Boomer the Bangle Boarding

SANS @ Night

To download and follow along with this presentation, you can retrieve it from:

https://github.com/itriskltd/Information-Security-and-Risk-Public-Presentations

SANS @ Night

Emerging Cyber Ranges
Competition to Compliance

Wednesday, 27 June 2018

7:15pm - 8:15pm

Matthew J. Harmon

GSEC, GCIH, GCIA, CISSP

 @mjharmon

Matthew J. Harmon

- IT Risk Limited, Principal Consultant
  - GRC, Technology Risk Assessments, Remediation, Interim CISO
- SANS Community & Mentor, 10 year anniversary!
  - SEC 401 Security Essentials
  - SEC 504 Hacker Tools, Techniques, Exploits & Incident Handling
  - SEC 464 Hacker Guard, IT Operations Baselining
- St. Paul College, CompSci Course Author & Instructor:
  - 2461 70 & 71 Computer Networking 3 - Linux
  - 2480 40 Network Security & Penetration Prevention
  - 2482 40 Security Incident Handling, Response and Disaster Recovery
  - 2484 40 Ethical Hacking & Countermeasures

Matthew J. Harmon

- Almost two year anniversary of two spinal operations
  - Re-learning how to walk and operate changes you
  - Learned cool new super powers through daily cross-training; incl. dancing, martial arts, jogging
- Cyber Security Summit (Oct 22-24, 2018)
  - Cyber Range Committee Member
  - Building team competition and hack-a-thon held before the summit
- NorSec Foundation
  - Cyber Range research and development
  - Malware analysis

What are we going to cover tonight?

- Cyber Ranges, what are they and why do we need more of them?
  - Offensive and defensive practice
  - Design and product validation proving grounds
  - Once interconnected, they can become more than the sum of their parts.
- Examples of some current large scale cyber ranges
- Considerations of Cyber Range design
- How to safely build your own Cyber Range.

Quick Terminology

- What is a Cyber Range in this presentation context?
- Any environment, that is representative of a realistic enterprise network that exclusively used for detonating malware, testing new Metasploit modules, or some random code you found on a pastebin or got uploaded to your not-a-honeypot-backup-dns-server.

Is my dev environment a Cyber Range?

- No, but…
- We'll talk about shortly about how a Cyber Range can help your dev team.

Cyber Ranges

- NATO War Games with JYVSECTEC
- SANS NetWars Series
- Capture the Flag events
- Follow the Maze style challenges (SANS Holiday Special)
- Scenario Simulation, Execution, and Observation. MITRE's CALDERA, Uber's Metta and…
- Defensive Exercises such as the CCDC
- Offensive Exercises such as the OSCP Lab

SANS NetWars: CyberCity

- 1:87 scale physical city.

https://www.sans.org/netwars/cybercity

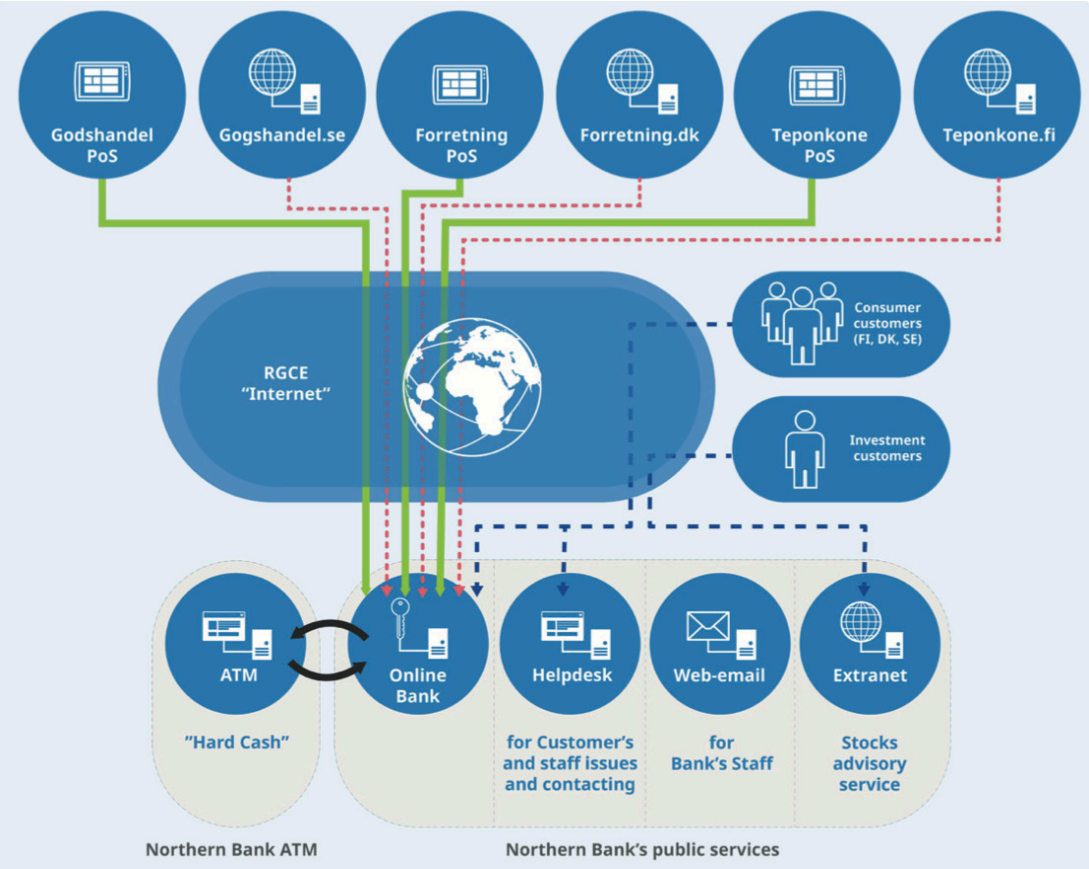
NetWars: DFIR Tournament

- Digital Forensics, Incident Response and Threat Hunting Scenarios

https://www.sans.org/netwars/dfir-tournament

JYVSECTEC

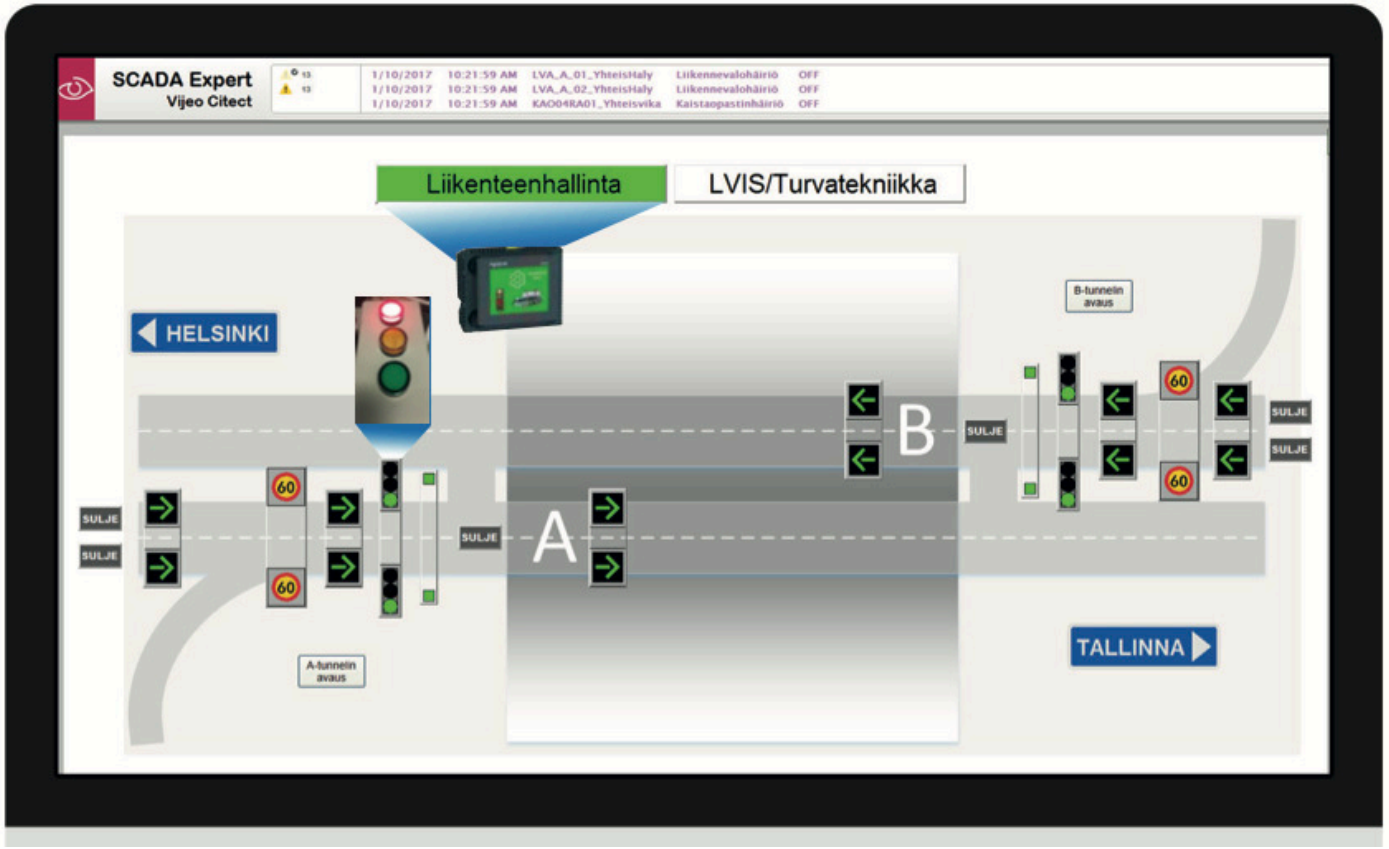
- Financial organization, NorthernBank



https://jyvsectec.fi/wp-content/uploads/2017/02/JYVSECTEC-cyber-range.pdf

JYVSECTEC

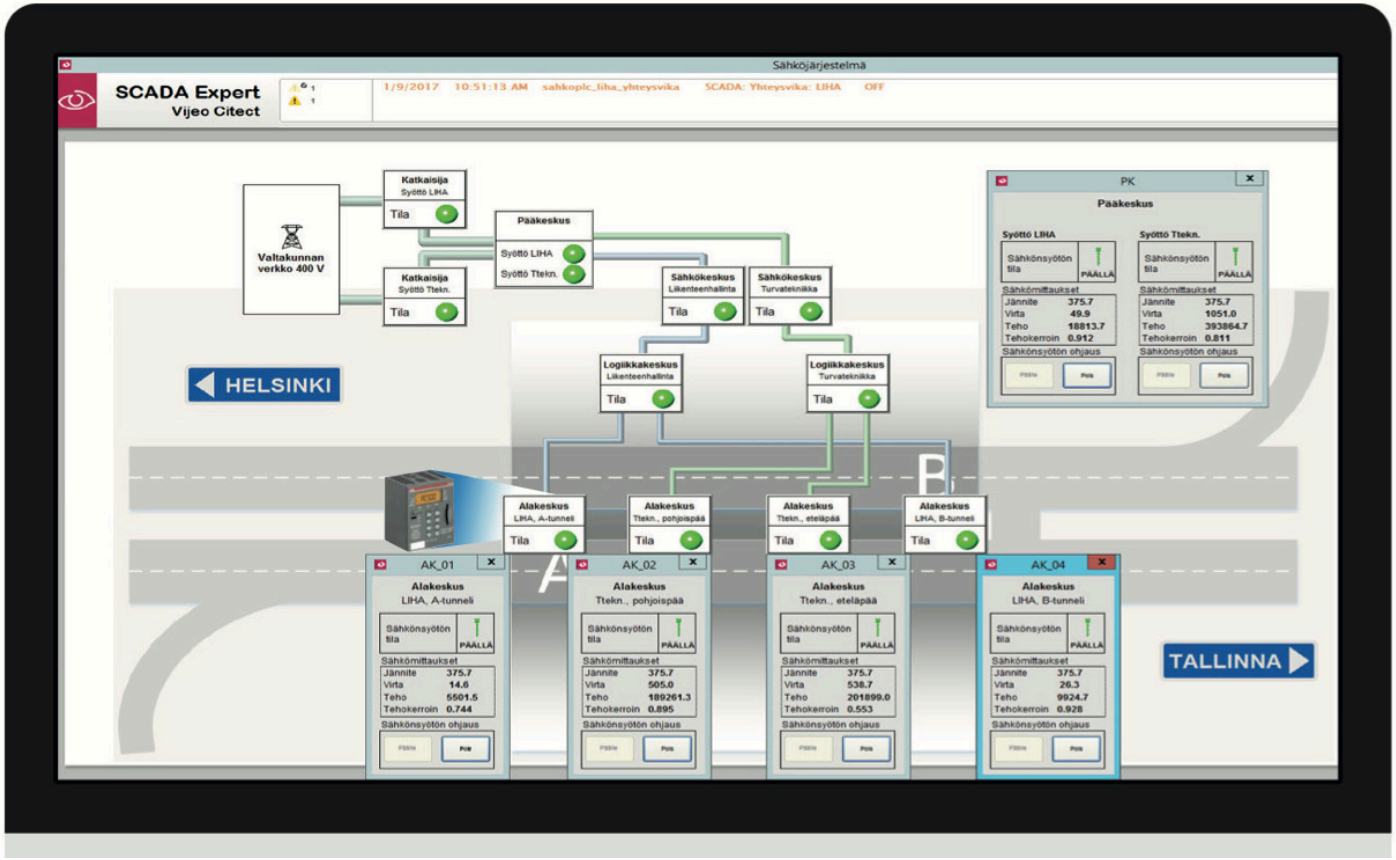
- Road tunnel provider, Funnel



https://jyvsectec.fi/wp-content/uploads/2017/02/JYVSECTEC-cyber-range.pdf

JYVSECTEC

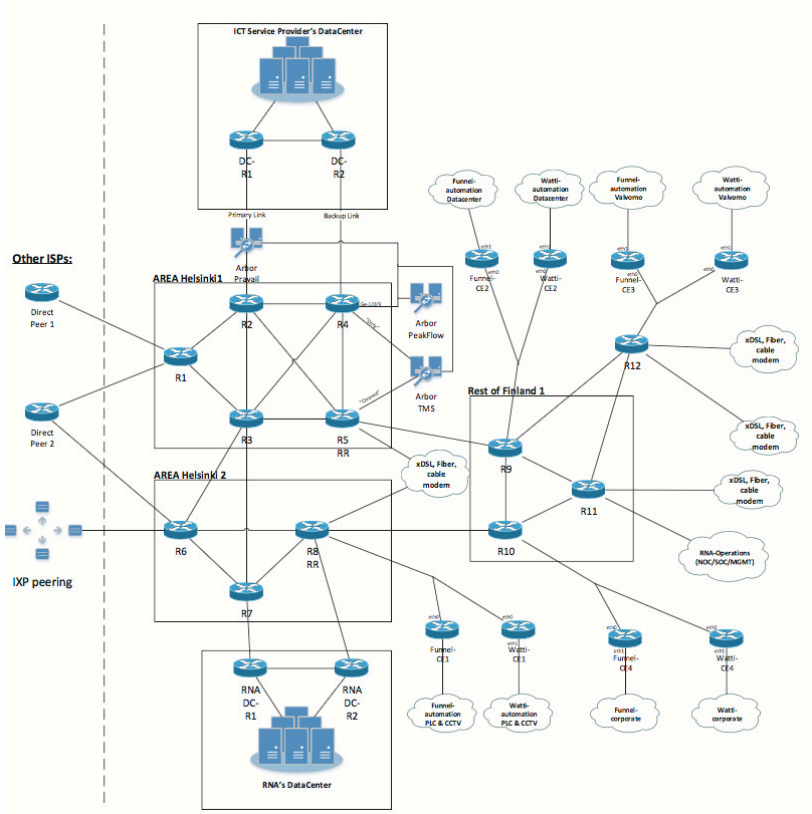
- Electricity Company, Watti



https://jyvsectec.fi/wp-content/uploads/2017/02/JYVSECTEC-cyber-range.pdf

JYVSECTEC

- Internet Service Provider, RNA



https://jyvsectec.fi/wp-content/uploads/2017/02/JYVSECTEC-cyber-range.pdf

MERIT

- MERIT's Cyber Range started in 2012
- YouTube Channel
  - https://www.youtube.com/user/michigancyberrange/videos
- "Powered by Merit Network, the nation's longest-running research and education network, the Michigan Cyber Range is the nation's largest unclassified, network accessible cybersecurity training platform."
  https://www.merit.edu/cyberrange/

merit

NETWORK. SECURITY. COMMUNITY.

MERIT's Alphaville

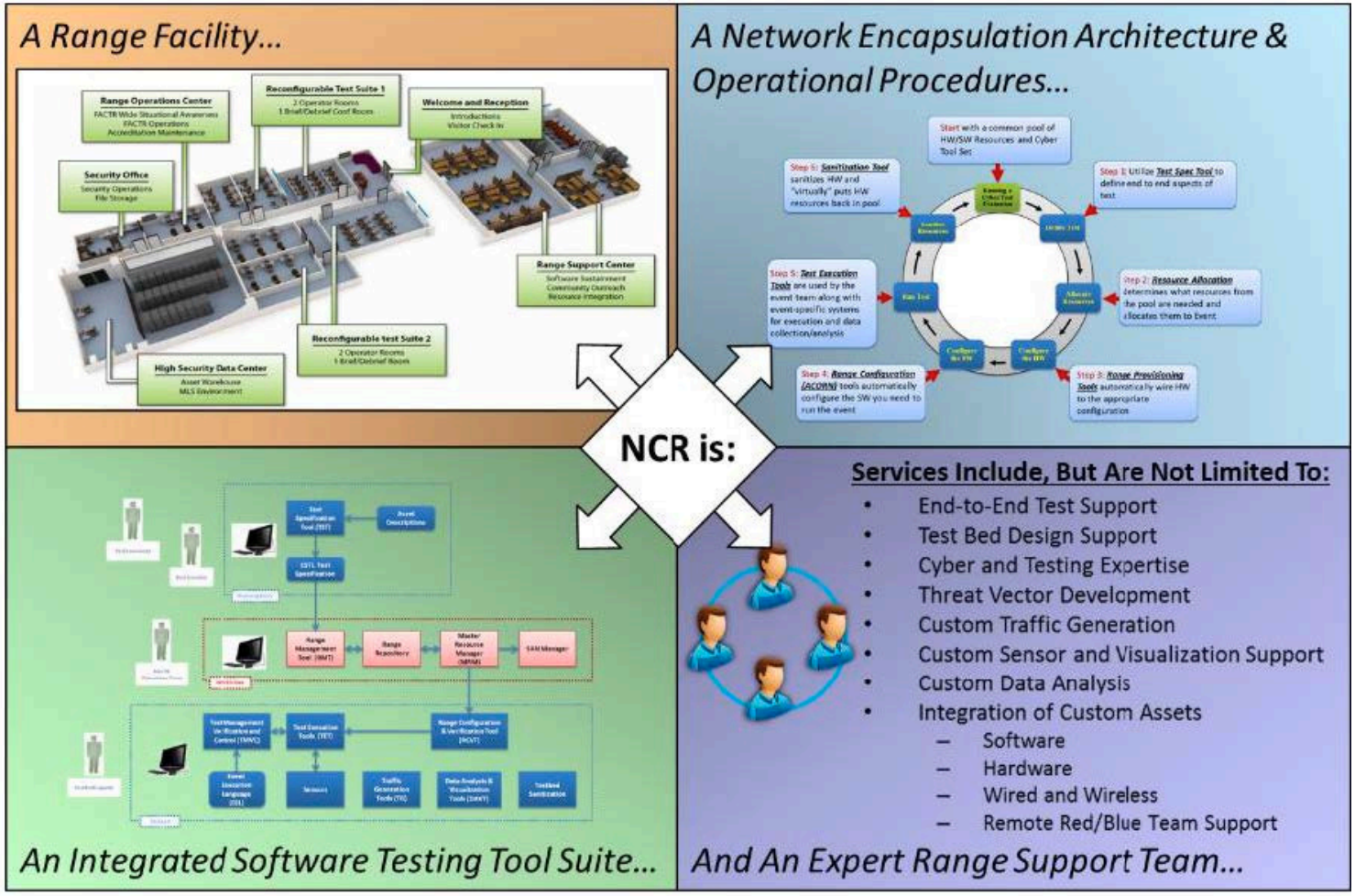
https://www.youtube.com/watch?v=9E08xSGviRI

National Cyber Range

- DARPA project 2009-2012
- DoD Test Resources Management Center
  - "..providing mission tailored, **hi-fidelity cyber environments** that enable independent and objective testing and evaluation of advanced cyberspace capabilities"
  - https://www.acq.osd.mil/dte-trmc/ncr.html

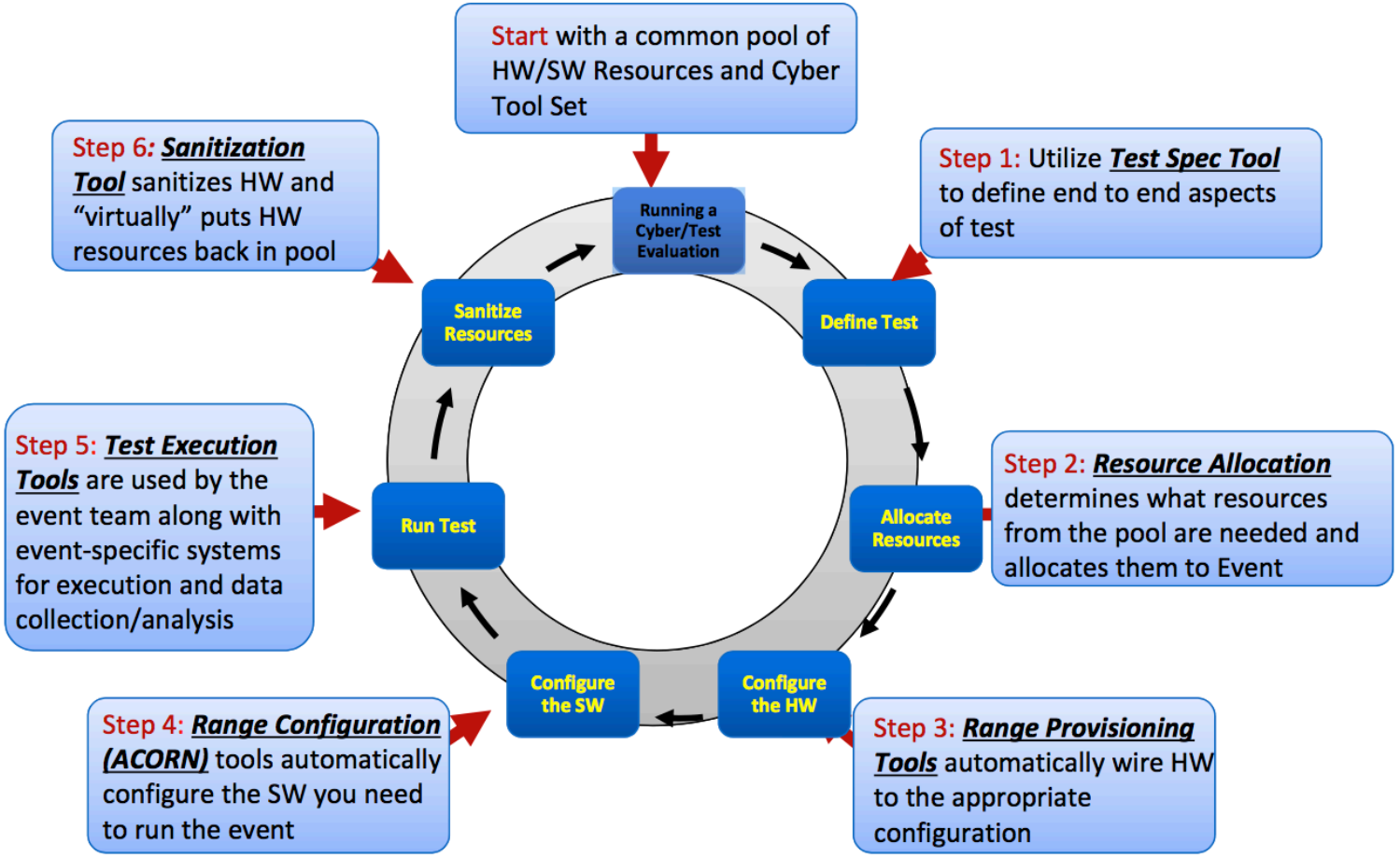
https://www.acq.osd.mil/dte-trmc/docs/20150224_NCR%20Overview_DistA.pdf

National Cyber Range



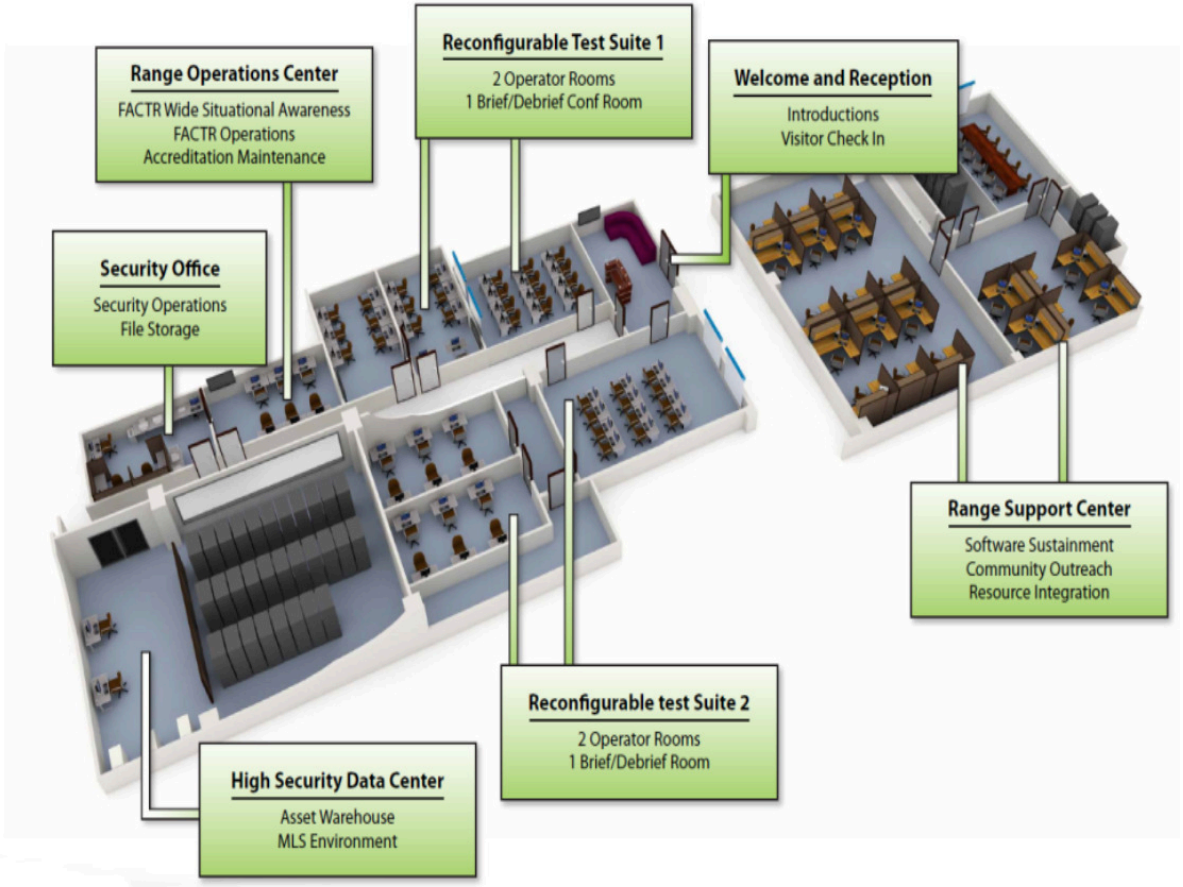
https://www.acq.osd.mil/dte-trmc/ncr.html

National Cyber Range



https://www.acq.osd.mil/dte-trmc/ncr.html

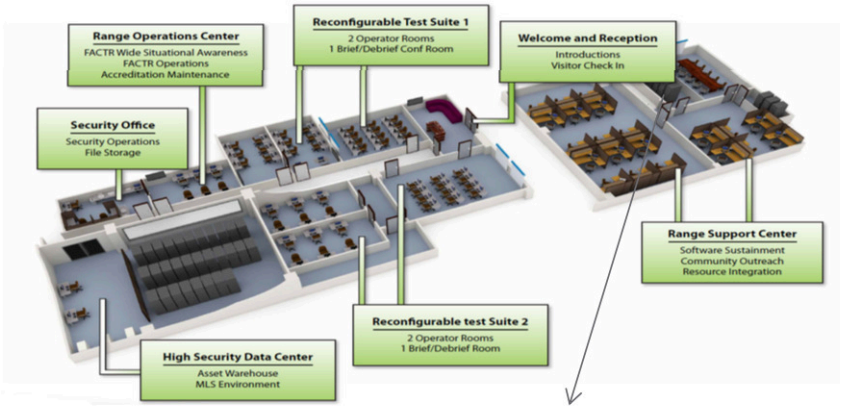
National Cyber Range



https://www.acq.osd.mil/dte-trmc/docs/20150224_NCR%20Overview_DistA.pdf

Distribution Statement A – Cleared for Open Publication by OSD on February 24, 2015 SB Case Number 15-S-0994

National Cyber Range



https://www.acq.osd.mil/dte-trmc/docs/20150224_NCR%20Overview_DistA.pdf

Distribution Statement A – Cleared for Open Publication by OSD on February 24, 2015 SB Case Number 15-S-0994

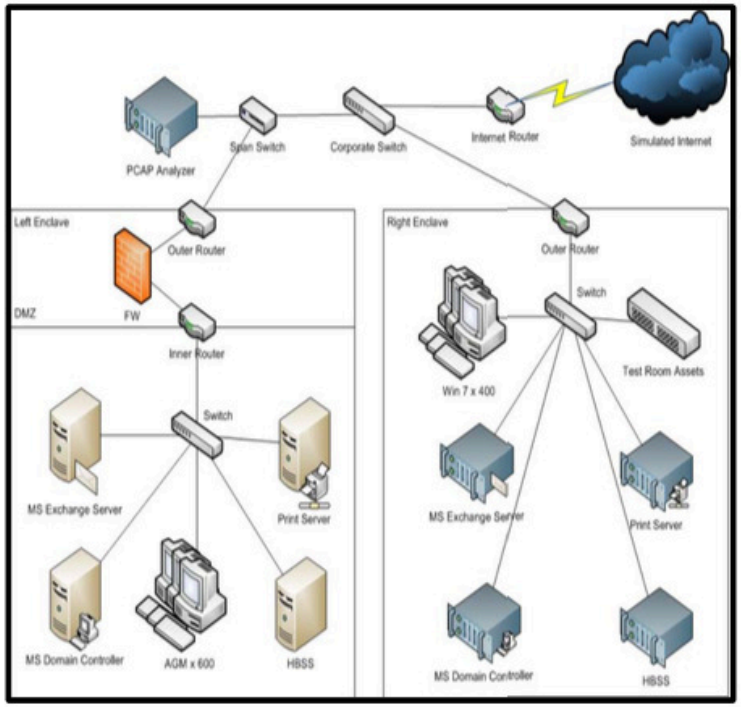
National Cyber Range

Question: Does Product "A" close a requirements gap?

- Does it mitigate a particular set of threats within my operational system?
- How well?
- What is my residual risk?

What you get:

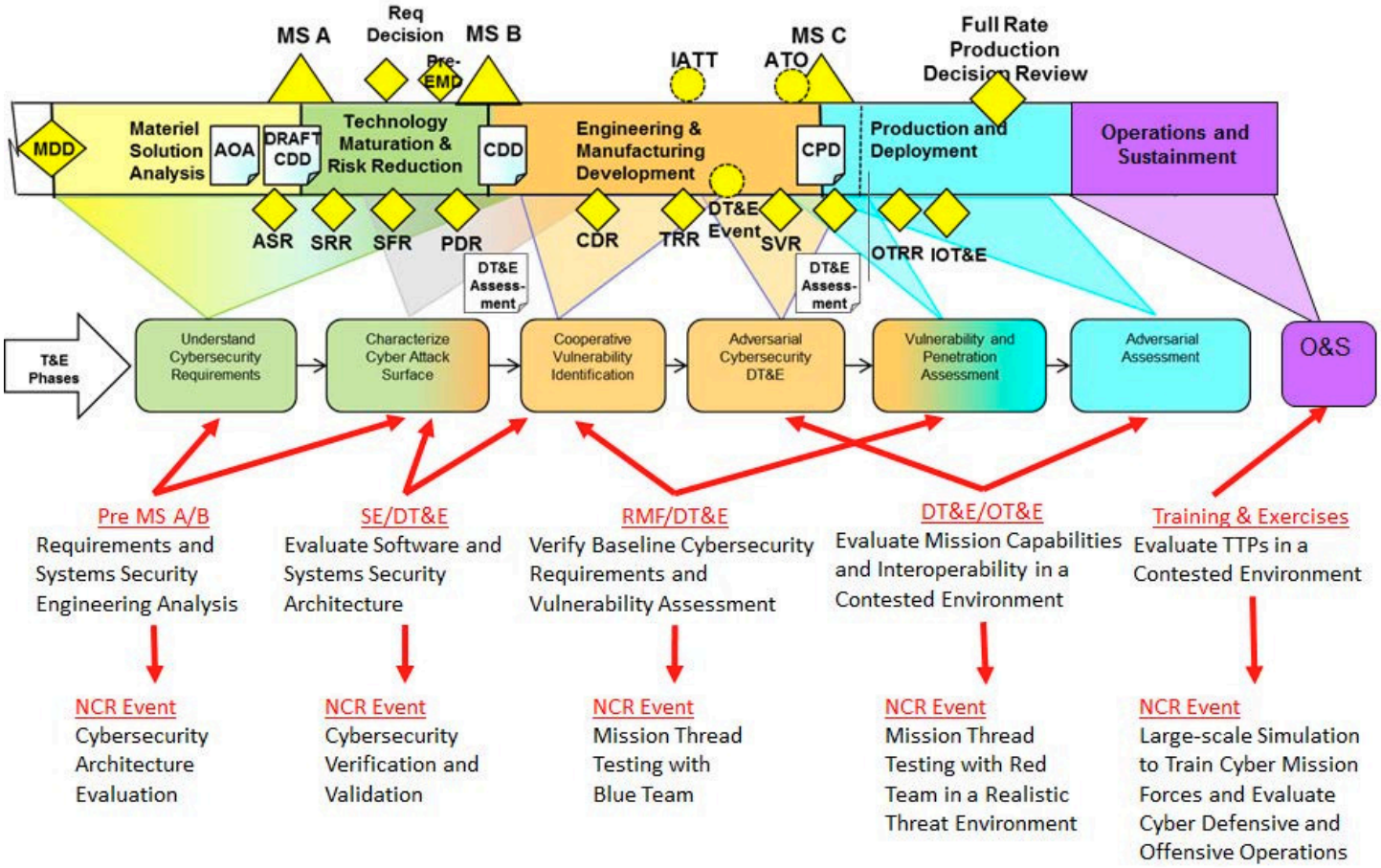
- Empirical evidence showing how the technology or product closes the requirements gap in your operational environment



How does adding a technology to my existing environment reduce my threat surface?

https://www.acq.osd.mil/dte-trmc/docs/20150224_NCR%20Overview_DistA.pdf

Integrating Compliance



https://www.acq.osd.mil/dte-trmc/docs/20150224_NCR%20Overview_DistA.pdf

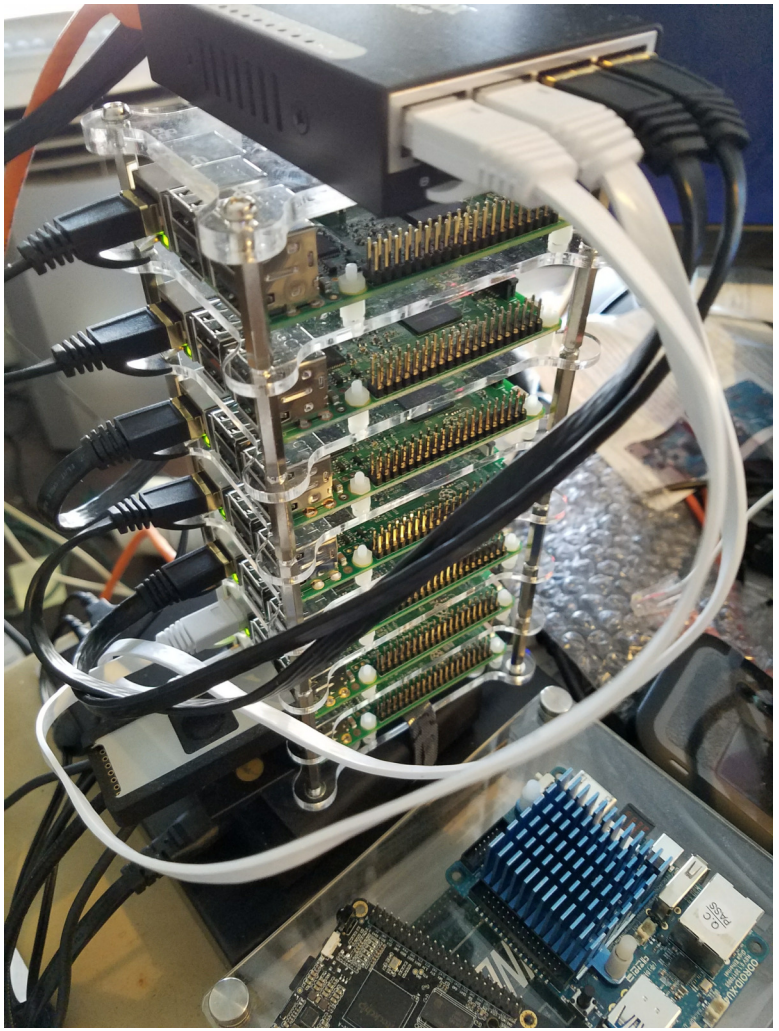
Distribution Statement A – Cleared for Open Publication by OSD on February 24, 2015 SB Case Number 15-S-0994

Cyber Range Principles

- Contained
- Auto Scaling
- Routing between separate networks
- Encrypted, routed, peer tunnels
- Explicit and Validated Authorization
- Rapid Restoration
- Portable

Proof of Concept

- Raspberry Pi Cluster
- apu2c4
- USB Armory
- YubiKey
- Modeled after dn42



Cyber Range Components

- BIRD & FRR
- tinc(GRE/BGP) & WireGuard(GRE/OSPF)
- iPXE, netboot.xyz
- QEMU (architecture emulation and shim)
- YubiKey

CrowdSupply Circumference

https://www.crowdsupply.com/ground-electronics/circumference/

Hostile Authentication Terminal

- init ram disk ++
- Assume everything is compromised
- dump & analyze ram, pull BIOS/EFI
- Validate known firmware
- Once state is known, begin bootstrap:
  - via iPXE over HTTPS (experimental[1])
  - via rsync'ed encrypted ZFS snapshot

[1] Experimental work by P. Danek, netbook.xyz, et al.

Multi Tier Authentication System

- init ram disk ++
- YubiKey Based, GPG, x509 Certificate
- fwknop with GPG
- credential and routing package.enc
- Unlock routing package via GPG
- Connect to bootstrap server
- Key to open ZFS snapshot
- Peer Configuration
- Peer Public Keys

YubiKey

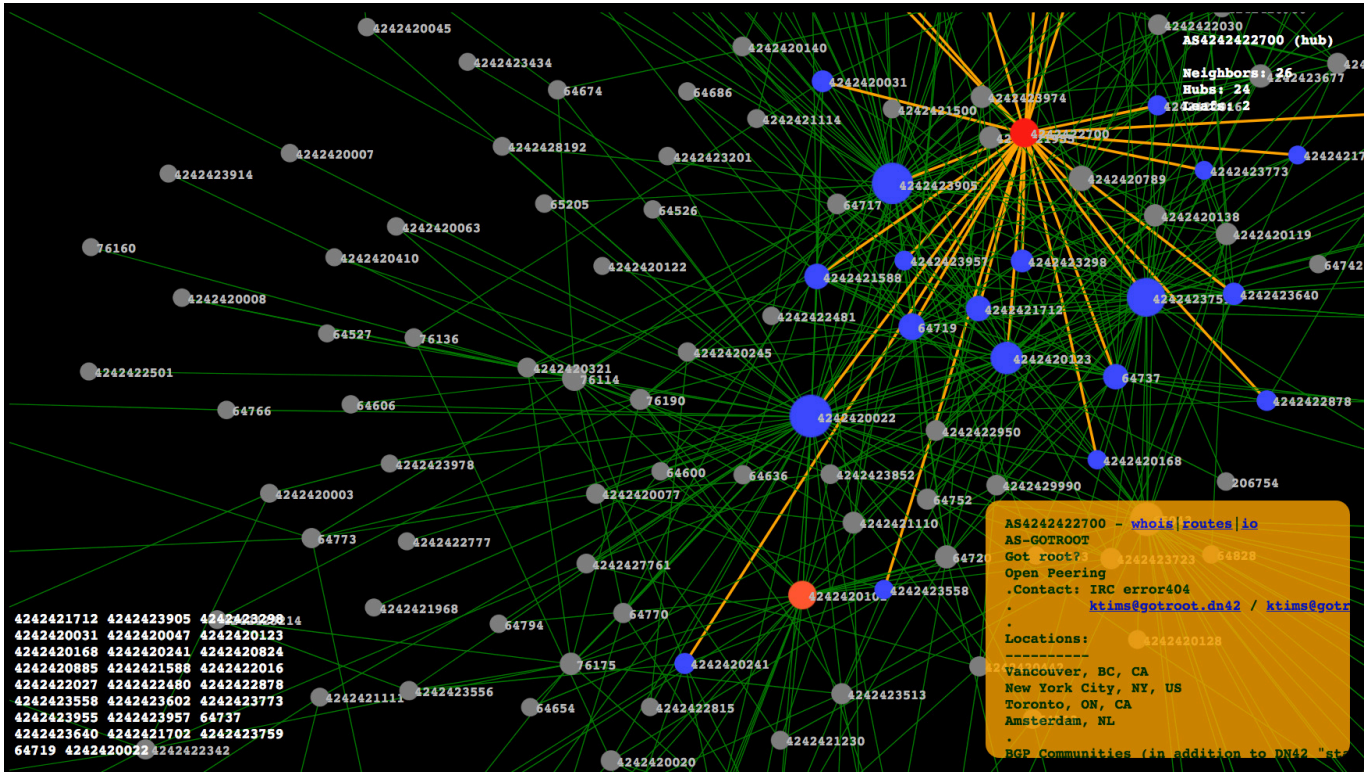
- HSM Key Storage
  - Set OTP + CCID + GPG mode
  - Require Touch before Authentication
  - libu2f-host
  - echo -e '\x06\x00\x00\x00' | u2f-host -d -a sendrecv -c c0

Adversary Simulation

- MITRE ATT&CK
  - CALDERA (Windows)
  - https://github.com/mitre/caldera
- Uber Metta (Windows, MacOS, Linux)
  - https://github.com/uber-common/metta
- Netflix
  - Simian Army: https://github.com/Netflix/
- Dumpster Fire
  - https://github.com/TryCatchHCF/DumpsterFire
- Malware Detonation

dn42

- Security Research Network



https://nixnodes.net/dn42/graph/

NOTE: I have no relation to dn42, only great admiration for their work.

Routing

- BGP through tinc, FRR
  - tinc chose due to solid history and peer recommendations, sends frequent PING / PONG packets discovering new routes. Perfect for the network edge to discover and add new BGP peers.
- OSPF through WireGuard, BIRD
  - Used as internal protocol as it is quiet and doesn't send any data when idle. WireGuard formally verified.

Calming the Route Chaos

```
(64511, 1) :: latency \in (0, 2.7ms]
(64511, 2) :: latency \in (2.7ms, 7.3ms]
(64511, 3) :: latency \in (7.3ms, 20ms]
(64511, 4) :: latency \in (20ms, 55ms]
(64511, 5) :: latency \in (55ms, 148ms]
(64511, 6) :: latency \in (148ms, 403ms]
(64511, 7) :: latency \in (403ms, 1097ms]
(64511, 8) :: latency \in (1097ms, 2981ms]
(64511, 9) :: latency > 2981ms
(64511, x) :: latency \in [exp(x-1), exp(x)] ms (for x < 10)

(64511, 21) :: bw >= 0.1mbit
(64511, 22) :: bw >= 1mbit
(64511, 23) :: bw >= 10mbit
(64511, 24) :: bw >= 100mbit
(64511, 25) :: bw >= 1000mbit
(64511, 2x) :: bw >= 10^(x-2) mbit
bw = min(up,down) for asymmetric connections

(64511, 31) :: not encrypted
(64511, 32) :: encrypted with unsafe vpn solution
(64511, 33) :: encrypted with safe vpn solution (but no PFS - the usual OpenVPN p2p
configuration falls in this category)
(64511, 34) :: encrypted with safe vpn solution with PFS (Perfect Forward Secrecy)
```

https://dn42.net/howto/Bird-communities

Certification & Accreditation

- Doesn't have to be boring
- Device Testing through Crowdsourced Penetration Tests over the Cyber Range network
- On-going Bug Bounties with explicit permission built in
- Hack-a-thons anywhere via an interconnected range

Cyber Range (Why not?)

- Proper Security Research
- Cyber eSport Competitions
- Corp-to-Corp War Games
- Device Testing & Claim Validation
  - Medical, ICS,
  - Toy Bears, Smart TVs
- Students Writing Malware
- Connect your range to your peers
  - Long distance LAN parties

Shoot for the stars.

Thank you!

matthew@itriskltd.com

Presentation Repository
https://bit.ly/ITRiskPres

Technology and Business Risk Management, (Pre-)Audit, Security Testing, Governance, Interim CISO Services

Sources, References & Credits

1. Colonel Stephanie Horvath US Army MN National Guard
2. JYVSECTEC
3. US Dept of Defense
4. SANS NetWars: https://www.sans.org/netwars/cybercity
5. dn42
    1. BIRD Communities: https://dn42.net/howto/Bird-communities
    2. BIRD Community Latency Script, https://github.com/Mic92/bird-dn42/blob/master/bgp-community.rb
6. SpaceX Night Launch, Original Videographer Unknown
7. CrowdSupply, Circumference Raspberry Pi Cluster Project:
    1. https://www.crowdsupply.com/ground-electronics/circumference/
8. YubiKey Configuration
    1. https://github.com/drduh/YubiKey-Guide#4.7-requiring-touch-to-authenticate
    2. https://github.com/Yubico/libu2f-host
    3. https://developers.yubico.com/libu2f-host/Mode_switch_YubiKey.html
9. Lou Ann Jensen
10. David La Belle

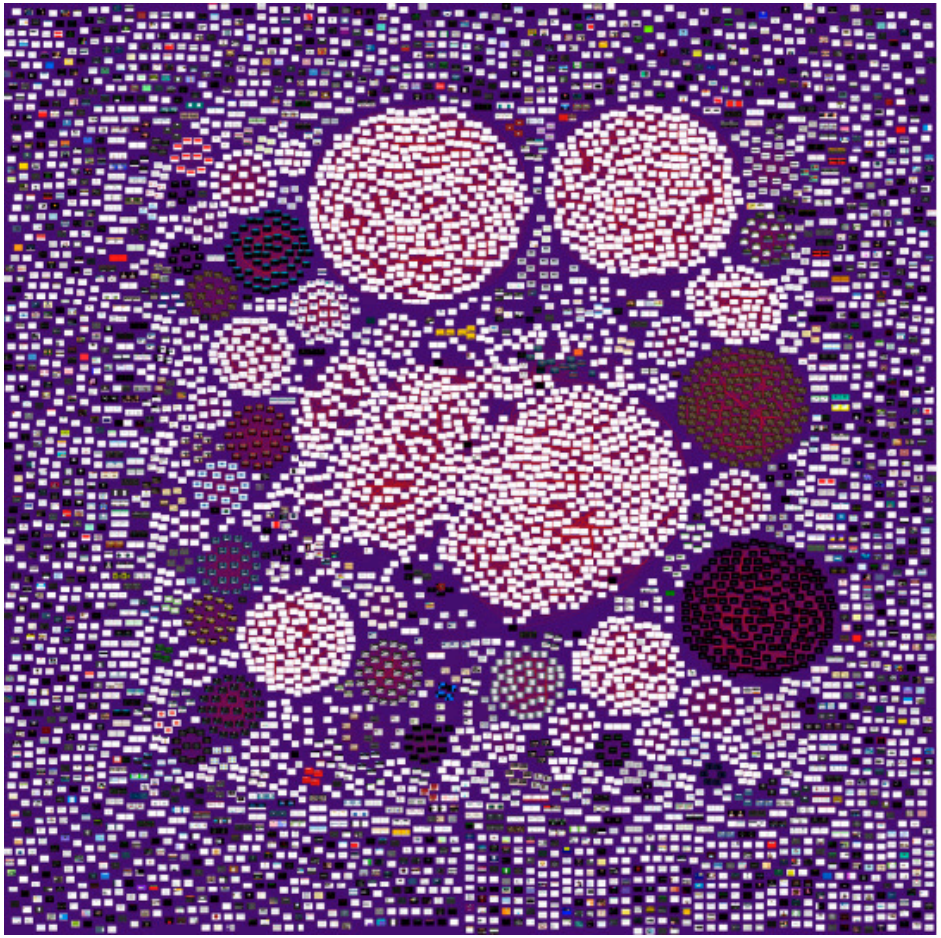
Sources, References & Credits

- Minneapolis Starry Night
- Uber metta
  - https://github.com/uber-common/metta
- MITRE CALDERA
  - https://github.com/mitre/caldera
- https://bsdrp.net/documentation/examples/bgp_route_reflector_and_confederation_using_quagga_and_bird
- https://github.com/Mic92/bird-dn42/blob/master/bgp-community.rb
- @HyperionGray Dark Web Map
  - https://blog.hyperiongray.com/dark-web-map-introduction/

Sources, References & Credits

- If you're a network engineer, the previous slide made you think about routing loops and other insanity.
- Introducing BIRD BGP community and automatic calculations.
  - https://bsdrp.net/documentation/examples/bgp_route_reflector_and_confederation_using_quagga_and_bird
  - https://github.com/Mic92/bird-dn42/blob/master/bgp-community.rb

The Dark Web Map by @HyperionGray



https://blog.hyperiongray.com/dark-web-map-introduction/