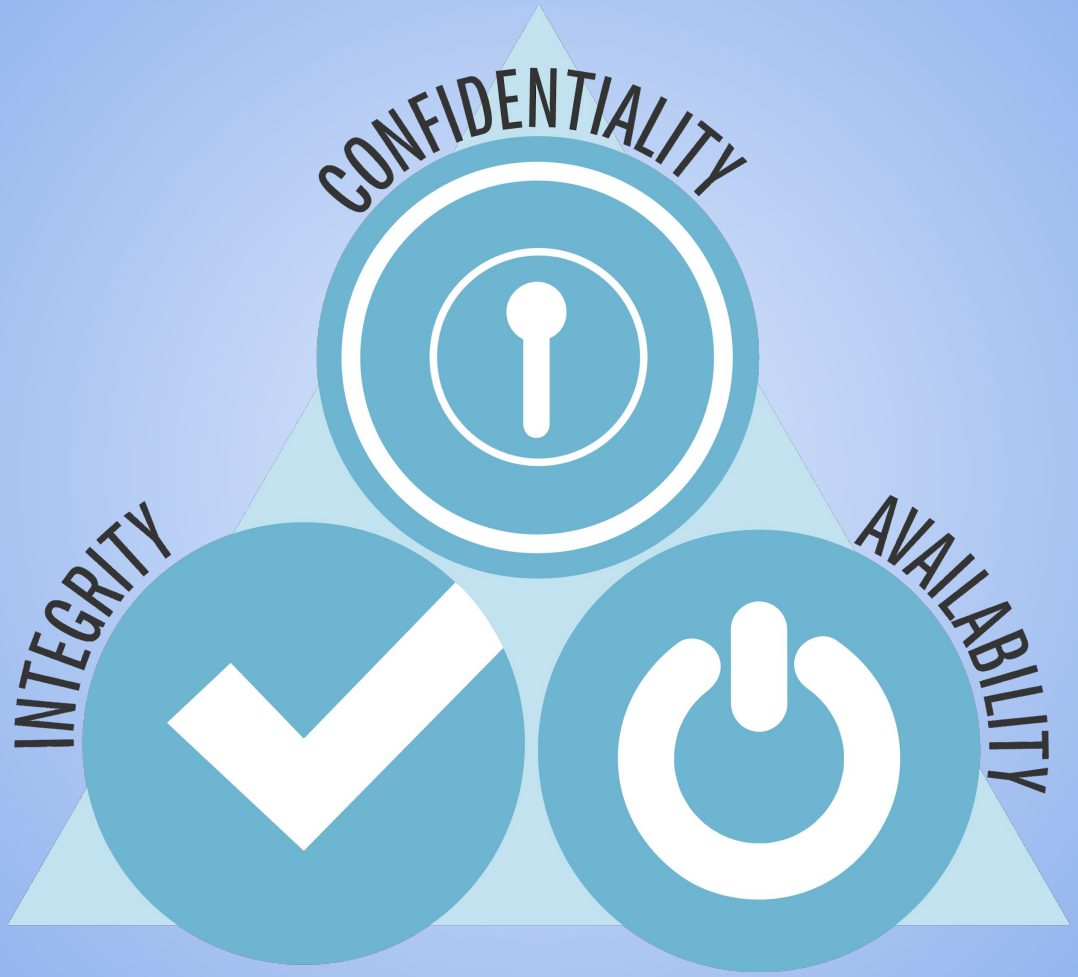
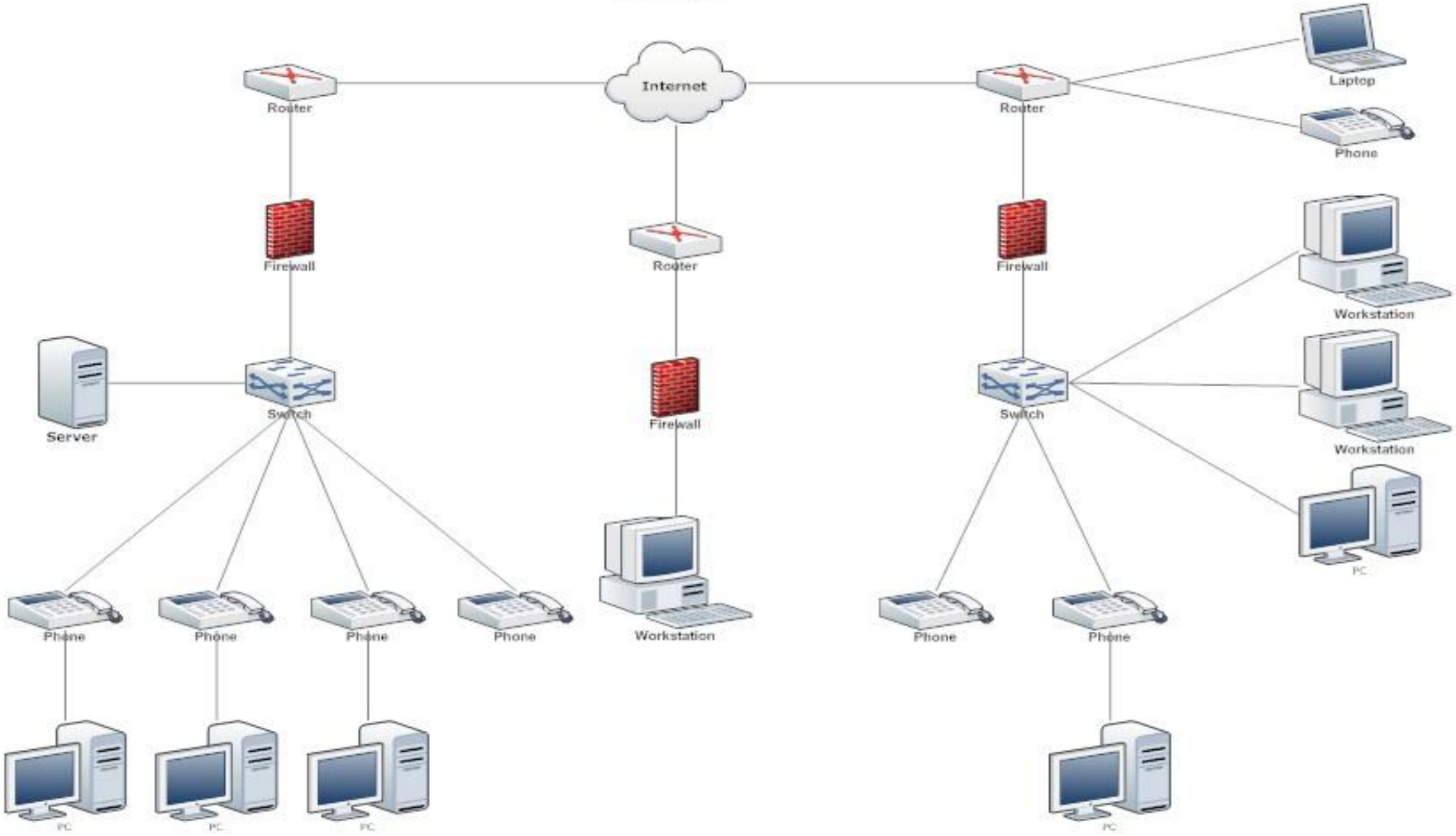
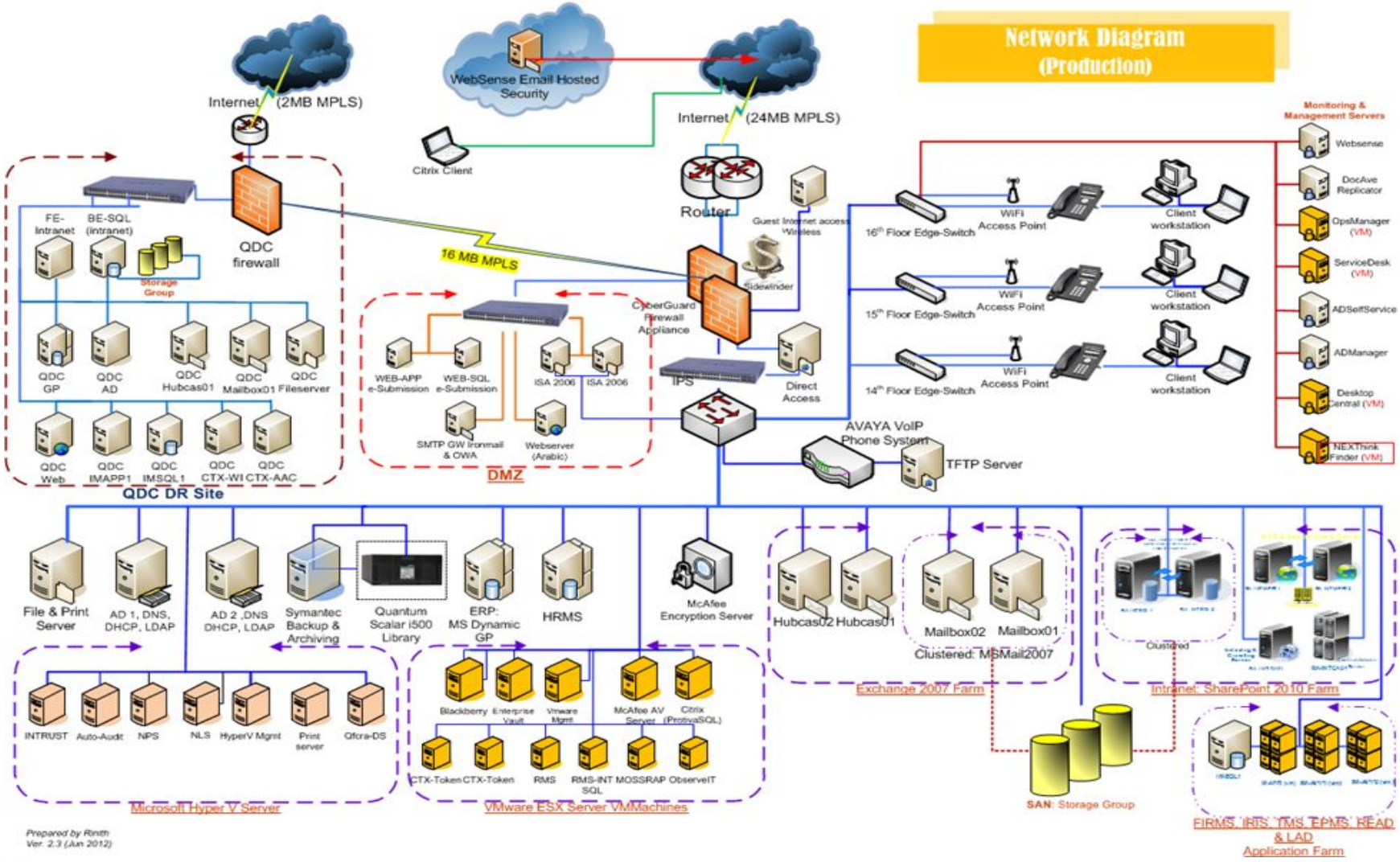
The 1,000 Mile Overview of Cybersecurity

security
Information
Management
technologies
based
services
standards
architecture
application
understanding
knowledge
client
role
Strong
development
applications
technical
systems
skills
access
design
Risk
Cyber
Knowledge
Team
advising
accreditation
delivery
service
senior
risk
audit
embedded
assessments
may
enterprise
external
C/C++
particularly
system
various
hardening
Encryption
Understanding
needs
protocols
strong
secure
Implementation
solutions
Analysis
lifecycle
Specialist
clients
processes
deep
Manager
Analytics
essential
techniques
technology
Linux
ISO
real-time
PKI
Oracle
and/or
project
Skills
solution
must
Infrastructure
level
Windows
delivering
designing
related
debug
environments
management
industry
mobile
devices
analysis
operation
RSA
UNIX
Netwo
frameworks
we
ISO27001
domain
Strategy
good
net
firm
driving
large
capture
hands
IPS/IDS
environment
e.g
work
makers
HMG
Ability
different
high
platforms
detection
financial
background
cyber
information
consultancy
server
business
software
network
relevant
successful
managing
best
experience
Identity
required
Penetration
using
one
Cloud
models
Identify
future
controls
leadership
Assurance
PCI-DSS
testing
team
patterns
adapt
following
strategy
Practices
degree
edge
Design
cutting
Responsibilities

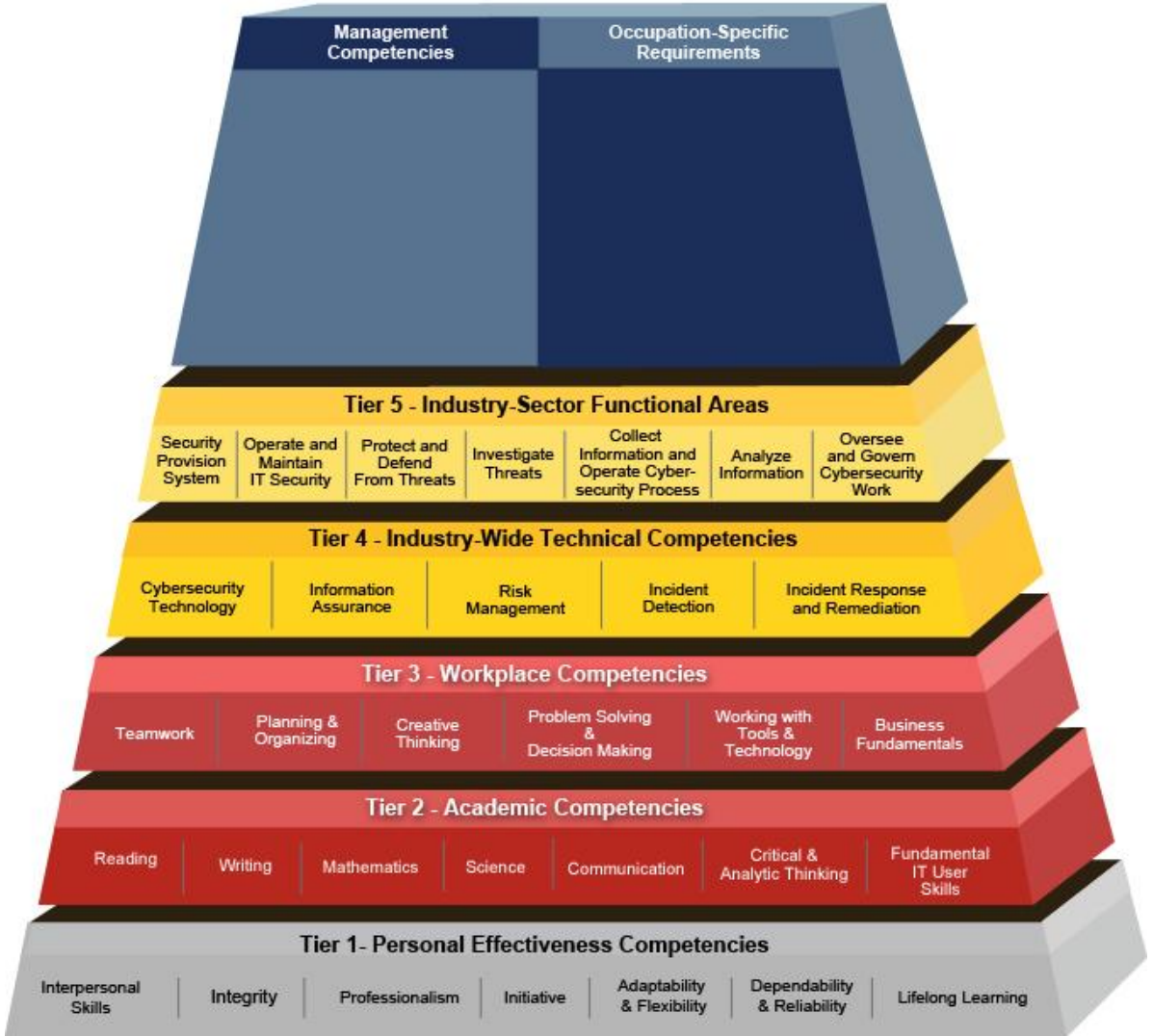

CONFIDENTIALITY
INTEGRITY
AVAILABILITY

Firewall

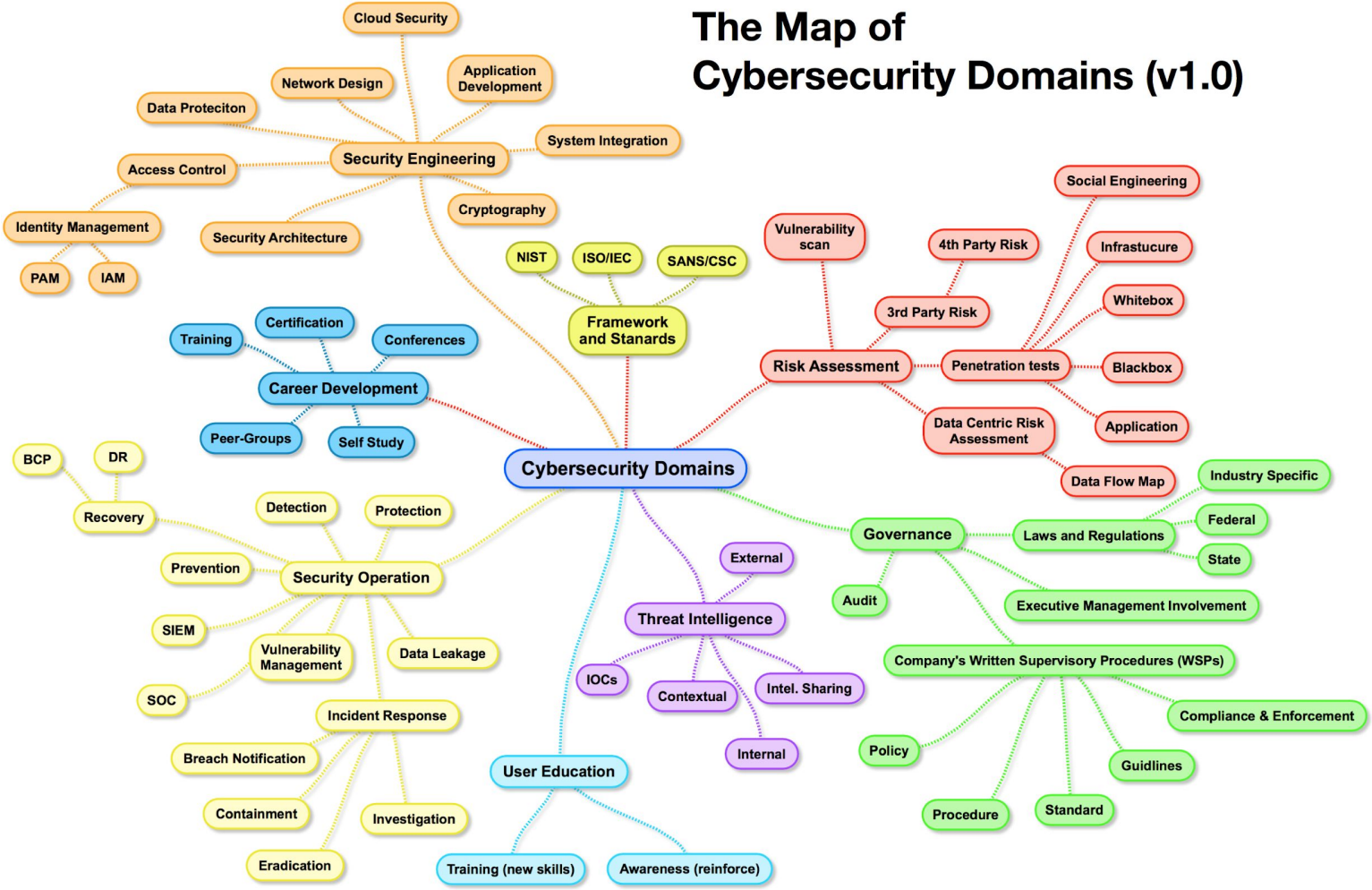

Internet
Router
Router
Router
Laptop
Phone
Firewall
Firewall
Firewall
Workstation
Server
Switch
Switch
Workstation
Workstation
PC
Phone
Phone
Phone
Phone
Workstation
Phone
Phone
PC
PC
PC
PC


Network Diagram
(Production)
Internet (2MB MPLS)
WebSense Email Hosted Security
Internet (24MB MPLS)
Citrix Client
Router
Guest Internet access Wireless
Sidewinder
16 MB MPLS
CyberGuard Firewall Appliance
IPS
Direct Access
FE-Intranet
BE-SQL (intranet)
Storage Group
QDC firewall
QDC GP
QDC AD
QDC Hubcas01
QDC Mailbox01
QDC Fileserver
QDC Web
QDC IMAPP1
QDC IMSQL1
QDC CTX-WI
QDC CTX-AAC
QDC DR Site
WEB-APP e-Submission
WEB-SQL e-Submission
ISA 2006
ISA 2006
SMTP GW Ironmail & OWA
Webserver (Arabic)
DMZ
16th Floor Edge-Switch
15th Floor Edge-Switch
14th Floor Edge-Switch
WiFi Access Point
Client workstation
AVAYA VoIP Phone System
TFTP Server
Monitoring & Management Servers
Websense
DocAve Replicator
OpsManager (VM)
ServiceDesk (VM)
ADSelfService
ADManager
Desktop Central (VM)
NEXThink Finder (VM)
File & Print Server
AD 1, DNS, DHCP, LDAP
AD 2 ,DNS DHCP, LDAP
Symantec Backup & Archiving
Quantum Scalar i500 Library
ERP: MS Dynamic GP
HRMS
McAfee Encryption Server
INTRUST
Auto-Audit
NPS
NLS
HyperV Mgmt
Print server
Qfcra-DS
Microsoft Hyper V Server
Blackberry Enterprise
Vmware Mgmt
McAfee AV Server
Citrix (ProtivaSQL)
CTX-Token
CTX-Token
RMS
RMS-INT SQL
MOSSRAP
ObserveIT
VMware ESX Server VMMachines
Hubcas02
Hubcas01
Mailbox02
Mailbox01
Clustered: MSMail2007
Exchange 2007 Farm
Clustered
Intranet: SharePoint 2010 Farm
SAN: Storage Group
FIRMS, IRIS, TMS, EPMS, READ & LAD
Application Farm
Prepared by Rinith
Ver. 2.3 (Jun 2012)


eocreveassim.com.br


Management Competencies
Occupation-Specific Requirements
Tier 5 - Industry-Sector Functional Areas
Security Provision System
Operate and Maintain IT Security
Protect and Defend From Threats
Investigate Threats
Collect Information and Operate Cyber-security Process
Analyze Information
Oversee and Govern Cybersecurity Work
Tier 4 - Industry-Wide Technical Competencies
Cybersecurity Technology
Information Assurance
Risk Management
Incident Detection
Incident Response and Remediation
Tier 3 - Workplace Competencies
Teamwork
Planning & Organizing
Creative Thinking
Problem Solving & Decision Making
Working with Tools & Technology
Business Fundamentals
Tier 2 - Academic Competencies
Reading
Writing
Mathematics
Science
Communication
Critical & Analytic Thinking
Fundamental IT User Skills
Tier 1- Personal Effectiveness Competencies
Interpersonal Skills
Integrity
Professionalism
Initiative
Adaptability & Flexibility
Dependability & Reliability
Lifelong Learning

The Map of Cybersecurity Domains (v1.0)

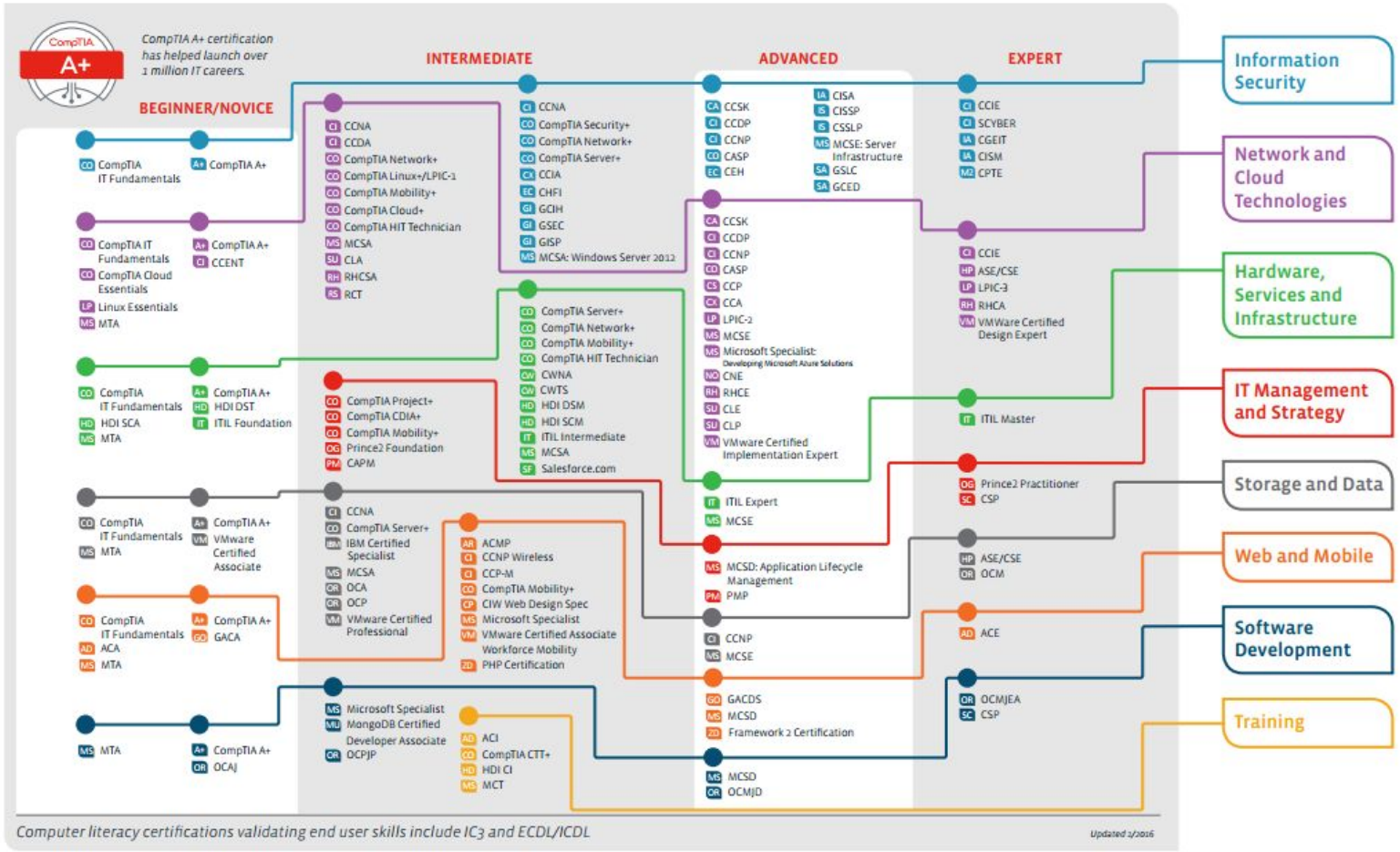


IT Certification Roadmap

Explore the possibilities with the CompTIA Interactive IT Roadmap at: CompTIA.org/CertsRoadmap

CompTIA

Certifications validate expertise in your chosen career.



Computer literacy certifications validating end user skills include IC3 and ECDL/ICDL

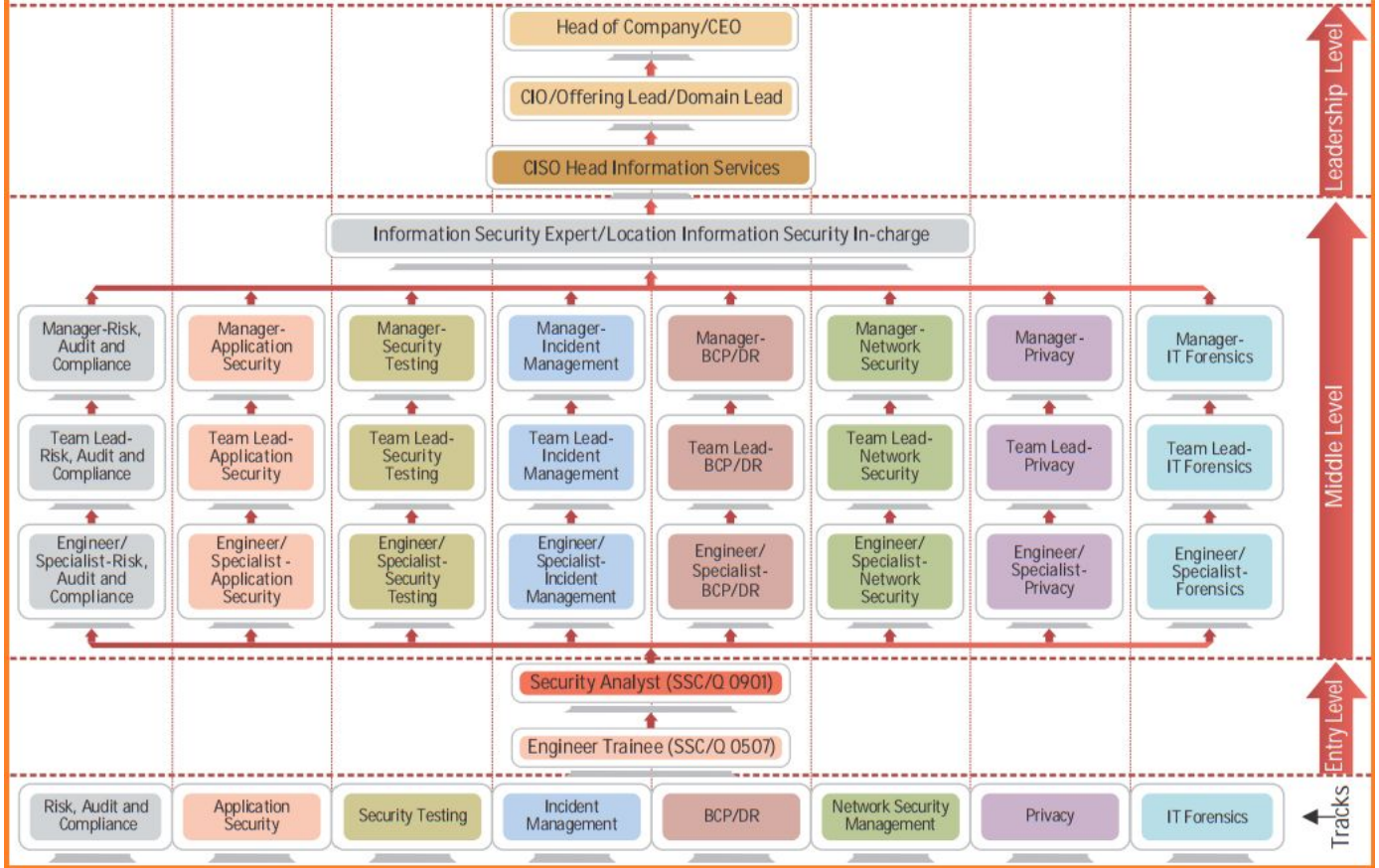
Updated 3/2016

Creating INFINITE Career Opportunities

Career Guide – IT Services

Source:- IT - ITeS SSC NASSCOM

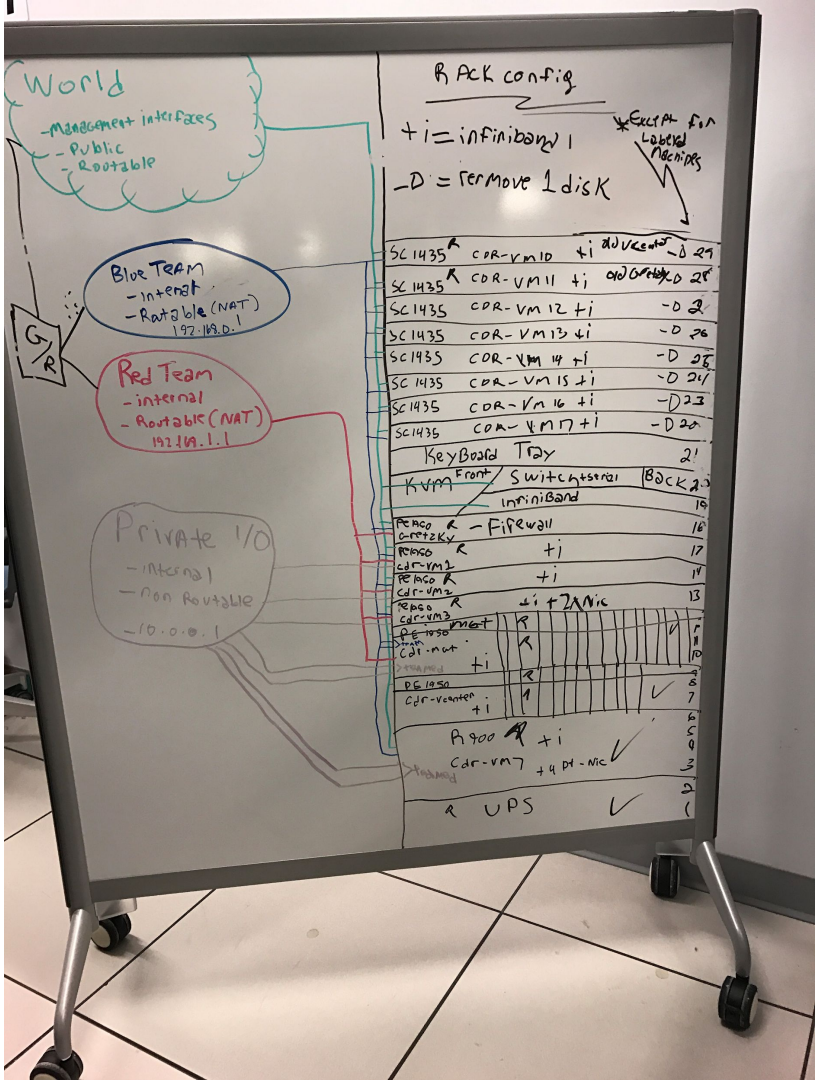
Career Map for Information Security

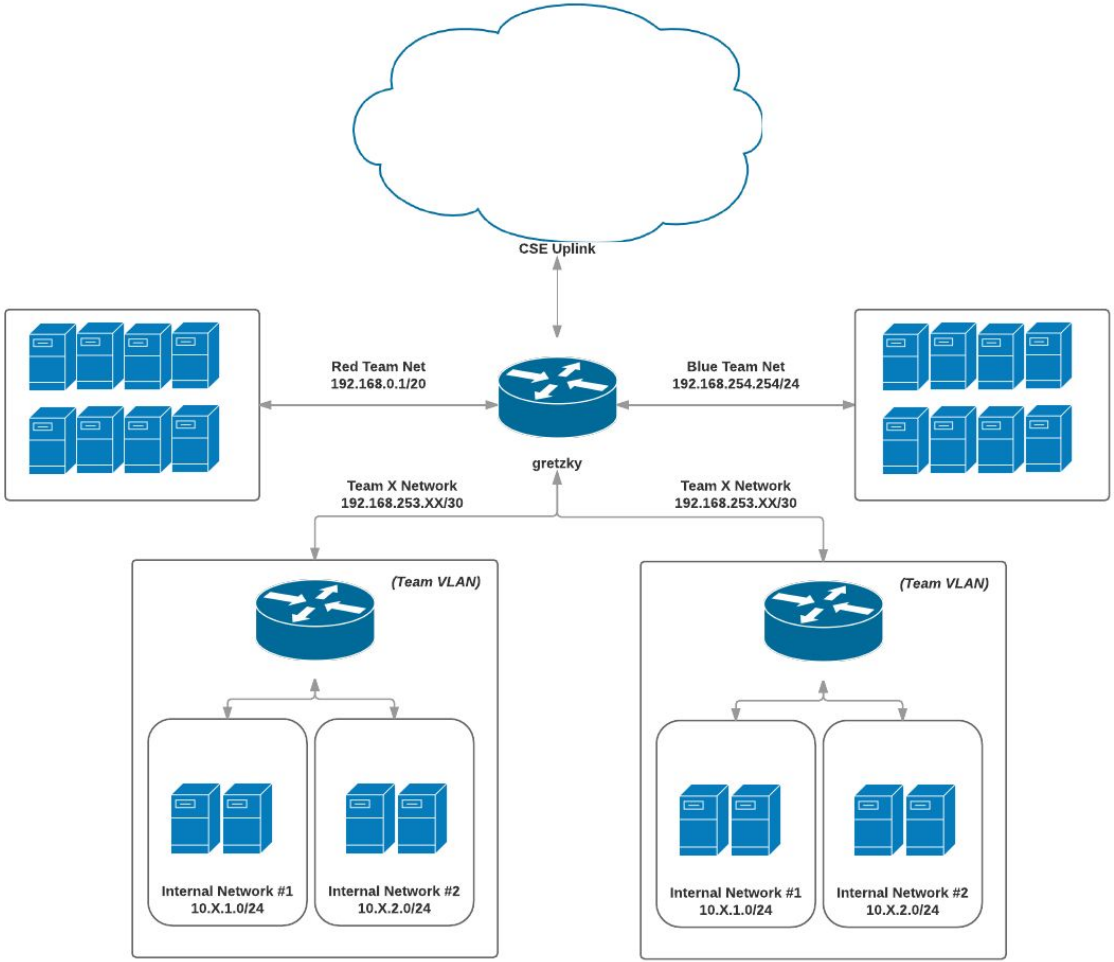



SO YOU'RE TELLING ME
CYBERSECURITY IS MORE THAN JUST CODING?
made with mematic

Competitions!!!

How Did We Get Here?




CSE Uplink
Red Team Net
192.168.0.1/20
Blue Team Net
192.168.254.254/24
gretzky
Team X Network
192.168.253.XX/30
Team X Network
192.168.253.XX/30
(Team VLAN)
(Team VLAN)
Internal Network #1
10.X.1.0/24
Internal Network #2
10.X.2.0/24
Internal Network #1
10.X.1.0/24
Internal Network #2
10.X.2.0/24

UBNetDef Infrastructure Overview

Overview of all of UBNetDef

Update in background | Fullscreen | Unlock / Edit

Drag widgets to any position you like in unlock / edit mode.

Failed vCenter Logins

a few seconds ago

3

vCenter Logins

a few seconds ago

Value	%	Count
Top values		
stefanja	27.78%	5
jamesdro	22.22%	4
sjames5	16.67%	3
peterfow	11.11%	2
acsiracu	11.11%	2
Others		
abitar	5.56%	1
CDR-VCENTER1$	5.56%	1

Top Blocked IPs

a few seconds ago

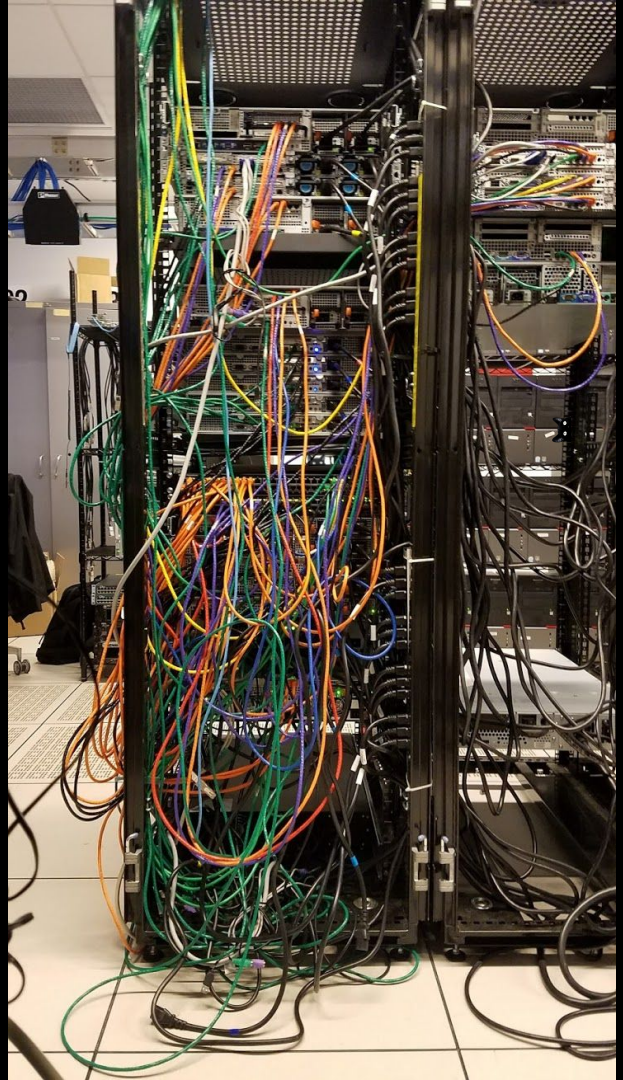
Value	%	Count
Top values		
128.205.44.129	33.94%	167
fe80::250:56ff:fea3:3899	15.24%	75
128.205.44.155	13.82%	68
fe80::250:56ff:fea3:3421	10.37%	51
::	9.76%	48
Others		
fe80::250:56ff:fea3:43d8	3.05%	15
fe80::250:56ff:fea3:4f4b	3.05%	15
fe80::f49f:b09f:2489:4348	2.44%	12
fe80::41f7:15f:4e33:8c85	2.44%	12
180.97.161.227	0.61%	3
218.60.112.227	0.61%	3
218.60.112.224	0.41%	2
128.205.159.69	0.41%	2
218.60.112.225	0.41%	2
180.97.161.226	0.20%	1
218.60.112.226	0.20%	1
37.143.9.64	0.20%	1

Top Blocked Interfaces

a few seconds ago

Value	%	Count
Top values		
bce1	53.66%	264
igb0	27.64%	136
bridge0	13.82%	68
igb3_vlan115	4.88%	24

An MBA and two
CSE students walk
into a server room…

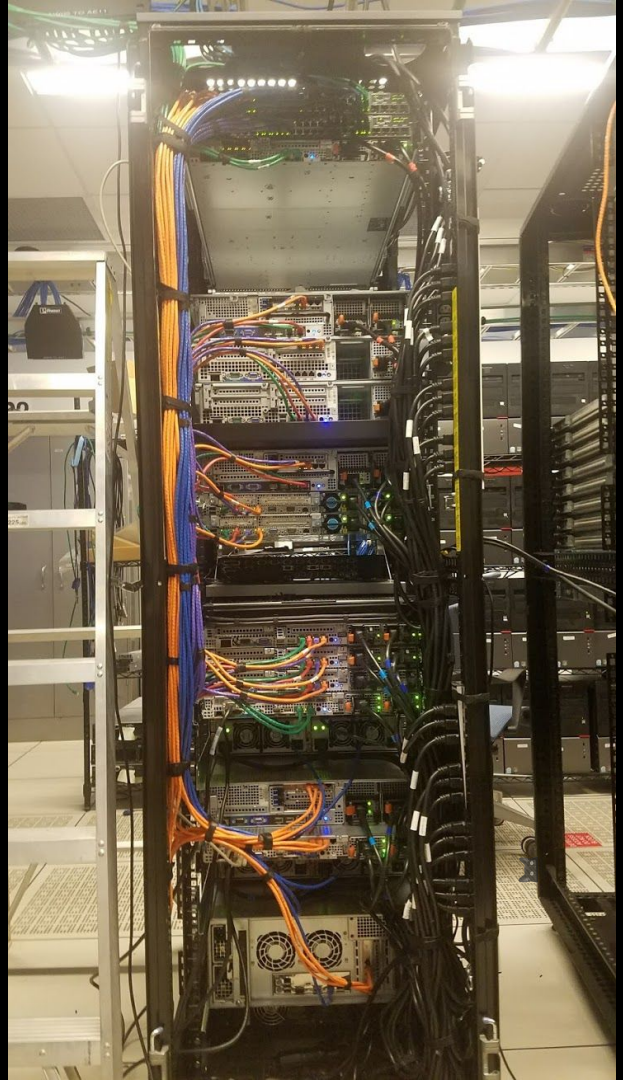


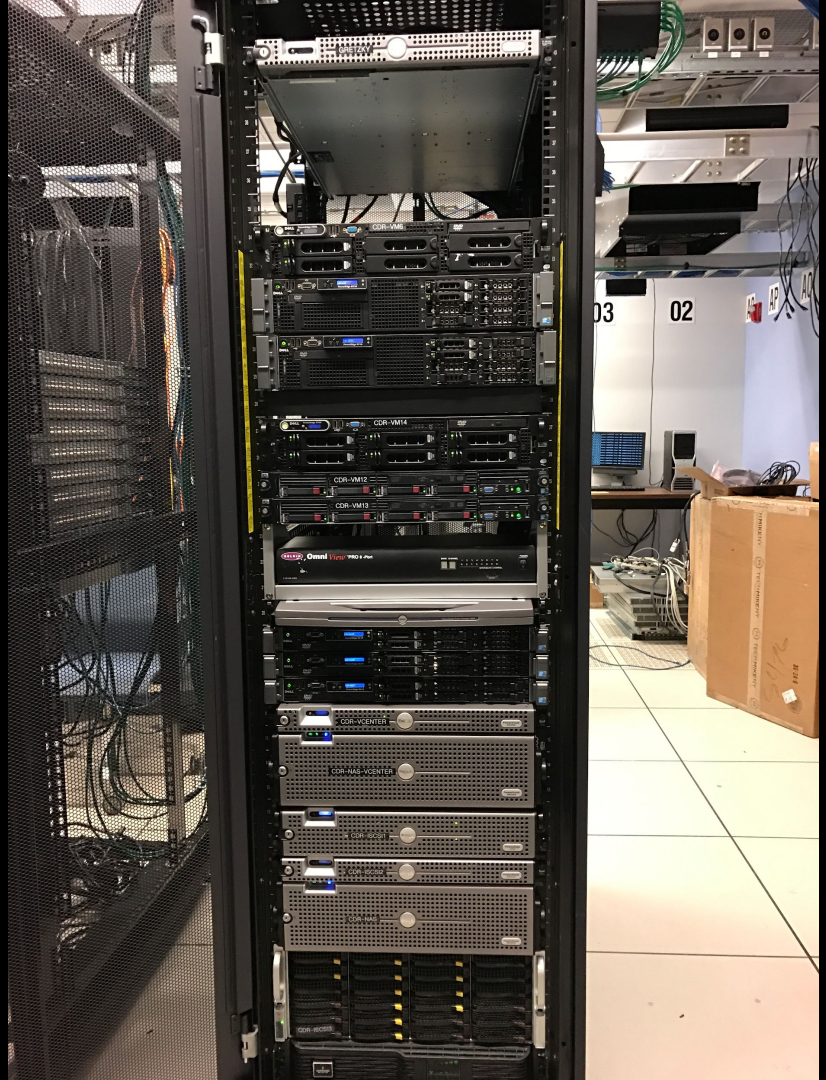
…only one leaves

#WorkingTogether

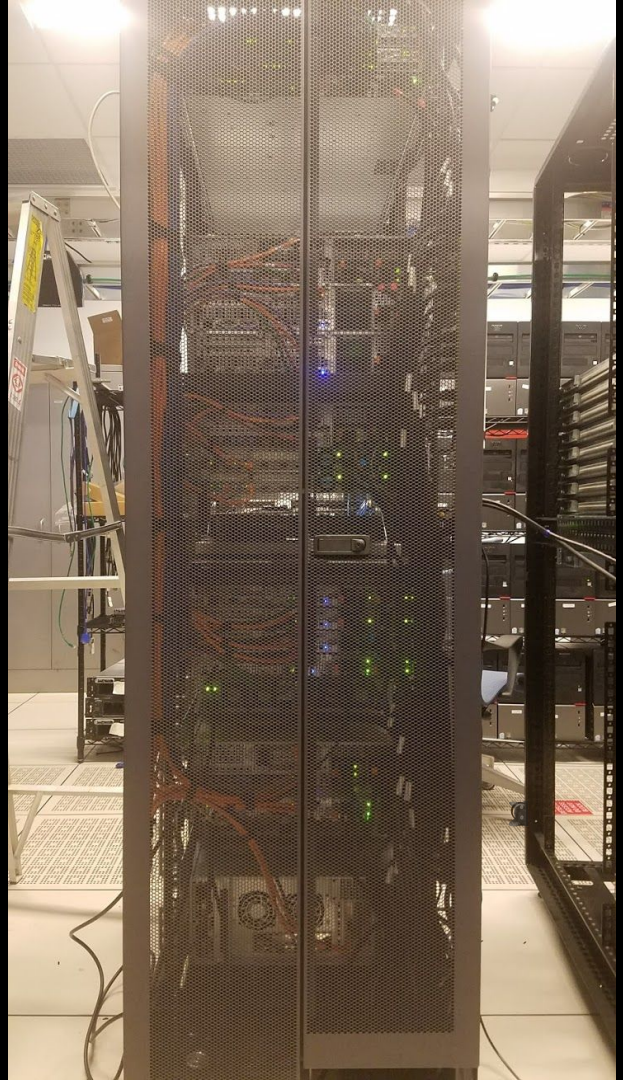

SECURITY


04




CDR-VM6
CDR-VM14
CDR-VM12
CDR-VM13
Omni View PRO 8-Port
CDR-VCENTER
CDR-NAS-VCENTER
03
02

THE DOORS CAN CLOSE!!!



BOTH OF THEM!!!!!

How to Access our Stuff

1. Fill out the Attendance Survey
   a. www.ubnetdef.org/attendance
2. Download Mattermost and Sign In
   a. https://chat.ubnetdef.org
3. For Windows Users:
   a. Go to https://cdr-vcenter.cse.buffalo.edu
4. For Mac Users:
   a. Go to https://cdr-vcenter.cse.buffalo.edu
   b. OR Download VMware Fusion
5. For Off-Campus Access:
   a. Download Cisco VPN from UBIT https://www.buffalo.edu/ubit/service-guides/software/downloading/windows-software/managing-your-software/anyconnect.html

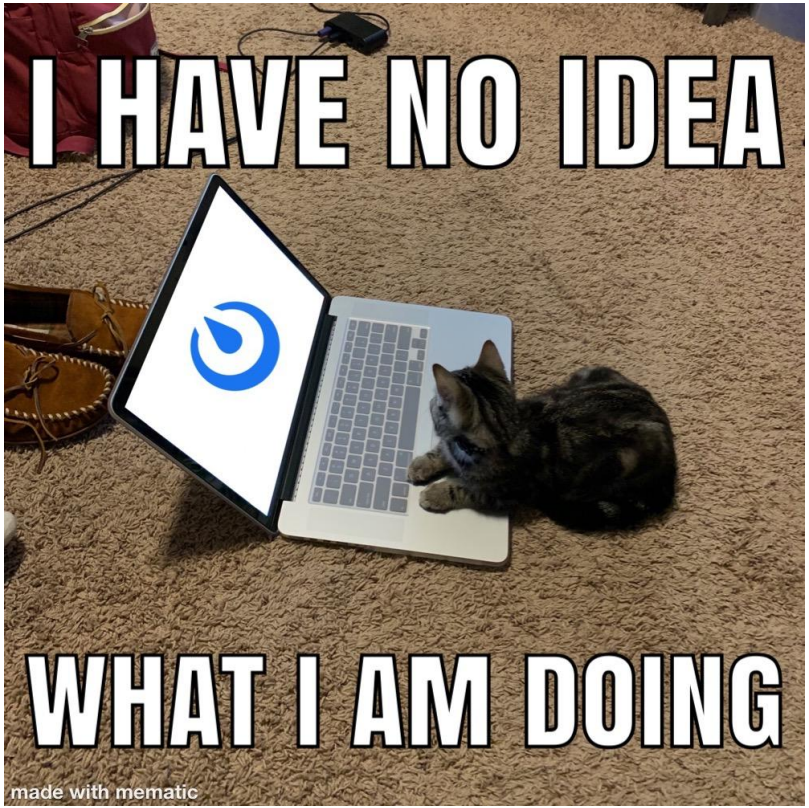
UB Internal Lockdown v0

1. Required as per syllabus (3 competitions total!)
2. Saturday, September 28, 2019
3. Teams of 4-5
4. Please contact us if you CANNOT make it

vSphere and our Environment

Remember, if you ever feel overwhelmed:

Contact us on Mattermost!



But keep in mind…

We are all also students, and we expect you guys to try your best!

Any Questions?