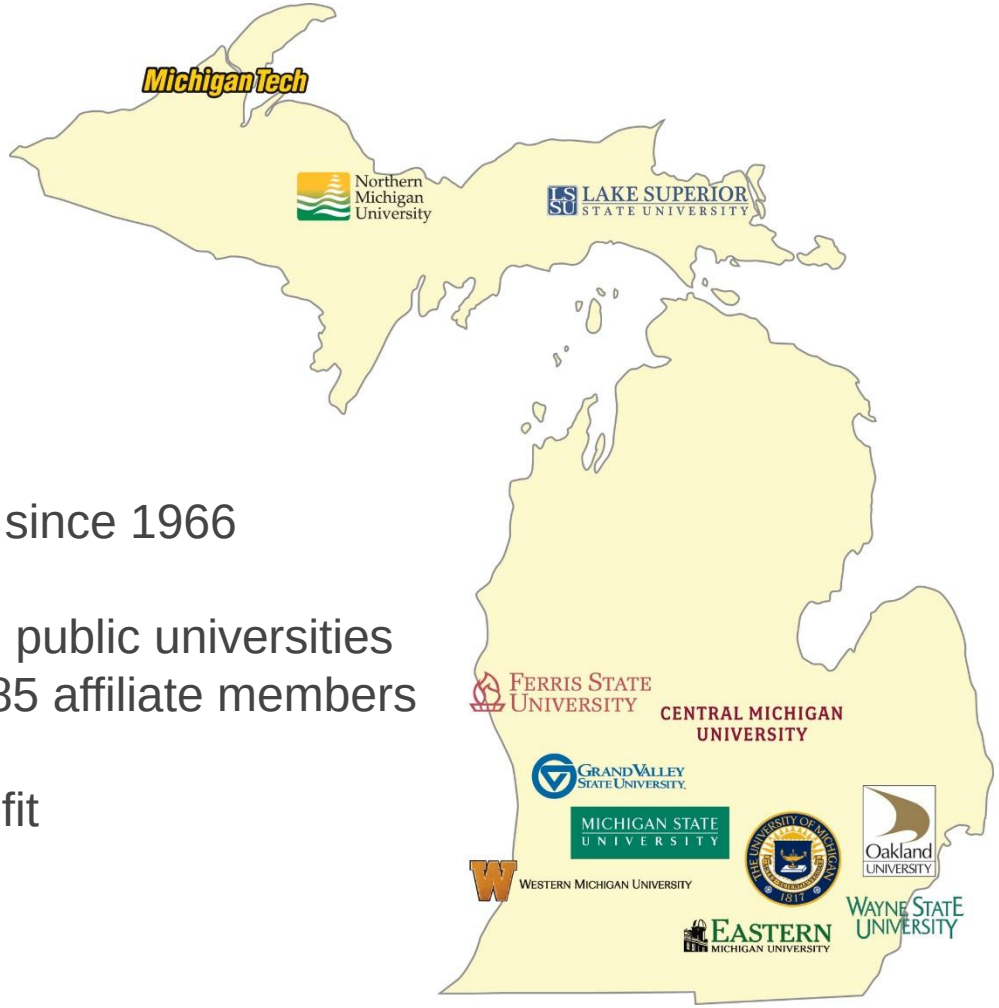
Cyber Threats & Alphaville

Jameka Williams

“Cyber Security – The Why and the How”

How Big was the CS Threat in 2014

Introduction



Merit

Member owned since 1966

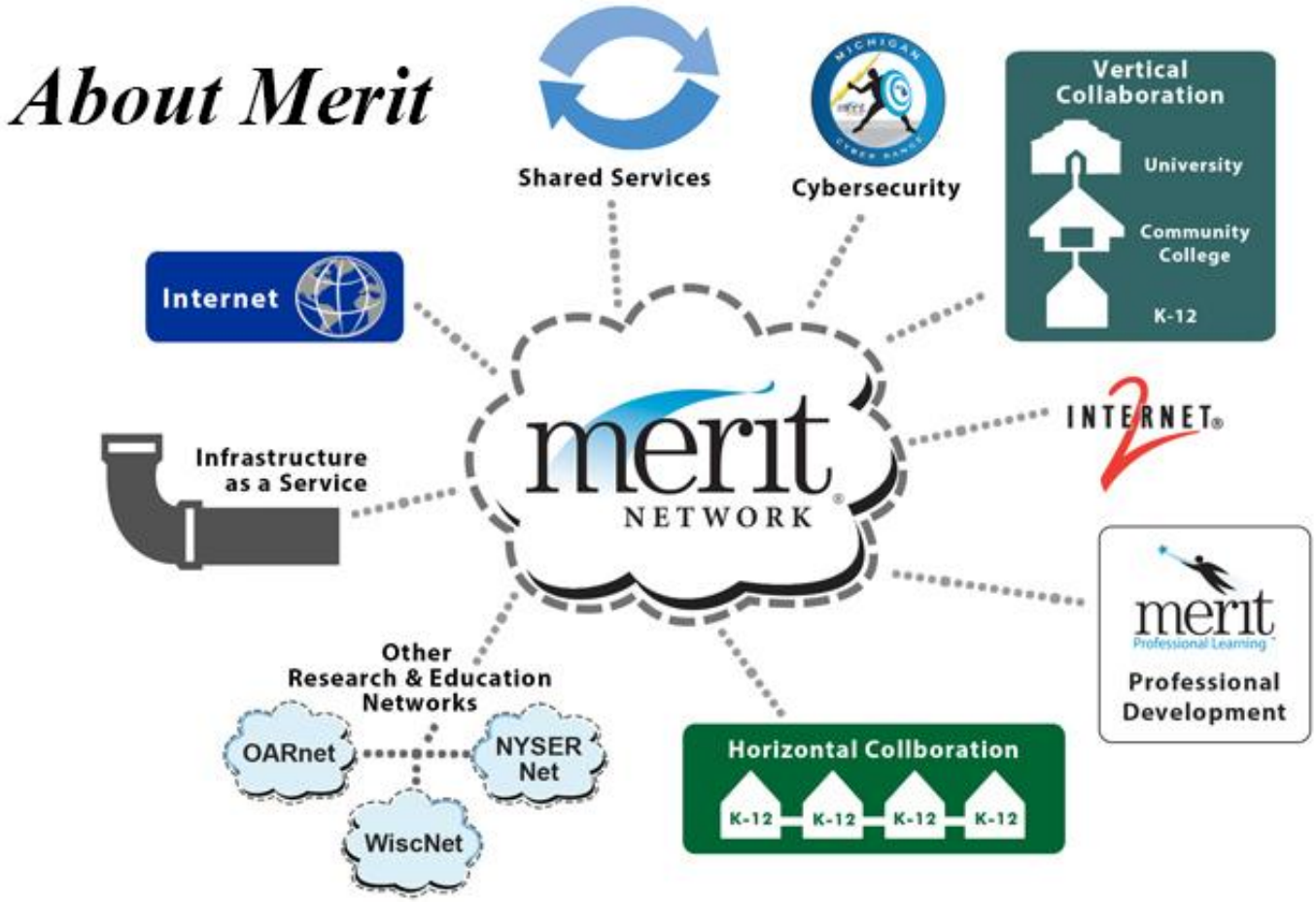
Governed by 12 public universities
Supported by 285 affiliate members

501(c)3 non-profit

MICHIGAN merit CYBER RANGE

Powerd by merit

Introduction



Background

- Merit Network – Sales Manager
  - Commercial Focus for Transport Services & Security Portfolio
- Michigan Cyber Range
  - Sales & Product Development

Governor Snyder's Strategy

Defend Michigan residents and commerce from cyber attacks

- Mitigate growing cyber threats
- Providing a more secure environment promotes economic development

Nurture a cyber security industry that leverages Michigan's unique advantages

- Educational institutions
- Large IT workforce
- Manufacturing and industrial base
- Federal cooperation and planning

Agenda

Why, What, How?

Threat

- Toward consumers and companies
- Work force shortage

Cyber Defense Requirements

- Realistic training environment
- Crawl-Walk-Run
- Team

Preparation Support

- Michigan Cyber Range

Tour of the Range

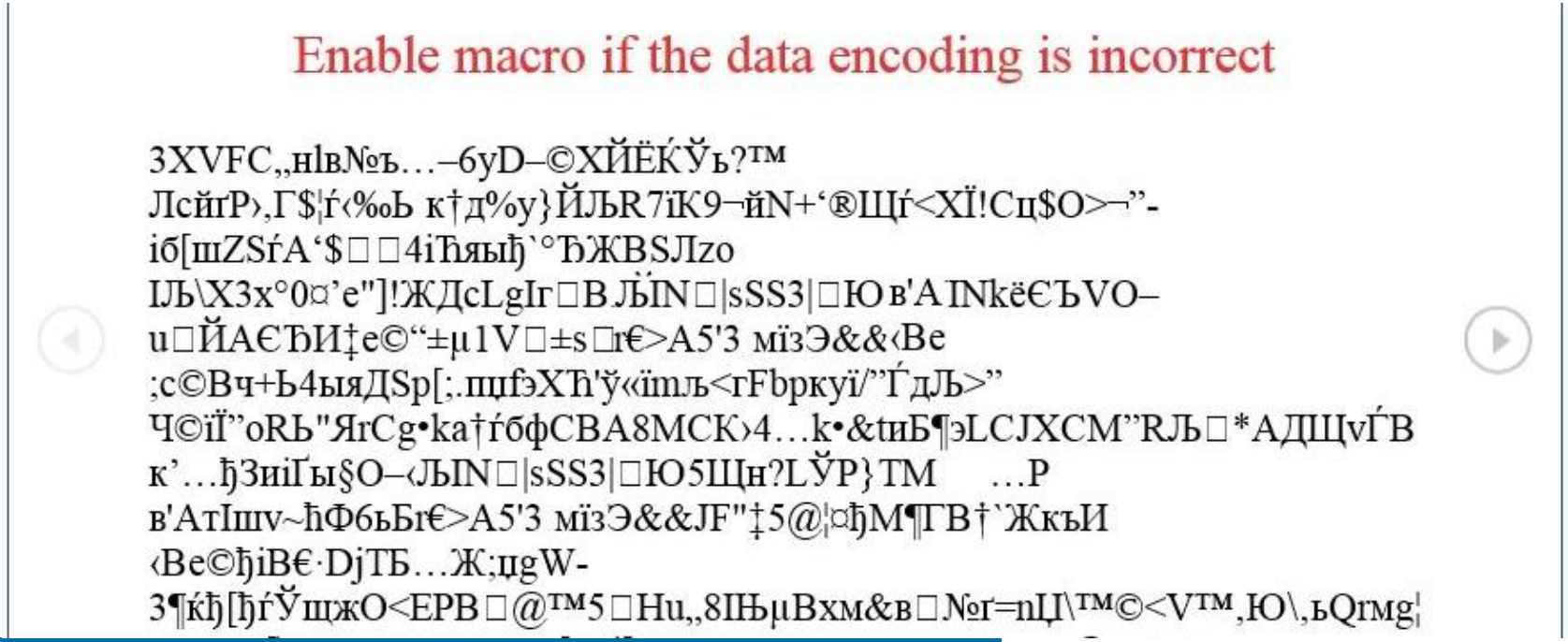
- Intro to Exercises & Classes

Ransomware

- Hospitals
  - Hollywood Presbyterian Medical Center in LA - $17,000
    - Patients were diverted to other area hospitals
  - Methodist Hospital in Henderson KY - $1,600
    - Hospital was moved to an “Internal State of Emergency”
    - Shutdown internal computers, servers and websites to contain outbreak
- Police Departments
  - Swansea, MA - $700
  - Midlothian, IL - $500
    - Encrypted local and backup files
- Utilities
  - Lansing Board of Water and Light

What Does It Do?

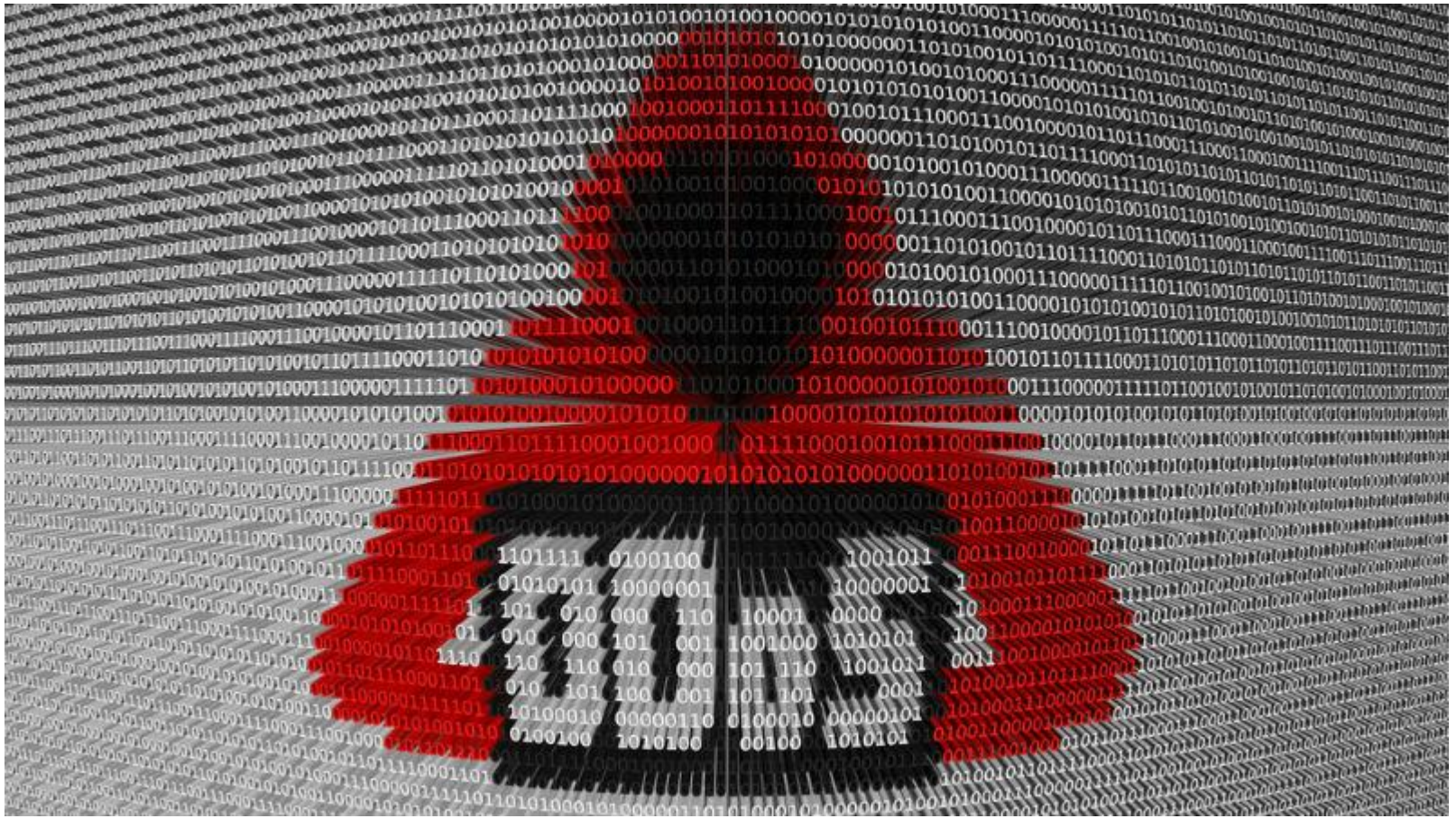
- CryptoLocker – 2013
  - Imitation is the highest form of flattery?
    - CryptoWall
    - TeslaCrypt – Exploited vulnerability in Adobe Flash
    - TorrentLocker – Spread through SPAM
- Common variant now “Locky”
  - Requires MS macros to be enabled or launched through JavaScript
- Encrypts files and folders
  - Desktops/Laptops
  - File shares
- Deletes original files



What Does Locky Look Like?

Must enable Microsoft Word macros to initiate payload

DDoS



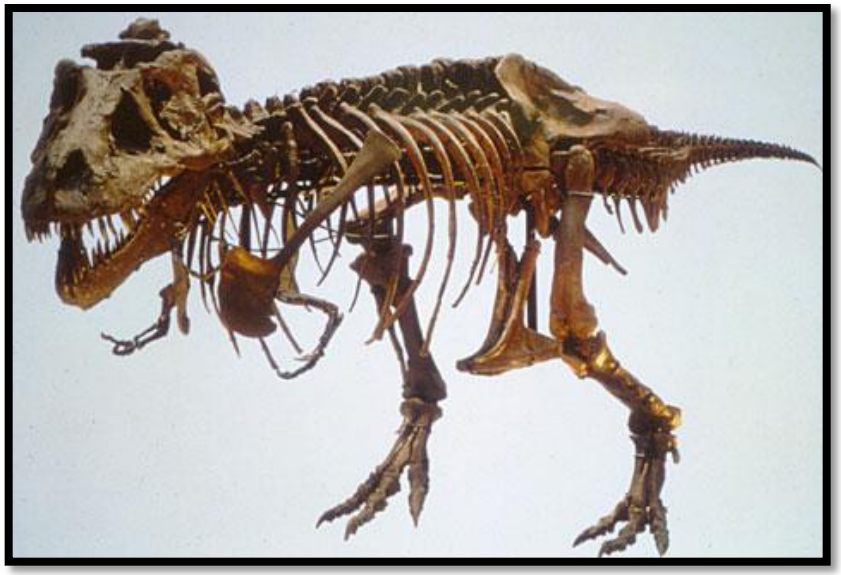
Phishing

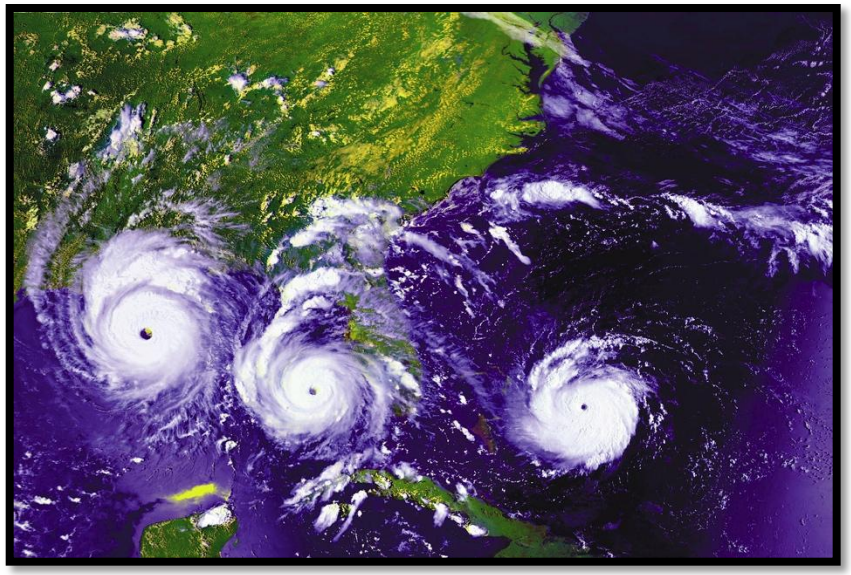
- Pomeroy investment company in Troy, MI
  - $495,000 transferred overseas to China
- As of March 31, 55 companies have released W-2's to unknown third parties

Another Day, Another Breach

- Wendy's – Class Action Lawsuit
- Credit card skimmers

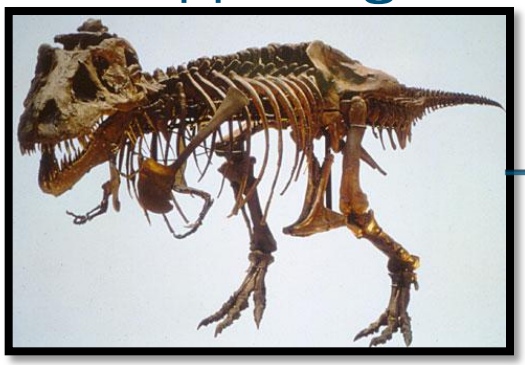
Paleontology versus meteorology





The missing link

What is happening



Why it's happening

What's going to happen next

Cyber security is not helping enough with this

Cyber Defense Needs

The Importance of CyberSecurity in Your Organization

Cyber Defense Needs

Worldwide spending on information security was $71.1 billion in 2014, an increase of 7.9 percent over 2013. (Gartner.com)

Total information security spending will grow a further 8.2 percent in 2015 to reach $76.9 billion. (Gartner.com)

43% said that their organization planned to add new IT staff positions in information security. (Networkworld.com)

Cyber Defense Needs

Cyber Defense Needs

43% of organizations have a problematic shortage of cloud computing and server virtualization security skills. (Networkworld.com)

31% of organizations have a problematic shortage of network security skills. (Networkworld.com)

30% of organizations have a problematic shortage of security analytics/forensic skills. (Networkworld.com)

Cyber Defense Needs

Crawl – Walk - Run

Crawl

Basic Technical Skills and Experience

Walk

Cyber security training

Certification

Experience

Run

- Experienced at out-thinking an adversary
- Practiced teamwork especially with the team
- Relationships and collaboration outside the team

Team Sport


URE WARNING
CO-PILOT CHECKLIST
1. DON'T TOUCH ANYTHING
2. KEEP YOUR MOUTH SHUT

Realistic Environment

Michigan Support

- State is a national leader
- Michigan State Police
- Michigan National Guard
- Civilian Cyber Corps
- Michigan Cyber Range

Civilian Cyber Corps

The Cyber Range

Cyber Range Perspective

Operated by Merit Network

Dedicated to:

- Basic cyber security education, training, and testing
- Advanced platform for Industrial Control Systems security

Build a trained workforce through:

- Accessible resources
- Experiential training
- Adaptable assessment

Michigan Cyber Range

Training and certification

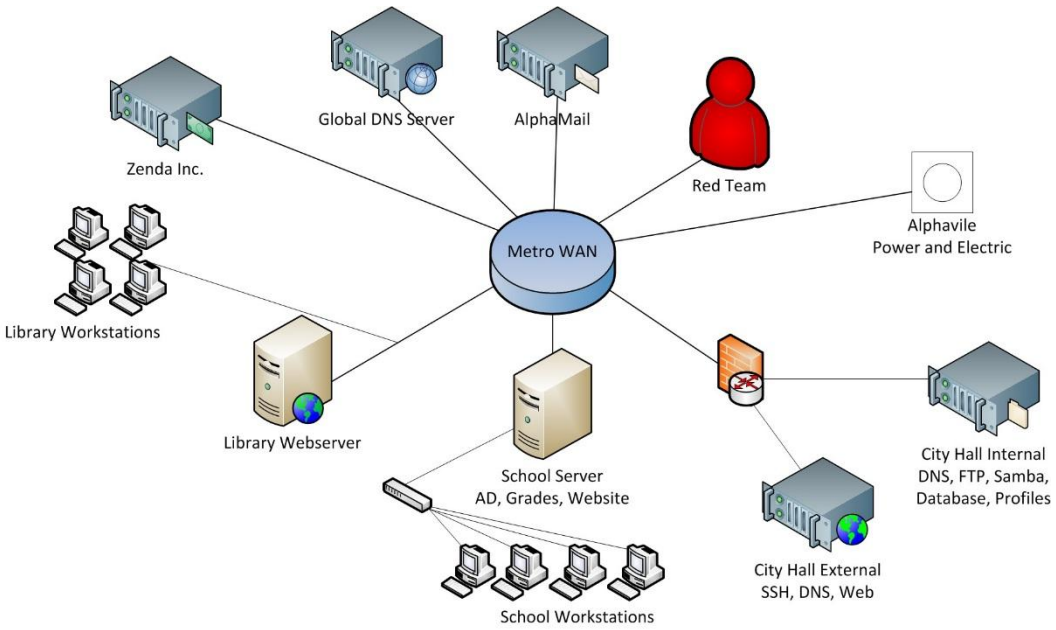
- On site
- Remote
- Self-paced

Realistic environment

- Alphaville
- Adding industries
- Your virtualized systems

Exercises

- Merit developed
- Specific to your environment



Rev 1.2.2

Powerd by merit

Crawl - Training & Certification - Classes

17 Certifications

- Pen Testing, Incident Handling, Ethical Hacking
- Forensics
- Leadership
- Disaster Recovery, Cloud Security

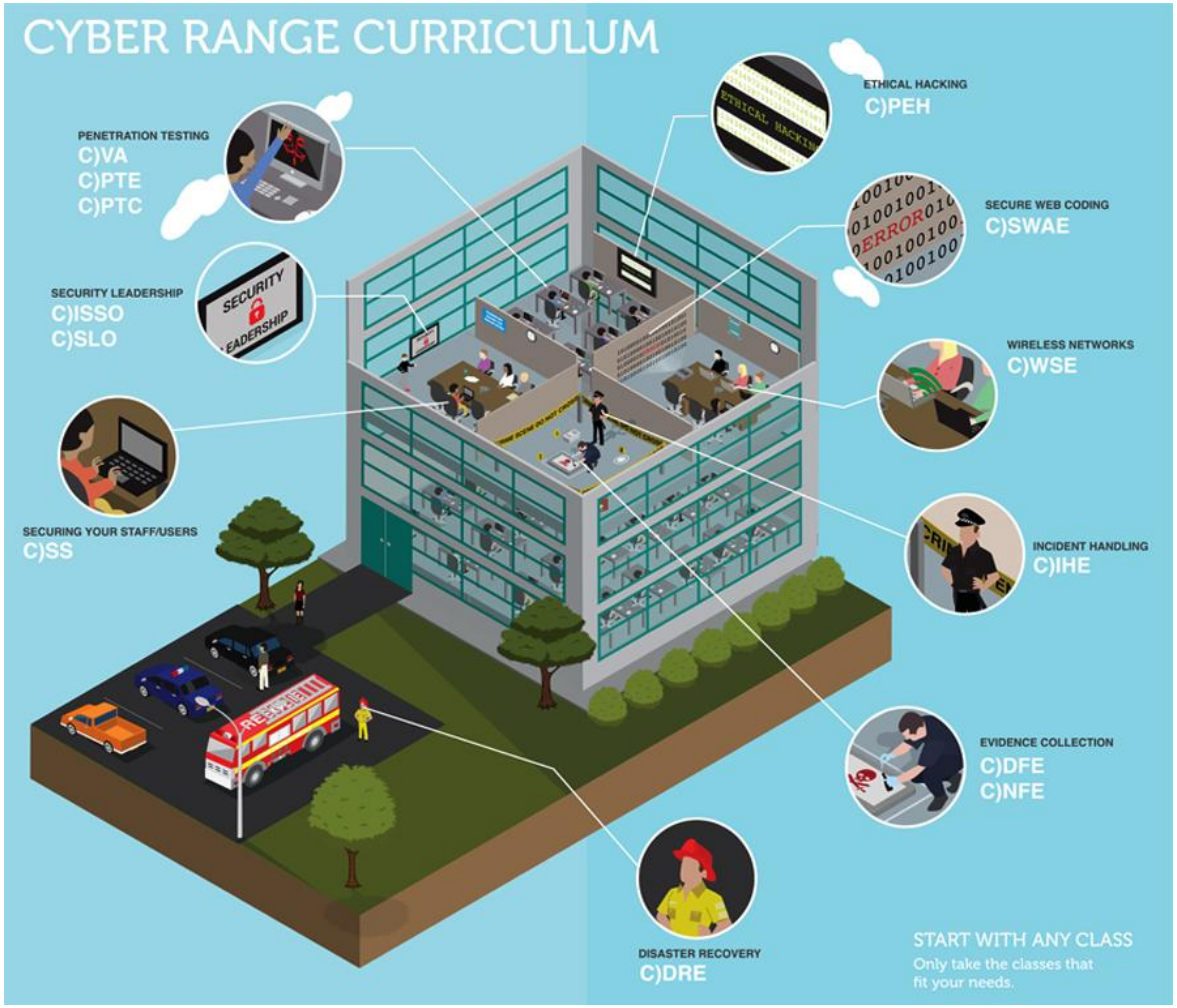
Taught through:

- Structured classes
- Self-paced labs
- Experiential learning

Classes held at Merit, your site, or Online

Cost includes Tuition and Exam

Progressive Certifications



Powerd by merit

Executive Seminars

Presentations

- Cyber Threat Environment
- Cyber Training Programs
- Critical Controls and Common Threats

One hour blocks

Organized into 4 or 8 hour seminars

Customizable upon request to focus on specific threats

Executive Seminars

Table Top Exercises

- Objective driven
- Scenario creation
- Facilitated discussion
- Assessment report

Six Hour seminar

Requires 3 month prep time

Walk

Small Group Training

- Work as a team
- Communication
- 2nd & 3rd order effects

Specialization

- System Controls
- Disaster Recovery
- Wireless Engineering
- Secure Coding

Advanced Courses

- Leadership

Walk - Capture the Flag

Self-Paced

Takes the training wheels off

- Same Tools & Techniques as in class

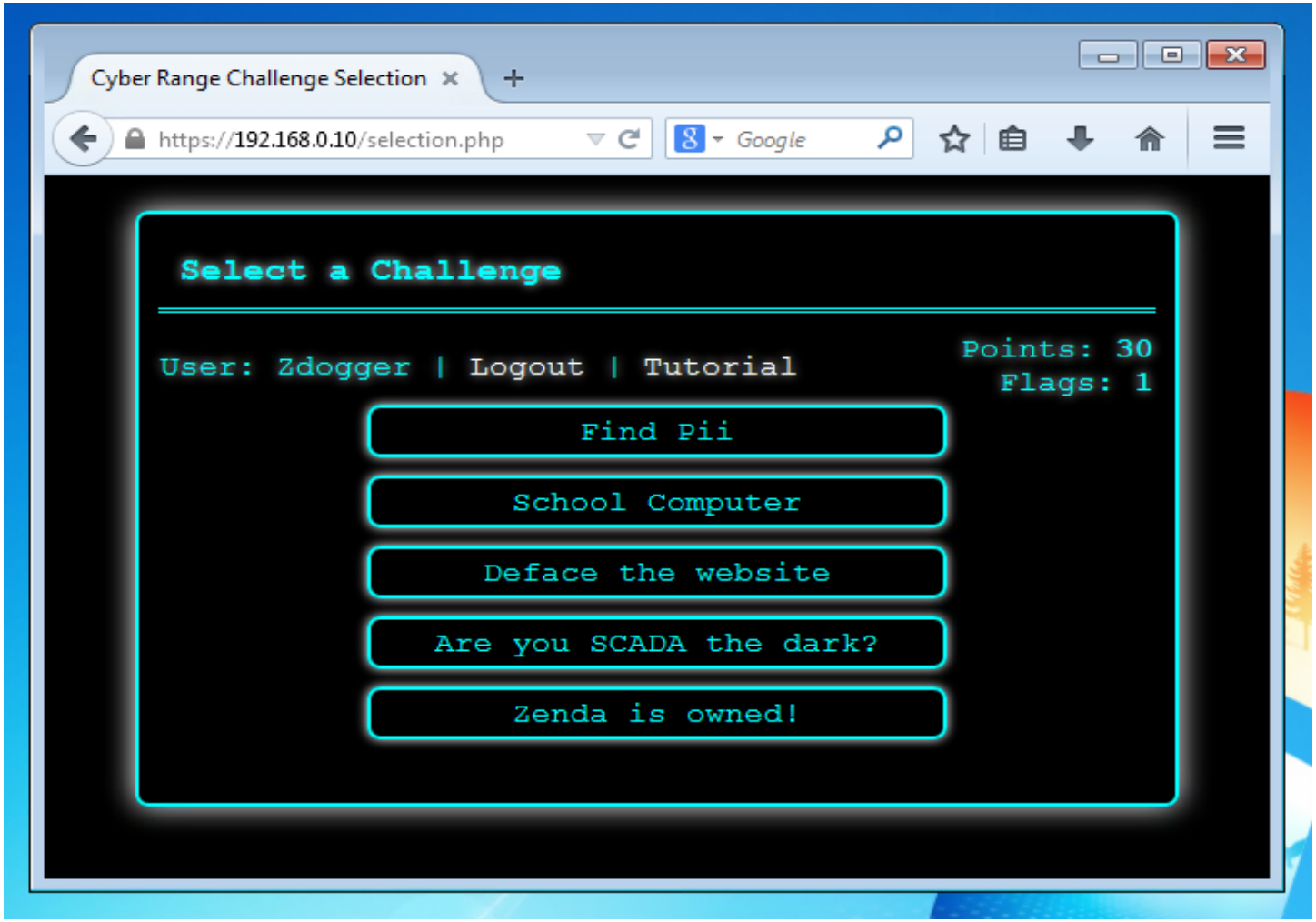
Individual Skill Threads

- Penetration testing
- Forensics
- SCADA
- PII
- Database security

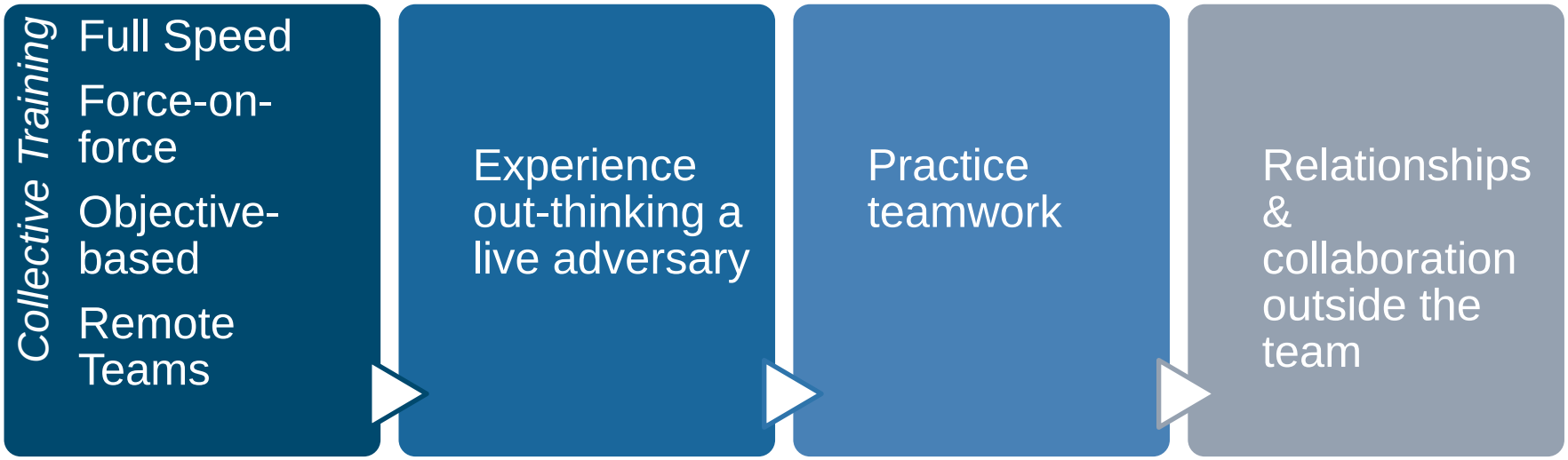
Scoring engine

- Encourages competition

Exercises – CTF – Gamification of Security Training



Run

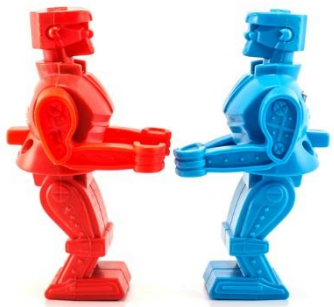

Collective Training
Full Speed
Force-on-force
Objective-based
Remote Teams
Experience out-thinking a live adversary
Practice teamwork
Relationships & collaboration outside the team

Exercises

Red vs Red

- Multiple teams; everyone for themselves
- Penetrate system, plant a flag, secure the system

Red vs Blue



- Focus on system & service; security and continuity
- Force on Force

Incident Response

- Asynchronous
- Red team creates havoc
- Blue team diagnoses and recovers

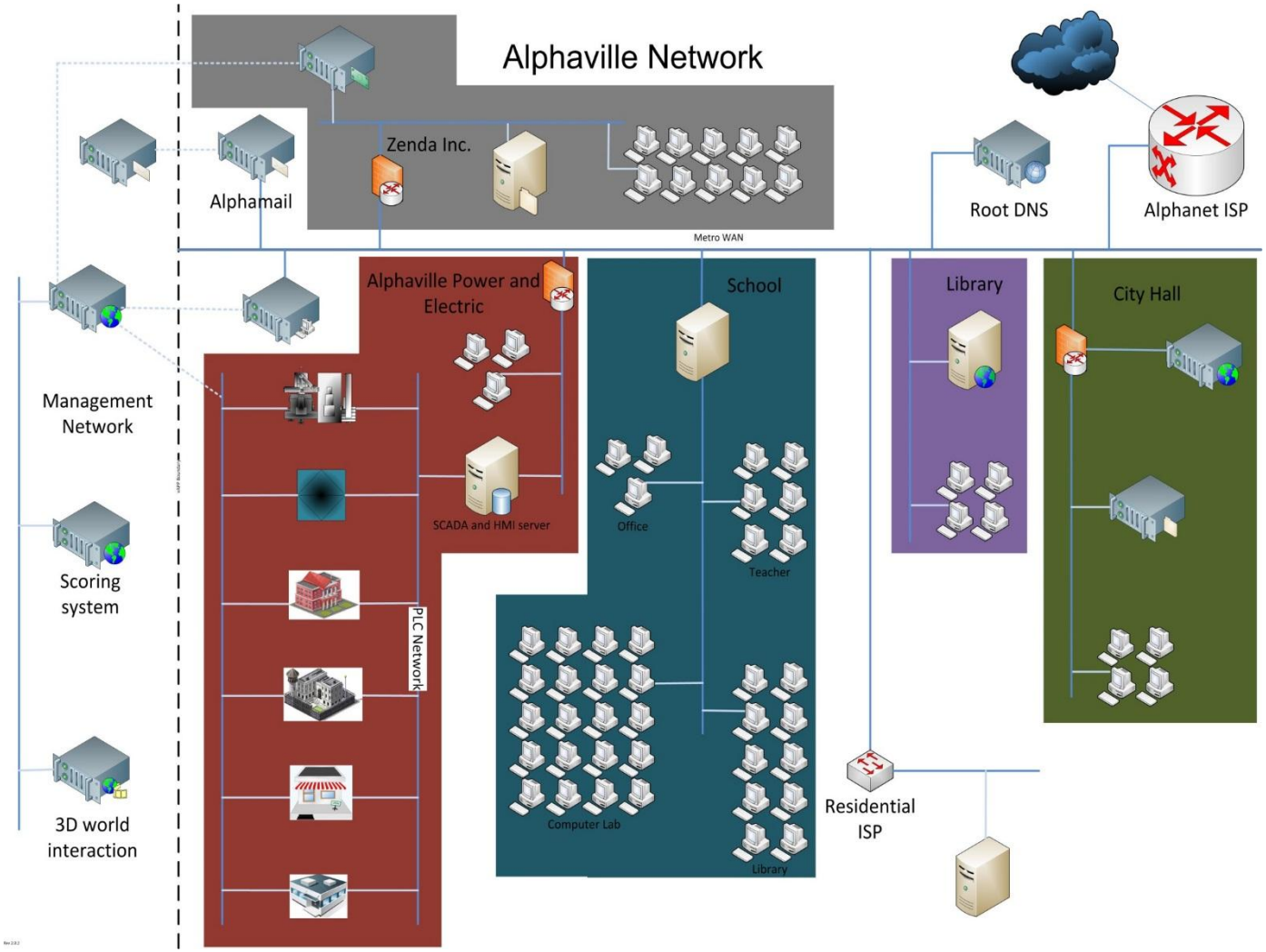
Realistic Environment - Alphaville

Alphaville is a virtual training environment specifically designed to test cyber security skills.

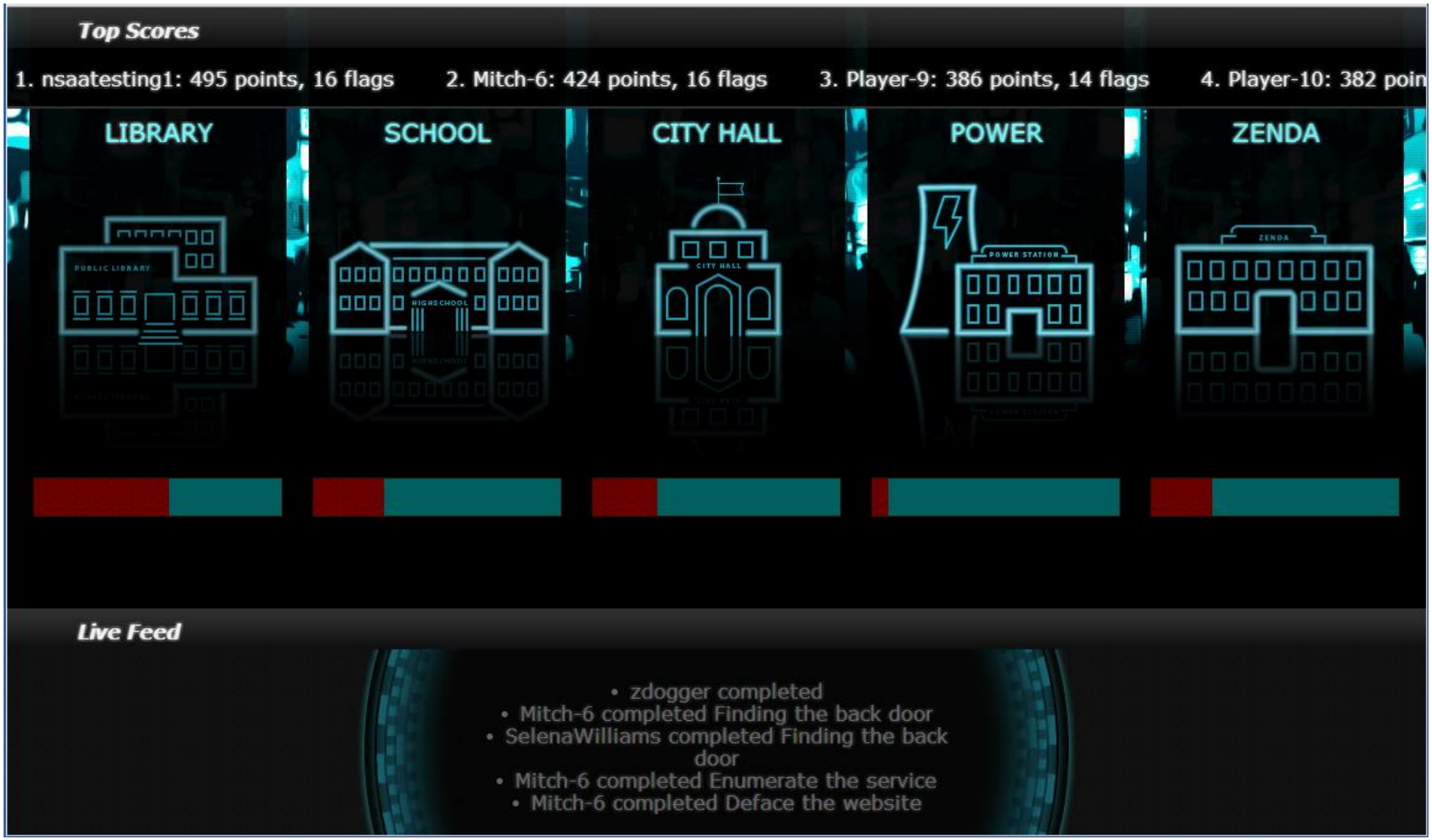
It consists of information systems and networks that are found in a typical information ecosystem.

Each location has different operating systems, different security priorities, and different challenges for participants to encounter and overcome.

Alphaville


Alphaville Network
Zenda Inc.
Alphamail
Root DNS
Alphanet ISP
Metro WAN
Alphaville Power and Electric
School
Library
City Hall
Management Network
Scoring system
3D world interaction
SCADA and HMI server
Office
Teacher
PLC Network
Computer Lab
Library
Residential ISP

Exercises


Top Scores
1. nsaatesting1: 495 points, 16 flags
2. Mitch-6: 424 points, 16 flags
3. Player-9: 386 points, 14 flags
4. Player-10: 382 poin
LIBRARY
SCHOOL
CITY HALL
POWER
ZENDA
Live Feed
• zdogger completed
• Mitch-6 completed Finding the back door
• SelenaWilliams completed Finding the back door
• Mitch-6 completed Enumerate the service
• Mitch-6 completed Deface the website

Alphaville 3D

Take Aways

The threat is real and everyone is a target

Preparation in Cyber Space is vital

- Basic technical skills
- Understanding system weaknesses and attacks
- Practice out-thinking adversaries as a team

Michigan is leading the nation in providing preparation support

- Michigan Cyber Range
- Civilian Cyber Corps

Questions?

Using the Cyber Range

Jameka Williams

- Cyber Range Sales
- jamekaw@merit.edu

Tonia Cronin

- Cyber Range Business Development
- tmcronin@merit.edu

www.merit.edu
734.527.5700

1000 Oakbrook Drive
Suite 200
Ann Arbor, Michigan
48104-6794

Thank You