ISSA Presentation

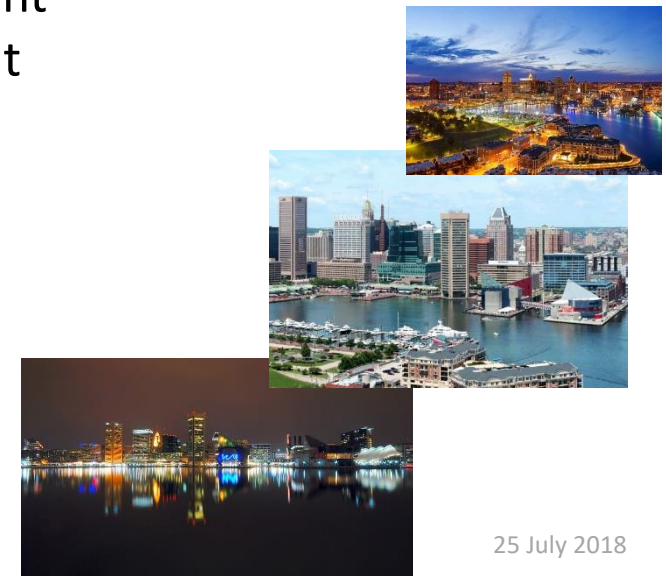
July 25, 2018

Baltimore Cyber Range
8 Market Place
Baltimore, Maryland 21202

Agenda

Baltimore Cyber Range

- Company Overview
- Primary Activities / Programs
- Resources
- Resource Development
- Questions / Comment



Company

Baltimore Cyber Range

- LLC Formed in May 2017
- Grew out of Governor Hogan's Trade Mission to Israel in 2016
- Focus IT / Cyber Training - Testing - Placement Services
- Emphasize Hands-on training and experience
- Operating in Downtown Baltimore – 'Power Plant Live'
  - Range Facility – 900 sq. ft. / 8 Market Place
  - Classroom – 800 sq. ft. / BCCC Reisterstown facility
- Customer Base
  - State / Federal Government / Commercial

Cyber 'Wild West'

Baltimore Cyber Range

- A dynamic industry in transition
- Data is 'King'
- Billing and Accounting
- Marketing / Operations / Intelligence / Targeting
- Collection / Data Types / Storage / Manipulation
  - Collection methods / Politics
  - Location / Spending Habits / relationships
  - Financial data / 'ethnic affinity'
- Data Concentration - Google / Facebook / Equifax
- Explosion of Threats / Risks / Liabilities
- Email – 269 B – 54% (Spam)- 1/131 - >2B
- Many more compromises / reported & unreported

Cyber 'Wild West'

Baltimore Cyber Range

- Established standards:
  - Industry certifications
  - NIST standardization
  - Education standardization
- Regulatory / Legal Requirements
  - Health Care / Financial / State & Federal / EU
- Formalization of Training requirements
  - Education / Certification / Experience
- Enforcement / Liability / Responsibilities Shifts
  - New congressional mandates (Uber notification)
  - NYD Financial Service – Equifax (consent order)
  - Morrison's employee case
  - Target
  - Wyndham (circa 2010)

Activities

Baltimore Cyber Range

- Work Force Development
- Placement Services
- Cyber Awareness Training
- Pre-employment / Proficiency testing
- Advanced Threat Training
- STEM

Work Force Development

Baltimore Cyber Range

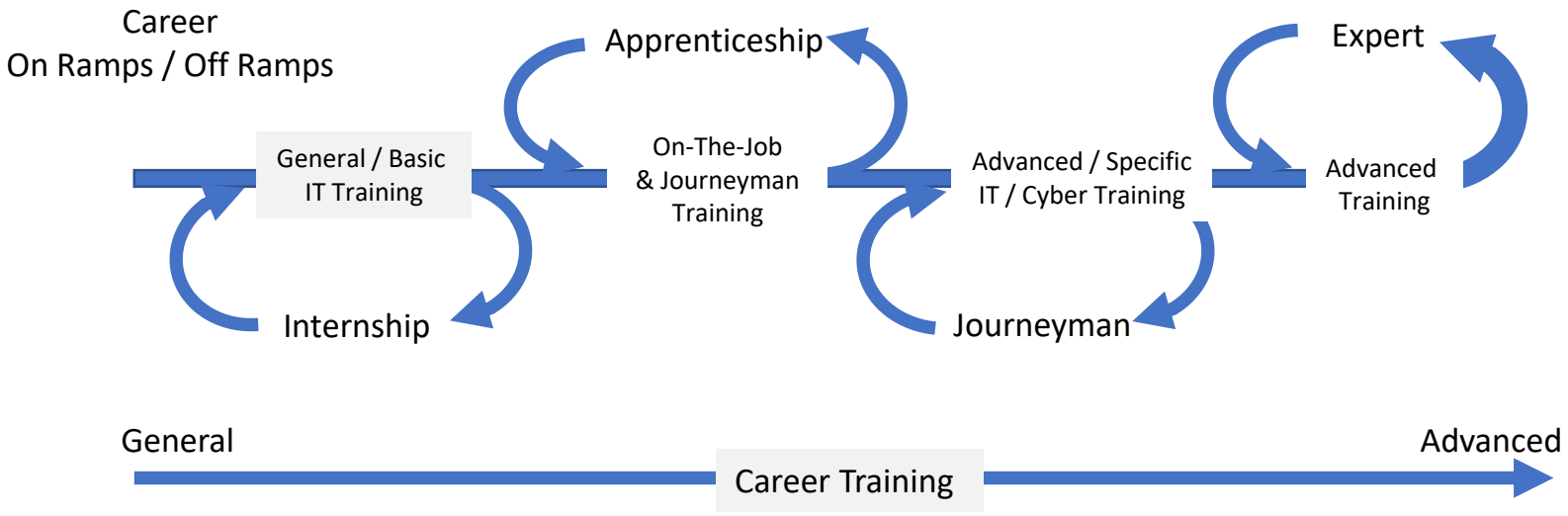
- Open Positions – 200,000, >12,000, 1.5M by 2019
- Unemployment (Apr 18) 4.3 / 5.8
  - (20-24 – Minority 37%)
- Activity primarily in support of the State of Maryland
- Targets underemployed and unemployed
- Program addresses three levels
  - Entry
  - Journeyman
  - Expert
- Program based on NIST/NICE document
- Emphasizes Hands-on Learning
- Regular Testing / assessment review
- Internally developed training material
- Consortium defines / reviews training requirements

Consortium Membership

- ASD, Inc.
- Atlantic Data Forensics, Inc.
- Azgard Group
- Baltimore City Community College
- Baltimore Cyber Range
- Blue Eye Technology, Inc.
- City of Baltimore Mayor's Office
- Crimson Vista Inc.
- Cyberbit Commercial Solutions, Inc.
- CyberPoint
- Electronic Technology Associates, LLC
- ManTech
- Metro Data Inc.
- M&T Bank
- Nexagen Networks, Inc.
- Persistent Surveillance Inc.
- Que Technology Group
- Stark Industries, LLC
- Synogy Consulting Group
- TeraSense, Inc.
- TranZed Apprenticeship Services
- WITS/Maalot Baltimore

Training / Employment Pipeline

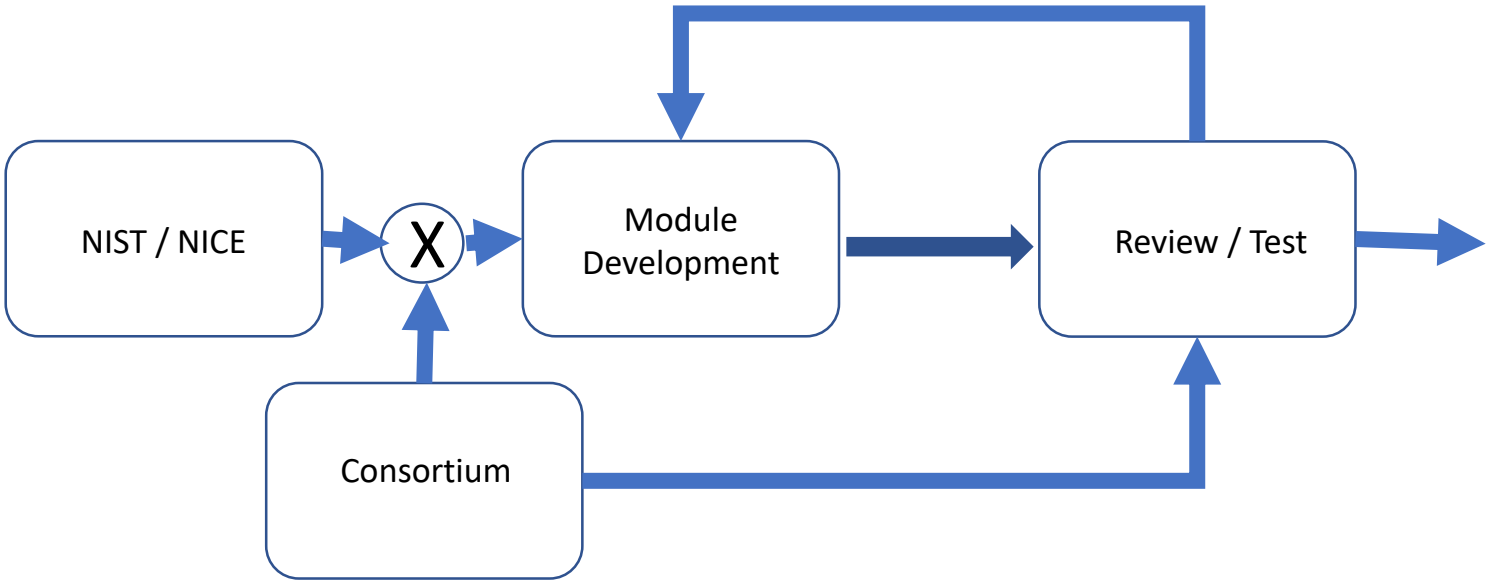
Baltimore Cyber Range



- Pipeline provides a training baseline that supports employment 'On' and Off' ramps
- Designed to accommodate entry through expert level career education and experience requirements

Training Module Development

Baltimore Cyber Range



Module #3 NIST / NICE Table

Key Topics	
x	Server and client operating systems
x	Operating Systems
x	Network architecture
x	Network Components
x	Interpreted and compiled computer languages
x	Communications and Routing
x	Local area network (LAN), wide area network (WAN) and enterprise principles and concepts, including bandwidth management
x	Computer networking concepts and protocols, and network security methodologies.
x	Network protocols (e.g., Transmission Critical Protocol (TCP), Internet Protocol (IP), Dynamic Host Configuration Protocol (DHCP)), and directory services (e.g., Domain Name System (DNS))
x	Operating system command line/prompt.
x	File extensions (e.g., .dll, .bat, .zip, .pcap, .gzip)
x	System implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).
x	System Administration Review
x	Install, update, and troubleshoot systems/servers
x	Workstation Build and Configuration
x	Monitor and maintain system/server configuration
x	Manage accounts, network rights, and access to systems and equipment
x	Execute, and verify data redundancy and system recovery procedures

WFD Training Modules

Baltimore Cyber Range

Entry Level

Module 1 –
Basic learn skills

Module 2 -
IT basics
Modeled on Comp TIA A+ Program

Cyber Skill Level / Focus :
Little or no IT - Cyber background / IT Basics

Number of Training Modules: 2

Duration: 1 Week / 10 Weeks

Training Provided by BCCC

Journeymen Level

Module 3 –
Workstations / Servers / Networks

Module 4 -
Networks / System Administration

Module 5 –
Administration / IT security / Cyber

Cyber Skill Level / Focus :
Medium – Working in IT / System Administration

Number of Training Modules: 3

Duration: 1 Week each

Training Provided by BCR

Expert Level

Module 6 –
Security Ops / Cyber Review / Tools

Module 7 -
Hands-on Cyber Range Training
Practice handling real-world threats

Module 8 –
Range Trainer of Trainers
Range Operation

Cyber Skill Level / Focus :
High – Cyber Security Experts / Hands-on Threat Simulation & Training

Number of Training Modules: 3

Duration: 1 Week / 2 Days / 1 Week

Training Provided by BCR

Workforce Development Status

Baltimore Cyber Range

Completed ICE-T I

Intrusion Countermeasures Education and Training

Competed ACT I

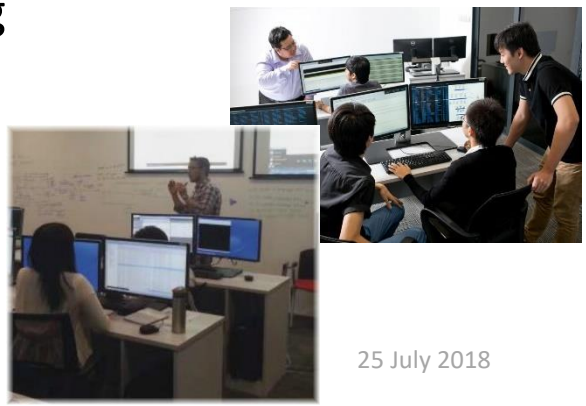
Advanced Cybersecurity Training

Awarded ICE-T II

ICE-T Basic

Planning ACT II

Advanced Cybersecurity Training



WFD Placement Services

Baltimore Cyber Range

Internships

- Interns generally work for three to six months
- Internships convey hands-on real-world work experience
- Employers have the opportunity to evaluate Intern / Interns work

Apprenticeships

- Apprenticeship programs combine academic training and on-the-job-training
- Generally conducted over twelve to twenty four months
- Apprentice progress by completing established milestones

Full Time Employment

- Where appropriate Baltimore Cyber Range is identifying full time positions for those completing BCR IT / Cyber training

Cyber Awareness Training

Baltimore Cyber Range

- Supports both private and public organizations
- Program addresses staff cyber training requirements
  - Regulatory / Legal / Corporate directed
- Programs to date have been customized for client
- Training is optimized for the targeted users
  - Admin staff, senior management, tech staff. etc.
- Class time varies with audience

Cyber Awareness Training

Baltimore Cyber Range

Senior Management

Training:

Cyber Security Introduction
Threat Review
- General overview
- Threat attack flow (high level)

Detection / Mitigation / Remediation (Basics)
Threat Response / Management
- Responding to particular Threats
- Working with Law enforcement
- Public Interaction / Relations

Consequences
- Regulatory Responsibilities
- Liability / corporate, shareholders etc.

Identifying key roles and responsibilities
Establishing organizational goals / objectives
Review / Establish Policies / Standards

Targeted Staff Group:
Senior organization decisions makers

Responsibilities:
Sets Organization direction, goals and objectives
Approves overall policies / standards
Responsible for overall performance / success

Cyber Skill Level / Focus :
Low / Consequences - Management

Duration:
2 Hours

Frequency:
1 X Year

System Users

Training:

Cyber Awareness Introduction
Threat Review
- Threat basics
- Threat detection

User Threat Response
Consequences
- Impact on Organization
- Personal Responsibility

Available resources
Review of Organization Policies / Standards

Targeted Staff Group:
System users / organization staff

Responsibilities:
Day-to-day Operations
Interact with IT resources & facilities

Cyber Skill Level / Focus:
Low / Why of Cyber Security

Duration:
1 Hours

Frequency:
2 X Year

Cyber Awareness Training

Baltimore Cyber Range

IT Professionals

Training:

Cyber Security Introduction
Threat Review
General overview
Detection / Mitigation / Remediation (Basics)
Threat Response / Management
Personal Responsibility
Review / Establish Policies / Standards
Enforcing Polices and Standards

Targeted Staff Group:
IT staff / Administrators / Support Desk
IT infrastructure operations / Maintenance

Responsibilities:
Operates / Maintains IT infrastructure
Enforces polices and standards
Works with SOC teams

Cyber Skill Level / Focus :
Medium / Security Management -Technical

Duration:
3 Hours

Frequency:
1 X Year

Cyber Security Team

Training:

Threat Review
Detection / Mitigation / Remediation
SIEM / Tools Review
Range Simulation (3 scenarios)
Review of Organization Policies / Standards
Personal Responsibility

Targeted Staff Group:
CISO / SOC Manager / Analysts

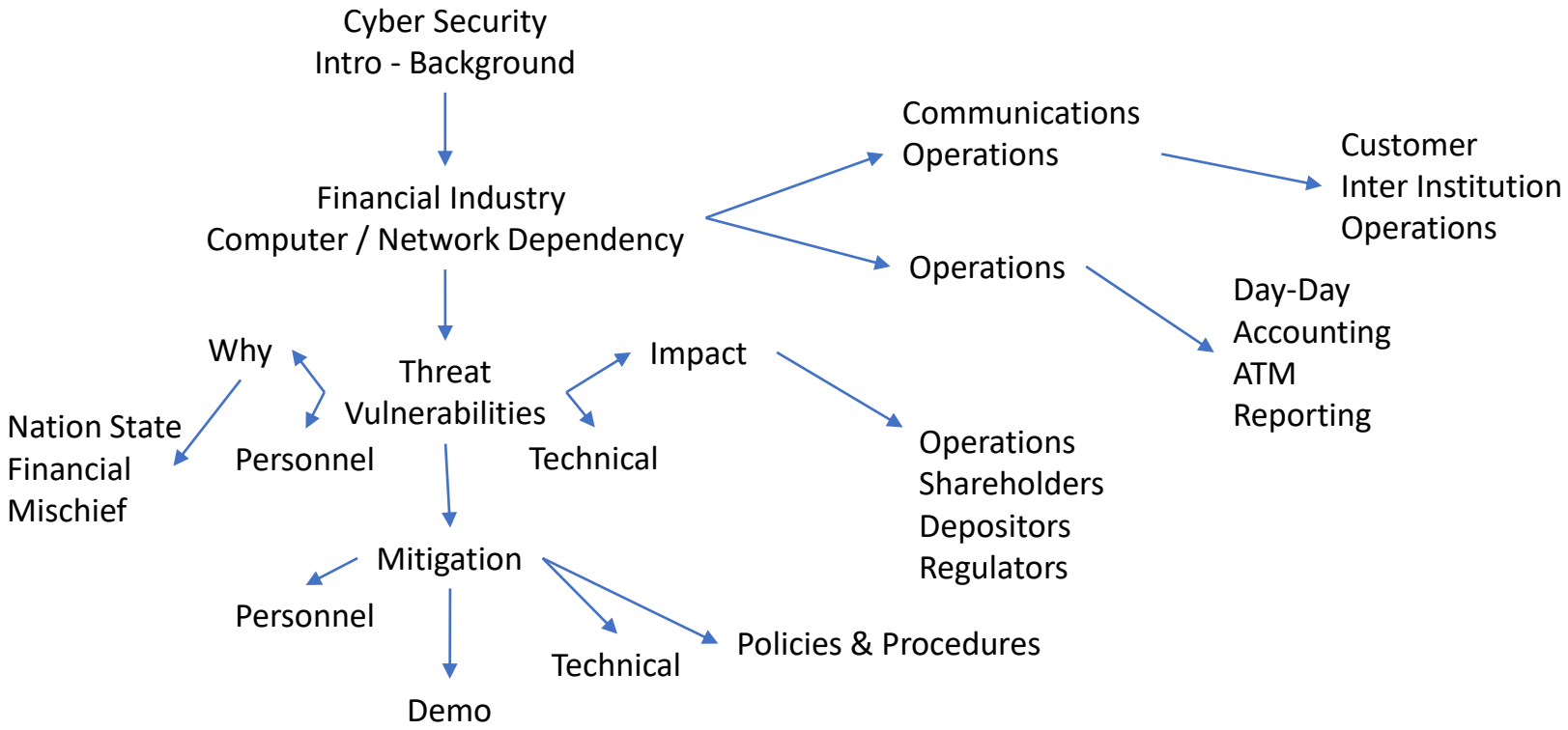
Responsibilities:
SOC operations
Threat Analysis / Remediation

Cyber Skill Level / Focus:
Expert / Hands-on Training - Technology

Duration:
2 Days

Frequency:
2 X Year

World Bank Flow



'…financial services firms are a whopping 300 times more likely to be hit by security incidents than other industries' Lloyd's

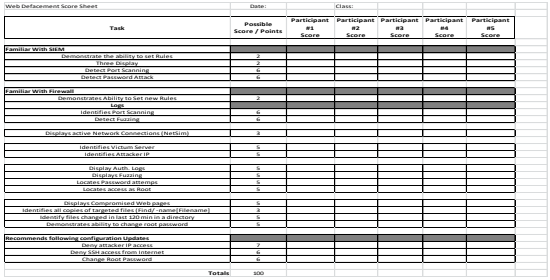
Pre-employment / Proficiency testing

Baltimore Cyber Range

- IT / Cyber Industry dynamic / in transition
- Key issues include regulatory, legal, business
- Three Issues for Employers
  - Education
    - Traditional / Specialized
  - Certification
  - Experience
- Testing, skill demo, accreditation manifesting
  - Contractual
  - Regulatory
  - Legal
  - Employment

Pre-employment / Proficiency testing

- Targets both Private and Public Organizations
- Evaluating new-hire proficiency is problematic
- Education and Credentials may not reflect job ability
- Program requires applicants to demonstrate capabilities
- Proficiency demonstration supporting accreditation
- Recent FedRAMP assessor accreditation
  - Based on Cyber Range
  - Demonstrates Linux, WS OS, Firewall knowledge



Web Defacement Score Sheet	Date:		Class:			
Task	Possible Score / Points	Participant #1 Score	Participant #2 Score	Participant #3 Score	Participant #4 Score	Participant #5 Score
Familiar With SIEM						
Demonstrate the ability to set Rules	2					
Thrive Dispity	2					
Detect Port Scanning	6					
Detect Password Attack	5					
Familiar With Firewall						
Demonstrates Ability to Set new Rules	2					
Logs						
Identifies Port Scanning	6					
Detect Fuzzing	5					
Displays active Network Connections (NetStm)	3					
Identifies Victum Server	5					
Identifies Attacker IP	5					
Display Auth. Logs	5					
Displays Fuzzing	5					
Locates Password attemps	5					
Locates access as Root	5					
Displays Compromised Web pages	5					
Identifies all copies of targeted files (Find/ -name(Filename)	3					
Identify files changed in last 120 min in a directory	5					
Demonstrates ability to change root password	5					
Recommends following configuration Updates						
Deny attacker IP access	7					
Deny SSH access from Internet	6					
Change Root Password	5					
Totals	100					

Pre-employment / Proficiency testing

Baltimore Cyber Range

- BCR has entered into a multi-year agreement with A2LA to provide assessor technical testing in support of FedRAMP
- The work is ISO/IEC 17020 based and targets NIST 800.53 requirements
- This new effort includes a great deal of course development and training aid development
- The A2LA effort positions BCR to access and participate in a wide range of Federal workforce Cyber Training and testing work

Team Proficiency testing

Baltimore Cyber Range

Web Defacement Score Sheet	Date:		Class:			
Task	**Possible Score / Points**	**Participant #1 Score**	**Participant #2 Score**	**Participant #3 Score**	**Participant #4 Score**	**Participant #5 Score**
Familiar With SIEM						
Demonstrate the ability to set Rules	2					
Three Display	2					
Detect Port Scanning	6					
Detect Password Attack	6					
Familiar With Firewall						
Demonstrates Ability to Set new Rules	2					
Logs						
Identifies Port Scanning	6					
Detect Fuzzing	6					
Displays active Network Connections (NetSim)	3					
Identifies Victum Server	5					
Identifies Attacker IP	5					
Display Auth. Logs	5					
Displays Fuzzing	5					
Locates Password attemps	5					
Locates access as Root	5					
Displays Compromised Web pages	5					
Identifies all copies of targeted files (Find/ -name[Filename]	3					
Identify files changed in last 120 min in a directory	5					
Demonstrates ability to change root password	5					
Recommends following configuration Updates						
Deny attacker IP access	7					
Deny SSH access from Internet	6					
Change Root Password	6					
Totals	100					

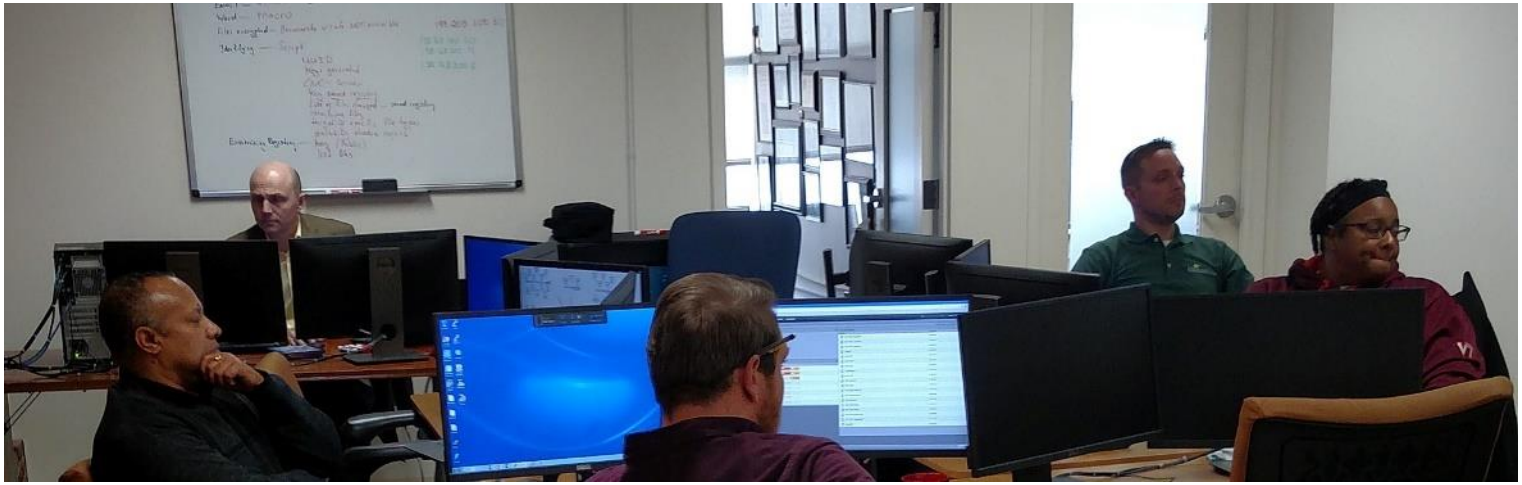
Advanced Threat Training

Baltimore Cyber Range

- Targets commercial and government organizations
- Provided for sophisticated practitioners (Expert Level)
- Hands-on Threat Training
- VM implementation of SOC
- Detection / Mitigation / Remediation
- Instructor lead
- Single day, two day and week long secessions
- Two threat scenarios / day
- Based on 14 Cyber Range Threat scenarios
- Foundation of ACT Program / for community colleges

Advanced Threat Training
Cyber Range

Baltimore Cyber Range



- Cyber Range supports the most advanced Cyber threat training
- Hands-on, ultra realistic training
- Supports five practitioners, an instructor and one observer
- Implements real-world attacks
- Current supports
  - Threat Training
  - Certification Activities
  - SOC Training

STEM Challenges

Baltimore Cyber Range

- STEM addresses far more than IT / Cyber
- Motivation / Making learning interesting
  - Gender Issues
- Resource allocation
  - Time available
  - Training aids available
- Current Institutions
- Formal training / experience requirements

STEM

Baltimore Cyber Range

- STEM efforts focused on State
- Participate in a Governors effort
- Believe hands-on training very important
- Looking at Aids and Learning systems

WFD Summary

Baltimore Cyber Range

- BCR allocates considerable time to WFD
- Worked in support of State efforts
  - Under employed / unemployed
  - Efforts to attract women to the IT / Cyber field
  - Relationships with 13 Maryland community colleges
  - STEM
- Each targeted group is unique / Similar approach
  - Target unique Interests
  - Unique Motivation Requirements
  - Must learn basics
  - Regular exposure
  - Hands-on

Resources

Baltimore Cyber Range

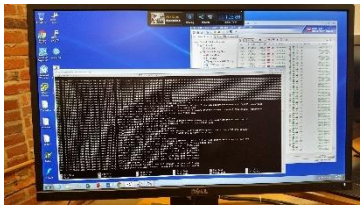
Key resources include:

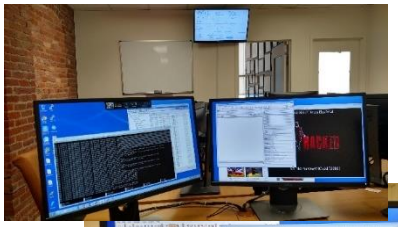
- Staff
- Cyber Range
- Boson
- WS 10 Workstation
- Pi Array

Resources / Range

Baltimore Cyber Range

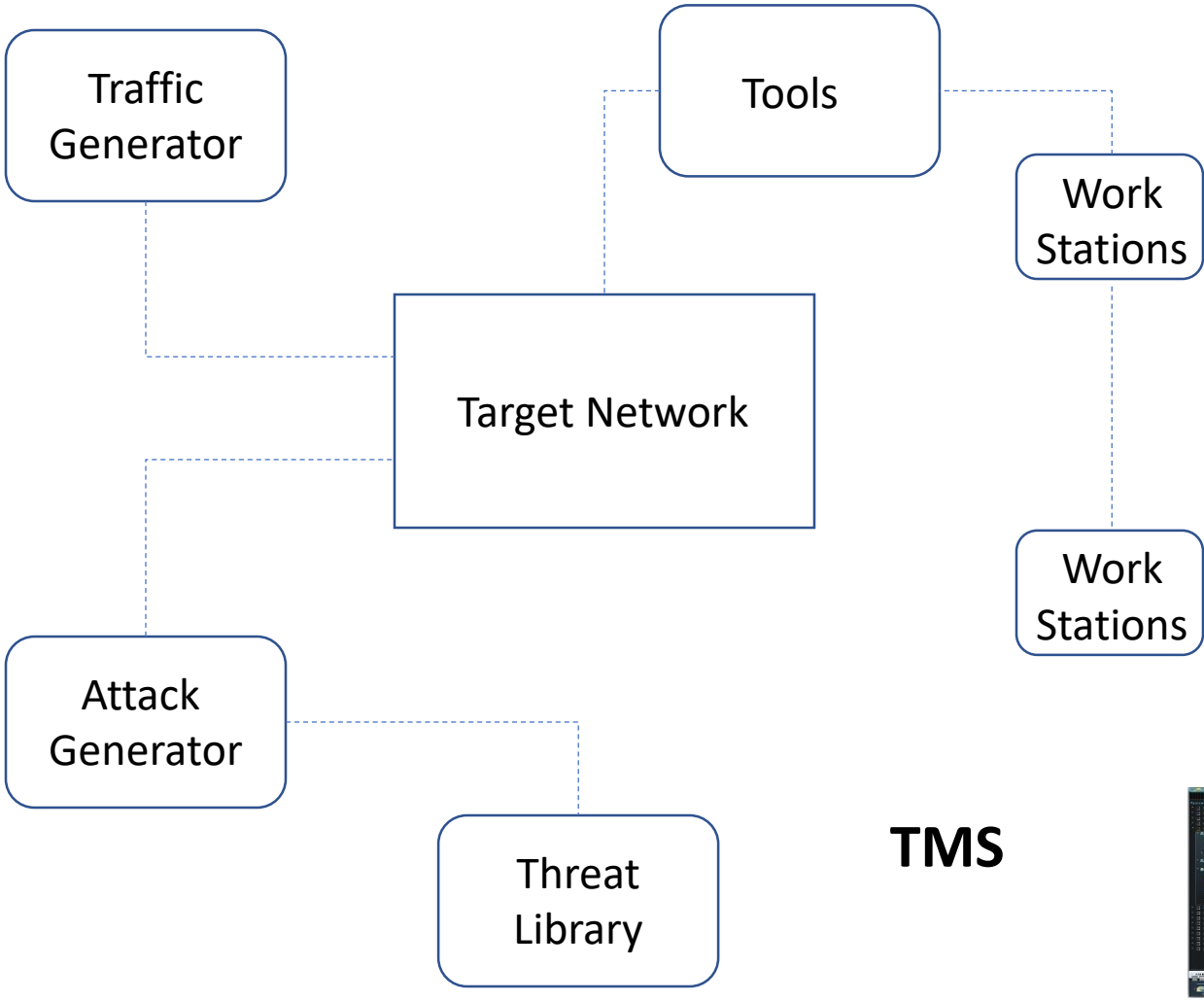
- Virtual System / Simulates an operating SOC
- Threat Library / Network / Traffic generator / Threat Generator
- Integrated Training Management System
- Multiple Windows and Linux servers / workstations
- Supports five practitioners / instructor / observer
- Supports Red / Blue / White Teams
- Fourteen Configurable Threat Scenarios
- Two – Four hour scenarios
- Supports local and remote log-in
- Records all practitioner / system actions
- Integrated After-Action-Review





Resources / Range

Baltimore Cyber Range



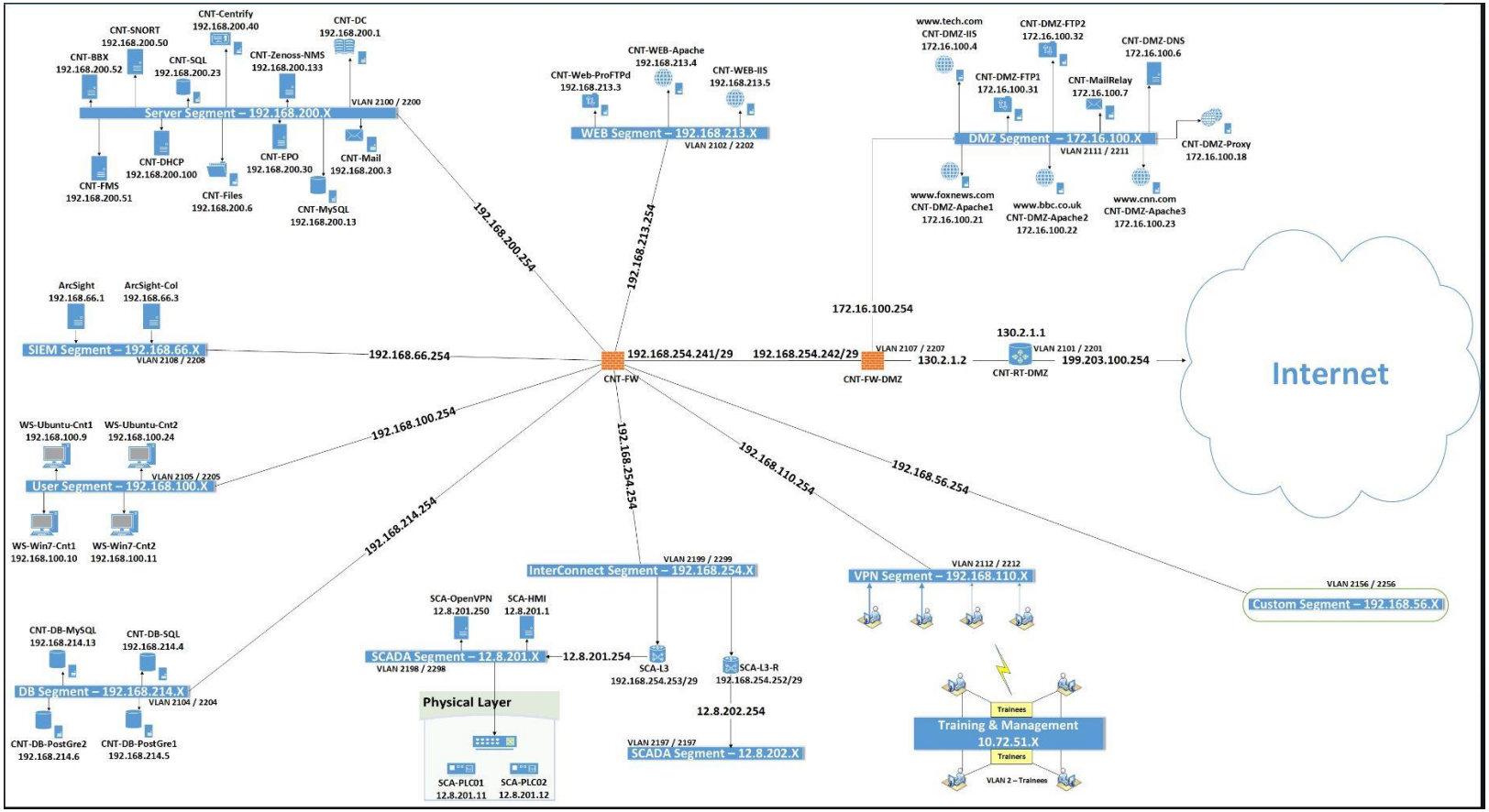
TMS

Resources / Range

Baltimore Cyber Range

No.	Item
1.	2xIntel Xeon E5-2650 v4 (12 cores, 2.2 GHz)
2.	384G RAM, 12x32GB DDR4
3.	2 x 800G SSD Drives 4 x 2T SATA 7.2K
4.	Raid Controller PERC H730
5.	2 x 1G network adapter
6.	2 x 10G Network Adapter (Includes 2 * SFP+ 10G)
7.	Dual SD Module with 2x 8GB SD Cards
8.	**Dual Redundant Power Supplies**

Resources / Range

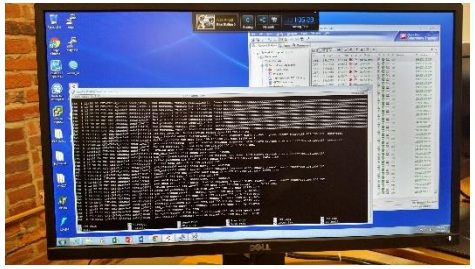


Resources / Range

Baltimore Cyber Range

Key Practitioner Tools:

- ArcSight (SIEM)
- Checkpoint
  - Smart Dash
  - Smart Tracker
- Putty (SSH Access)
- Zenoss (NMS)
- WireShark
- IE
- Chrome
- Vmware vShere



Range Scenarios

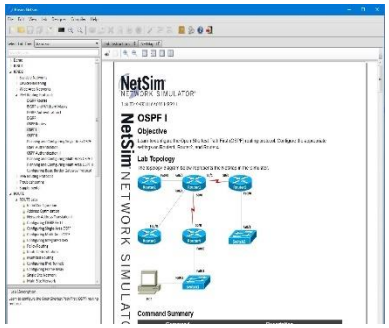
Baltimore Cyber Range

- SQL Injection
- Apache Shutdown
- Web Defacement
- Trojan Data Leakage
- Java SendMail
- Java NMS Kill
- DB Dump via FTP Exploit
- Killer Trojan
- Trojan Share Privilege Escalation
- Windows Management Instrumentation Worm
- Ransomware

Boson

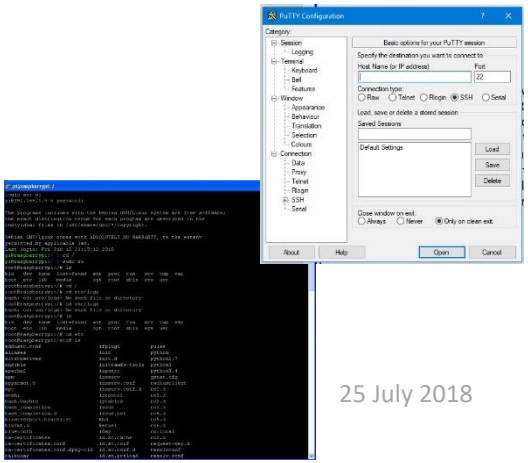
Baltimore Cyber Range

- NetSim 11
- Entry and Journeyman level classes
- Classroom instruction / Cisco training
- Supports hands-on training for each student
- Includes Labs for routers & switches
- Build, configure and test networks
- Many ‘canned’ scenarios



Pi Array

- Goal - Provide each student Linux Server
- Fourteen Raspberry Pi-3 B servers in briefcase
- Interfaces directly to facility network
- Includes integrated Switch
- Supports network operations
- Linux command line instruction
- Allows tool use practice e.g. Nmap
- Audit log training



Resource Development

Baltimore Cyber Range

- The Cyber Range, most sophisticated training resource
- Very complex and very expensive
- BCR is expanding training and testing activities
- Non- traditionally Cyber Range applications
- Range maybe a sub-optimal approach
- Training aid analysis is required to identify appropriate approaches
- Complexity / Suttons Law
- First principles analysis and review of the Cyber Range is one element of the BCR analysis

Fundamental Principles

Baltimore Cyber Range

- Complex systems are intrinsically difficult to model / virtualize
- Virtual implementations add layers of complexity
- Virtual systems support simplified distribution / access
- Complexity & scope drive cost, reliability and flexibility
- Off-the-shelf Hardware can mitigated virtual implementation complexity
- Complex, integrated tasks can be broken down into manageable sub-tasks
- Limited scope solutions are easier to implement
- There is a large base of existing supporting resources e.g. hardware, threats, instruction material, etc.

Conclusions

Baltimore Cyber Range

- The Range addresses ‘niche’ high-end Cyber training requirements
- Cyber Range advanced, integrated technology limits its applicability for many targeted training / evaluation tasks
- Complex virtual systems are expensive to implement, support, upgrade and enhance
- Complexity can limit applicability
- Limiting scope reduces system complexity, reduces support requirements and provides better resource utilization
- Implement Off-the-shelf hardware solutions where possible
- Simply user interfaces are more widely applicable
- Design and build to the requirement (limit scope and complexity)
- Break problems down into manageable tasks (Divide & Conquer)
- Simple solutions often better target & address training requirements

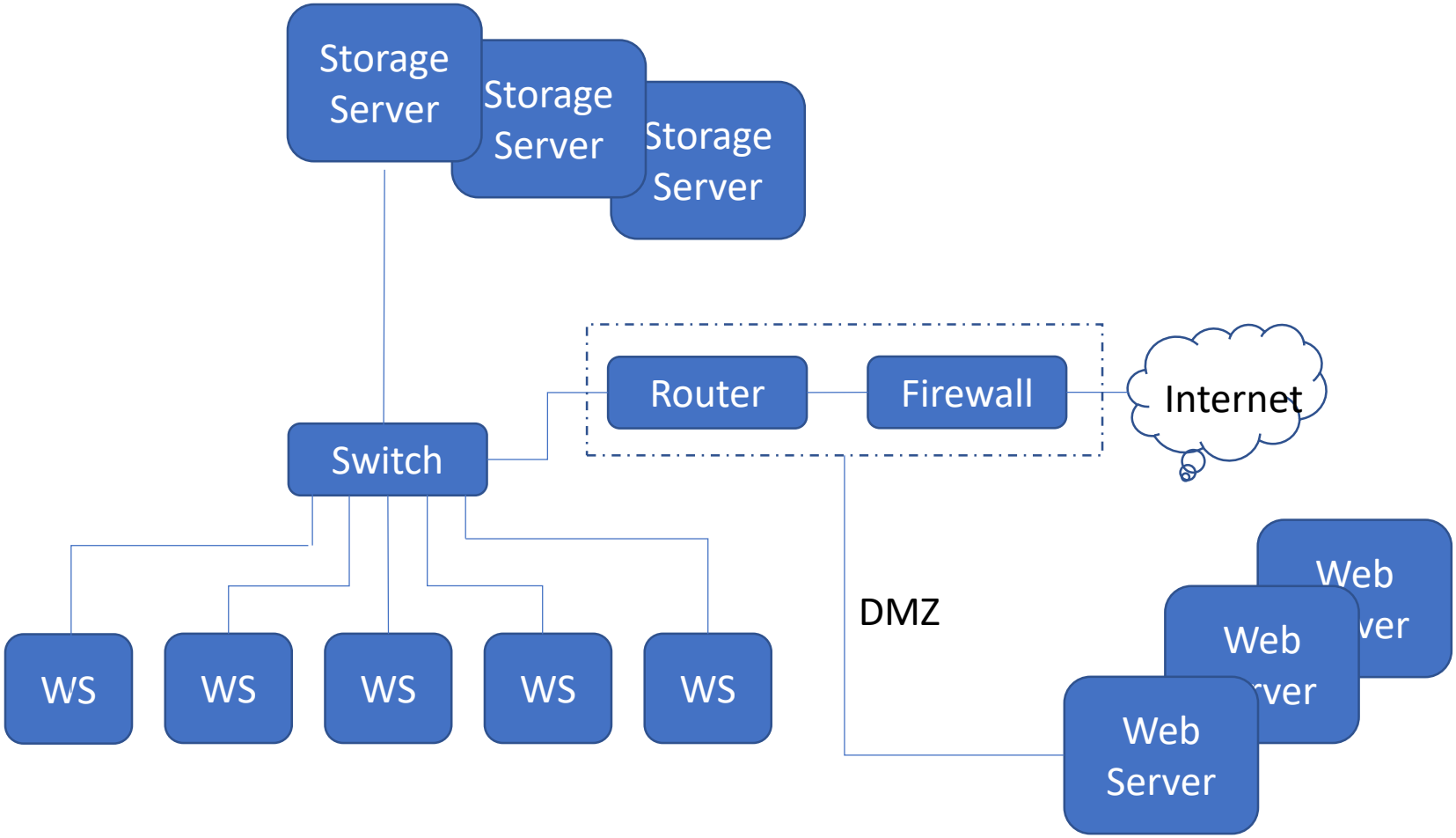
Flexible Training Network

Baltimore Cyber Range

- What would an optimized, scope limited network training device look like?
- FedRAMP 3PAO evaluation requirement baseline / example
- Cyber Range is currently being utilized for the FedRAMP effort
- FedRAMP system implementation goals include:
    - Simple user interfaces / multiple users
    - Scalable
    - Architecture supporting future enhancement
    - Include Storage Servers / Web Server / Router / Firewall / Workstations
    - Realization of a real-world network
    - Support quick update / configuration changes
    - Minimal complexity / Maximum flexibility
    - Support large set of characteristics identified in NIST 800.53

FedRAMP Logical

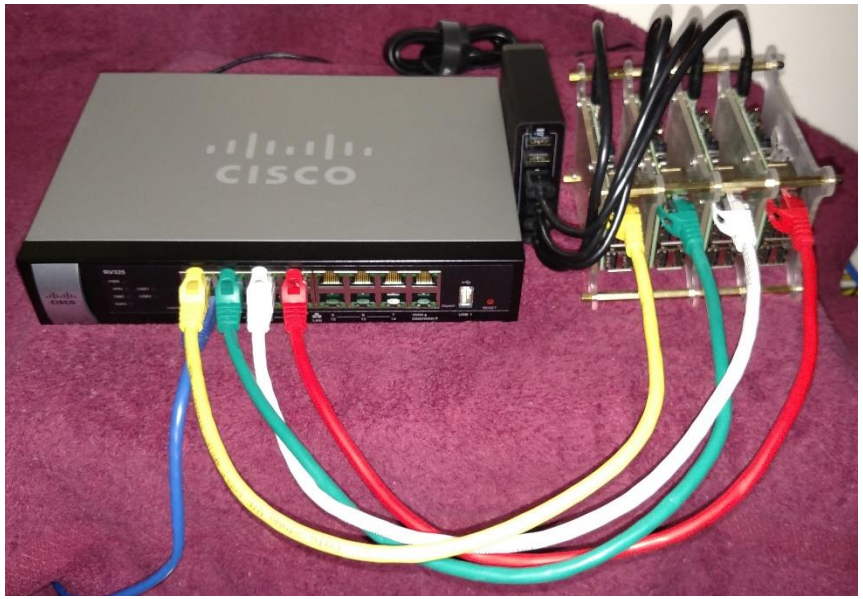
Baltimore Cyber Range



Engineering Prototype

Baltimore Cyber Range

Includes four Linux processors
Scalable
Router – Firewall – Switch
Local network – DMZ – Internet access
Supports wireless interfaces
Processor dedicated to Management
Supports up to Ten Workstations
Low Cost / Low Power
Fits in to briefcase (less workstations)
Linux based – Hugh base of Software



Baltimore Cyber Range

Questions
Discussion