DEFENDING TOMORROW'S INFRASTRUCTURE TODAY

Argonne NATIONAL LABORATORY

CATALYZING CYBER SECURITY INNOVATION THROUGH CYBER DEFENSE COMPETITIONS

JENNIFER FOWLER
Cyber Security Analyst
jfowler@anl.gov
630-252-8707

AMANDA JOYCE
Cyber Security Analyst
amanda@anl.gov
630-252-3470

July 17, 2017 – Paris, France

CURRENT PROBLEM

- The Cyber Security Workforce continues to experience unprecedented shortages.
  - The ISACA, a non-profit information security advocacy group, predicts there will be a global shortage of two million cyber security professionals by 2019.[1]
- Finding and training professionals with the skills to keep pace with the constantly-changing threat landscape and ever-evolving state of Information Technology is a challenge faced by National Laboratories and the private sector alike.

[1] Kauflin, J. (2017, March 16). *The Fast-Growing Job With A Huge Skills Gap: Cyber Security*. Retrieved June 23, 2017, from https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/#33eabbf65163

PROPOSED SOLUTION

- Create an unique and challenging competition for the collegiate academia to begin cyber security workforce development.
- Hands-on learning and experience with real world scenarios
- Cyber-physical cause and effect of defense implementations
- Encourage innovated out-of-the-box defense strategies

WHAT IS A CYBER DEFENSE COMPETITION

- A Cyber Defense Competition (CDC) is a competition that focuses on the defensive/hardening nature of cyber security. A typical CDC has a Blue Team (defenders) that protects a network infrastructure from the Red Team (attackers). A blue team consists of high school or college students who secure and harden their competition system. A red team consists of students or industry professionals that work to cause cyber destruction to the blue teams' network infrastructures. The competition is scored utilizing a point system. Points can be both given and taken away depending on the actions or lack of action from both blue and red teams. The blue team with the most points at the end of the competition is declared the winner of the event.

CYBER DEFENSE COMPETITION

Exponential Growth and Interest in One Year

2017 STATISTICS

- 27 teams registered
- 15 competing teams
- 20 unique universities
  - 6 returning schools
- 9 different states
- 100 volunteers
  - Red
  - Green
  - Pink
  - White

2016 STATISTICS

- 9 teams registered in 2016
- 8 competing teams
- 7 unique universities
- 2 different states
- 20 volunteers
  - Red
  - Green
  - White

CYBER DEFENSE COMPETITION

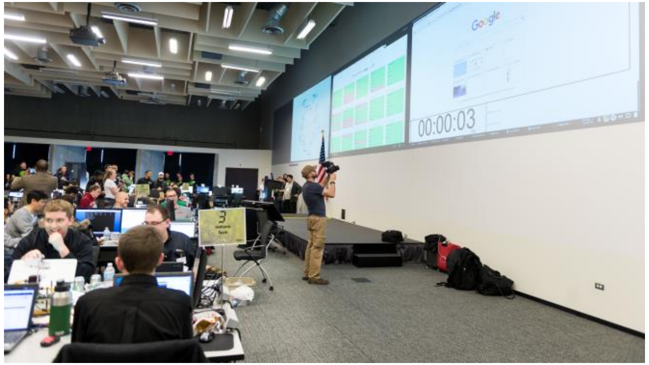
Team Breakdown

BLUE TEAM

- Students of universities that are tasked to defend their networks from exploitation.

WHITE TEAM

- Individuals that assist the teams in their technical setup of infrastructure.



CYBER DEFENSE COMPETITION

Team Breakdown

PINK TEAM

- Individuals who are mentored on what the attackers are doing throughout the day.

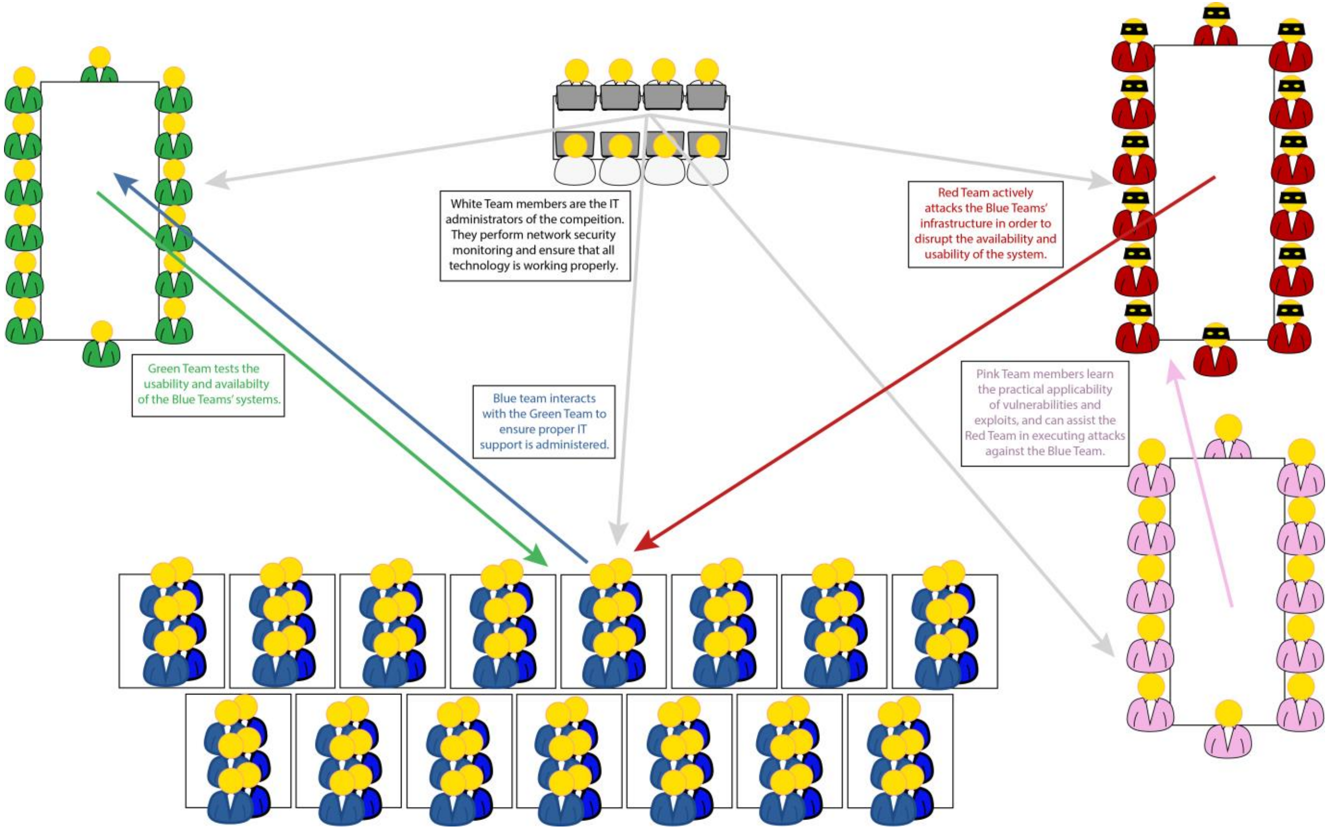
GREEN TEAM

- Individuals who play the role of a typical user of the system.

RED TEAM

- Individuals with technical background that play the role of the attacker.

COMMUNICATION CHANNELS



White Team members are the IT administrators of the compeition. They perform network security monitoring and ensure that all technology is working properly.

Red Team actively attacks the Blue Teams' infrastructure in order to disrupt the availability and usability of the system.

Green Team tests the usability and availabilty of the Blue Teams' systems.

Blue team interacts with the Green Team to ensure proper IT support is administered.

Pink Team members learn the practical applicability of vulnerabilities and exploits, and can assist the Red Team in executing attacks against the Blue Team.

CYBER DEFENSE COMPETITION

Energy-focused Scenarios with a Physical Device

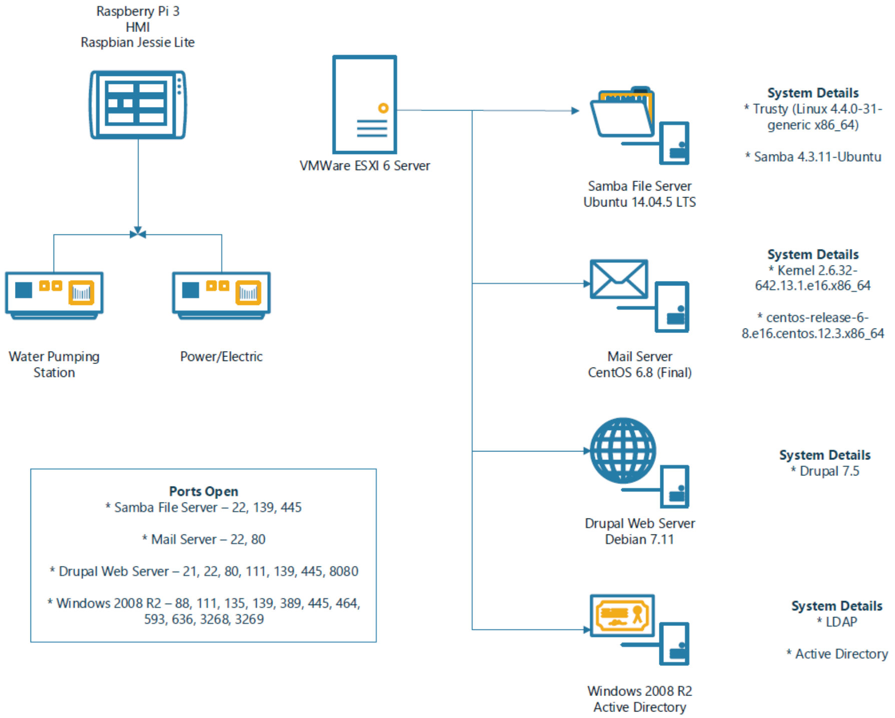
2018 CYBER DEFENSE COMPETITION ARGONNE NATIONAL LABORATORY

2017 CYBER DEFENSE COMPETITION ARGONNE NATIONAL LABORATORY

2016 CYBER DEFENSE COMPETITION ARGONNE NATIONAL LABORATORY

- Oil and Natural Gas Fracking
- Water and Power Delivery System
- Corporate Energy Distribution

PROVIDED ENVIRONMENT TO BLUE TEAM



Raspberry Pi 3
HMI
Raspbian Jessie Lite

Water Pumping
Station

Power/Electric

VMWare ESXI 6 Server

Samba File Server
Ubuntu 14.04.5 LTS

System Details
* Trusty (Linux 4.4.0-31-generic x86_64)

* Samba 4.3.11-Ubuntu

Mail Server
CentOS 6.8 (Final)

System Details
* Kernel 2.6.32-642.13.1.e16.x86_64

* centos-release-6-8.e16.centos.12.3.x86_64

Drupal Web Server
Debian 7.11

System Details
* Drupal 7.5

Windows 2008 R2
Active Directory

System Details
* LDAP

* Active Directory

Ports Open
* Samba File Server – 22, 139, 445

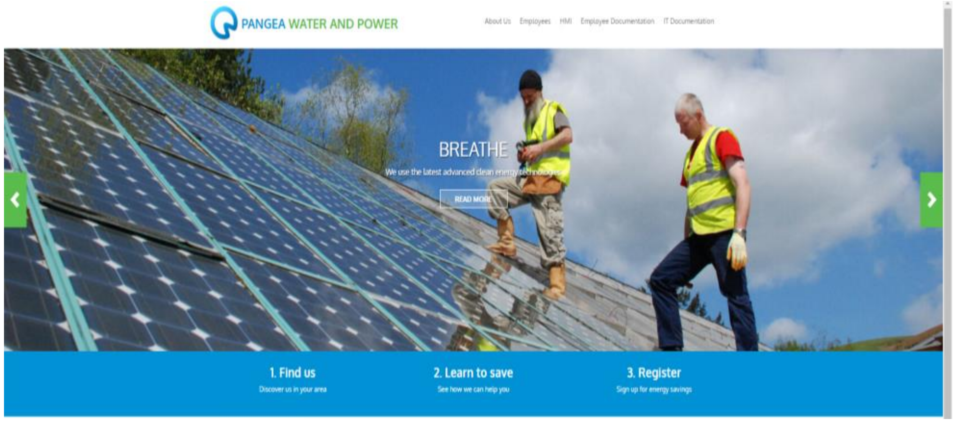
* Mail Server – 22, 80

* Drupal Web Server – 21, 22, 80, 111, 139, 445, 8080

* Windows 2008 R2 – 88, 111, 135, 139, 389, 445, 464, 593, 636, 3268, 3269

BLUE TEAM REQUIREMENTS

- Services required to run at all times included:
  - Website/Web Server
  - Help Desk
  - Email Server
  - File Server
  - Active Directory Server
  - Human Machine Interface
  - Industrial Control System
- Encouragement on Unique Defenses of their networks



BREATHE

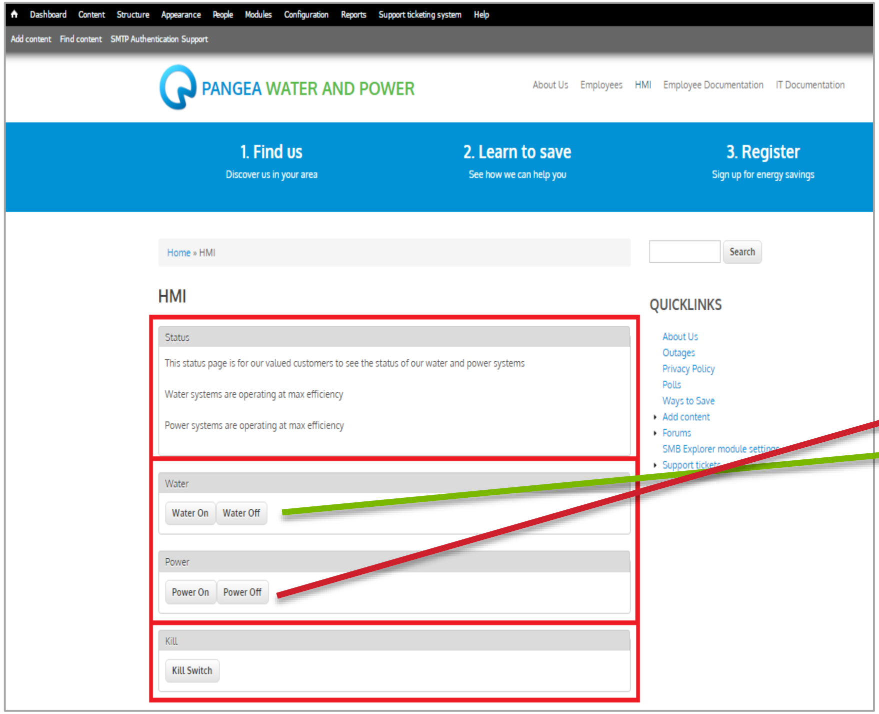
We use the latest advanced clean energy technologies

1. Find us
Discover us in your area

2. Learn to save
See how we can help you

3. Register
Sign up for energy savings

HUMAN MACHINE INTERFACE



Dashboard Content Structure Appearance People Modules Configuration Reports Support ticketing system Help

Add content Find content SMTP Authentication Support

PANGEA WATER AND POWER

About Us Employees HMI Employee Documentation IT Documentation

1. Find us
Discover us in your area

2. Learn to save
See how we can help you

3. Register
Sign up for energy savings

Home » HMI

Search

HMI

Status

This status page is for our valued customers to see the status of our water and power systems

Water systems are operating at max efficiency

Power systems are operating at max efficiency

Water

Water On Water Off

Power

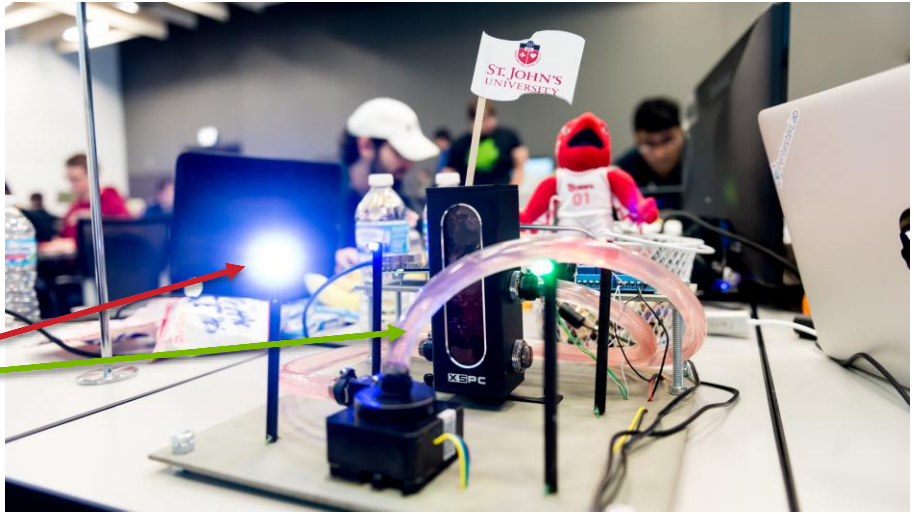
Power On Power Off

Kill

Kill Switch

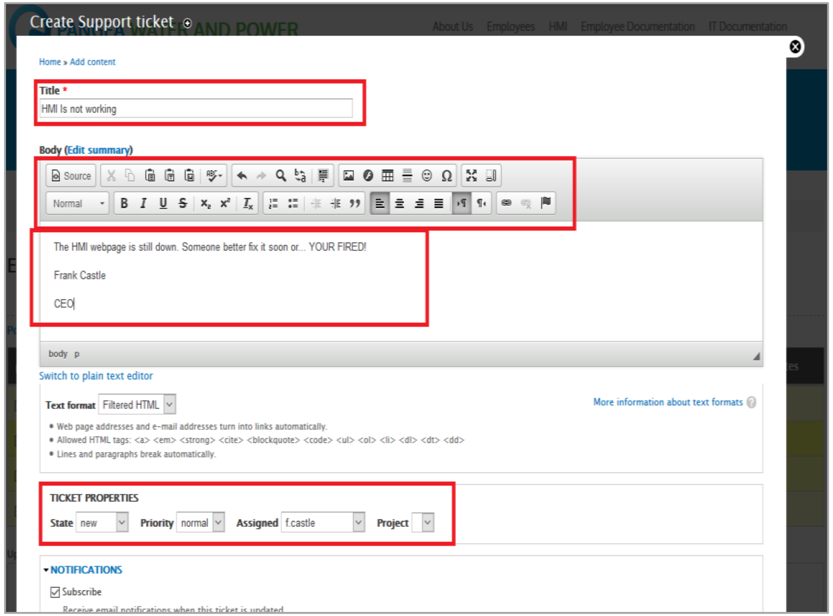
QUICKLINKS

- About Us
- Outages
- Privacy Policy
- Polls
- Ways to Save
- Add content
- Forums
- SMB Explorer module settings
- Support tickets



USABILITY CONSTRAINTS

- Blue team had to maintain functionality so that users could still:
  - Log in
  - Upload and download files
  - Add Comment to Posts
  - Access ICS HMI
  - Request support through help desk
  - Answer a request from help desk



Title *
HMI Is not working

Body (Edit summary)

The HMI webpage is still down. Someone better fix it soon or... YOUR FIRED!

Frank Castle

CEO

Text format: Filtered HTML

- Web page addresses and e-mail addresses turn into links automatically.
- Allowed HTML tags: <a> <em> <strong> <cite> <blockquote> <code> <ul> <ol> <li> <dl> <dt> <dd>
- Lines and paragraphs break automatically.

TICKET PROPERTIES

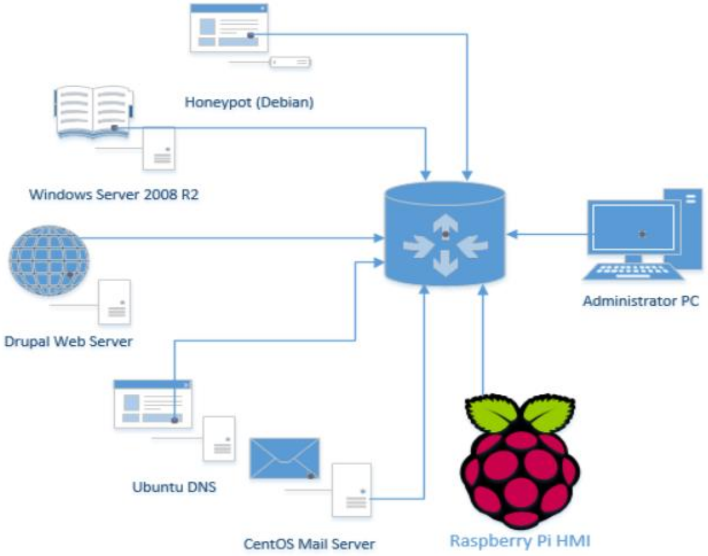
State: new　Priority: normal　Assigned: f.castle　Project:

☑ Subscribe

Receive email notifications when this ticket is updated

UNIQUENESS IN DEFENSE

- Teams added their own unique defenses such as:
  - Hosting the web application inside of Docker
  - Rewriting authentication scripts
  - Isolating mail servers
  - “Jailing” services and users to containers
  - Adding “banned” constraints
  - Adding honeypots
  - Custom written operating systems



PROFESSIONAL DEVELOPMENT

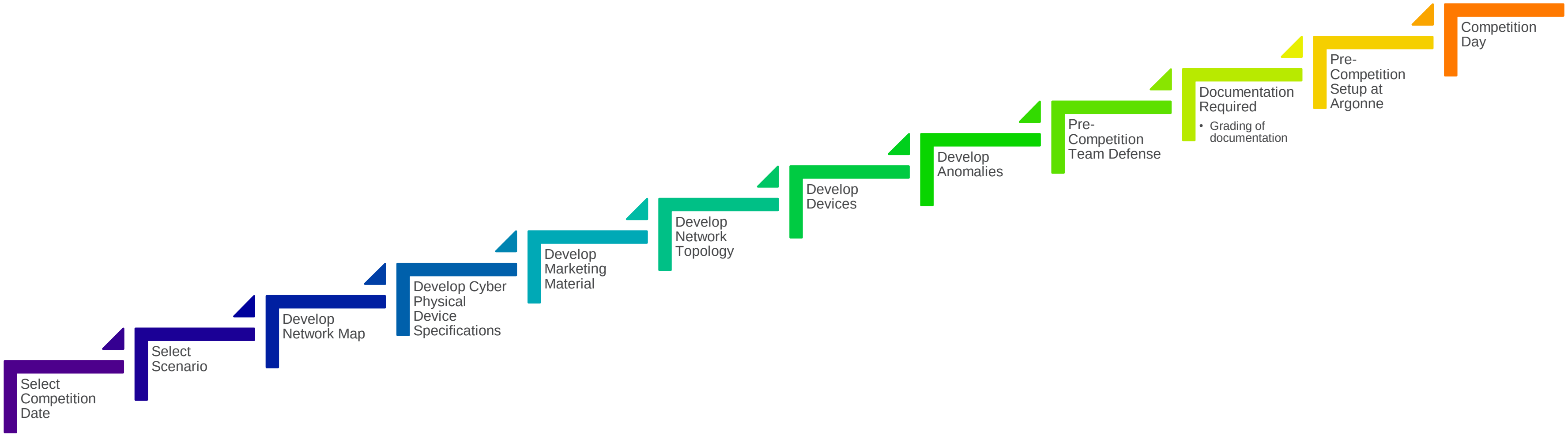
- Teams are required to provide
  - Documentation on their networks
  - User manual documentation
  - 5 minute presentation to both technical and non-technical group
- All these items are required by a specific deadline and the teams are graded on
  - Professionalism
  - Creativity
  - Uniqueness
  - Readability
  - Clarity
  - Completeness
  - Supporting diagrams

REAL WORLD COMPLICATIONS

- Besides the normal defense and operations of the system, there are “anomalies” that are provided that a real-world administrator may come into play.

- For example,
  - Administrators are called into a standing meeting for 20 minutes.
  - Teams are asked for a quick turn on a specific threat seen.
  - Teams are asked to change their architecture for no apparent reasoning.
  - Website upgrades
  - “FUN” crypto games
  - Red teams have ability to roam room for shoulder surfing.

TIMELINE



Select Competition Date

Select Scenario

Develop Network Map

Develop Cyber Physical Device Specifications

Develop Marketing Material

Develop Network Topology

Develop Devices

Develop Anomalies

Pre-Competition Team Defense

Documentation Required

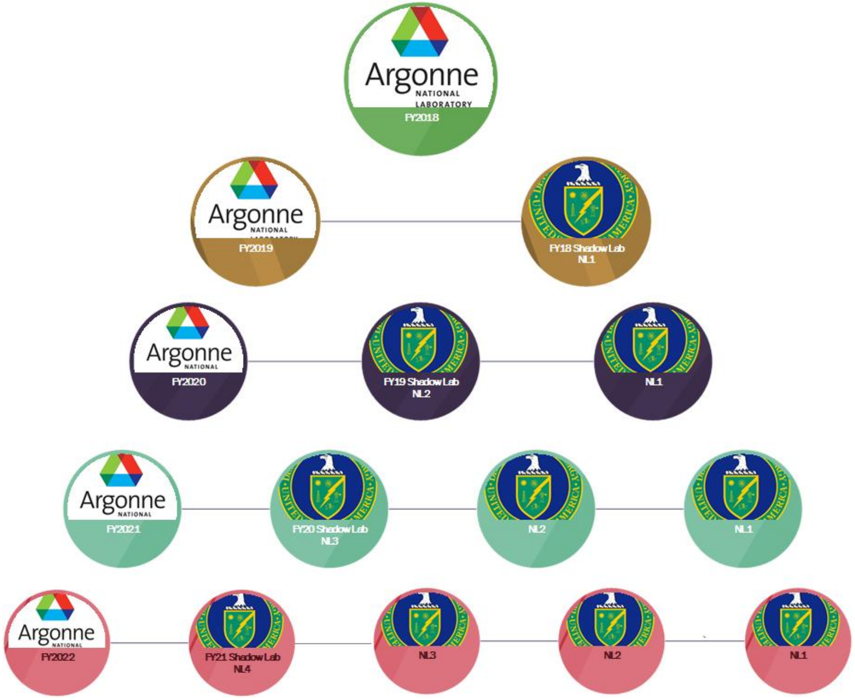
- Grading of documentation

Pre-Competition Setup at Argonne

Competition Day

FUTURE GROWTH PLAN

- The goal is to expand this to multiple laboratories.
- Current Layout
  - April 2018
    - Argonne National Laboratory
      - *Pacific Northwest National Laboratory (Shadow Lab)*
      - *Oak Ridge National Laboratory (Shadow Lab)*
  - October 2018
    - All three laboratories synchronize their event.



QUESTIONS OR COMMENTS?

Jennifer Fowler – jfowler@anl.gov

Amanda Joyce – amanda@anl.gov

https://coar.risc.anl.gov
https://cyberdefense.anl.gov