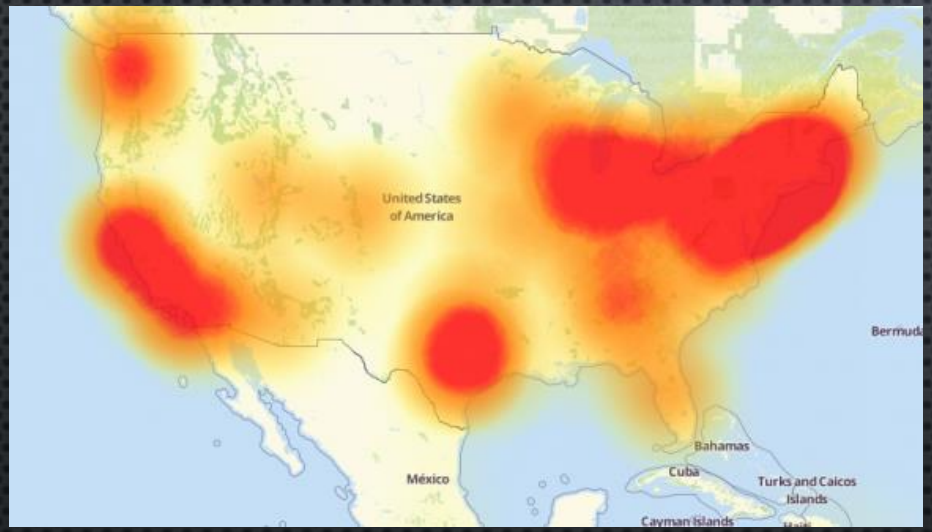
CYBER WARGAMING

LESSONS LEARNED IN INFLUENCING SECURITY STAKEHOLDERS INSIDE AND OUTSIDE YOUR ORGANIZATION

JULY 2017

CYBER IS GETTING…INTERESTING



RECENT EXAMPLES:

- MIRAI VS. INTERNET
- IS IT RANSOMWARE OR ? NOT SURE IF THE GROCERY SHOPPERS CARE

ISSUE #1: CYBER WAS CHALLENGING, IS GETTING HARDER

- CYBER IS GETTING COMPLICATED
  - IOT DIVERSIFIES ATTACK VECTORS
  - VIRTUALIZATION / ABSTRACTION
  - BLURRED LINES BETWEEN THREAT ACTORS

VERIZON: INDUSTRY "HOT SPOTS"

EXAMINATION OF 2017 DATA BREACHES SHOWS DIVERSE MAP OF PATTERN, ACTION & ASSET ACROSS INDUSTRIES

Issue #2: Skill Deficit

"A report from Cisco puts the global figure at one million cybersecurity job openings. Demand is expected to rise to 6 million globally by 2019, with a projected shortfall of 1.5 million, says Michael Brown, CEO at Symantec..."

- Sources:
  - Cisco: http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf
  - Forbes Magazine: https://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016

Issue #3 – Knowledge in Non-IT Positions

Many Activities that affect security are performed by people that don't understand security. Examples:

- Executive Management: Whaling / CEO Fraud
- Finance: Whaling, Spear Phishing
- Staffing / Recruitment: Do new Hires understand security? What skills are most important?
- Procurement: Are products secure?
- Contracting: Are there guarantees / requirements for product & service security?

Issue #4: Tech Staff

There is an increasingly concerning issue in IT / IoT about Security in the Supply Chain:

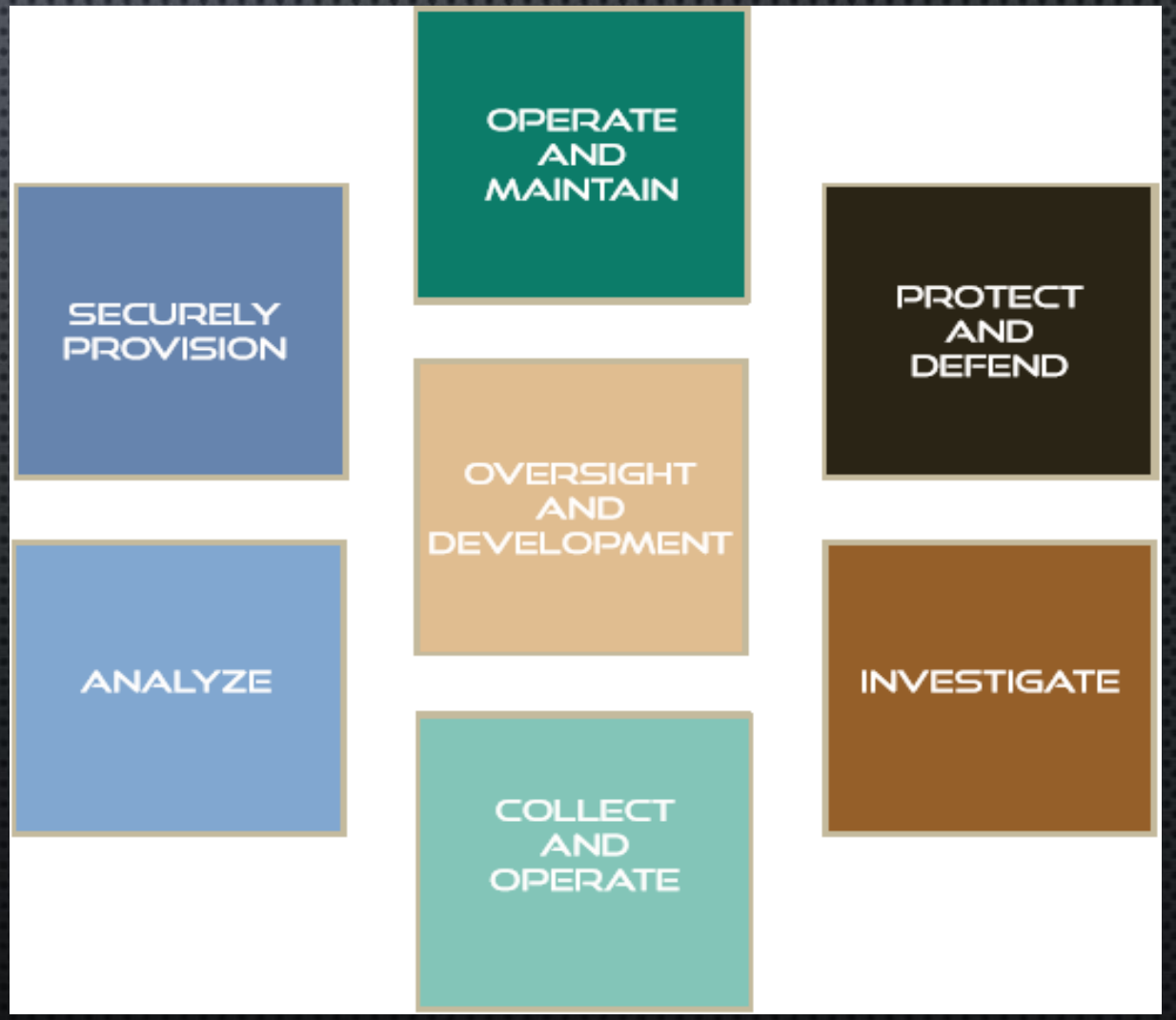
- Product design (software, Hardware)
- Software development: secure code practices
- Test & evaluation: test for security
- Customer Support / Product Maintenance: Deliver with Integrity

MeDoc anyone?
https://www.theregister.co.uk/2017/07/05/ukraine_authorities_raid_me_docs_in_notpetya_investigation/

Issue #5: Specialization within Cyber

- Some cyber pros don't know the "other side"
  - Where are You in the Taxonomy?
    - If you specialize, you may have blind spots
    - If you generalize, you may miss skills
- Tradecraft improves if:
  - Defender knows how an attacker thinks and operates
  - Operations planner knows how a defender looks for intrusion
  - operators see latest tools, vulnerabilities, exploits
  - Operators reinforce techniques with best practices

Source: NIST National Initiative for Cybersecurity Education (NICE)



Traditional Training

Why does most cyber security training fail today?*

1. It's boring
2. It lacks user interaction and involvement
3. There's no measurement
4. We scare versus teach
5. Education is not a security team's core competency

*Source: Wombat Security

Traditional Product Demonstration

Recognize this picture? Many product demonstrations:

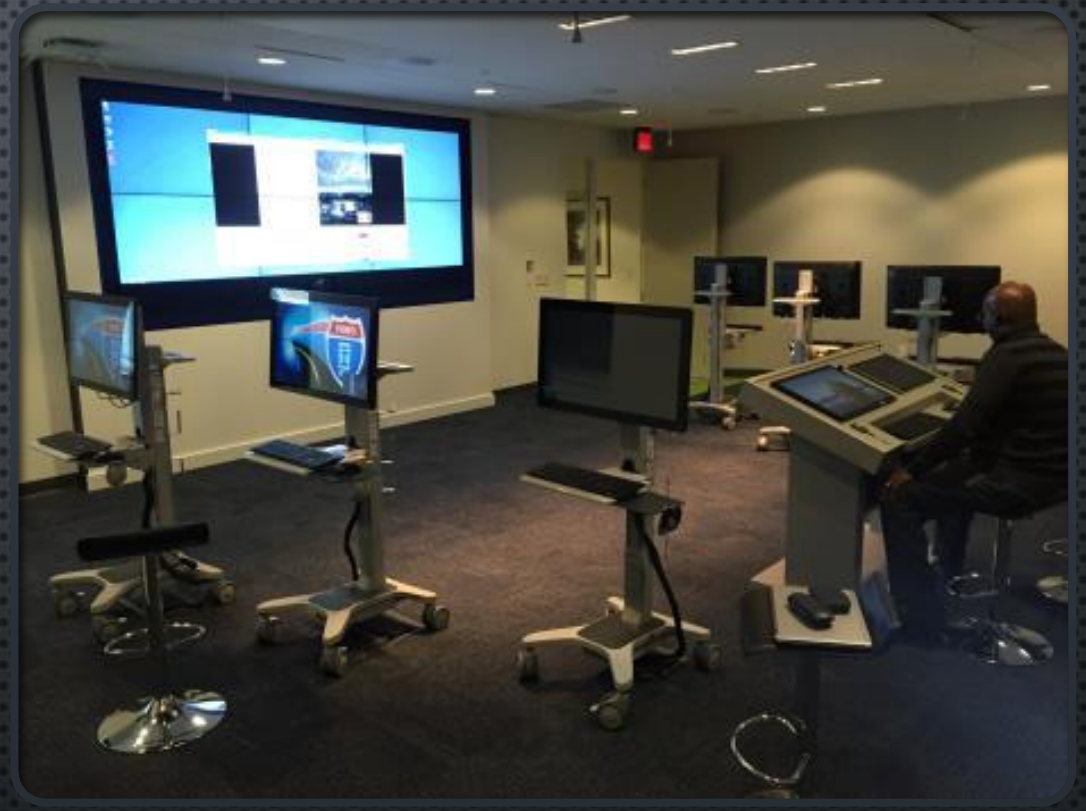
- Are Briefing-based
- Are Not Interactive
- Do not engage the Audience

And therefore Do not compel the audience to think about and retain key messages

Source: The Language Lab, "6 Quick Tips on How Not To Be Boring…" http://www.thelanguagelab.ca/posts/6-quick-tips-on-how-not-to-be-boring-improve-your-presentation-delivery-skills/

SOLUTION

- Engage with all stakeholders
- Create realistic, immersive, entertaining environment
- Use gaming techniques to enable team-based play
- Encourage participation by novices, teamed with and supported by experts
- Use the game as platform to both train and demonstrate



SAIC iSpace Collaboration Lab – Matrix Room

SERIOUS GAMING; WARGAMING

A **SERIOUS GAME** OR **APPLIED GAME** IS A GAME DESIGNED FOR A PRIMARY PURPOSE OTHER THAN PURE ENTERTAINMENT…THE IDEA SHARES ASPECTS WITH SIMULATION GENERALLY, INCLUDING FLIGHT SIMULATION AND MEDICAL SIMULATION, BUT EXPLICITLY EMPHASIZES THE ADDED PEDAGOGICAL VALUE OF FUN AND COMPETITION

SHOWN TO LEFT: SOLDIERS FROM THE U.S. ARMY AND UKRAINIAN ARMY ACTING AS OBSERVER CONTROLLER TRAINERS WATCH AS UKRAINIAN SOLDIERS REACT TO ENEMY FIRE … (U.S. ARMY PHOTO BY SGT. 1ST CLASS WHITNEY HUGHES/RELEASED)

SOURCES: WIKIPEDIA: SERIOUS GAME; WWW.EUR.ARMY.MIL/EXERCISES

WARGAME SUMMARY

- QUICK – 2.5 HOURS TOTAL
- MOST VALUABLE ACTIVITY IS IN POSTBRIEF WHERE PARTICIPANTS PRESENT CHALLENGES, SUCCESSES, RELEVANCE
- COACHES START THE GAME, BUT ABOUT MID-WAY, PLAYERS TAKE OVER
  - POST-BRIEF DEVELOPED AND PRESENTED BY PLAYERS
  - PLAYERS TEACH EACH OTHER

11:00 – 11:15	Team Gathers
11:15 – 11:30	Game Introduction • Cyber Warfare • Game Overview • Objectives • Team assignment
11:30 – 11:45	Team In-Briefs
11:45 – 12:45	Gameplay
12:45 – 1:00	Team Out Brief Development
1:00 – 1:30	Debrief and Brainstorming Scoring

WARGAME TEAMS

- 3 TEAMS: 2 ATTACKING,1 DEFENDING
- IDEAL COMPOSITION IS 15: 4-4-7
- ALL TEAMS COMPETE, ARE SCORED, WITH A WINNER
- EACH TEAM ROLE-PLAYS WITH VARYING MOTIVATION, RESPONSIBILITIES, ASSETS

Team 1: Nation State

Team 2: Hactivist

Team 3: Govt-Industrial Organization

WARGAME INFLUENCED BY REAL EVENTS

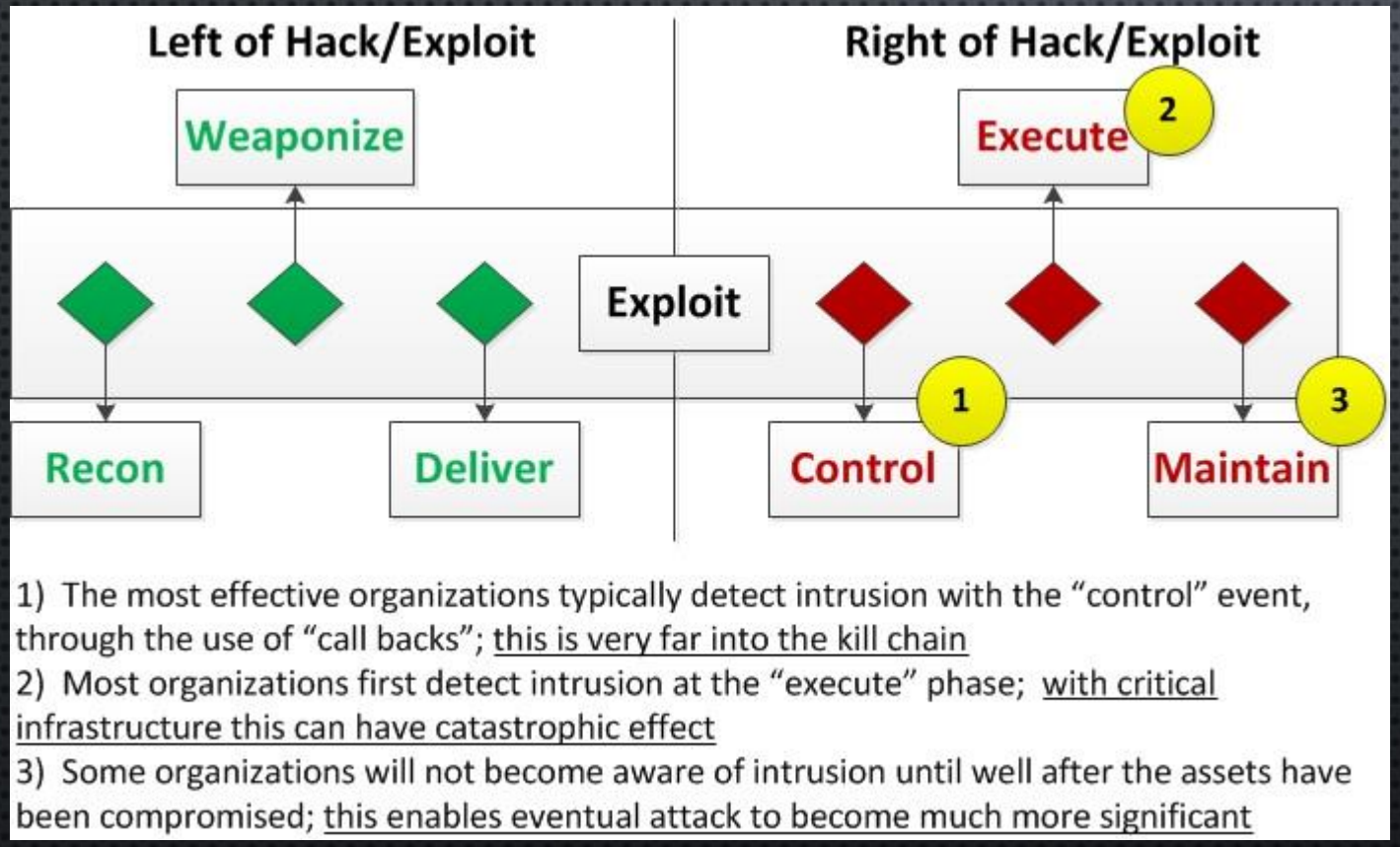
Influencing Event	Content
Stuxnet (2010)	• Industrial Control System Target • Pivot from Information Technology (IT) over to Operational Technology (OT)
HB Gary Federal (2011)	• Social Engineer Help Desk • Exfiltrate Sensitive Data
Numerous…	• Vulnerable Website Plugins • Machines exposed to internet • Permissive Firewalls inside company • Insider Threat • Open Ports, Services

OUR CYBER WARGAME – PLAYER COACHES

- PLAYER COACHES RESPONSIBLE FOR TOOLS, TECHNIQUES, EXECUTION
- USE DETAILED SCRIPTS FOR SEQUENCE, TIMING, SYNTAX
- PARTICIPANTS EASE INTO THEIR ROLES; SOME TAKE OVER

25 – 35	**Kill Chain Step 2- Weaponize** **Generate backdoor** • weevely generate -BACKDOOR PASSWORD- ~/BACKDOOR NAME.php **Prepare the deface page** • Use gedit to modify deface page. Open a terminal 1. `gedit index.html` 2. Type whatever the red team members wish in the text file. ▪ Their names, a taunt to the blue team, whatever ▪ Firefox index.html 3. cp index.html index.php **Prepare social engineering story** • Browse fake facebook page, gain understanding of DB admin • Goal is find name, DoB, address, phone number (new) • Challenge team to construct story to make their case more believable • Call helpdesk for attempt
35 – 45	**Kill Chain Step 3- Deliver** • Take backdoor script and upload using WordPress exploit • Log in with credentials as user –pw: Password1 • Upload backdoor through file upload, Create good name
40 – 50	**Kill Chain Step 4- Exploit** • Explain that a backdoor has been uploaded and we must now connect to it • Open terminal and type: 1. `weevely terminal http://web.epi.com/wp-content/uploads/user_uploads/user/BACKDOOR NAME.php BACKDOOR PASSWORD` **SPOOF IP Address**

METHODOLOGY FOR OPERATIONS



1) The most effective organizations typically detect intrusion with the "control" event, through the use of "call backs"; this is very far into the kill chain
2) Most organizations first detect intrusion at the "execute" phase; with critical infrastructure this can have catastrophic effect
3) Some organizations will not become aware of intrusion until well after the assets have been compromised; this enables eventual attack to become much more significant

SAIC CYBER SECURITY EDGE™

- DISCOVER
  - DETECT INTRUSIONS, OTHER CONCERNING ACTIVITY
- MITIGATE
  - BLOCK ACTIVE ATTACKS; SHUT DOWN VULNERABILITIES
- MANAGE
  - KEEP CRITICAL SYSTEMS UP

Cyber Kill Chain based on: http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html

Cyber Security Edge: https://www.saic.com/services-solutions/technology-solutions/cybersecurity

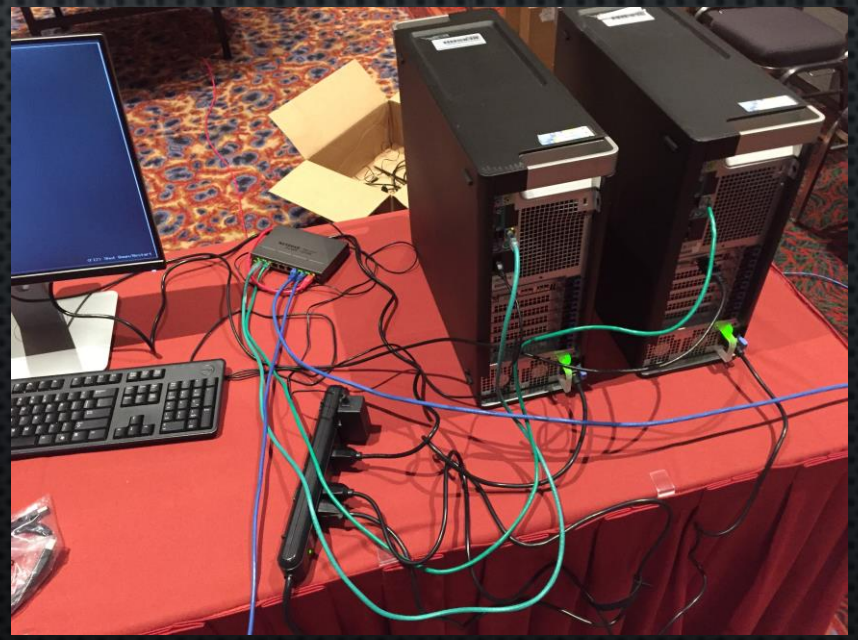
INBRIEF, OUTBRIEF, PLAYER ENABLEMENT

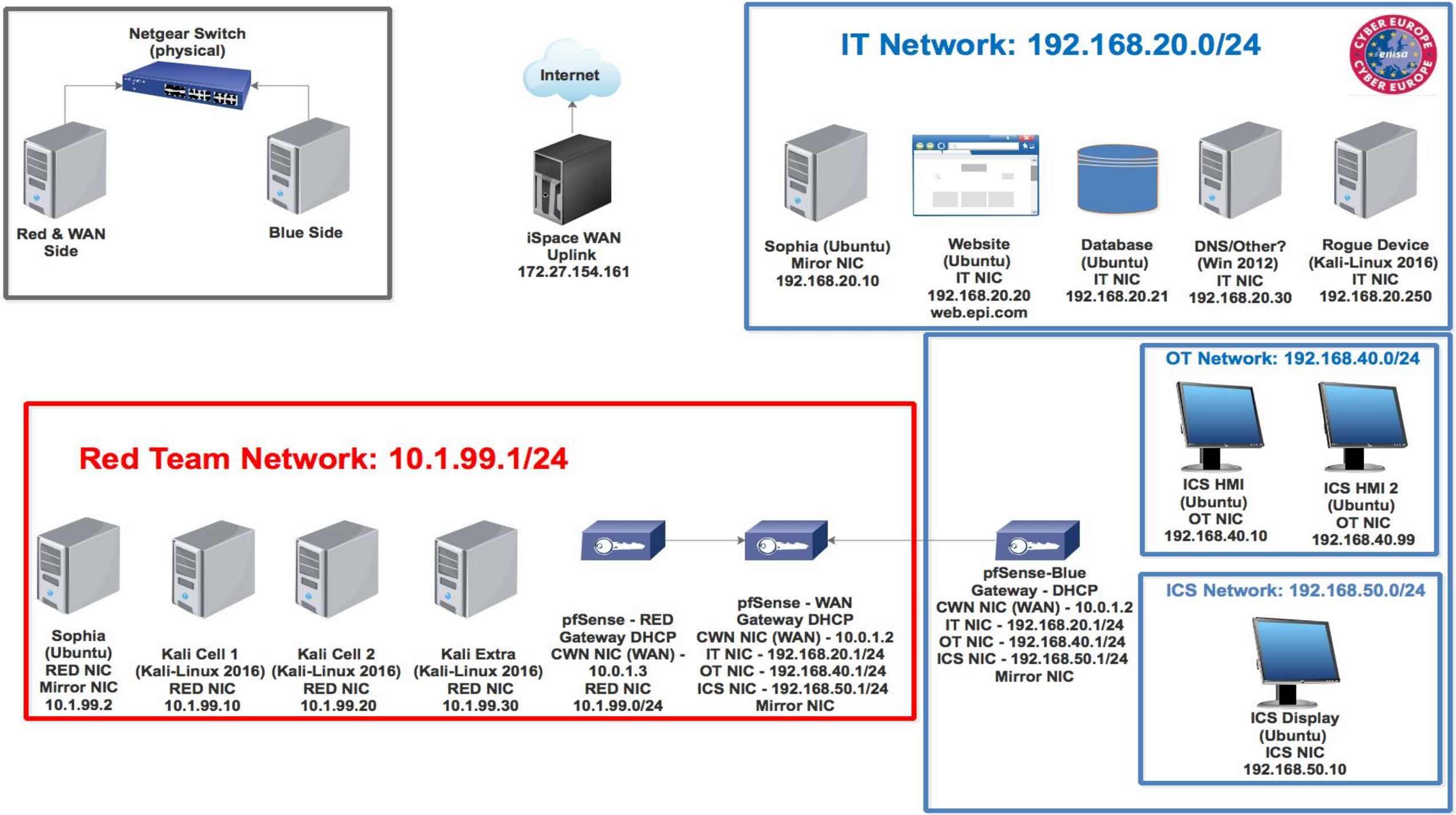
- Most players walk in with little to know understanding
- At 2 hour mark, players with no prior experience are presenting on cyber kill chain, technical vs. social vectors, lessons learned, applicability to their role, and other informed, nuanced cyber concepts

GAME ARCHITECTURE

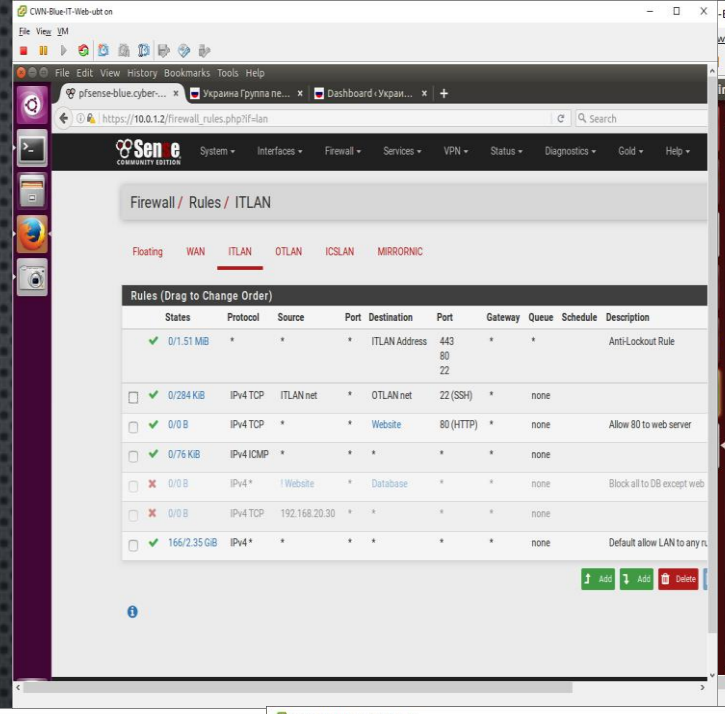
- Virtualized platform; VMware vSphere
- pfSense Routing, Firewalls
- Physical switches for laptop connection to game environment
- Red team network mimics internet
- multiple blue team nets emulating an industrial corporation with asset segmentation
- Modified open source emulation of oil refinery
  - Modbus/TCP communications
- Vulnerable web and ftp servers
- Attackers pivot from IT over to OT
- Persistent environment located at Reston, VA lab
- Separate roadshow environment which we take to conferences/remote locations

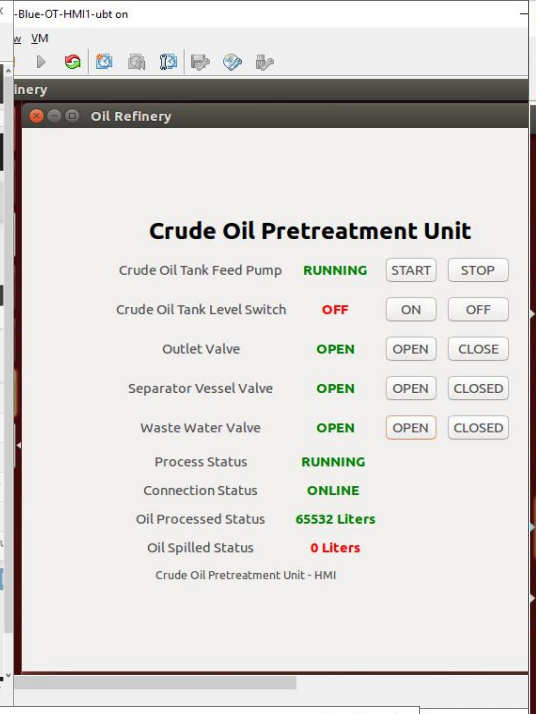
Vendor + Product
VMWare vSphere Server and Client
Offensive Security Kali Linux
NexDefense Sophia
pfSense
Ubuntu Server for Web, DNS, Mail
WordPress, MySql
Open Source / github.com/jseidl/virtuaplant

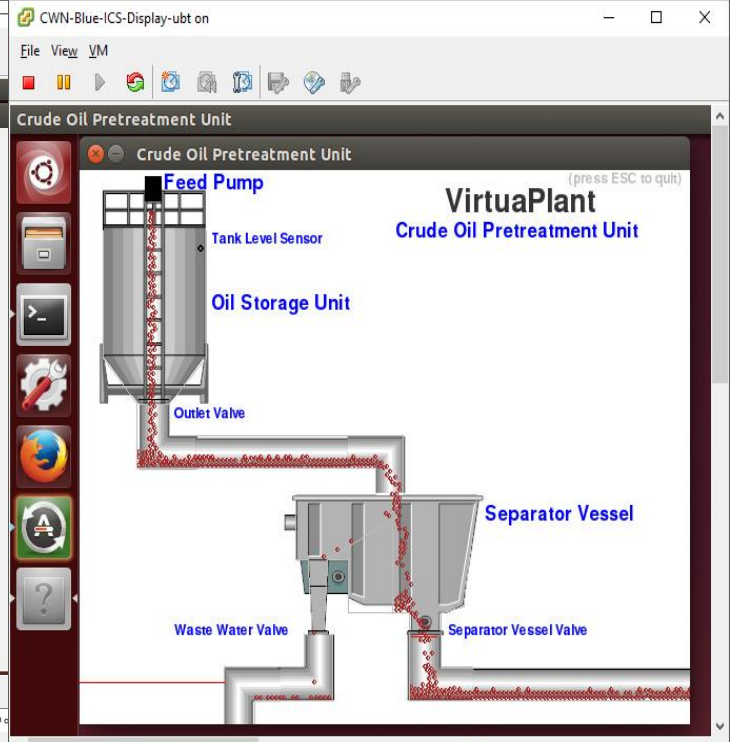


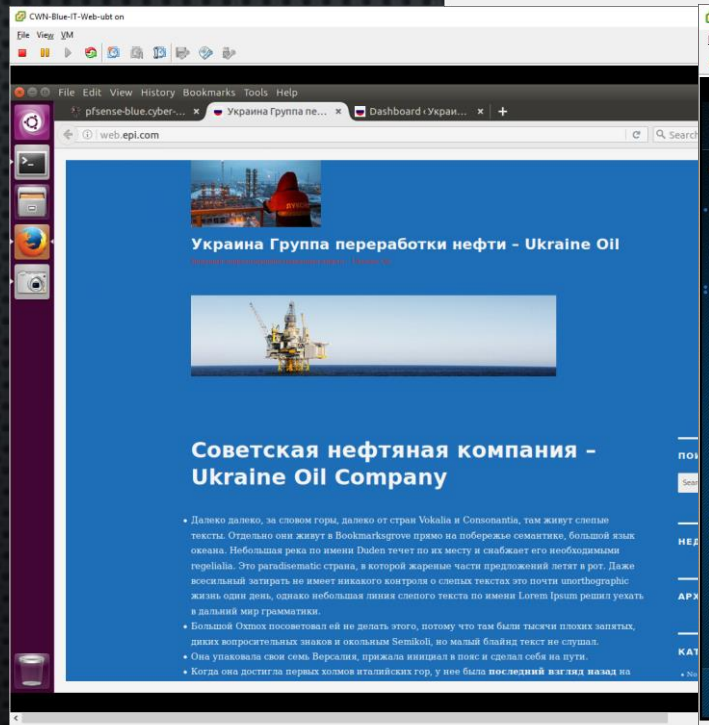

Netgear Switch
(physical)
Red & WAN
Side
Blue Side
Internet
iSpace WAN
Uplink
172.27.154.161
IT Network: 192.168.20.0/24
Sophia (Ubuntu)
Miror NIC
192.168.20.10
Website
(Ubuntu)
IT NIC
192.168.20.20
web.epi.com
Database
(Ubuntu)
IT NIC
192.168.20.21
DNS/Other?
(Win 2012)
IT NIC
192.168.20.30
Rogue Device
(Kali-Linux 2016)
IT NIC
192.168.20.250
OT Network: 192.168.40.0/24
ICS HMI
(Ubuntu)
OT NIC
192.168.40.10
ICS HMI 2
(Ubuntu)
OT NIC
192.168.40.99
ICS Network: 192.168.50.0/24
ICS Display
(Ubuntu)
ICS NIC
192.168.50.10
pfSense-Blue
Gateway - DHCP
CWN NIC (WAN) - 10.0.1.2
IT NIC - 192.168.20.1/24
OT NIC - 192.168.40.1/24
ICS NIC - 192.168.50.1/24
Mirror NIC
Red Team Network: 10.1.99.1/24
Sophia
(Ubuntu)
RED NIC
Mirror NIC
10.1.99.2
Kali Cell 1
(Kali-Linux 2016)
RED NIC
10.1.99.10
Kali Cell 2
(Kali-Linux 2016)
RED NIC
10.1.99.20
Kali Extra
(Kali-Linux 2016)
RED NIC
10.1.99.30
pfSense - RED
Gateway DHCP
CWN NIC (WAN) -
10.0.1.3
RED NIC
10.1.99.0/24
pfSense - WAN
Gateway DHCP
CWN NIC (WAN) - 10.0.1.2
IT NIC - 192.168.20.1/24
OT NIC - 192.168.40.1/24
ICS NIC - 192.168.50.1/24
Mirror NIC

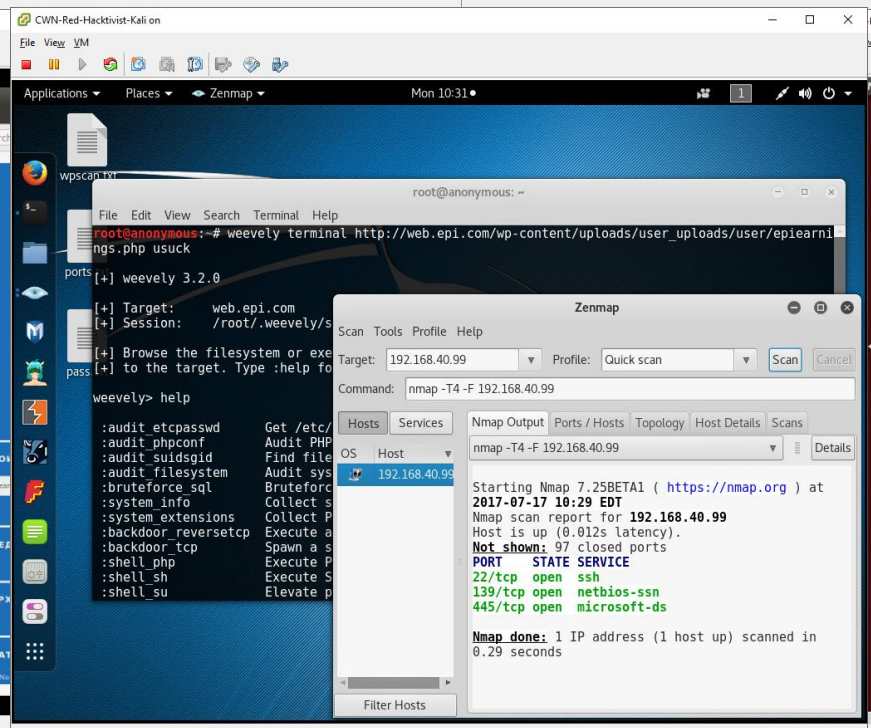
GAME CONTENT

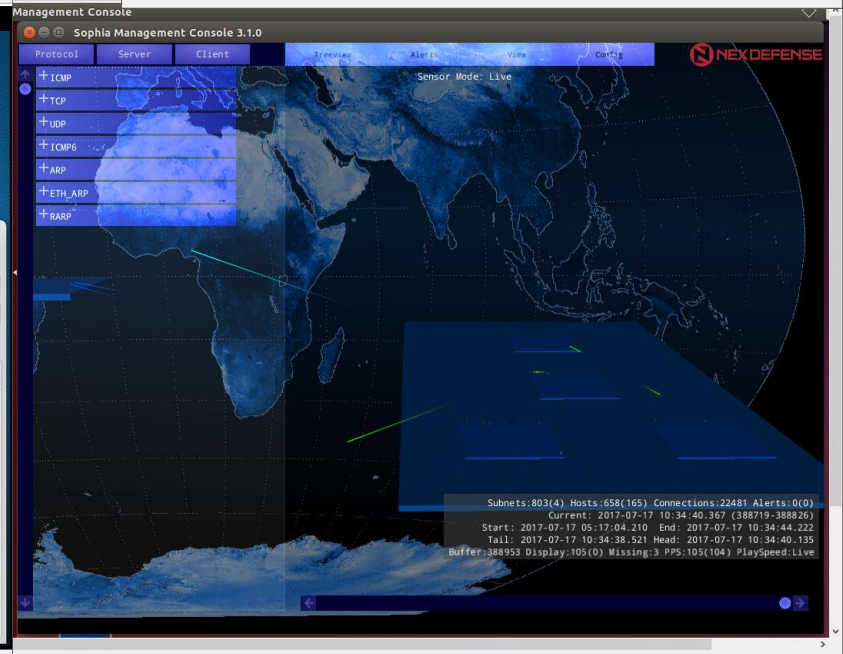




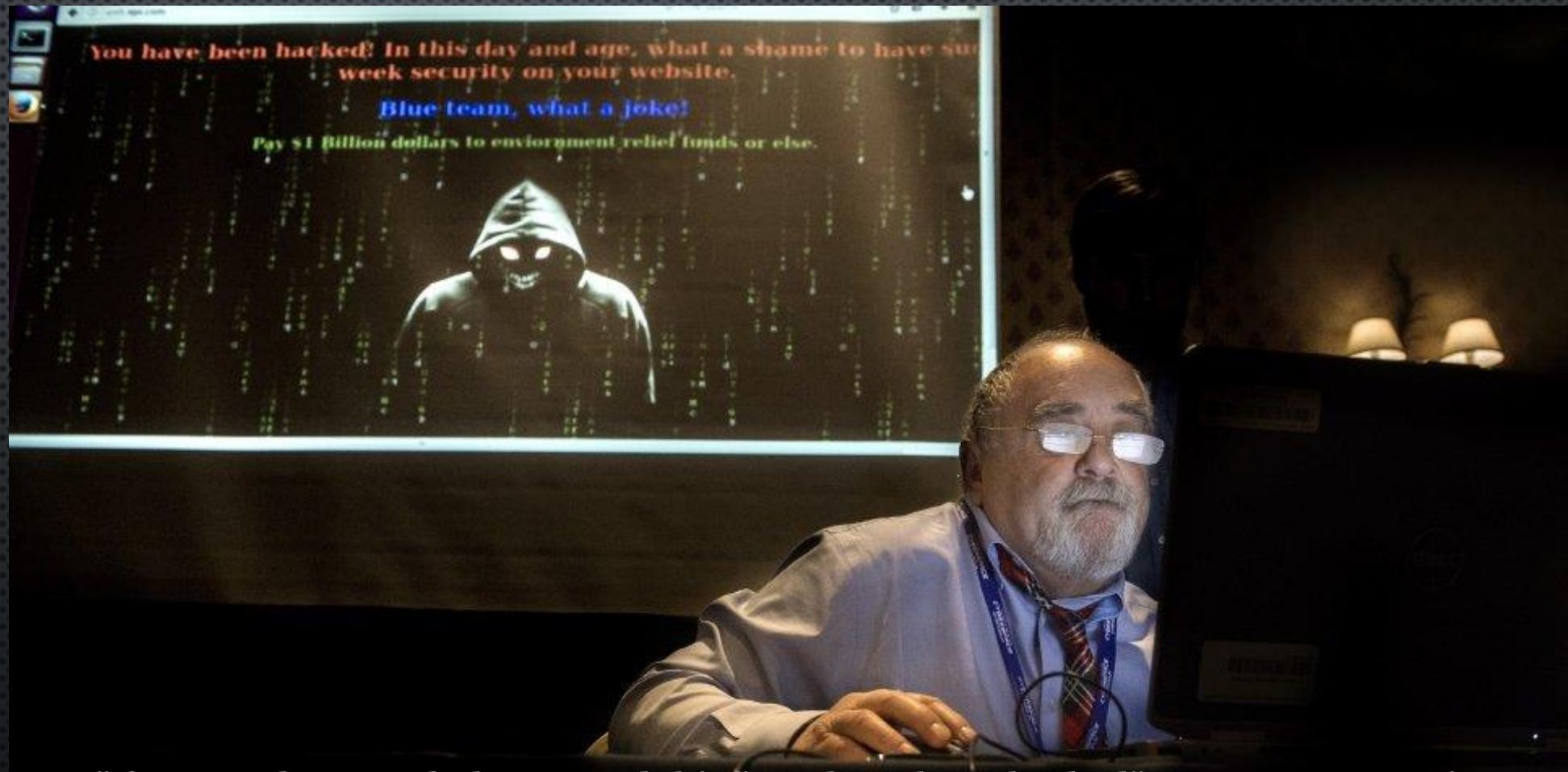








WARGAME IN PICTURES



...works to defend the "Blue Team" from a cyber attack that posted this "You have been hacked" message on team's website during a cyber wargame exercise Monday, February 6, 2017 at the Rocky Mountain Cyberspace Symposium. Photo by Mark Reis, The Gazette

WARGAME IN PICTURES

..."Red Team" attacking the "Blue Team" during a cyber wargame exercise Monday, February 6, 2017 at the Rocky Mountain Cyberspace Symposium. Photo by Mark Reis, The Gazette

WARGAME IN PICTURES

The "Red Team Field Manual" during a cyber wargame exercise Monday, February 6, 2017 at the Rocky Mountain Cyberspace Symposium. Photo by Mark Reis, The Gazette

WARGAME IN PICTURES

"Red Team" members, ... work to attack the "Blue Team" during a cyber wargame exercise Monday, February 6, 2017 at the Rocky Mountain Cyberspace Symposium. Photo by Mark Reis, The Gazette

WARGAME ROADSHOW: BASIC ROOMS, COMMODITY HARDWARE

Generic conference center room; Zach Kleine (SAIC), wargame lead pictured

WARGAME USE-CASE: ENHANCE YOUR BRAND

Typical Corporate Booth, but powered with wargame; Ray Caetano (SAIC), Jake Kleine (SAIC)

GAME EVOLUTION

Game Iteration	How did we evolve?
2016-July: Board of Directors	• Designed game for cyber novices • Converted attack/defense demo into a scripted, team-based activity • Introduced multiple social vectors
2017-January: Vendor Alliance Partners	• Enhanced content to appeal to technical audience
2017-February: AFCEA Cyber Symposium	• Ported environment to roadshow hardware • Made material professional quality
2017-June: GEOINT 2017 Symposium	• Tailored attack and defense to include IP/geospatial content
2017-July: Internal Corporate Staff	• Enhanced social media content • Implemented survey for metrics capture
2017-August: TechNet 2017	• Tailored for military support for allied government, critical infrastructure

RESULTS

Game Use Case	Stakeholder	Results
Education	Non-Technical Corporate Staff	• Increased awareness of social engineering • Improved understanding of recruiters for cyber skills
Education	Technical Community	• Sharpened offensive and defensive skills with hands-on, live access • Exposure to industry best practice operational frameworks
Brand Awareness	Conference Attendees	• Senior-level customer has asked for gaming proposal • Have 40 military staff signups for upcoming training
Opportunity Generation	Targeted Customers	• Senior-level customer provided detailed insight on current gaps, best strategies for engaging
Alliance Strengthening	Partner Program	• Invitation by a partner to bring game to vendor event

RESULTS

"more now (cyber understanding) after the game, interesting how social engineering can make such an impact" – contracts associate

"A lot of fun!!!!" – senior recruiter

"Cyber security is paramount to day to day operations" – pricing analyst

"[I can now better recruit for defensive and offensive cyber operations staff because I better understand what they do]" - recruiter

"[this is one of our agency's top four strategic research priorities…we look forward to you submitting a paper]" – Director of Innovation, Government Agency

"this is cool" – Deputy Director of National Intelligence

Where is this headed?

- More efficient roadshow equipment (single server, all laptops)
- Support for Additional game seats
- More targets to support MitM attacks
- More Networks and assets to mimic integrated government/industrial assets
- Internet of Things assets for both attack and defense
- Strengthening of Alliance Partner Content
- Integration with company IR&D product for internet simulation, OSINT, Scenario Automation

I'd like to thank Black Hat for hosting me.

I'd like to thank all of you for listening ☺

My contact info:

- @jasenich
- Jason.a.nichols@saic.com