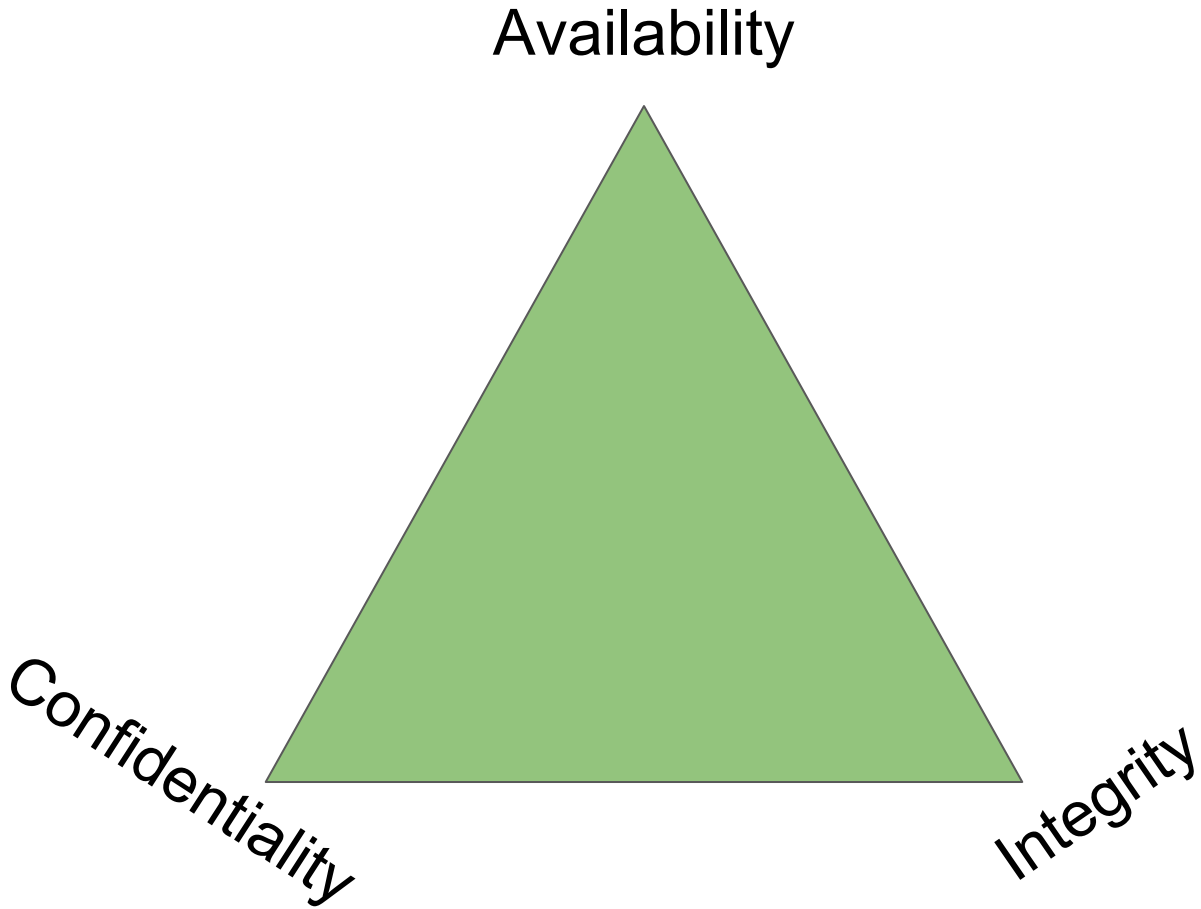
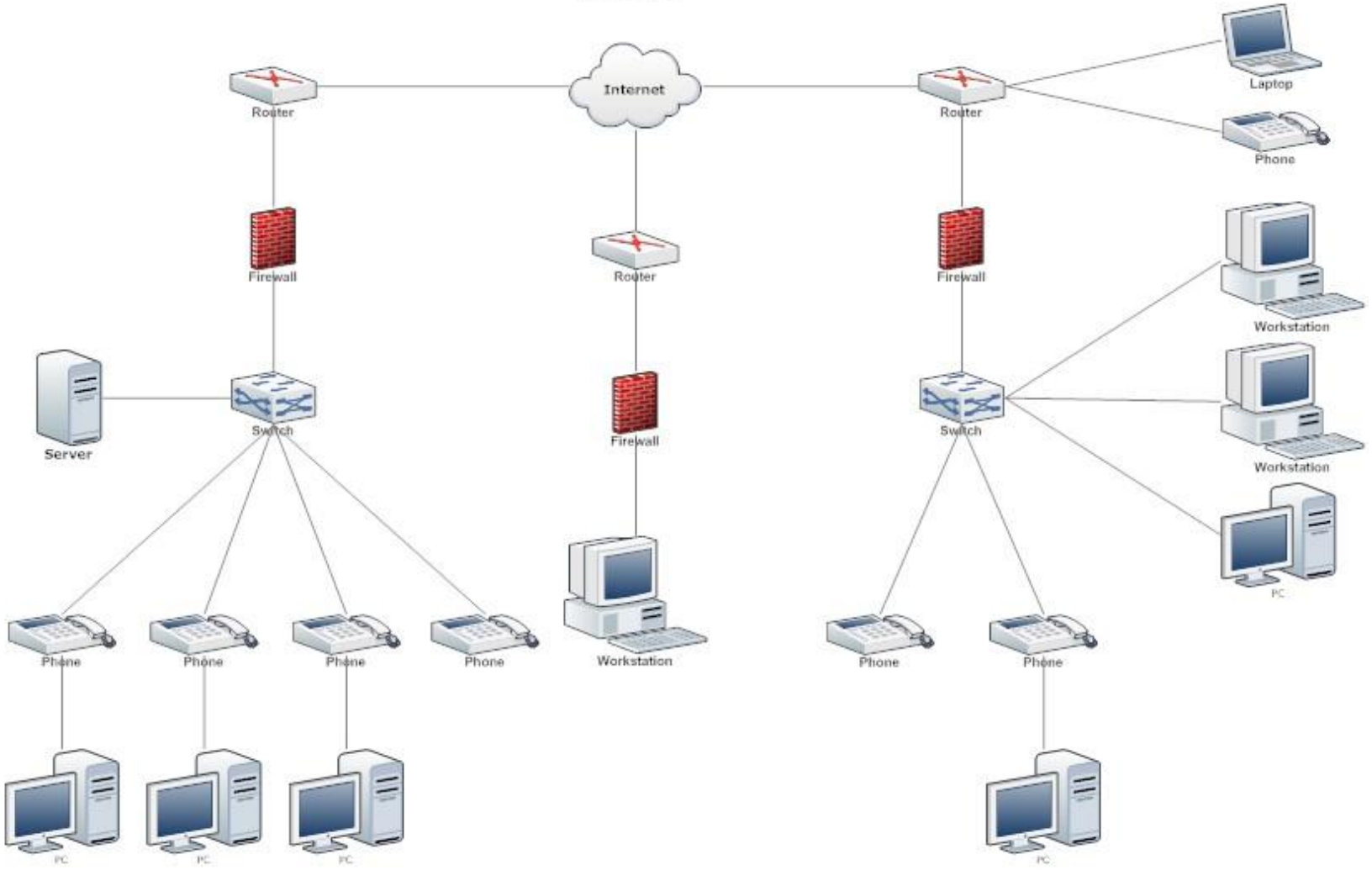
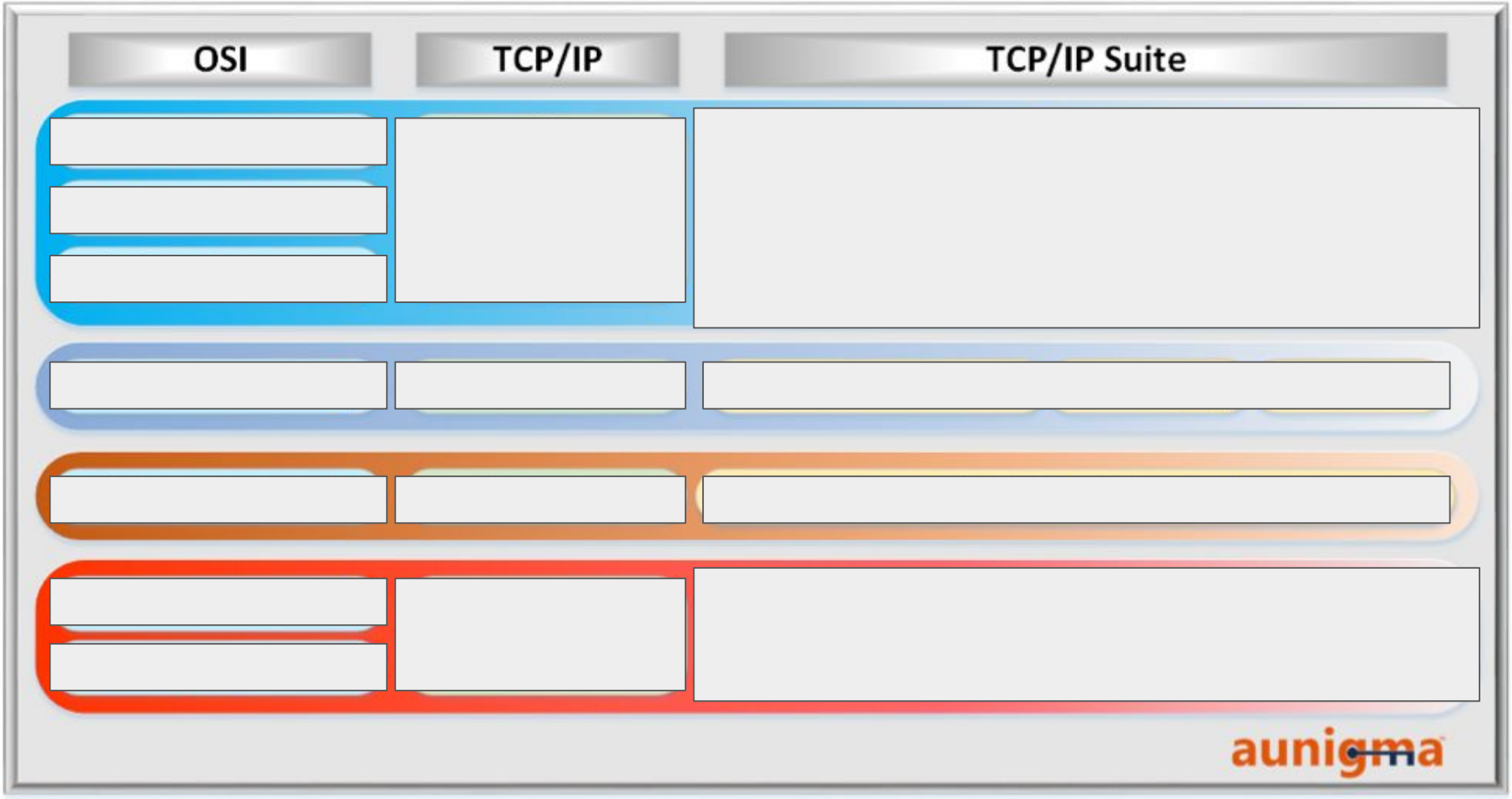
Basic Concepts: 1,000 Mile Overview

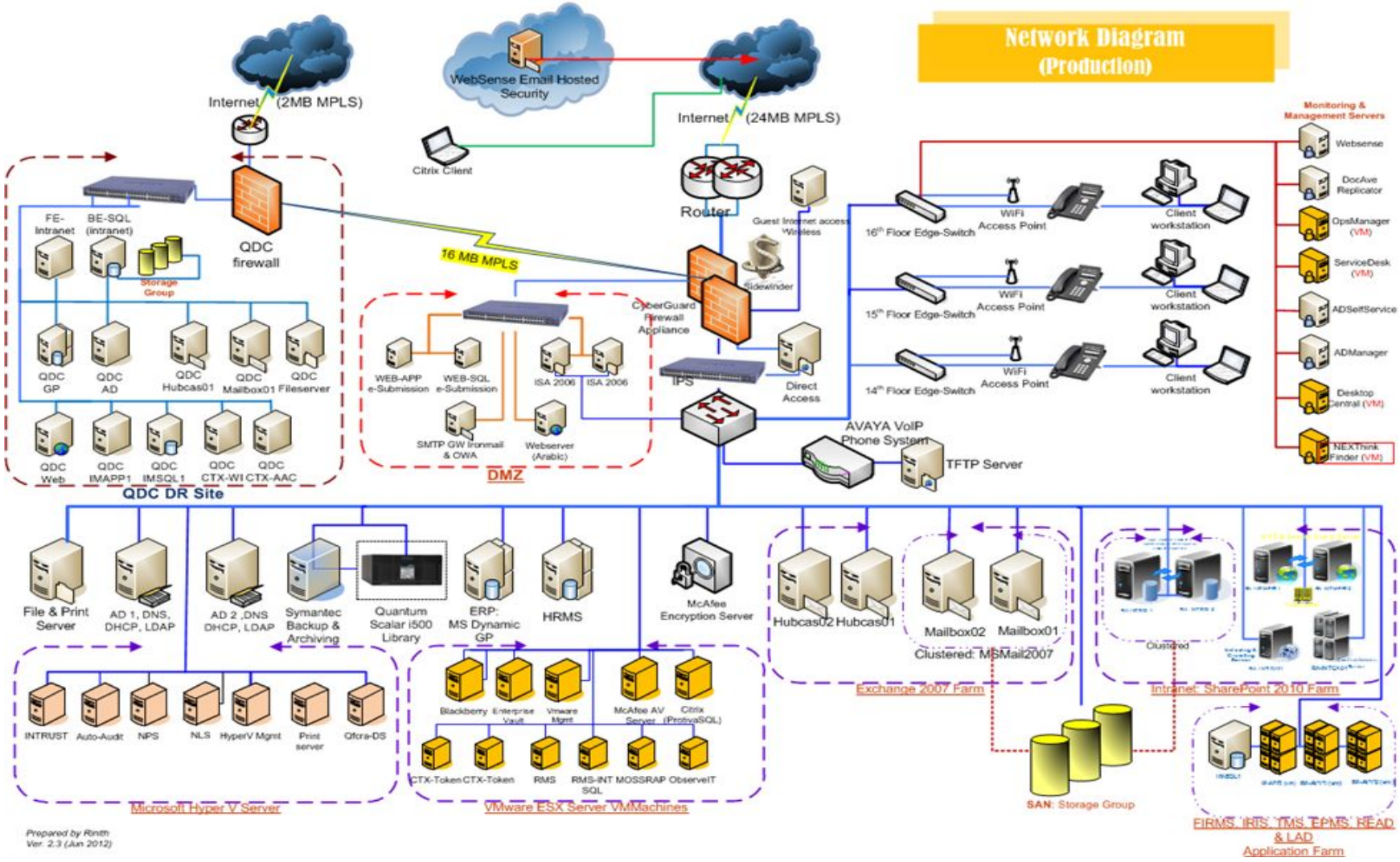
security
Information
technologies
based
Management
services
standards
Strong
architecture
clientrole
application
understanding
Risk
Ability
different
knowledge
skills
Windows
Analytics
essential
techniques
technical
systems
applications
devices
design
processes
clients
solutions
Linux
technology
ISO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


Availability
Confidentiality
Integrity

Firewall

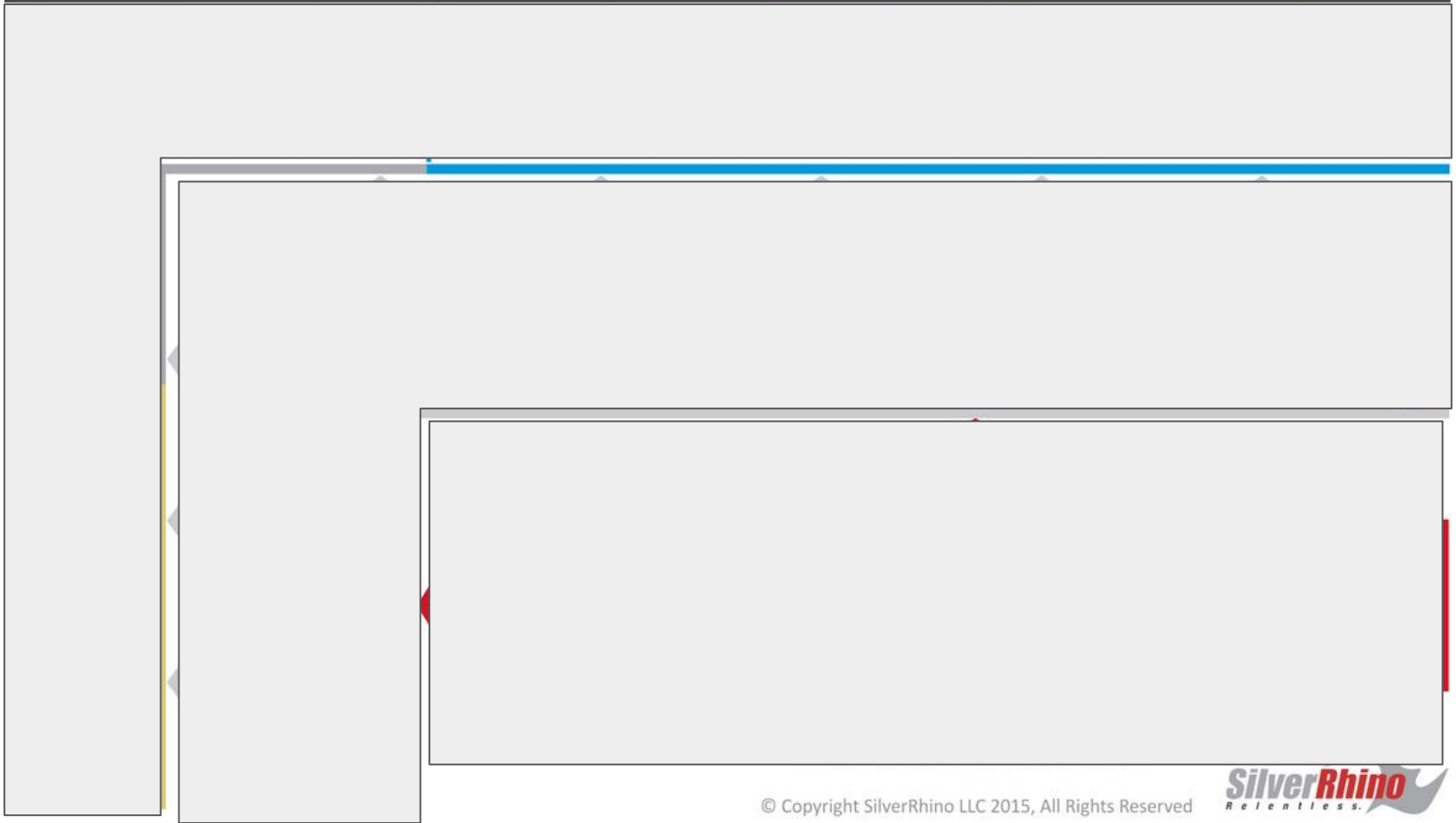

Internet
Router
Router
Router
Laptop
Phone
Firewall
Firewall
Firewall
Workstation
Server
Switch
Switch
Workstation
Workstation
Phone
Phone
Phone
Phone
Phone
Phone
PC
PC
PC
PC


OSI
TCP/IP
TCP/IP Suite
aunigma


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 Vault
Vmware Mgmt
McAfee AV Server
Citrix (ProvisaSQL)
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)

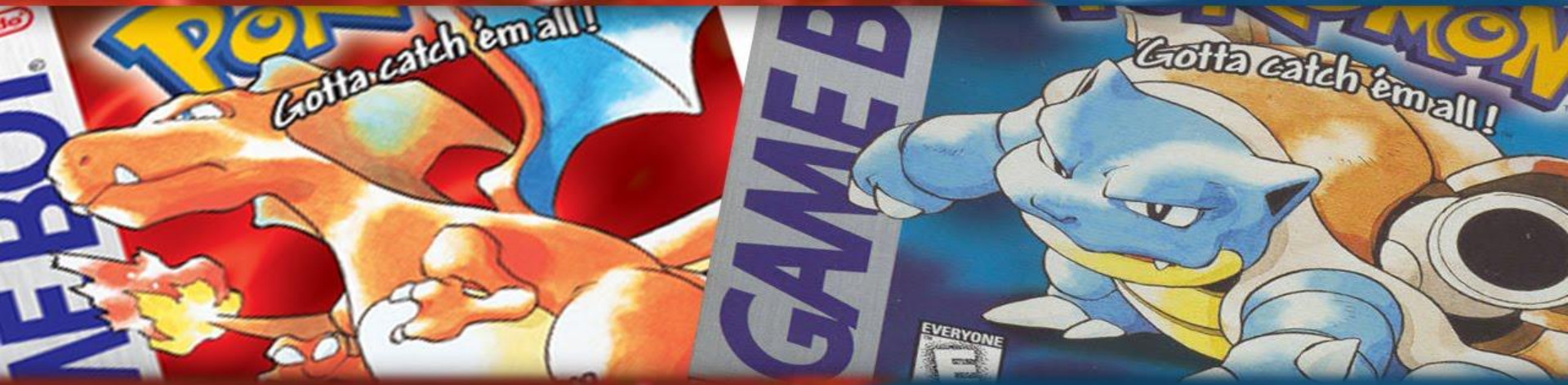
eocreveassim.com.br

Cyber Threatscape Framework

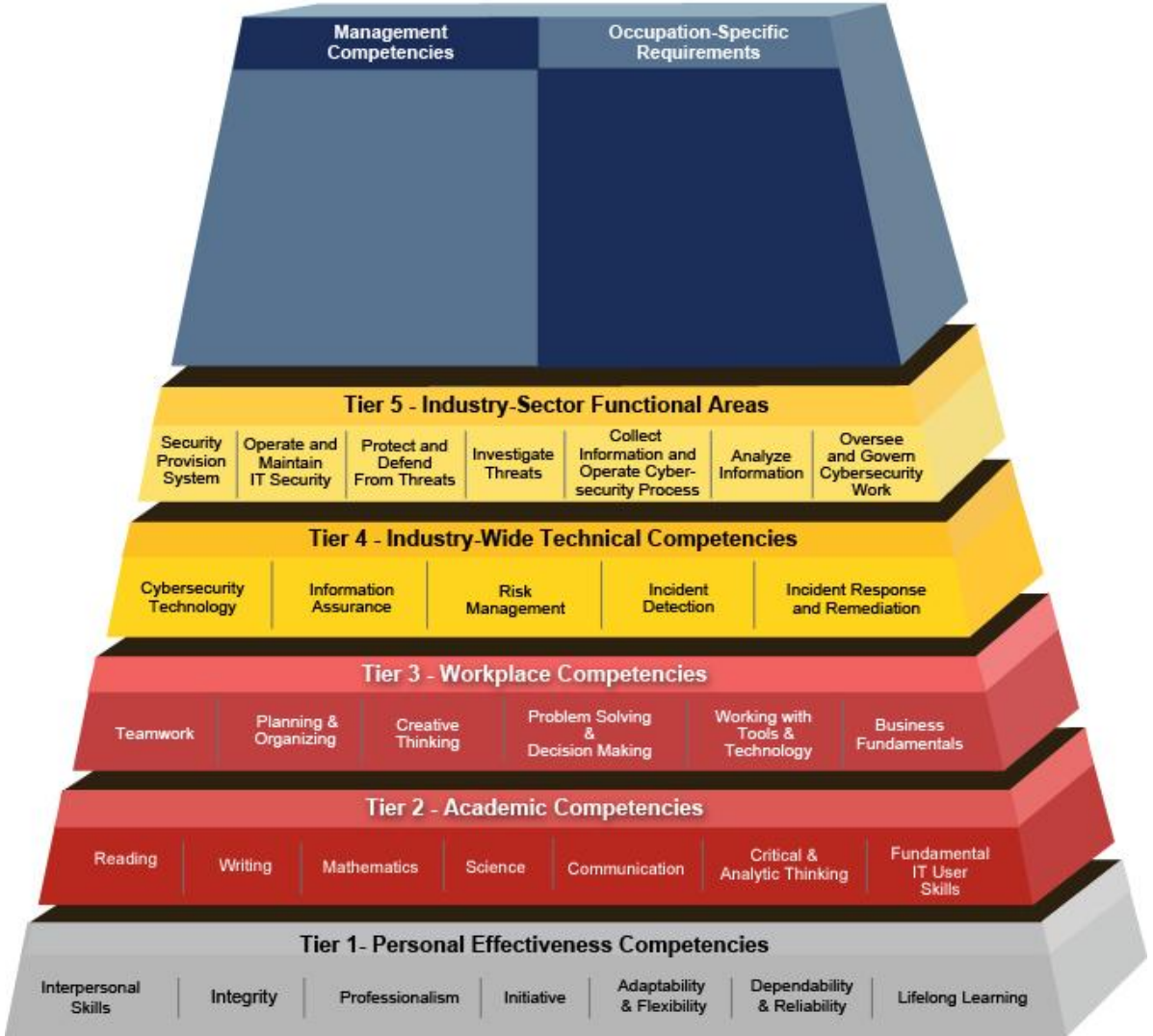


© Copyright SilverRhino LLC 2015, All Rights Reserved

THE BEST



TEAM!

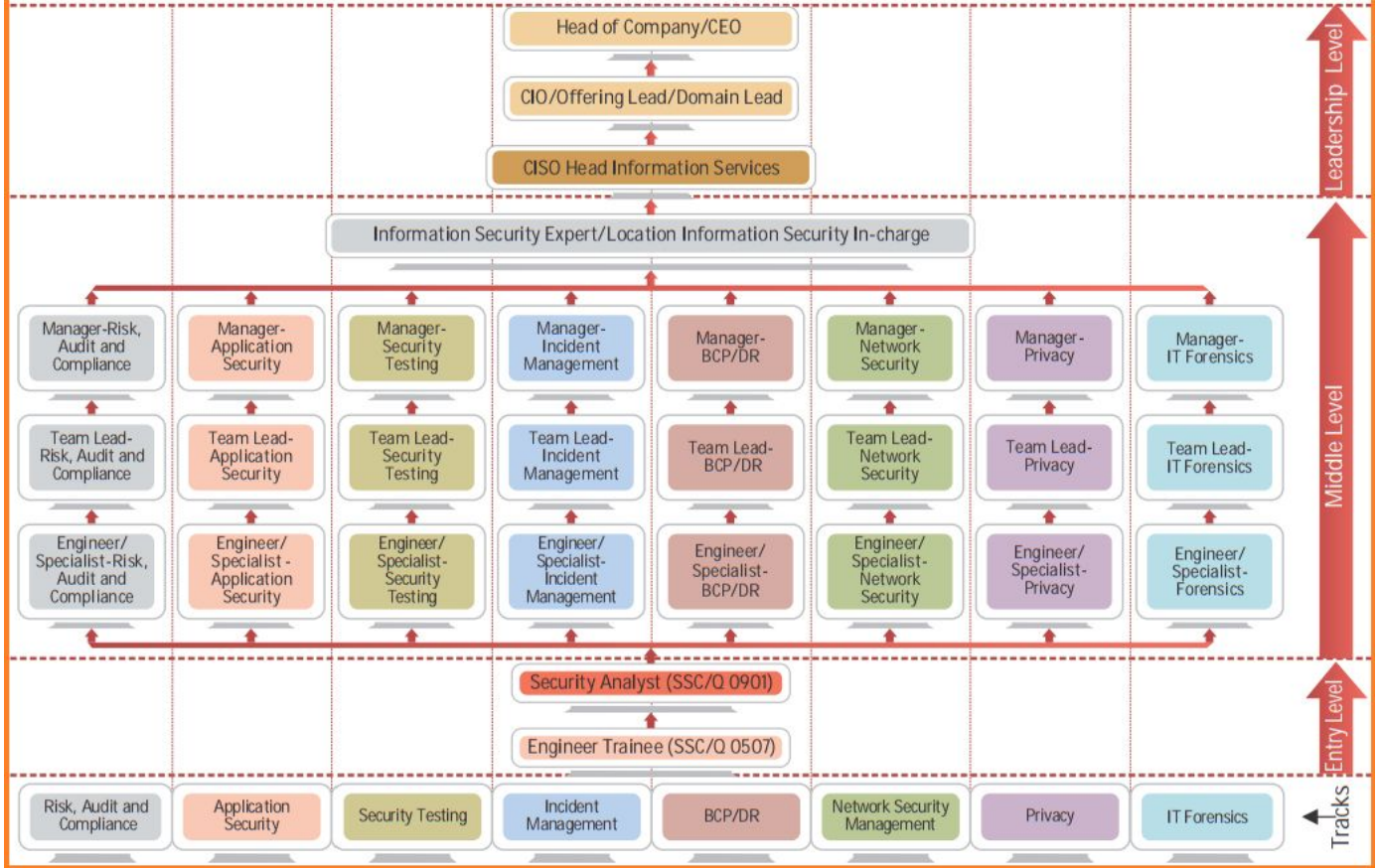

Management Competencies
Occupation-Specific Requirements
Tier 5 - Industry-Sector Functional Areas
Security Provision System
Operate and Maintain IT Security
Protect and Defend From Threats
Investigate Threats
Collect Information and Operate Cyber-security Process
Analyze Information
Oversee and Govern 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

Creating INFINITE Career Opportunities

Career Guide – IT Services

Source:- IT - ITeS SSC NASSCOM

Career Map for Information Security

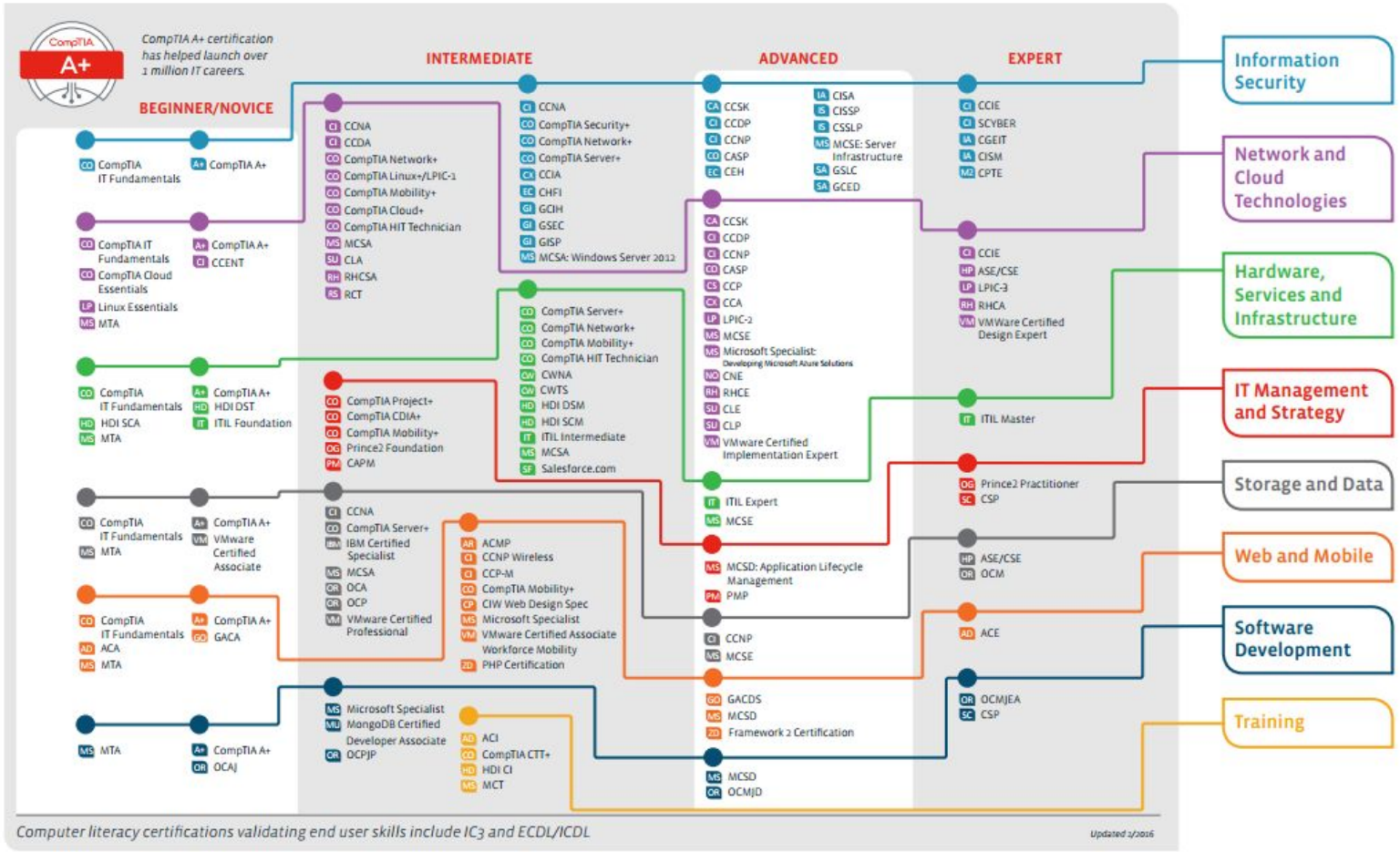


IT Certification Roadmap

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

We Will Now Have A
10 MINUTE
INTERMISSION
BEFORE STARTING OUR
NEXT SHOW

VIRTUALIZATION

And connecting to remote resources

Deloitte.

Are you ready to hone your business acumen and cyber skills?

Compete in the Deloitte Foundation Cyber Threat Competition*.

First Round: September 19 at 9:00 AM EST - October 6 at 5:00 PM EST
Final Round: November 10 - 12 at Deloitte University

*See Official Rules at **www.deloitte.com/us/getyourhackon**

Don’t delay: learn about the Deloitte Foundation Cyber Threat Competition Today!

The Deloitte Foundation sponsors the Cyber Threat Competition as a fun and innovative way to pique the interest of students like you who are interested in cyber security and are exploring what a career in professional services may look like.

Every day, our Deloitte Advisory Cyber Risk Services professionals help complex organizations more confidently leverage advanced technologies to achieve their strategic growth, innovation, and performance objectives through proactive management of the associated cyber risks.

If you want to:

- Advance your cyber knowledge and understand how cyber risk is affecting enterprises in today’s digital economy
- Test your skills working with top Deloitte Advisory professionals from across the country
- Learn about one of the world’s leading professional services firms

Then find out how the Deloitte Foundation Cyber Threat Competition can help you.
To learn more, visit **www.deloitte.com/us/getyourhackon**

As used in this document, “Deloitte” means Deloitte LLP and its subsidiaries. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2016 Deloitte Development LLC. All rights reserved.

Join Deloitte for a Cyber Threat Competition Information Session
Monday, Sept. 12, 6 - 7:30 p.m. in Knox 4
RSVP in BizLink |Events | Information Sessions

https://www.youtube.com/watch?v=o8JXiCYNuDo

iOS
ANDROID

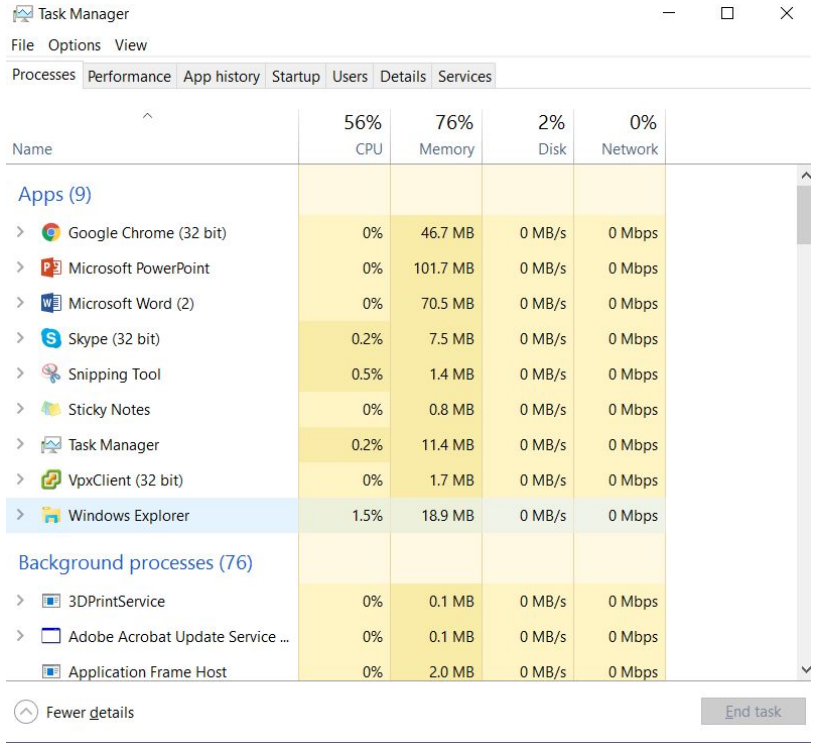
SYSTEM RESOURCES

Memory (RAM)

Storage (HDD)

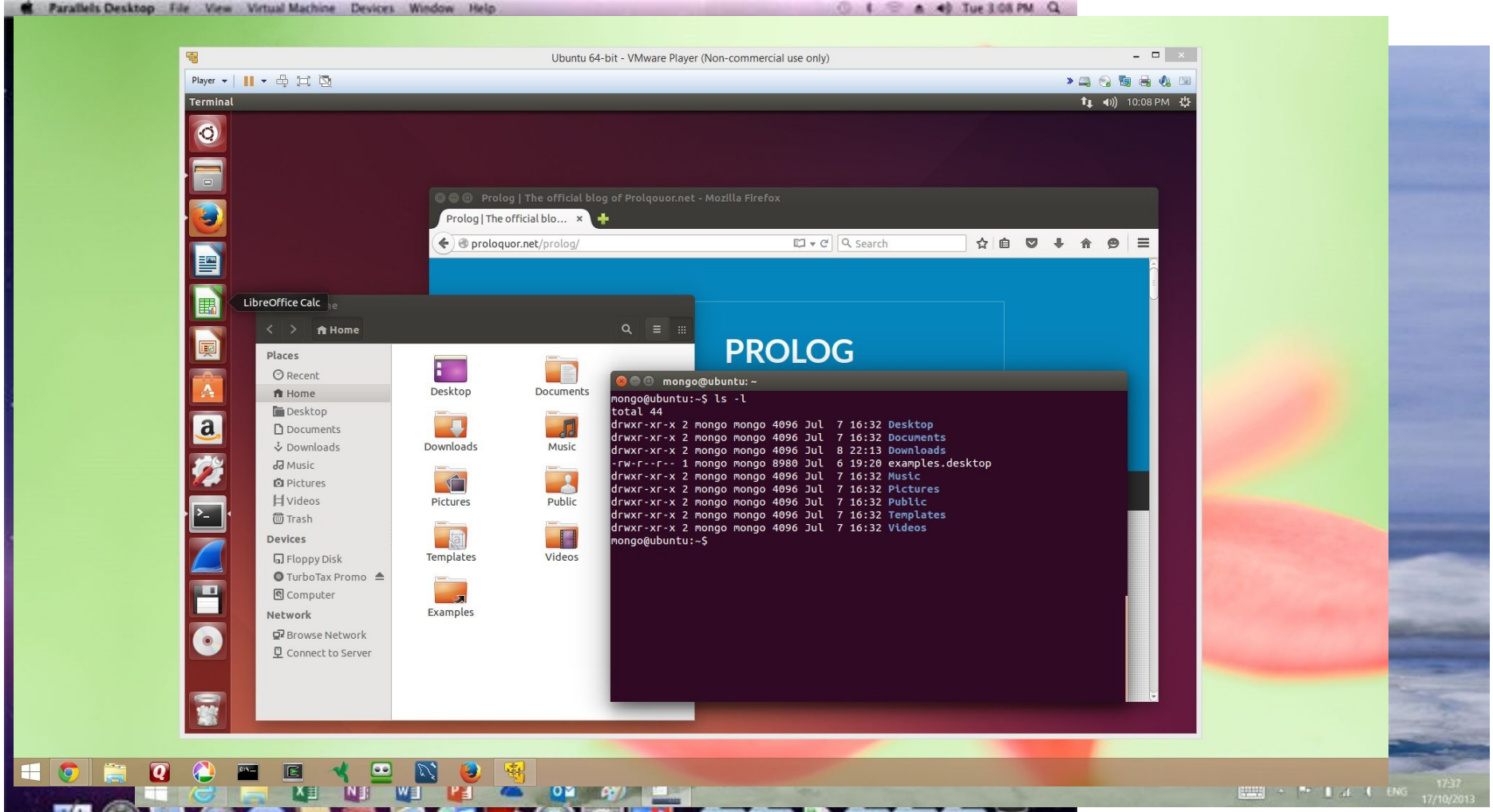
Processor (CPU)

Etc.



Whats a Virtual Machine? (VM)

- Computers within computers
- All running on same set of resources
- Can do different things at the same time
- Can run multiple VM's on one set of hardware
- VM's typically run on virtual hard drive
    - Can easily transfer


Parallels Desktop File View Virtual Machine Devices Window Help
Tue 3:08 PM
Ubuntu 64-bit - VMware Player (Non-commercial use only)
Player
Terminal
10:08 PM
Prolog | The official blog of Prolqouor.net - Mozilla Firefox
Prolog | The official blo...
proloquor.net/prolog/
Search
PROLOG
LibreOffice Calc
Home
Places
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Devices
Floppy Disk
TurboTax Promo
Computer
Network
Browse Network
Connect to Server
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
Examples
mongo@ubuntu: ~
mongo@ubuntu:~$ ls -l
total 44
drwxr-xr-x 2 mongo mongo 4096 Jul 7 16:32 Desktop
drwxr-xr-x 2 mongo mongo 4096 Jul 7 16:32 Documents
drwxr-xr-x 2 mongo mongo 4096 Jul 8 22:13 Downloads
-rw-r--r-- 1 mongo mongo 8980 Jul 6 19:20 examples.desktop
drwxr-xr-x 2 mongo mongo 4096 Jul 7 16:32 Music
drwxr-xr-x 2 mongo mongo 4096 Jul 7 16:32 Pictures
drwxr-xr-x 2 mongo mongo 4096 Jul 7 16:32 Public
drwxr-xr-x 2 mongo mongo 4096 Jul 7 16:32 Templates
drwxr-xr-x 2 mongo mongo 4096 Jul 7 16:32 Videos
mongo@ubuntu:~$
ENG
17:37
17/10/2013

BENEFITS OF VIRTUALIZATION?

Security: Separate applications from interfering with each other

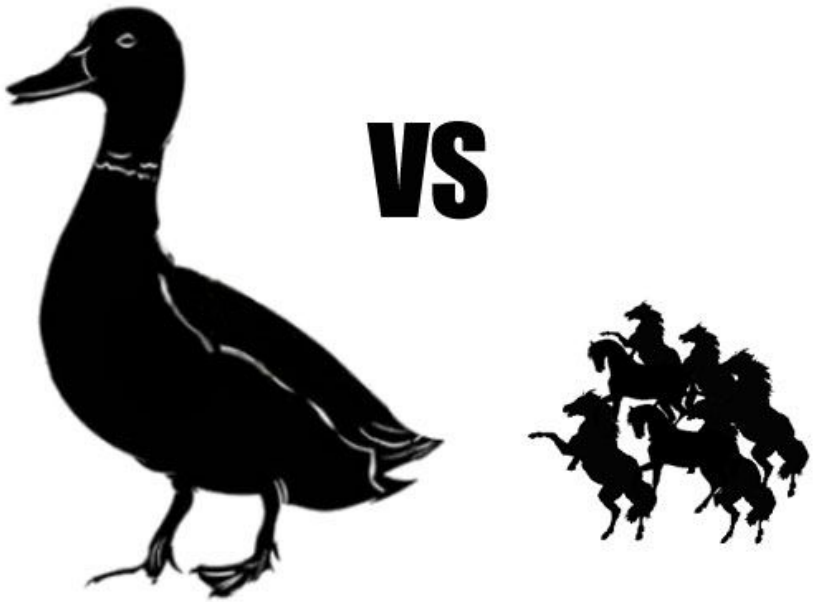
Testing: Open unknown, potentially malicious files

Learning: Try out new programs without having to worry

Resource optimization: Use what you have more efficiently

Many more!

Would you rather fight 100 desktop sized servers or 1 server sized desktop?



So How Does Virtualization Work?

Hypervisor!!

Microsoft
Hyper-V

VMware Fusion

VirtualBox

So How Does Virtualization Work?

Hypervisor

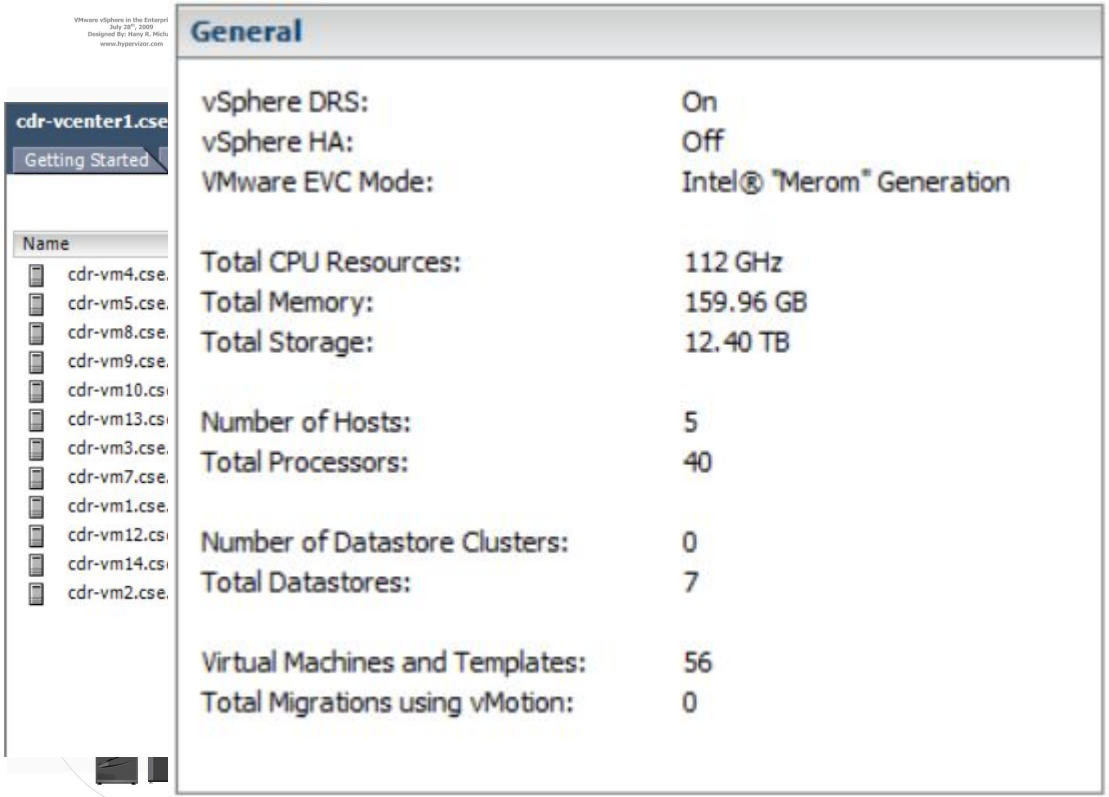
- Fancy word for software that runs at the OS level to manage VM's
- Type 1 vs Type 2
- Ex) Thin clients
  - Used at all libraries on campus
  - Spin up VM at login

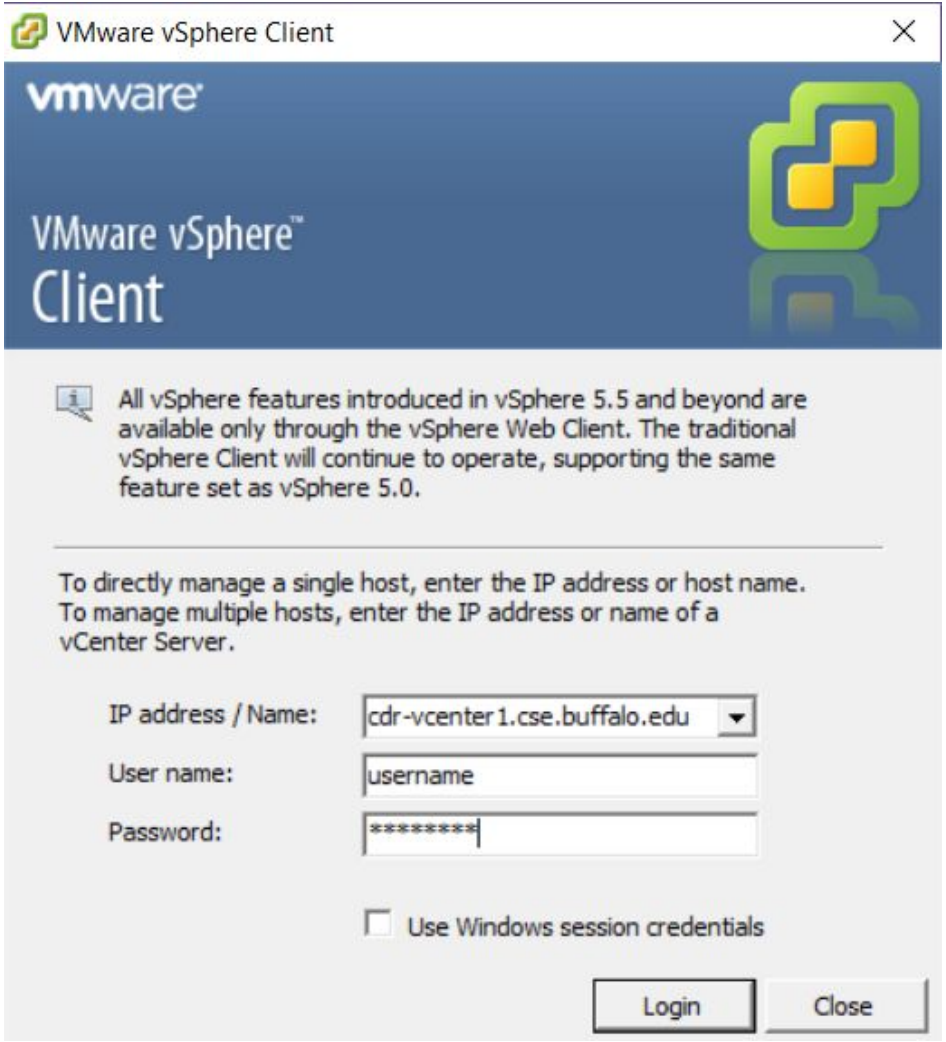
Type 1 B

002.006
002.005
002.004

Clustering

- One server to rule them all
- Ability to manage multiple hypervisors at once
- Combine resources
- Redundancy




VMware vSphere Client
vmware
VMware vSphere™
Client
All vSphere features introduced in vSphere 5.5 and beyond are available only through the vSphere Web Client. The traditional vSphere Client will continue to operate, supporting the same feature set as vSphere 5.0.
To directly manage a single host, enter the IP address or host name.
To manage multiple hosts, enter the IP address or name of a vCenter Server.
IP address / Name:
cdr-vcenter1.cse.buffalo.edu
User name:
username
Password:
****
Use Windows session credentials
Login
Close

Ubnetdef.org/vcenter

Server:

cdr-vcenter1.cse.buffalo.edu

Username: