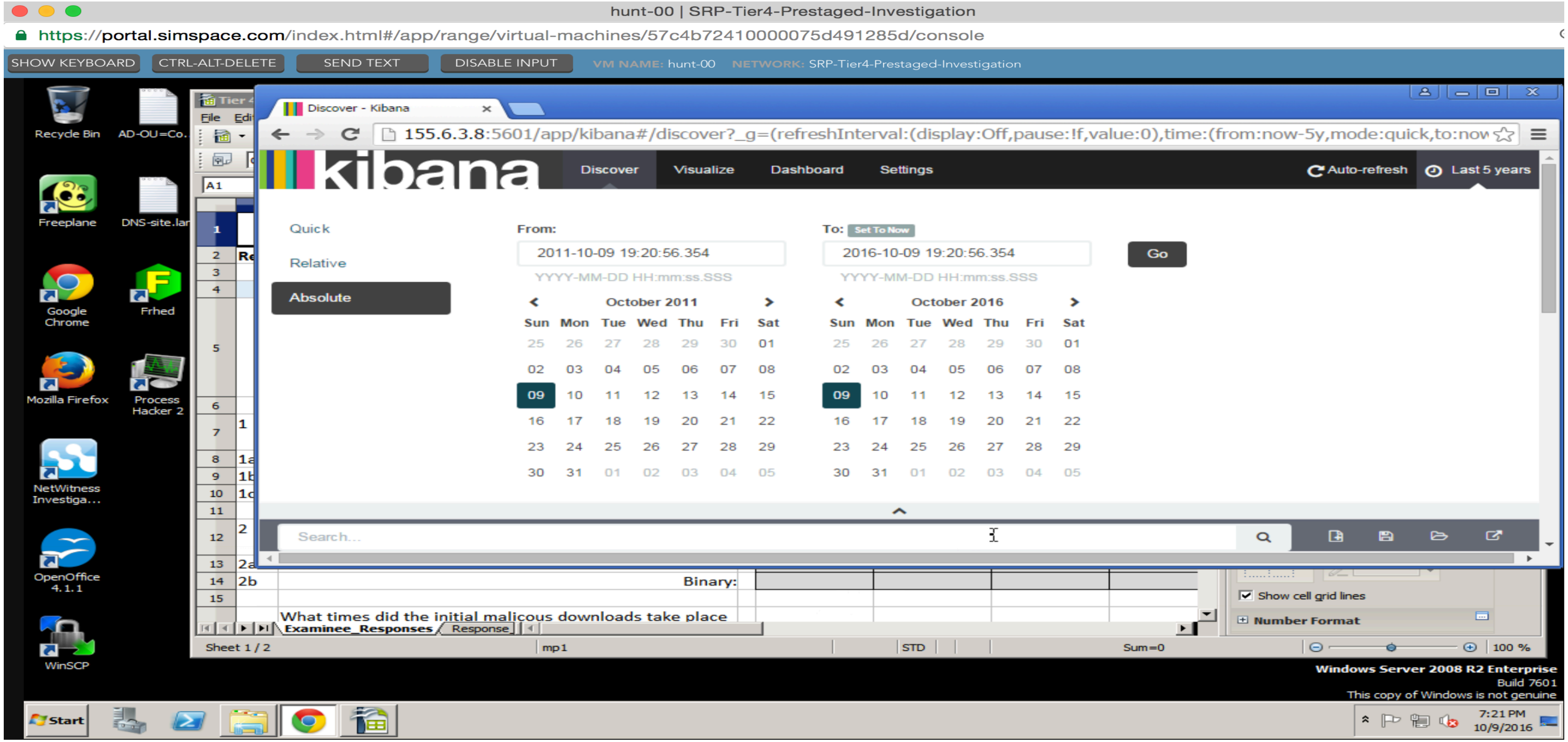
hunt-00 | SRP-Tier4-Prestaged-Investigation

https://portal.simspace.com/index.html#/app/range/virtual-machines/57c4b72410000075d491285d/console

VM NAME: hunt-00 NETWORK: SRP-Tier4-Presta...

site\Administrator

Using Kibana from hunt-00



hunt-00 | SRP-Tier4-Prestaged-Investigation

https://portal.simspace.com/index.html#/app/range/virtual-machines/57c4b72410000075d491285d/console

VM NAME: hunt-00 NETWORK: SRP-Tier4-Prestaged-Investigation

155.6.3.8:5601/app/kibana#/discover?_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from:now-5y,mode:quick,to:now

From: 2011-10-09 19:20:56.354

To: 2016-10-09 19:20:56.354

October 2011

Sun	Mon	Tue	Wed	Thu	Fri	Sat
25	26	27	28	29	30	01
02	03	04	05	06	07	08
09	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	01	02	03	04	05

October 2016

Sun	Mon	Tue	Wed	Thu	Fri	Sat
25	26	27	28	29	30	01
02	03	04	05	06	07	08
09	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	01	02	03	04	05

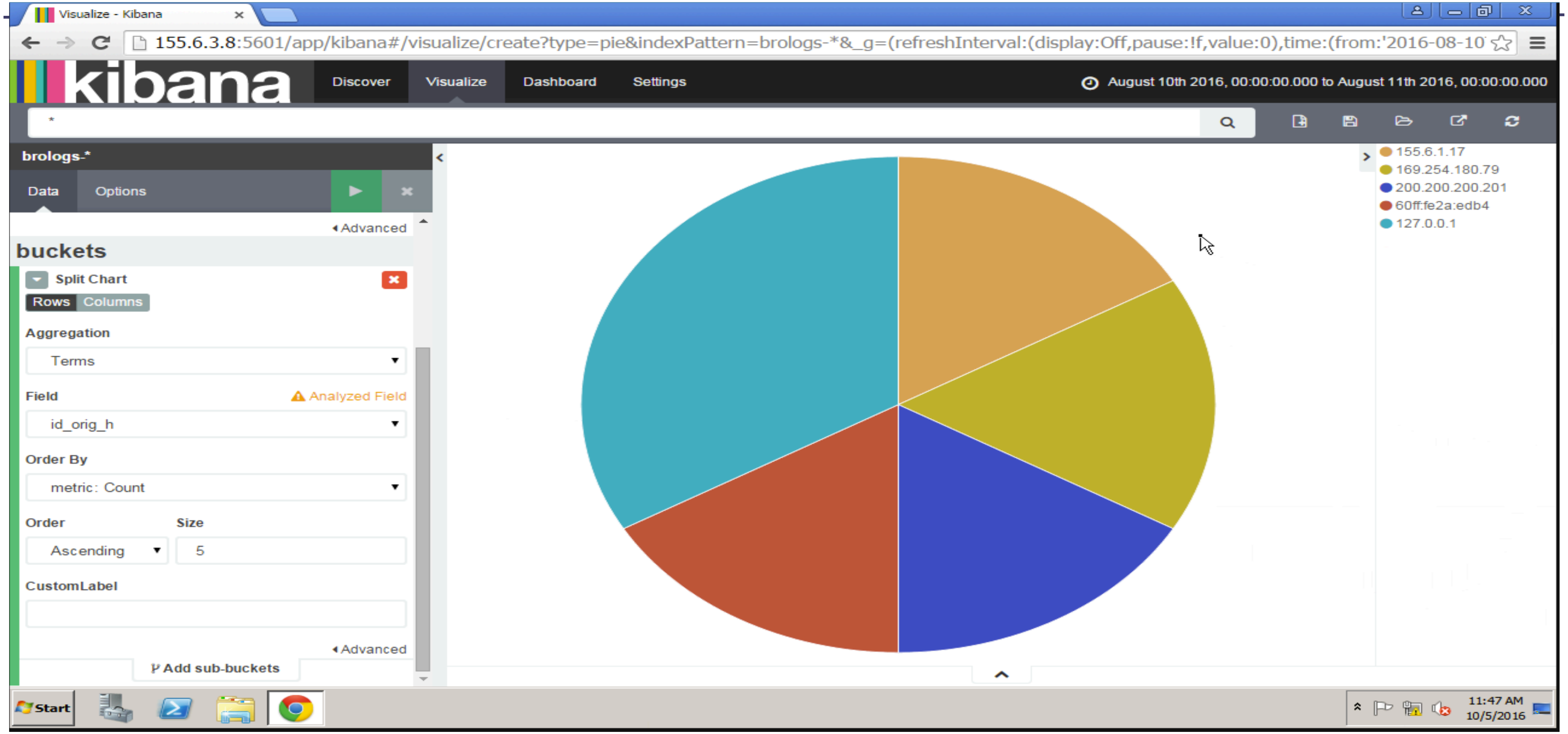
Binary:

What times did the initial malicous downloads take place

Windows Server 2008 R2 Enterprise
Build 7601
This copy of Windows is not genuine

7:21 PM
10/9/2016

Kibana features many visualization aids



155.6.3.8:5601/app/kibana#/visualize/create?type=pie&indexPattern=brologs-*&_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from:'2016-08-10

August 10th 2016, 00:00:00.000 to August 11th 2016, 00:00:00.000

brologs-*

buckets

Split Chart: Rows

Aggregation: Terms

Field: id_orig_h

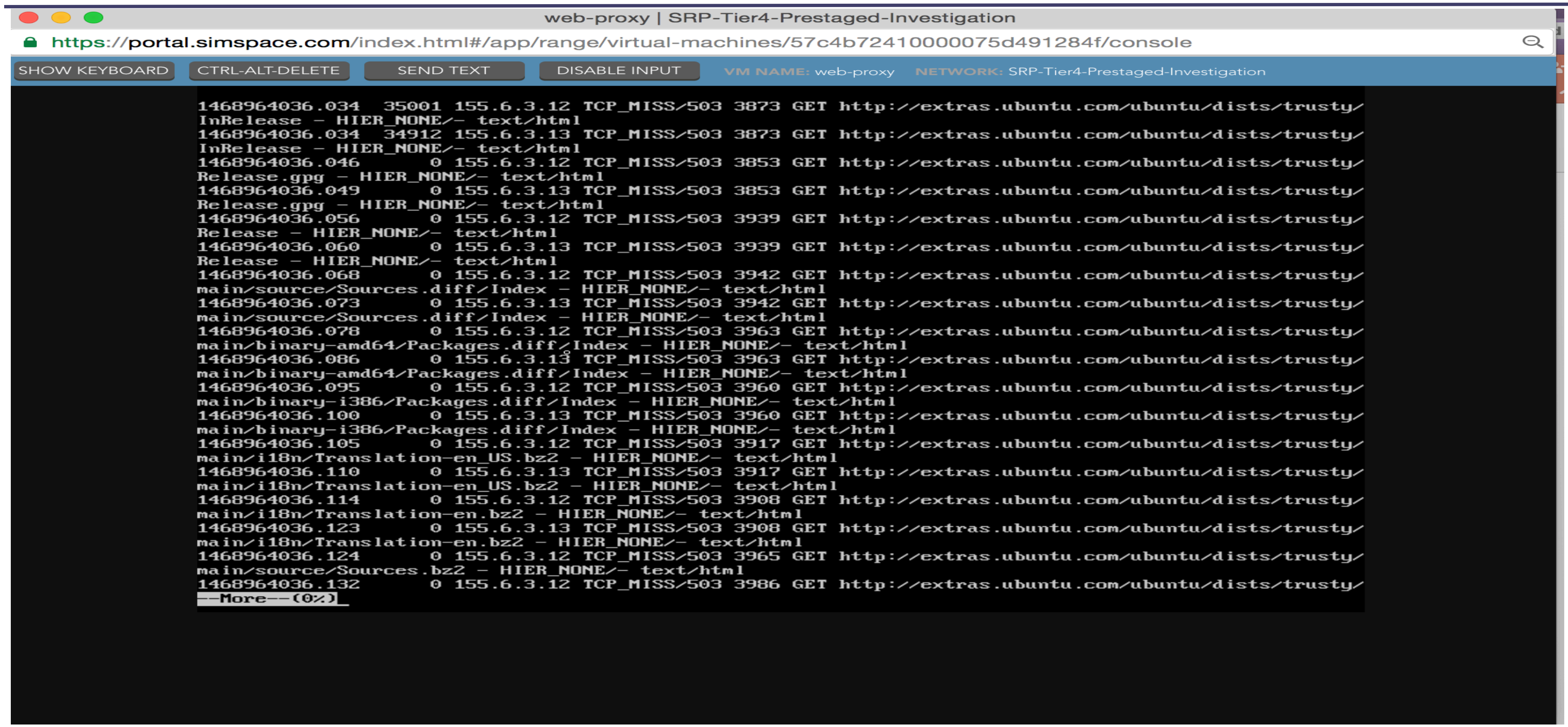
Order By: metric: Count

Order: Ascending

Size: 5

CustomLabel:

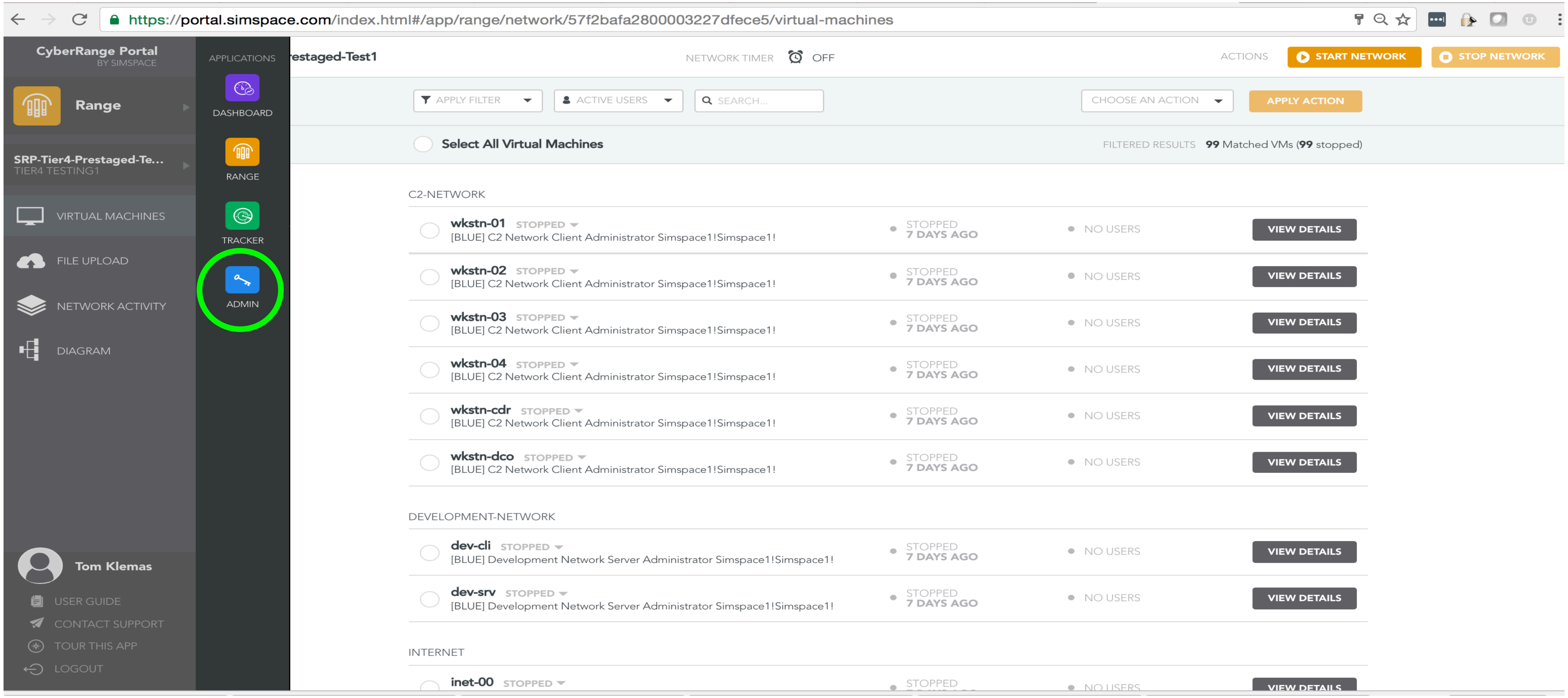
Web Proxy Log Access


web-proxy | SRP-Tier4-Prestaged-Investigation
https://portal.simspace.com/index.html#/app/range/virtual-machines/57c4b72410000075d491284f/console
SHOW KEYBOARD
CTRL-ALT-DELETE
SEND TEXT
DISABLE INPUT
VM NAME: web-proxy
NETWORK: SRP-Tier4-Prestaged-Investigation

```
1468964036.034  35001 155.6.3.12 TCP_MISS/503 3873 GET http://extras.ubuntu.com/ubuntu/dists/trusty/
InRelease - HIER_NONE/- text/html
1468964036.034  34912 155.6.3.13 TCP_MISS/503 3873 GET http://extras.ubuntu.com/ubuntu/dists/trusty/
InRelease - HIER_NONE/- text/html
1468964036.046      0 155.6.3.12 TCP_MISS/503 3853 GET http://extras.ubuntu.com/ubuntu/dists/trusty/
Release.gpg - HIER_NONE/- text/html
1468964036.049      0 155.6.3.13 TCP_MISS/503 3853 GET http://extras.ubuntu.com/ubuntu/dists/trusty/
Release.gpg - HIER_NONE/- text/html
1468964036.056      0 155.6.3.12 TCP_MISS/503 3939 GET http://extras.ubuntu.com/ubuntu/dists/trusty/
Release - HIER_NONE/- text/html
1468964036.060      0 155.6.3.13 TCP_MISS/503 3939 GET http://extras.ubuntu.com/ubuntu/dists/trusty/
Release - HIER_NONE/- text/html
1468964036.068      0 155.6.3.12 TCP_MISS/503 3942 GET http://extras.ubuntu.com/ubuntu/dists/trusty/
main/source/Sources.diff/Index - HIER_NONE/- text/html
1468964036.073      0 155.6.3.13 TCP_MISS/503 3942 GET http://extras.ubuntu.com/ubuntu/dists/trusty/
main/source/Sources.diff/Index - HIER_NONE/- text/html
1468964036.078      0 155.6.3.12 TCP_MISS/503 3963 GET http://extras.ubuntu.com/ubuntu/dists/trusty/
main/binary-amd64/Packages.diff/Index - HIER_NONE/- text/html
1468964036.086      0 155.6.3.13 TCP_MISS/503 3963 GET http://extras.ubuntu.com/ubuntu/dists/trusty/
main/binary-amd64/Packages.diff/Index - HIER_NONE/- text/html
1468964036.095      0 155.6.3.12 TCP_MISS/503 3960 GET http://extras.ubuntu.com/ubuntu/dists/trusty/
main/binary-i386/Packages.diff/Index - HIER_NONE/- text/html
1468964036.100      0 155.6.3.13 TCP_MISS/503 3960 GET http://extras.ubuntu.com/ubuntu/dists/trusty/
main/binary-i386/Packages.diff/Index - HIER_NONE/- text/html
1468964036.105      0 155.6.3.12 TCP_MISS/503 3917 GET http://extras.ubuntu.com/ubuntu/dists/trusty/
main/i18n/Translation-en_US.bz2 - HIER_NONE/- text/html
1468964036.110      0 155.6.3.13 TCP_MISS/503 3917 GET http://extras.ubuntu.com/ubuntu/dists/trusty/
main/i18n/Translation-en_US.bz2 - HIER_NONE/- text/html
1468964036.114      0 155.6.3.12 TCP_MISS/503 3908 GET http://extras.ubuntu.com/ubuntu/dists/trusty/
main/i18n/Translation-en.bz2 - HIER_NONE/- text/html
1468964036.123      0 155.6.3.13 TCP_MISS/503 3908 GET http://extras.ubuntu.com/ubuntu/dists/trusty/
main/i18n/Translation-en.bz2 - HIER_NONE/- text/html
1468964036.124      0 155.6.3.12 TCP_MISS/503 3965 GET http://extras.ubuntu.com/ubuntu/dists/trusty/
main/source/Sources.bz2 - HIER_NONE/- text/html
1468964036.132      0 155.6.3.12 TCP_MISS/503 3986 GET http://extras.ubuntu.com/ubuntu/dists/trusty/
--More--(0%)
```

Numerous tools available for detection, investigation, administrative actions, and more!

Enabling Customer Led Training



https://portal.simspace.com/index.html#/app/range/network/57f2bafa2800003227dfece5/virtual-machines

estaged-Test1

NETWORK TIMER OFF

ACTIONS START NETWORK STOP NETWORK

○ Select All Virtual Machines

FILTERED RESULTS **99** Matched VMs (**99** stopped)

C2-NETWORK

○	**wkstn-01** STOPPED [BLUE] C2 Network Client Administrator Simspace1!Simspace1!	● STOPPED 7 DAYS AGO	● NO USERS	VIEW DETAILS
○	**wkstn-02** STOPPED [BLUE] C2 Network Client Administrator Simspace1!Simspace1!	● STOPPED 7 DAYS AGO	● NO USERS	VIEW DETAILS
○	**wkstn-03** STOPPED [BLUE] C2 Network Client Administrator Simspace1!Simspace1!	● STOPPED 7 DAYS AGO	● NO USERS	VIEW DETAILS
○	**wkstn-04** STOPPED [BLUE] C2 Network Client Administrator Simspace1!Simspace1!	● STOPPED 7 DAYS AGO	● NO USERS	VIEW DETAILS
○	**wkstn-cdr** STOPPED [BLUE] C2 Network Client Administrator Simspace1!Simspace1!	● STOPPED 7 DAYS AGO	● NO USERS	VIEW DETAILS
○	**wkstn-dco** STOPPED [BLUE] C2 Network Client Administrator Simspace1!Simspace1!	● STOPPED 7 DAYS AGO	● NO USERS	VIEW DETAILS

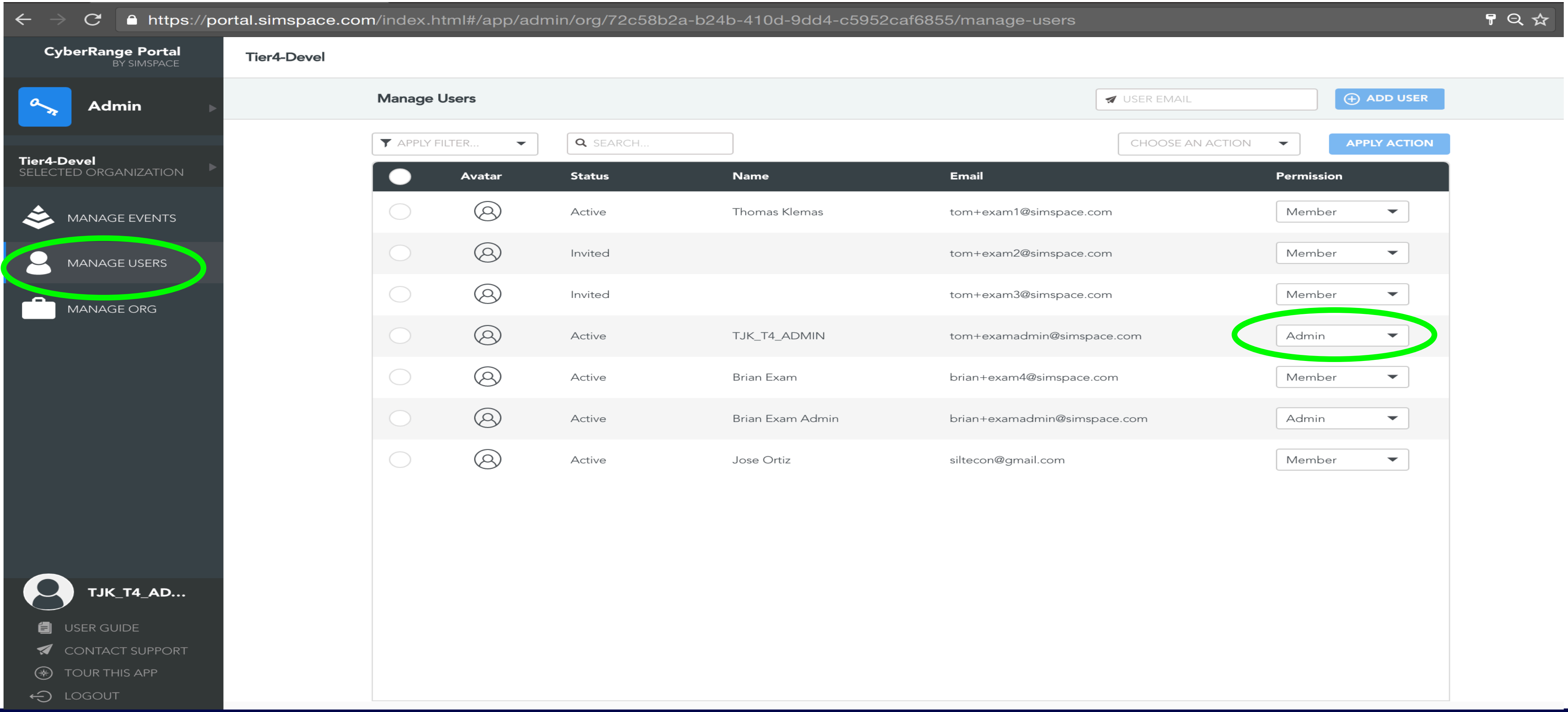
DEVELOPMENT-NETWORK

○	**dev-cli** STOPPED [BLUE] Development Network Server Administrator Simspace1!Simspace1!	● STOPPED 7 DAYS AGO	● NO USERS	VIEW DETAILS
○	**dev-srv** STOPPED [BLUE] Development Network Server Administrator Simspace1!Simspace1!	● STOPPED 7 DAYS AGO	● NO USERS	VIEW DETAILS

INTERNET

○	**inet-00** STOPPED	● STOPPED	● NO USERS	VIEW DETAILS

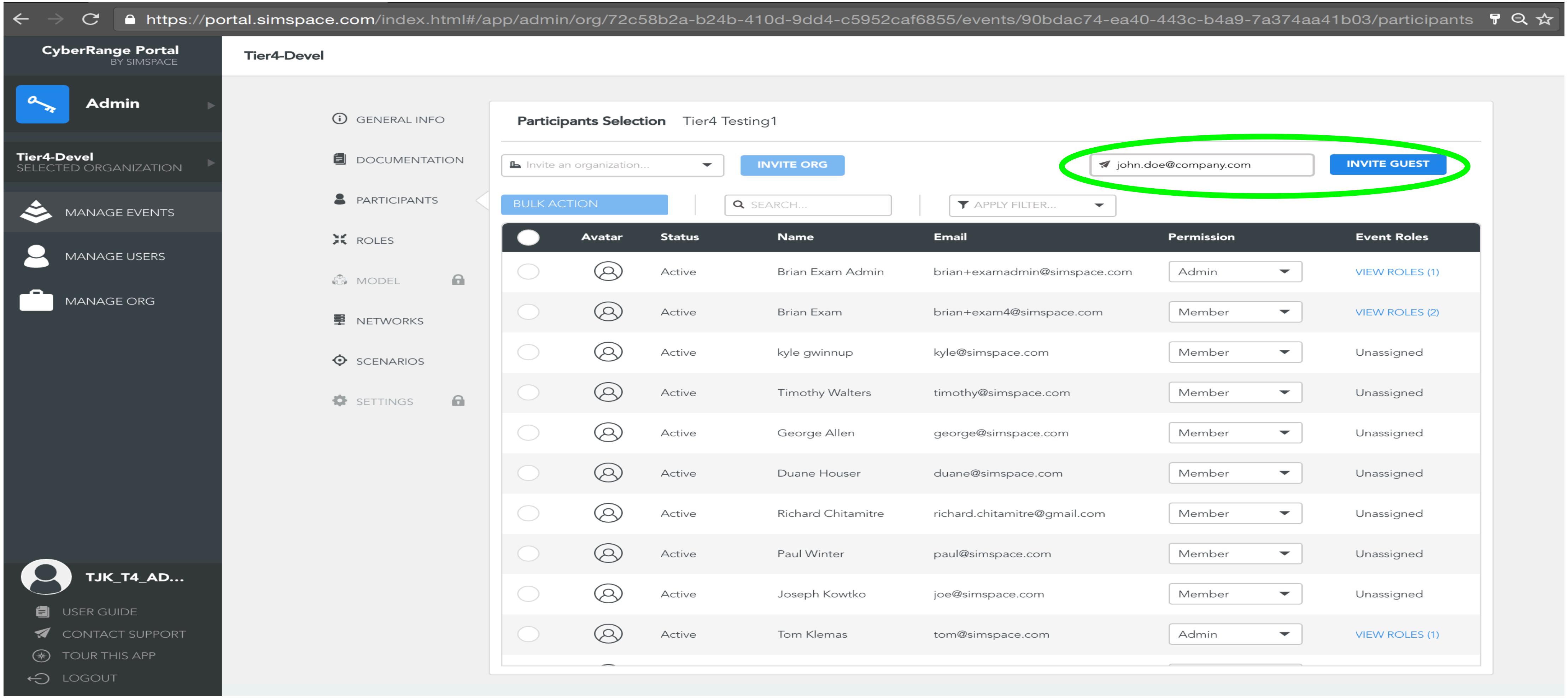
Provide admin privileges to training monitor



https://portal.simspace.com/index.html#/app/admin/org/72c58b2a-b24b-410d-9dd4-c5952caf6855/manage-users

Avatar	Status	Name	Email	Permission
	Active	Thomas Klemas	tom+exam1@simspace.com	Member
	Invited		tom+exam2@simspace.com	Member
	Invited		tom+exam3@simspace.com	Member
	Active	TJK_T4_ADMIN	tom+examadmin@simspace.com	Admin
	Active	Brian Exam	brian+exam4@simspace.com	Member
	Active	Brian Exam Admin	brian+examadmin@simspace.com	Admin
	Active	Jose Ortiz	siltecon@gmail.com	Member

Invite participants to organization



https://portal.simspace.com/index.html#/app/admin/org/72c58b2a-b24b-410d-9dd4-c5952caf6855/events/90bdac74-ea40-443c-b4a9-7a374aa41b03/participants

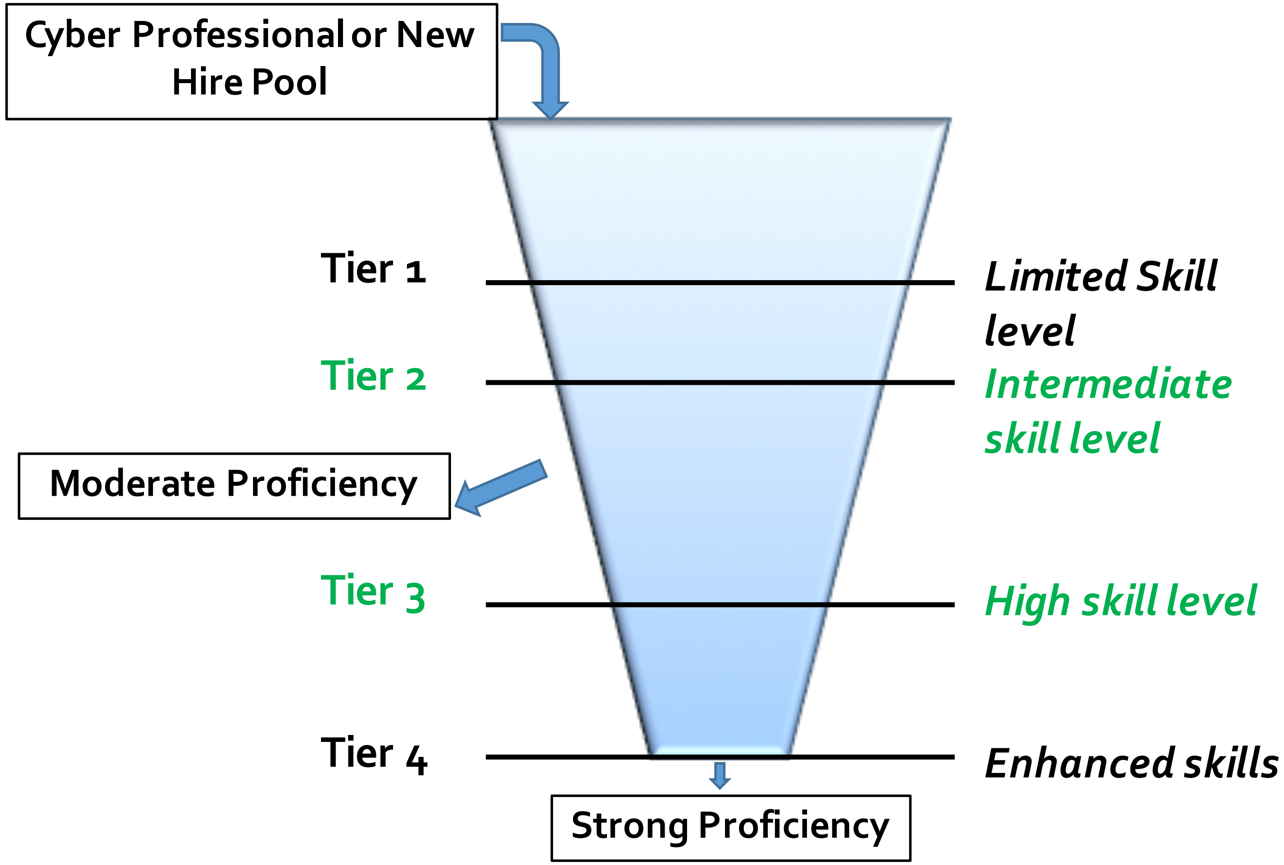
○	Avatar	Status	Name	Email	Permission	Event Roles
○		Active	Brian Exam Admin	brian+examadmin@simspace.com	Admin	VIEW ROLES (1)
○		Active	Brian Exam	brian+exam4@simspace.com	Member	VIEW ROLES (2)
○		Active	kyle gwinnup	kyle@simspace.com	Member	Unassigned
○		Active	Timothy Walters	timothy@simspace.com	Member	Unassigned
○		Active	George Allen	george@simspace.com	Member	Unassigned
○		Active	Duane Houser	duane@simspace.com	Member	Unassigned
○		Active	Richard Chitamitre	richard.chitamitre@gmail.com	Member	Unassigned
○		Active	Paul Winter	paul@simspace.com	Member	Unassigned
○		Active	Joseph Kowtko	joe@simspace.com	Member	Unassigned
○		Active	Tom Klemas	tom@simspace.com	Admin	VIEW ROLES (1)

Motivations for Cyber Assessment

- Difficult challenges faced by cybersecurity officers
  - Hiring, training, and re-vectoring of employees
  - Early Identification of employees with high potential for advancement
  - Composing balanced cyber defense teams
- Cost of mistake is high
  - Hiring the wrong person can be quite costly
  - Interviewing the wrong people is also too expensive

Cyber Assessor for Individuals

- Tiers 1 and 2
  - multiple choice
  - critical thinking, reasoning, and knowledge
  - Web-based
- Tier 3
  - Emulates primarily single computer tasks
  - hands-on
  - self-contained
  - Tests skills and knowledge
  - Web-based
- Tier 4
  - Virtual cyber range that emulates real networks
  - Examines skill & knowledge
  - User emulator can create "typical" user noise



Cyber Professional or New Hire Pool

Tier 1 — *Limited Skill level*

Tier 2 — *Intermediate skill level*

Moderate Proficiency

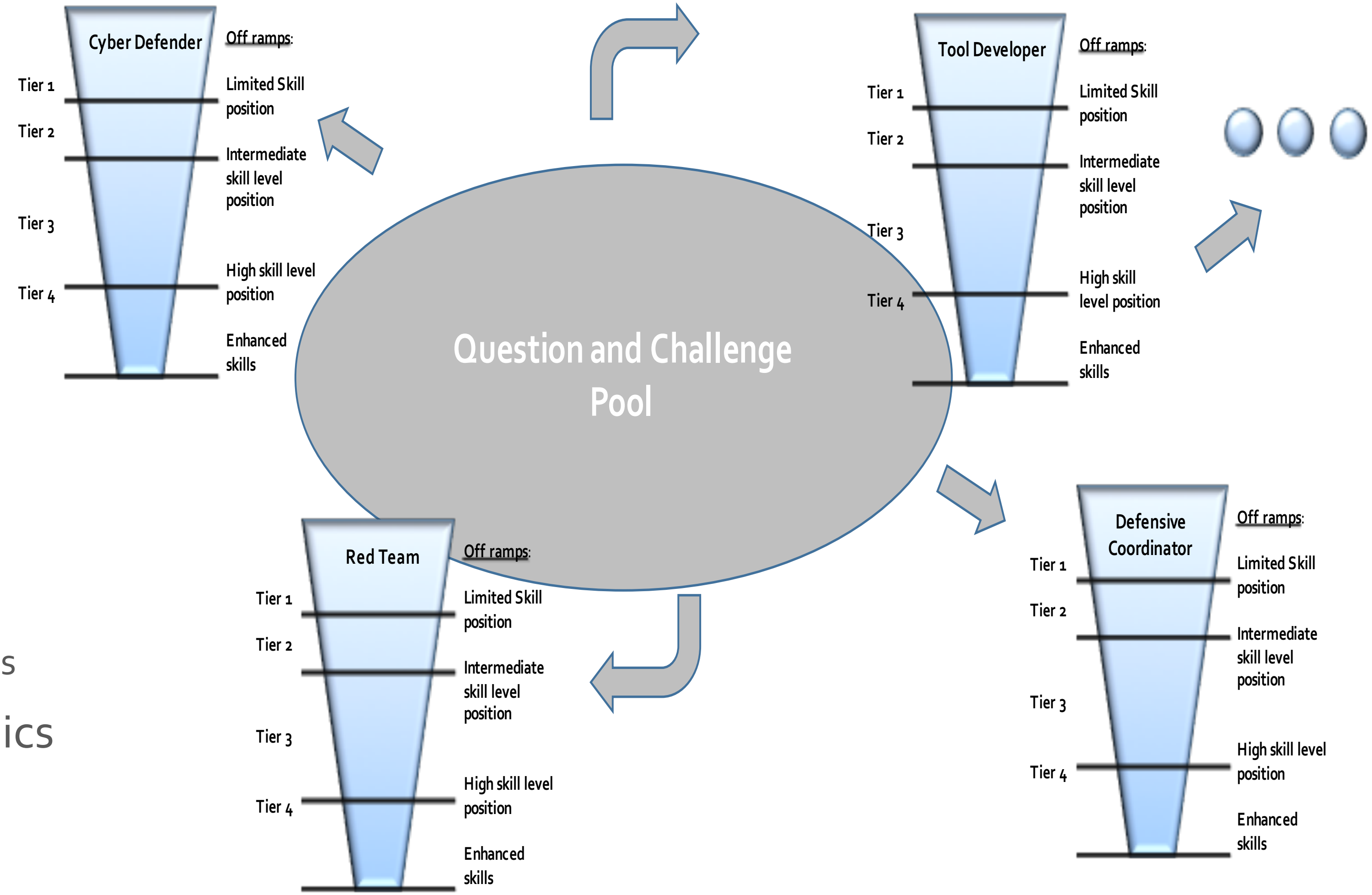
Tier 3 — *High skill level*

Tier 4 — *Enhanced skills*

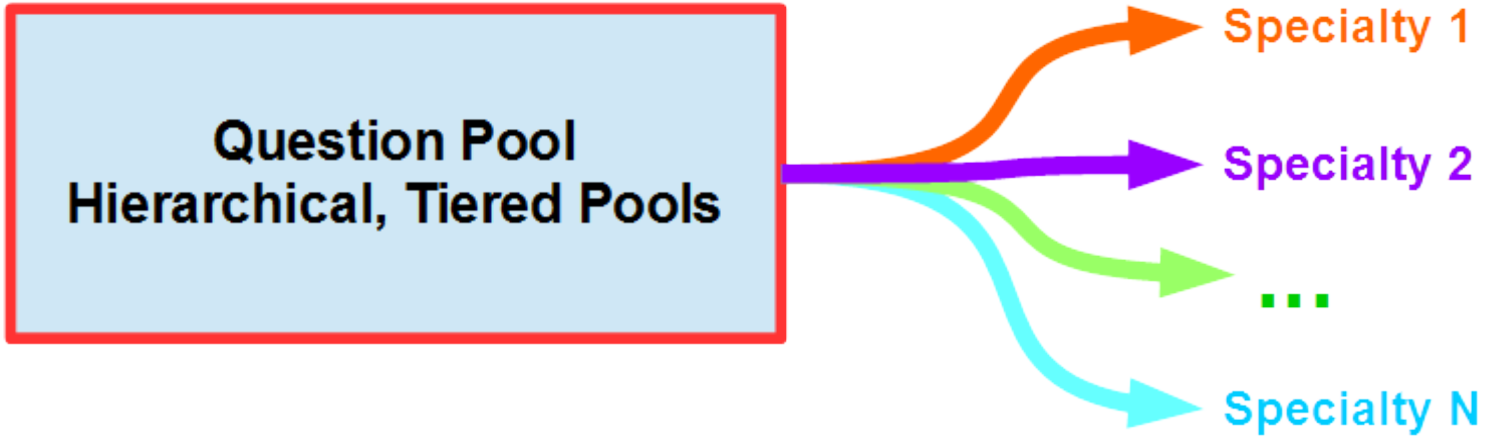
Strong Proficiency

Characterization Capabilities

- Characterizing individual skills
  - Question to Specialty Mappings
  - Enables Skill sub-scores
- Multiple Classification Systems
  - Customer custom specialities
  - SimSpace specialties
  - Standard Frameworks
- Team Composition
  - Determine strengths/weaknesses
  - Balance multiple teams
  - Construct high performance teams
- Identify & prioritize training topics



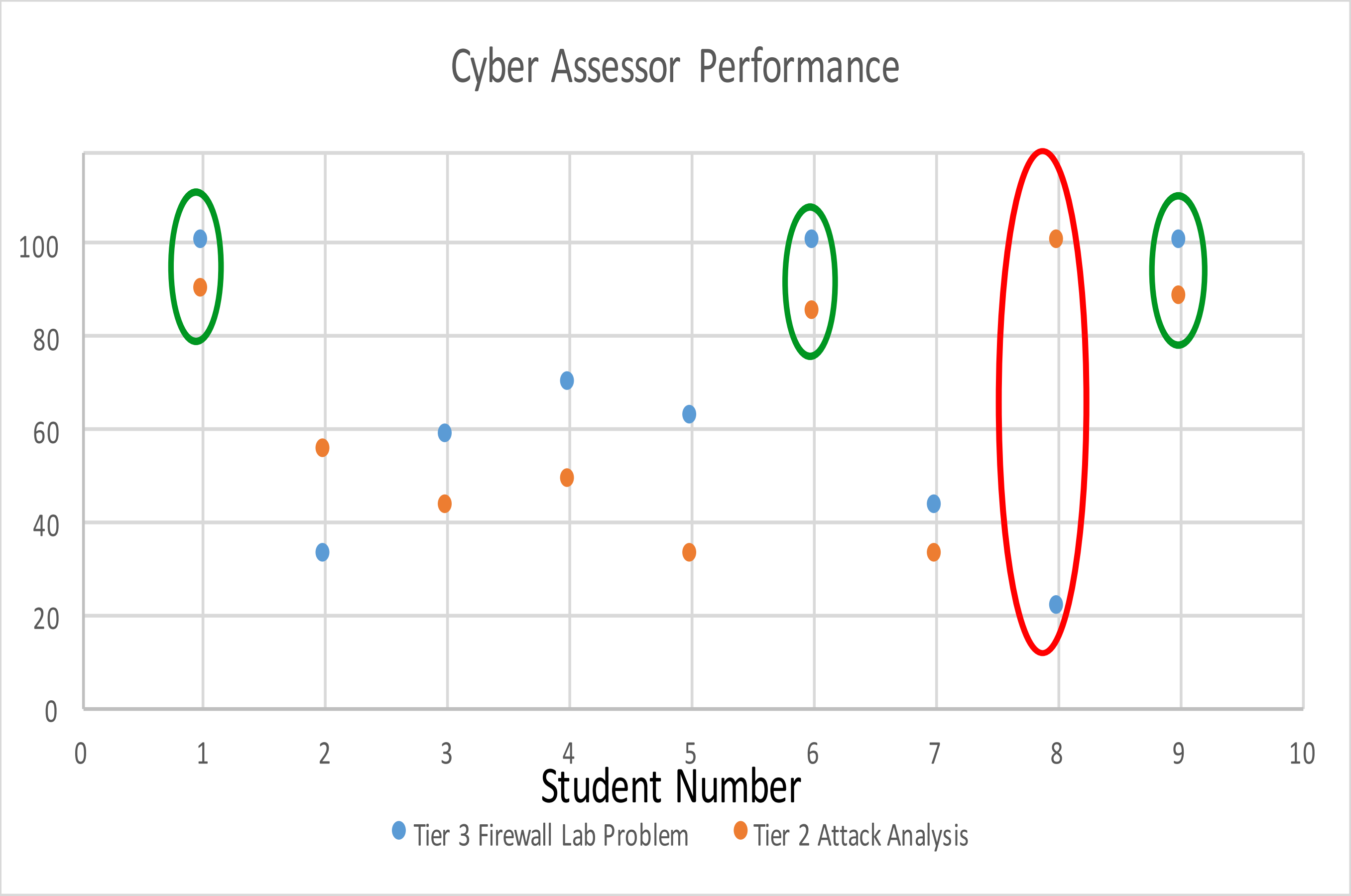
Exam Composition



- Create exams for particular specialties
- Characterize examinee skills across a spectrum of specialties

Example Result: Performance

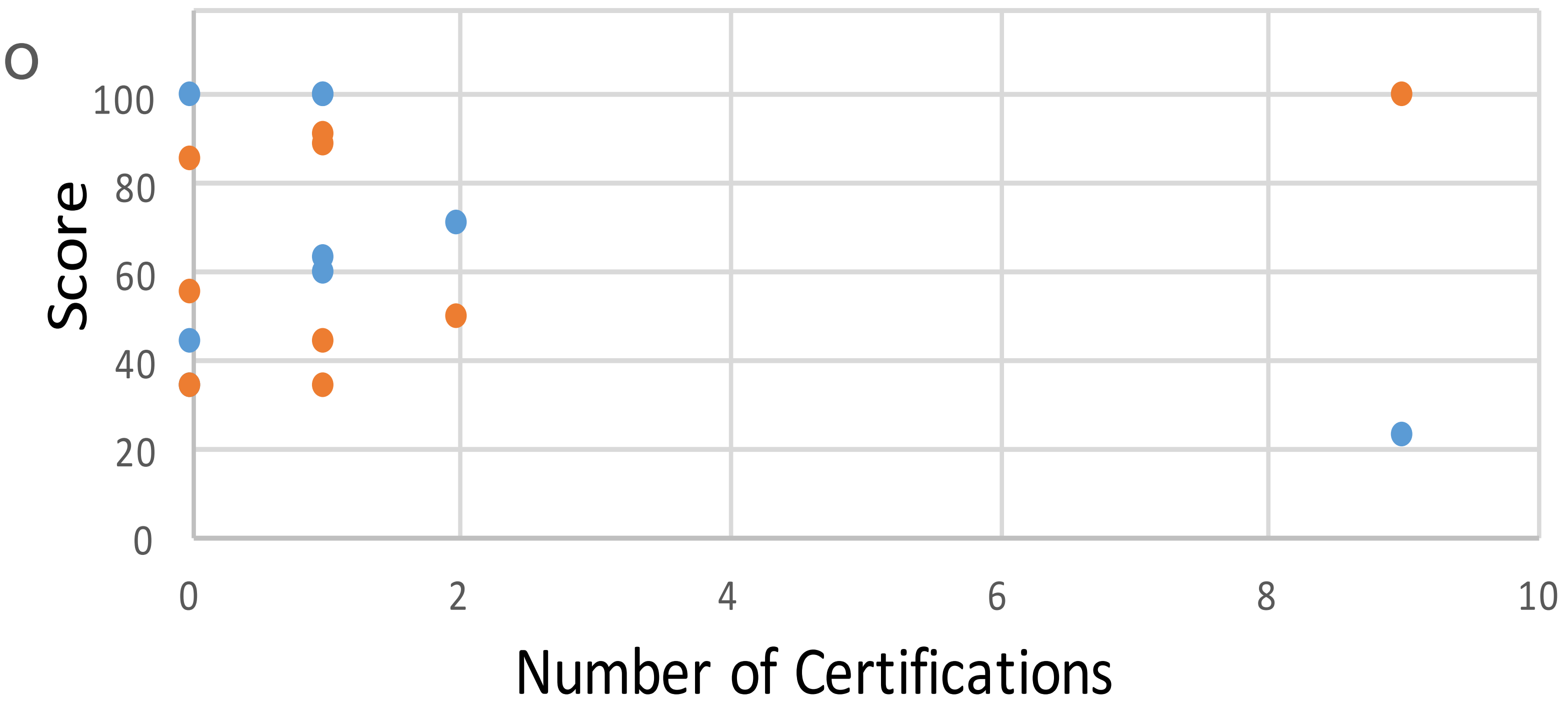
- Tier 2 results in orange
- Tier 3 results in blue
- 3 strong performers
  - Students 1,6, 9
- "Anti-correlation"
  - Student 8



Example Result: Understanding Scores

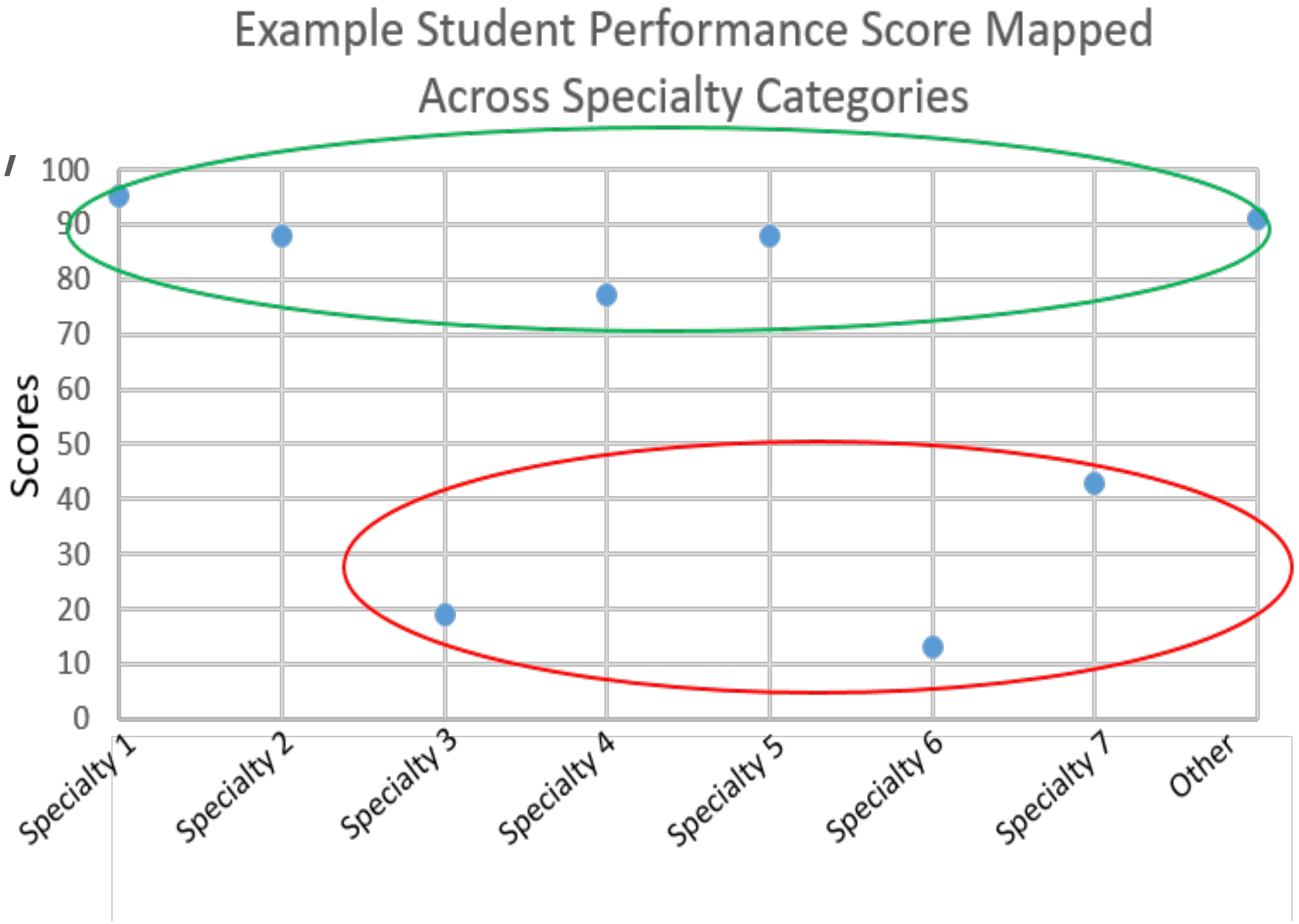
- Explore factors that contribute to score
- Plot scores relative to other examinee attributes

Cyber Assessor Performance vs Number of Certifications



Example Result: Score Characterization

- Examinee scored much better in Specialties 1,2,4,5, and "other"
- Examinee had weaker performance in Specialties 3,6, and 7



Summary

- The need for motivated researchers and engineers to apply skills and knowledge to cyber field is great!
- Need for cybersecurity improvements is urgent
  - Personnel
  - Assessment and Training
  - Technologies
- There are many applications for data analytics in cybersecurity

QUESTIONS?

Thank you!