Ohio Cyber Collaboration Committee (OC3)

Ohio's cyber community working together to help Ohio's citizens and organizations achieve world class cyber security

https://www.oc3.ohio.gov/

Ohio Cyber Collaboration Committee (OC3)

Ohio must posture itself with an enterprise-wide approach that allows for a statewide cyber governance structure. More importantly, Ohio must develop and implement the appropriate authority to provide the capability to respond to and prevent cyber-attacks.

https://www.oc3.ohio.gov/

Ohio Cyber Collaboration Committee (OC3)

Our Mission: To provide an environment for collaboration between key stakeholders, including education, business and local government to strengthen cyber security for all in the State of Ohio and to develop a stronger cyber security infrastructure.

Our Goals/Committees: OC3 has established four subcommittees to help it achieve its primary goals: Education/Workforce Development, Cyber Range, Cyber Protection and Preparedness, and Governance and Public Awareness. The committees are composed of Ohioans with a wide range of cyber and educational expertise dedicated to making Ohio a leader in how to integrate public-private partnerships into solving the cyber security problem.

https://www.oc3.ohio.gov/

Ohio Cyber Collaboration Committee (OC3)

Education/Workforce Development Subcommittee:

Grow the workforce and improve the training and education of users and students in cyber security by:

a. Encouraging individuals of all ages to consider cyber security as a career, help individuals to further develop their cyber security skills at the K-12 and higher education level or as adult learning.

b. Identifying critically needed skills and developing training and educational paths to meet the growing need for skilled workers in the cyber security field. Giving students the hands-on experience needed to be ready to work on day one.

c. Training users/students at all levels in good, age appropriate, cyber hygiene and best cyber security practices.

d. Provide educators the skills and tools needed to support this growing workforce.

https://www.oc3.ohio.gov/

Ohio Cyber Collaboration Committee (OC3)

Education/Workforce Development Subcommittee:

Major Projects:

a. Review curriculum at K-12 and Higher Ed to ensure students are ready to go to work on day 1.

b. Created Cyber Pathway for K-12 students.

c. Created Cyber Club Tool Kit.

d. Developing Apprenticeship, Co-op and Internship program

e. Membership on State Computer Science Committee

f. Addressing shortage in Higher Ed professors and instructors

Cyber Club toolkit link:
http://education.ohio.gov/Topics/Learning-in-Ohio/Computer-Science/Resources-for-Computer-Science/Cyber-Club-Toolkit

Ohio Cyber Collaboration Committee (OC3)

Why is Cyber Education/Workforce Development so important?

18,504 advertised vacancies in cyber security in Ohio!
Very high paying positions well about state average.

a. https:// cyberseek.org/heatmap.html

b. https://www.nist.gov/itl/applied-cybersecurity/nice/resources/career-pathways

c. NICE Framework for Cybersecurity

https://www.oc3.ohio.gov/

Cyber Club Update …

Those interested should contact John at:
john.wiseman@education.ohio.gov

Cyber Club toolkit link: http://education.ohio.gov/Topics/Learning-in-Ohio/Computer-Science/Resources-for-Computer-Science/Cyber-Club-Toolkit

Cyber Club Toolkit

1. How to work with your school or organization to create a cyber club.

2. Understanding the different cyber club advisor roles

3. Finding a mentor for your cyber club

4. Using membership agreements in your cyber club

5. Marketing your cyber club

Ohio Cyber Collaboration Committee (OC3)

Ohio Cyber Range/OCRI:

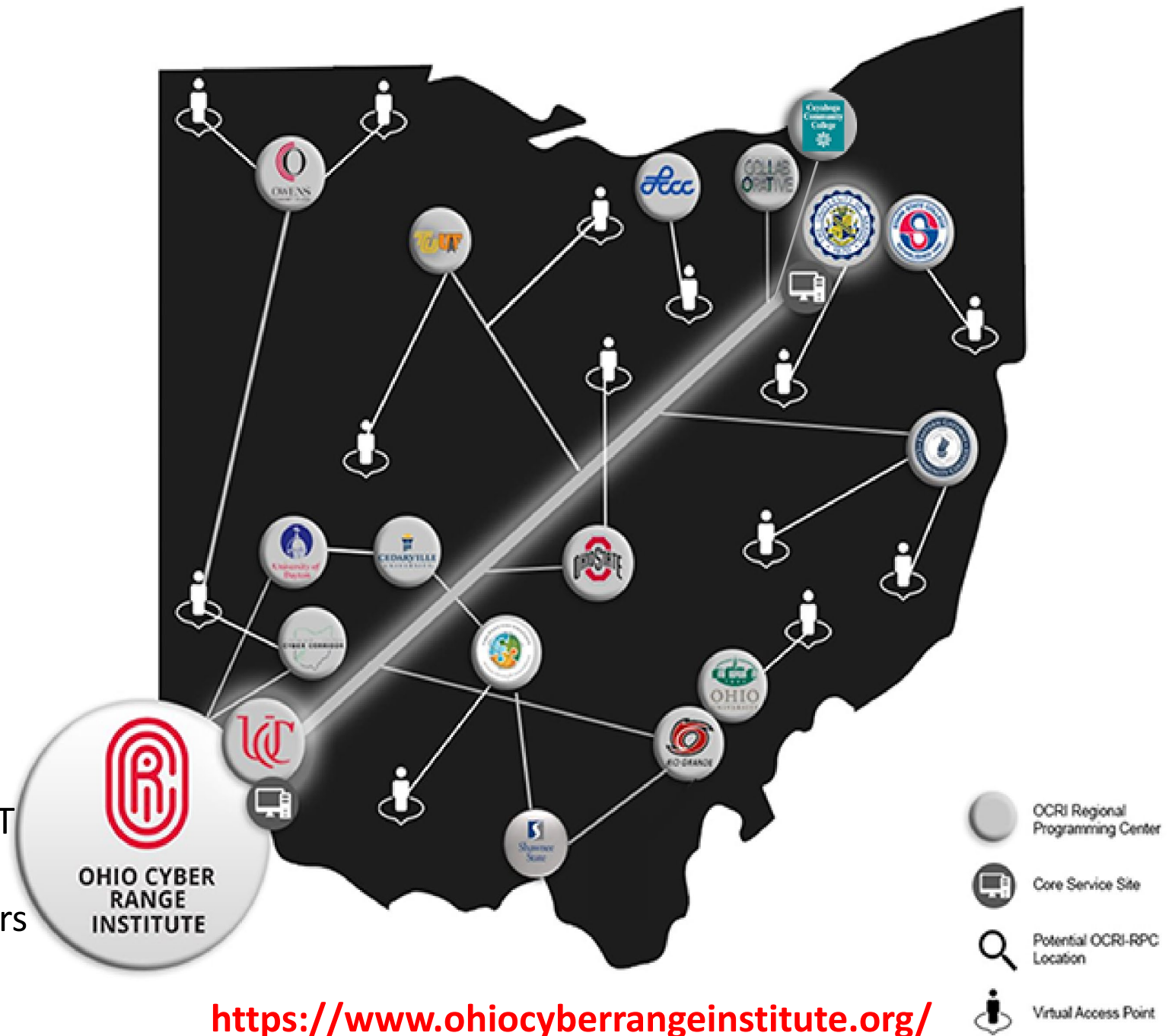Provide a secure cyber security test and training environment, known as a cyber range, to:

a. Support the education of students at the K-12 and University level.

b. Conduct cyber security exercises and competitions to hone cross organizational incident response capabilities and develop future cyber security professionals.

c. Research and test industry-standard best practices, evaluate and test innovative technologies and processes.

d. Enable a training environment for the current and future cyber security workforce, including National Guard personnel, state and local government personnel, faculty and students in the education community, and private sector entities.

e. Provide a Cyber Portfolio for learners, and support internships.

f. Will be able to connect from any location with OARnet access.

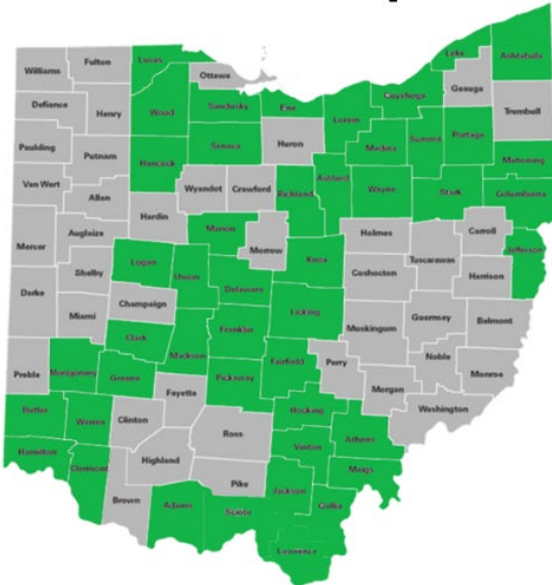**https://www.oc3.ohio.gov/**

OCRI Ecosystem

17 RPCs / 25 Institutions:

- University of Cincinnati
- University of Akron
- Ohio State University
- University of Dayton
- Ohio University
- Rio Grande
- Eastern Gateway CC
- Cin-Day Cyber at SOCHE
- Cedarville University
- Owens CC
- Lorain County CC
- Stark State CC
- PAST Foundation
- Cleveland State/Case Western IoT Collaborative
- Tiffin University & Findlay Partners
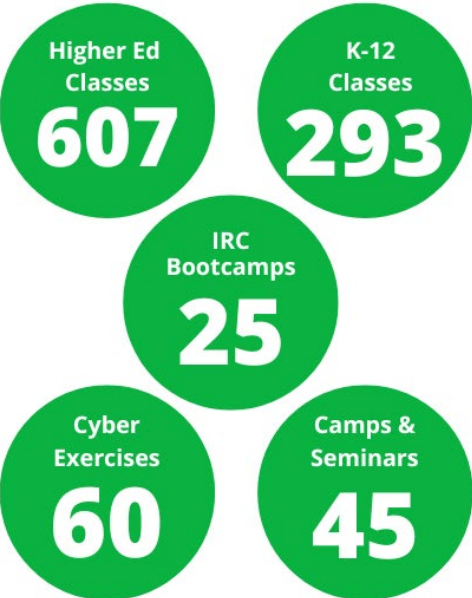- Shawnee State University
- **Cuyahoga Community College**

https://www.ohiocyberrangeinstitute.org/
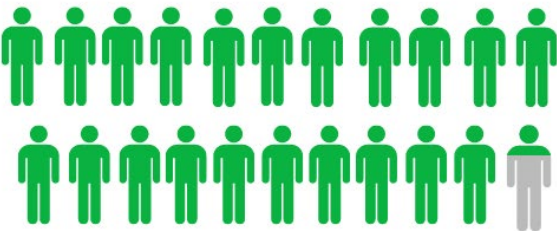

OCRI Regional Programming Center

Core Service Site

Potential OCRI-RPC Location

Virtual Access Point

Impact Report:
1/2018 – 2/2023

46 Counties Impacted*

*K-12 & Higher Ed courses tracked at institution county.

Programming

Higher Ed Classes 607

K-12 Classes 293

IRC Bootcamps 25

Cyber Exercises 60

Camps & Seminars 45

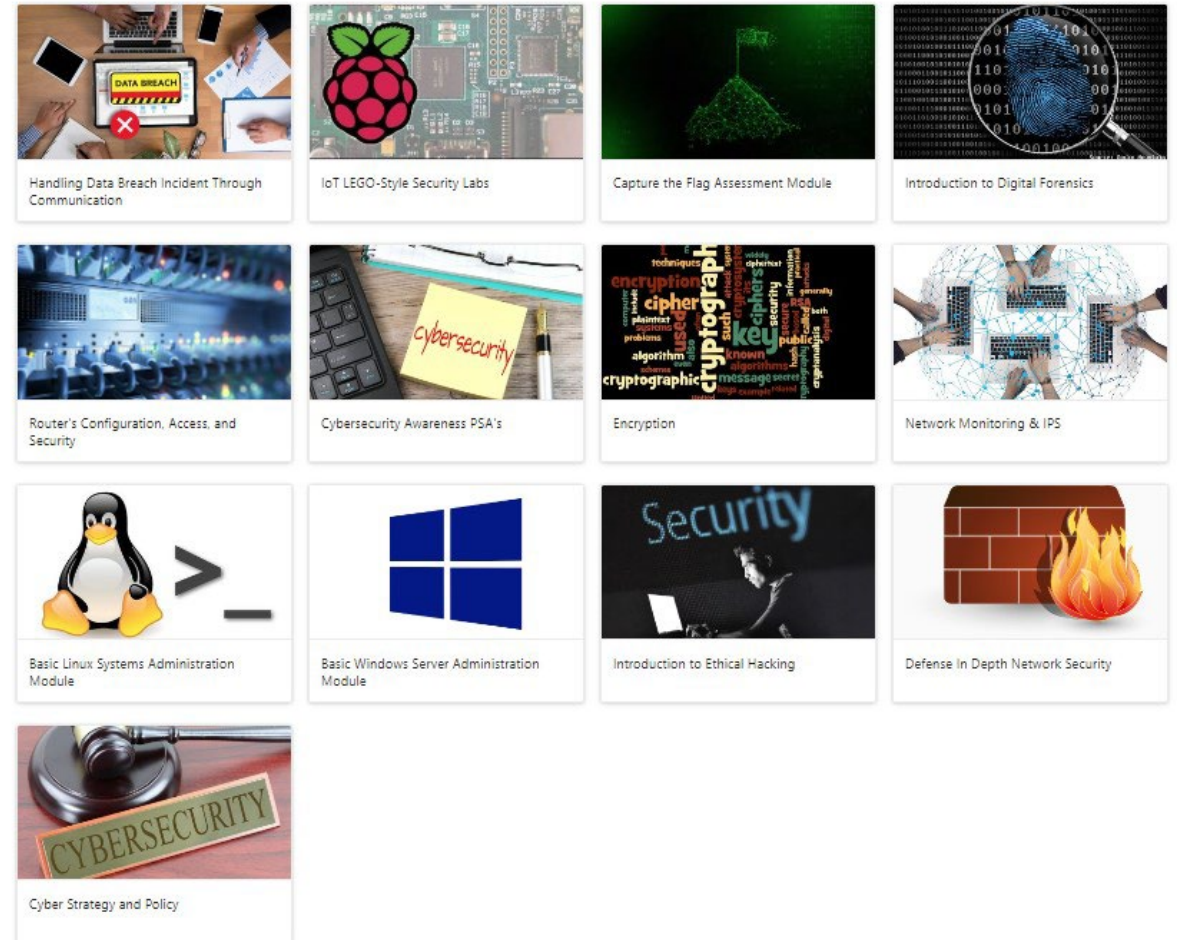## 20,561 Cyber Citizen Users

222 Instructors

10 Instructors per 👤

OCRI Education Module

- A collection of learning materials
  - Instructional materials
  - Assessment materials
  - Hands-on component
- Geared towards K-12, Higher Ed, and/or Workforce Development
- Developed to be shared
  - Choose parts to develop your own courses
  - Build upon what others have created
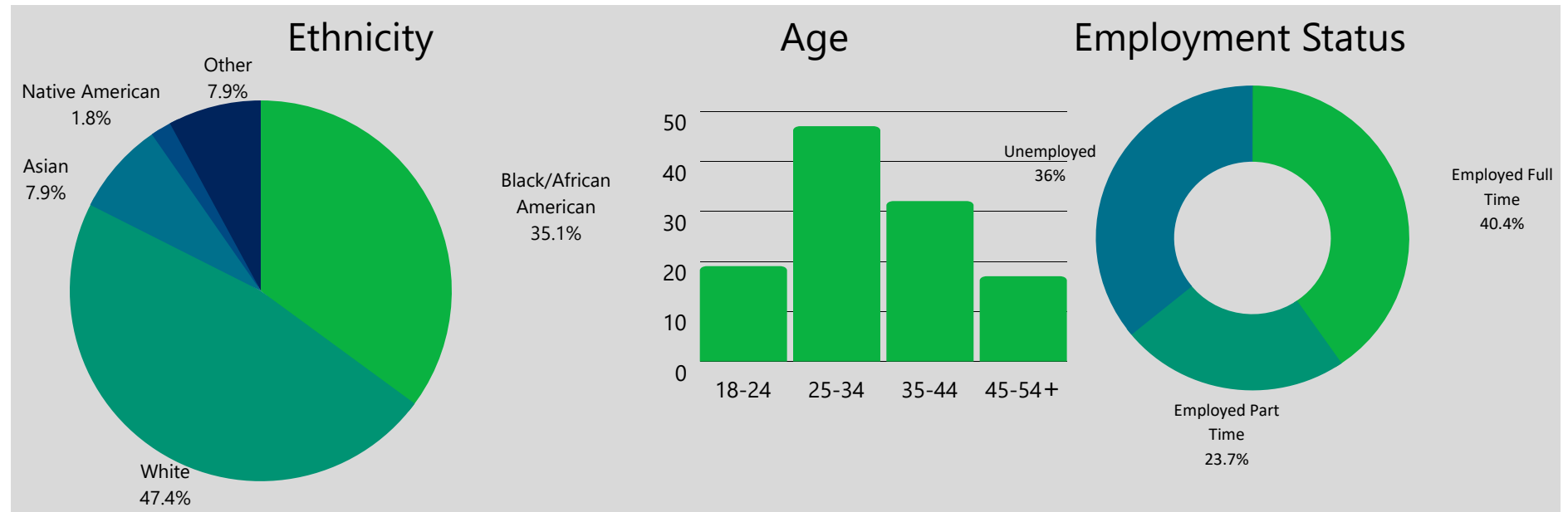 - Contribute and collaborate

OCRI Education Resources

Handling Data Breach Incident Through Communication	IoT LEGO-Style Security Labs	Capture the Flag Assessment Module	Introduction to Digital Forensics
Router's Configuration, Access, and Security	Cybersecurity Awareness PSA's	Encryption	Network Monitoring & IPS
Basic Linux Systems Administration Module	Basic Windows Server Administration Module	Introduction to Ethical Hacking	Defense In Depth Network Security
Cyber Strategy and Policy			

OHIO CYBER RANGE INSTITUTE
UNLOCKING POTENTIAL, SECURING THE FUTURE

IRC Bootcamps

🎟 **144** CompTIA Network+ & Security+ Vouchers Distributed
85 MSFT Azure Vouchers Distributed

CompTIA A+
CompTIA Network+
CompTIA Security+
Azure Fundamentals
Azure Data
Fundamentals
Azure Data Engineer

Ethnicity

Native American 1.8%
Other 7.9%
Asian 7.9%
Black/African American 35.1%
White 47.4%

Age

Age range	Value
18-24	~21
25-34	~48
35-44	~33
45-54+	~19

Employment Status

Unemployed 36%
Employed Full Time 40.4%
Employed Part Time 23.7%

CISSP® Certified Information Systems Security Professional

CompTIA IT Certifications
CompTIA Network+ CompTIA A+ CompTIA Security+

C|EH Certified Ethical Hacker

Bootcamp Registration Now Open!!

Spring Offerings Now Open:

MS Azure Administrator Associate: 2/20-3/19

MS DevOps Engineer Expert: 3/27-4/23

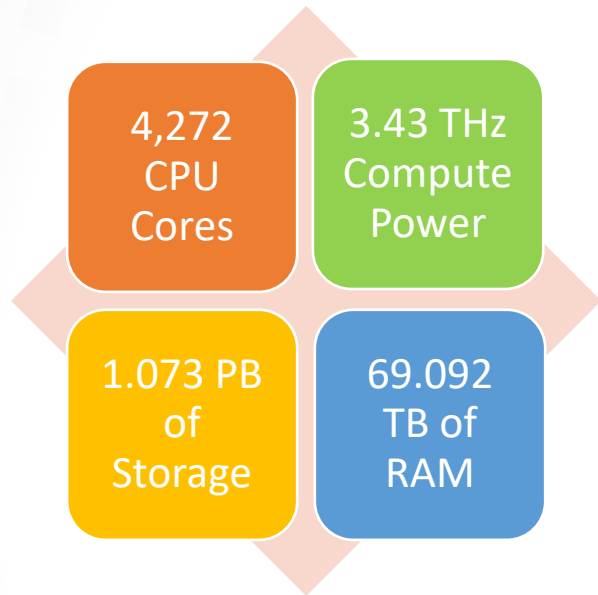CompTIA Security+: 5/1-5/28

DevOps Foundation: 5/1-5/28

Google UX/UI Professional: 5/1-5/28

❑ All offerings have capacity for 40 students
❑ Multiple grants may cover tuition for Ohio residents
❑ Register today via EventBrite to hold your spot!
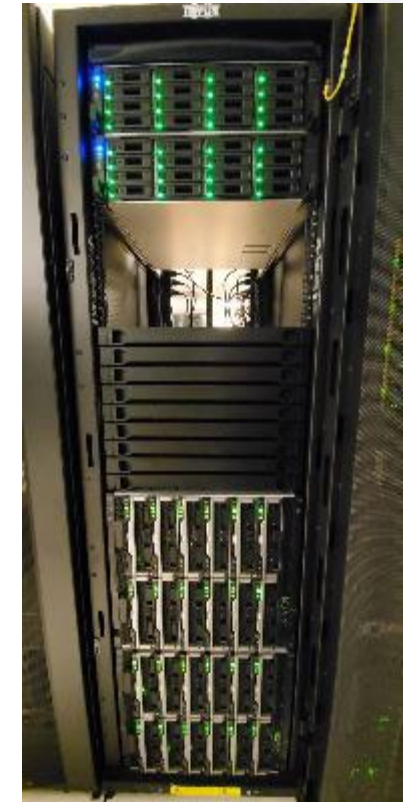❑ Direct questions to Larry Allen @allenw2@ucmail.uc.edu

https://www.ohiocyberrangeinstitute.org/programs-events

CISSP® Certified Information Systems Security Professional

CompTIA IT Certifications
CompTIA Network+ | CompTIA A+ | CompTIA Security+

C|EH Certified Ethical Hacker

Ohio Cyber Range

4,272 CPU Cores

3.43 THz Compute Power

1.073 PB of Storage

69.092 TB of RAM

Average Students/semester: 2500-3000
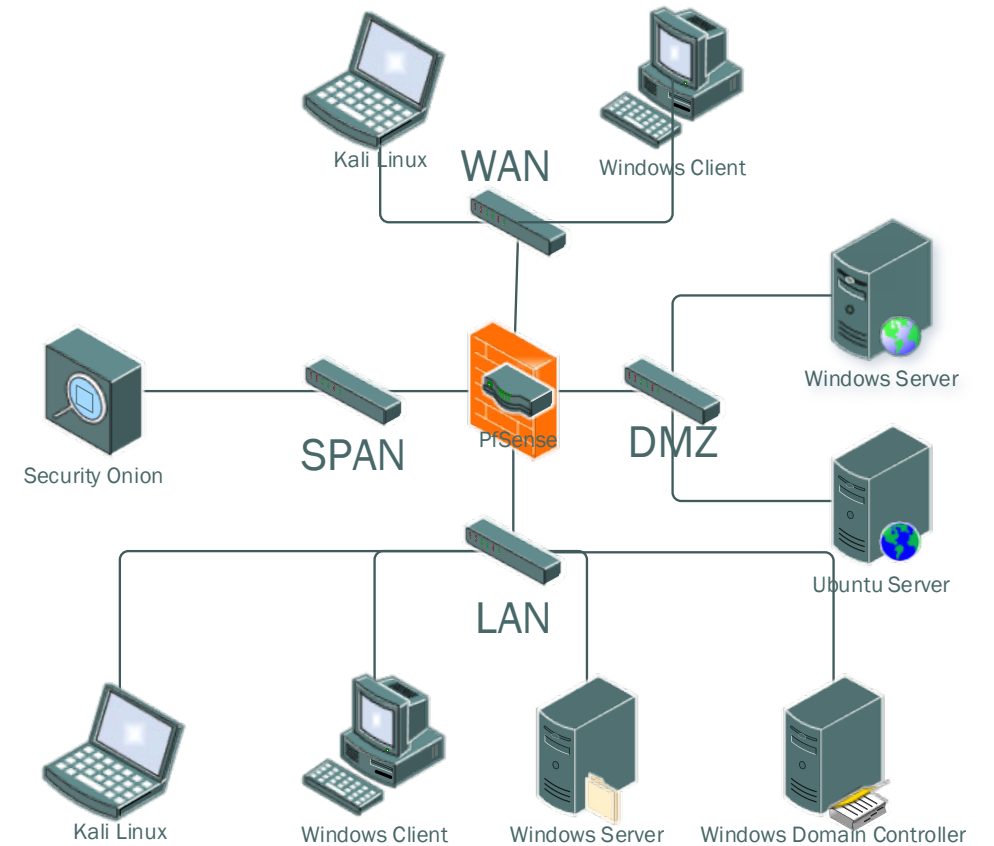
Average Virtual Machines/semester: 4500

OHIO CYBER RANGE INSTITUTE
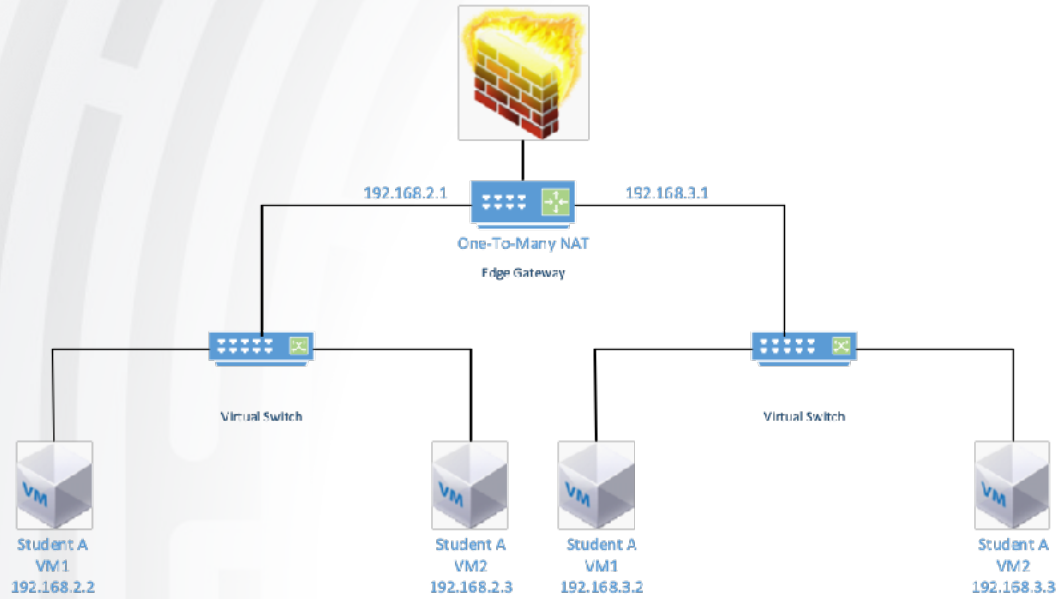UNLOCKING POTENTIAL, SECURING THE FUTURE

Virtual Learning Environments
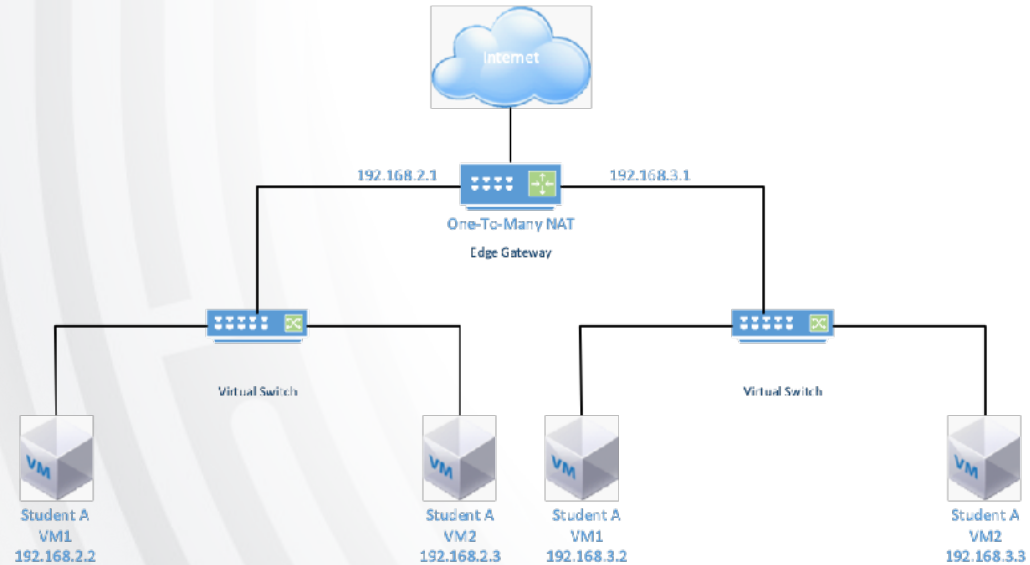
Structured lab environments

Real world examples
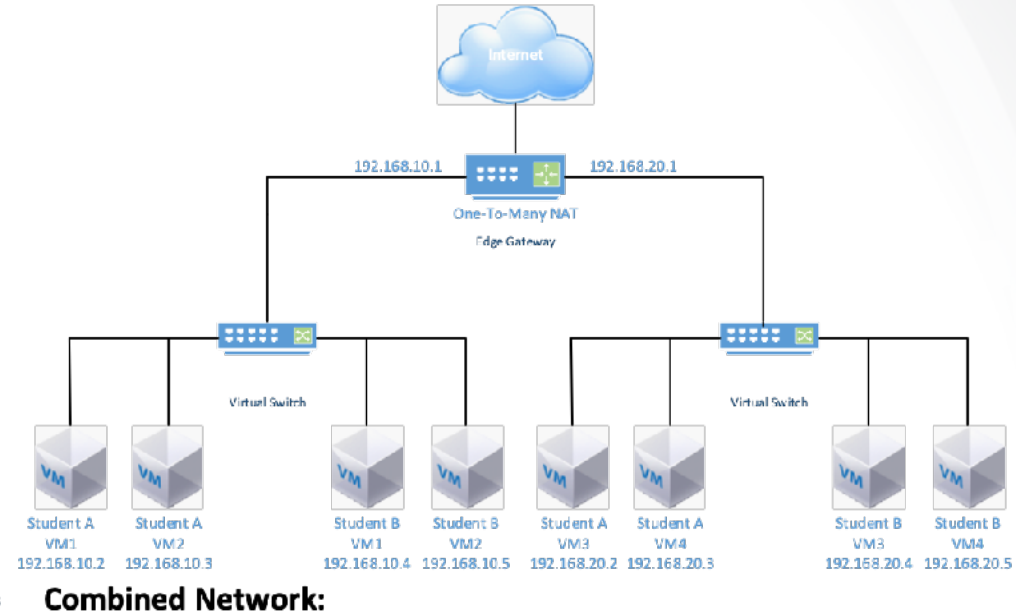
Project based learning
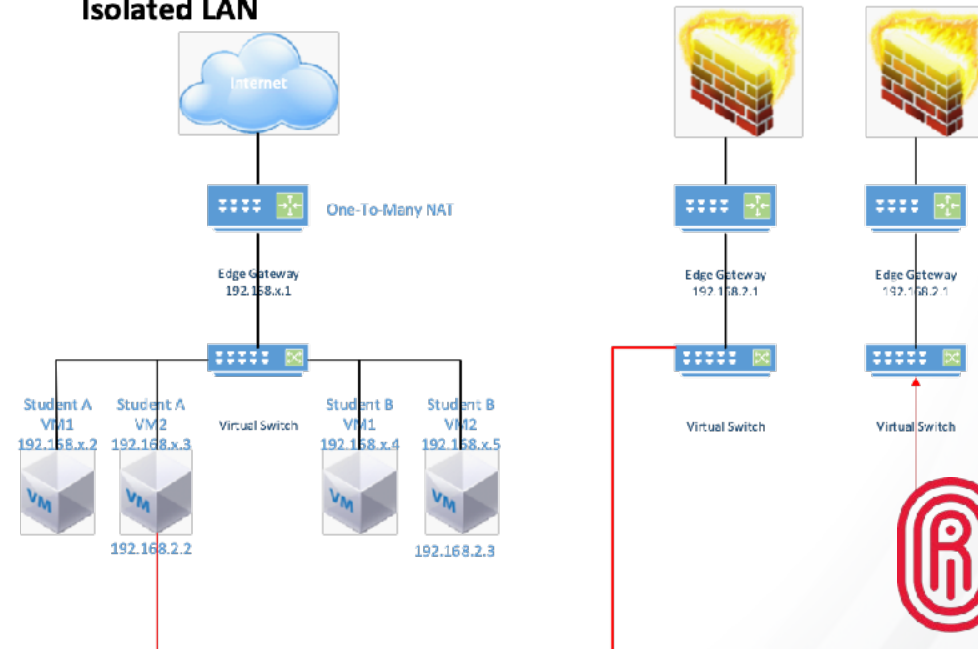
OpFor v Blue Pilot Exercise:

Capture the Flag (CTF)

Red Team vs. Blue Team
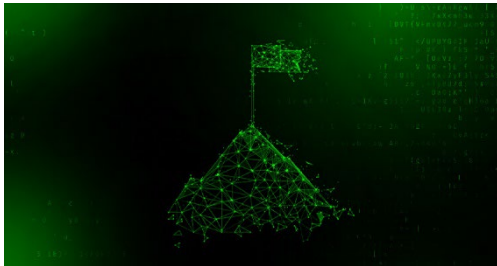
Security Analysts

Blue team

Penetration Testing / Vulnerability

Red team

https://www.ohiocyberrangeinstitute.org/

Fifth Annual Cybersecurity Education Symposium

Save the Date: Friday, October 13th, 2023 at University of Cincinnati

Program will include keynote speakers, panel discussion, breakout sessions, CTF exercises, demonstration booths, and RPC highlights

Kickoff planning committee meeting: Monday, March 6th at 8:00am
Call for proposals out soon!

OC3 Cyber Protection Subcommittee

Deliverables

→ **Ohio Cybersecurity Strategic Plan –** **Complete!**

→ **K-12 Cyber Challenge –** **IN PROGRESS**

→ **OC3 Website Development –** **IN PROGRESS**

→ **Cyber TTX Exercises –** **IN PROGRESS**

→ **Cyber Toolkit / User's Guidebook of Best Practices –** **IN PROGRESS**

→ **Mock Cyber Incident**

→ **Cyber Risk Assessment**

→ **Cyber Symposium / Annual Conference**

→ **Ransomware Awareness Campaign**

https://www.oc3.ohio.gov/

Ohio Cyber Collaboration Committee (OC3)

Governance and Public Awareness Subcommittee:

Identify and share best practices, policies and technologies for all Ohioans by:

a. Providing a collaborative research and development environment for the development and testing of innovative technologies and processes.

b. Ensuring cyber threats are part of emergency planning at all levels both public and private.

c. Using public awareness tools to educate and inform key decision makers of good cyber security practices and the latest information.

d. Educating the general public on the importance of cyber security for the "Internet of Things."

e. Sharing threat intelligence between both public and private sector entities, facilitated through the Ohio Homeland Security State Fusion Center.

https://www.oc3.ohio.gov/

The Ohio Cyber Reserve

Bringing Cyber Talent to the Fight

The Ohio Cyber Reserve

OhCR Mission Set

1. **Assist** - While in a volunteer status, the Cyber Response Teams will provide outreach, training, education, and security assessments to eligible governmental entities and critical infrastructure to reduce cyber vulnerability and increase resiliency.

2. **Educate** - While in a volunteer status, the Cyber Response Teams will assist K-12 educational efforts supporting cyber clubs and mentoring students in support of the Ohio Cyber Collaboration Committee's (OC3) Education and Workforce Development efforts.

3. **Respond** - When called to paid state active duty status, the Cyber Response Teams, under the direction of the Adjutant General's Department will be available to respond to cyber incidents at eligible governmental entities and critical infrastructure.

The Ohio Cyber Reserve

Want to be a member?

1. Register for an account @ APAN.org

2. Navigate to the link below and register. Volunteer Registration Site: https://wss.apan.org/ng/ONG_CPT/OHCR/SitePages/Home.aspx

3. This site will have all the information of prerequisites, ideal candidates, etc.

4. For more information contact:

Craig Baker

Program Administrator,

Ohio Cyber Reserve (OhCR)

2825 W Dublin Granville Road

Columbus Ohio 43232-2789

O: 614-336-7992

Craig.w.baker2.nfg@army.mil

Ohio Cyber Collaboration Committee (OC3)
The Threat

- Cyber crime is projected to cost the global economy $8.0 trillion by 2023, more than 10 times the cost since 2015. Average per attack is 9.44 million.

- There were over 4,100 recorded data breaches and those breaches exposed 22 billion records in 2022

- The cyber-insurance industry is already estimated to be worth well over $10.33 billion growing to 27.8 billion by 2026.

- Multiple firms project that by 2023, 30 billion devices will be connected to the "Internet of things," a huge growth in the number of devices that connect ever more of daily life to the Web.

- Prevention is cheaper than remediation.

https://www.oc3.ohio.gov/

Ohio Cyber Collaboration Committee (OC3)

Threat Actors

- Nation State actors
- Criminal enterprises
- "Hacktivists"/terrorists
- Intellectual property theft/industrial espionage
- Personal/political attacks/insiders
- Malicious Acts/Vandalism
- Rogue Malware

https://www.oc3.ohio.gov/

Ohio Cyber Collaboration Committee (OC3)
Types of Attacks

- Phishing – emails over 90% of attacks, Vishing, Smishing, Spear Fishing, whaling
https://www.cisa.gov/sites/default/files/publications/phishing-infographic-508c.pdf

    Block (SPF DKIM DMARC), Educate, Report, Protect (segment, least privilege, updates)

- Ransomware – Every 14 seconds – New threat - Blackmail

- DDOS Attacks - (distributed denial-of-service) attempts to disrupt normal web traffic and take a site offline by overwhelming a system, server or network with more access requests than it can handle.

- "Man in the middle" – Public wi-fi or weak link on your own network

- Social Engineering

- Insider attacks/physical security/vendor 3rd party corruption

- Password attacks/hacks/brute force

- "Typo squatting" fake login pages, click jacking

- Viruses/other Malware

https://www.oc3.ohio.gov/

Ohio Cyber Collaboration Committee (OC3)
Common Vectors of Attack

- Emails and email attachments
- Unpatched vulnerabilities – OS, Apps
- Compromised/weak credentials (username/password)
- Infected downloads (Trojan horse)
- Compromised thumb drives/CDs/DVDs/SD cards
- Malicious links/advertising/QR codes, Domain Shadowing
- Drive by downloads (infected web sites)
- Man in the middle, Open Wi-Fi or weak link on your own network
- Windows Macros
- Deception/social engineering
- Unsecured venders/support programs

https://www.oc3.ohio.gov/

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

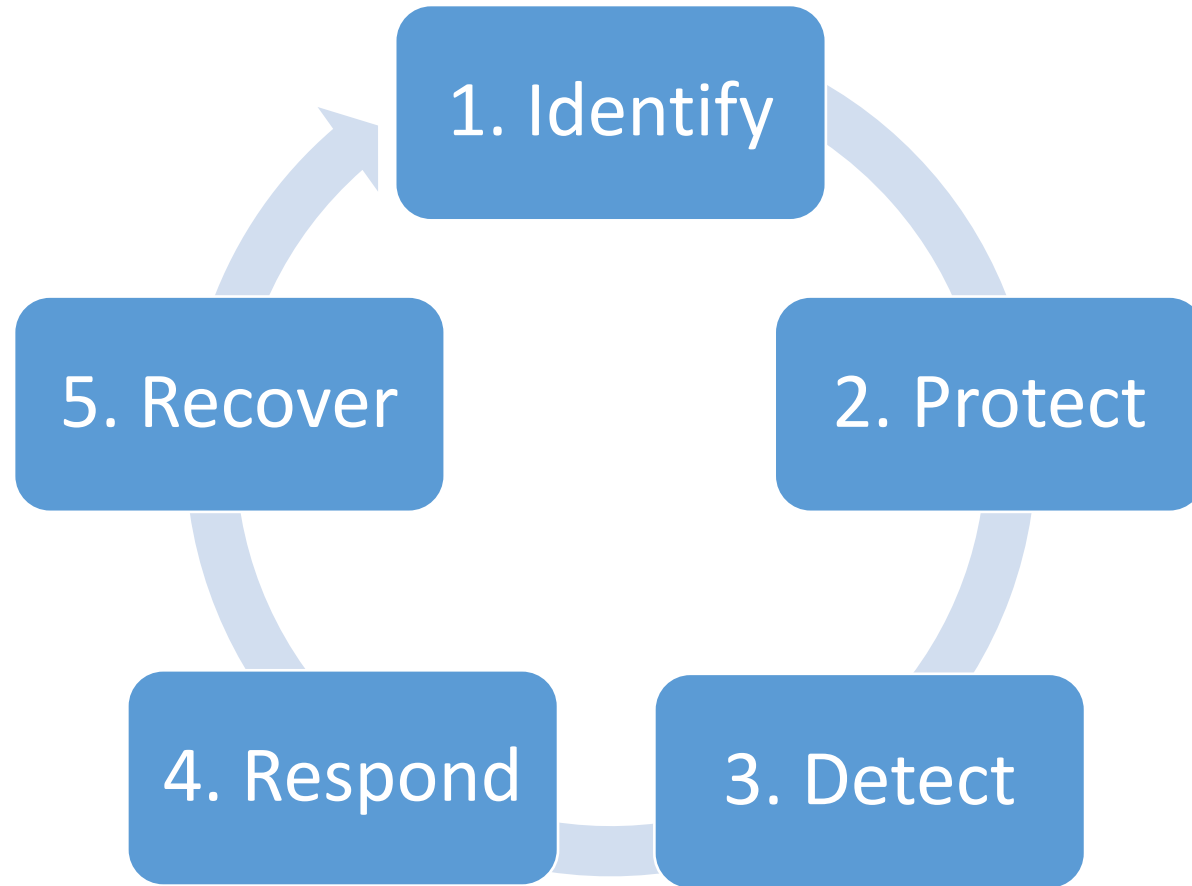# Ohio Cyber Collaboration Committee (OC3)
Password Strategies

- Never reuse or duplicate passwords

- use long complex passwords – 12 minimum with numbers, upper- and lower-case letters, and symbols - longer is better (74 characters per slot)

- Avoid words in the dictionary, part of your name, where you work, your school, the current year, DOB, anniversaries, pets' names, etc.

- Use embeds

- Use the first letters of phrases i.e. The Beatles The Long and Winding Road – $TlAwRtLtYdWnDiStRb76 21 characters, all 4 options, no dictionary words - (trillions of years to brute force attack!)

- Use a password manager (does have some risks)

- Add multi factor authentication (something you know with something you have) i.e. password plus cell phone and pin number

- Set maximum number of tries, then lock out or freeze account

- Change password any time something bad happens

https://www.oc3.ohio.gov/

NIST Framework

https://www.oc3.ohio.gov/

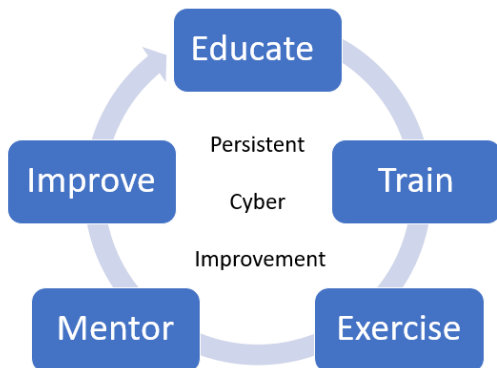# Ohio Cyber Collaboration Committee (OC3)
Simple Solutions

- Update OS and Programs, Delete old or unused programs (Windows 10, Big Sur)
- Change default usernames and passwords on hardware/systems (Mirai malware)
- Use strong passwords and Use Multi Factor Authentication (MFA)
- "Least Privilege" Separate admin accounts from work accounts
- Use/turn on firewall and antivirus programs
- Inventory your network, block unknown devices
- Isolate internet of things/wireless devices from computers (segmentation)
- Have a separate guest network accounts for visitors/IOT/kid's accounts/old tech
- Don't click links in emails or on web pages – look it up, type it in
- Treat outside/unknown thumb drives/CDs/DVDs as highly risky
- Treat outside attachments as risky
- Don't go to sketchy web sites
- Beware of free stuff
- Don't trust something just because you think you know someone
- Backup your data everyday – Use encryption on sensitive data, airgap backup (3-2-1)
- Don't forget physical security, screen locks etc. – "windows L" - don't lend your phone
- Be careful on social media, don't give up your PII - GPS in pictures

Ohio Cyber Collaboration Committee (OC3)
Steps to get better

- Train - users, managers, IT staffs, executives
- Complete Cyber inventory – hardware, software, data, policies
- Audit/implement best practices – NIST standards (OhCR)
- Develop Cyber Response/Recovery Plan
- Develop Continuity of Operations Plan
- Develop and Conduct Tabletop Exercise (CISA)
- Practice all in a red on blue Cyber Range Exercise
- AARs and improve, Audits/Pen tests - not a "one and done" project – "Persistent Cyber Improvement" (PCI) is the key

https://www.oc3.ohio.gov/

Ohio Cyber Collaboration Committee (OC3)
Resilience is the Key

- Will never be 100% safe from cyber attack
- Protect as best you can - minimize threat
- Segment network and limit horizontal movement
- Least privilege - limit Admin rights and access to servers and data
- Monitor network in real time/review logs
- Back up data daily or in real time, 3/2/1 rule
- Encrypt sensitive data – both at rest and in transit
- Have a Response and Recovery Plan
- Have a Continuity of Effort Plan
- Practice Plan – TTX
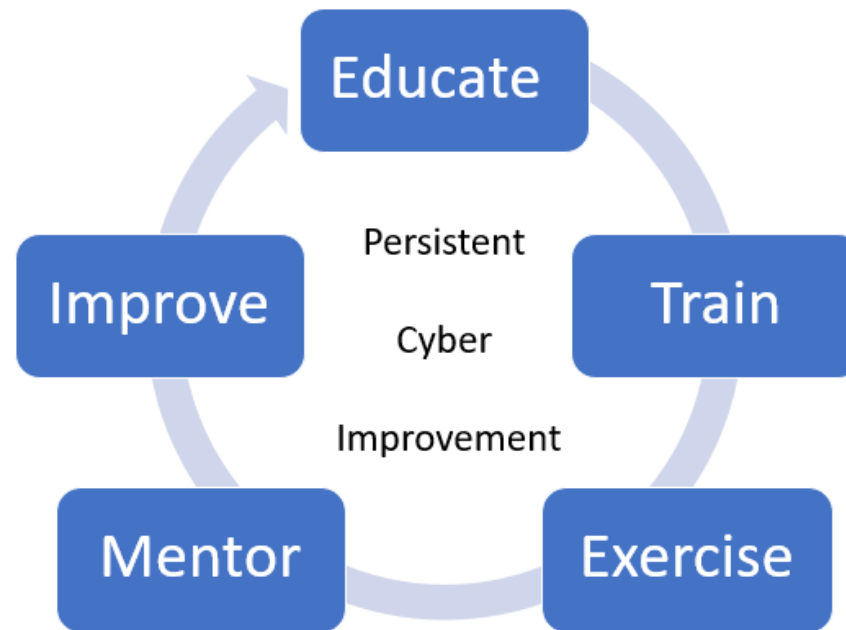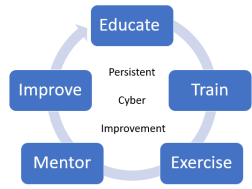- Goal - Have malware be rare, with limited spread, and a fast full recovery

Educate

Persistent Cyber Improvement

Improve

Train

Mentor

Exercise

https://www.oc3.ohio.gov/
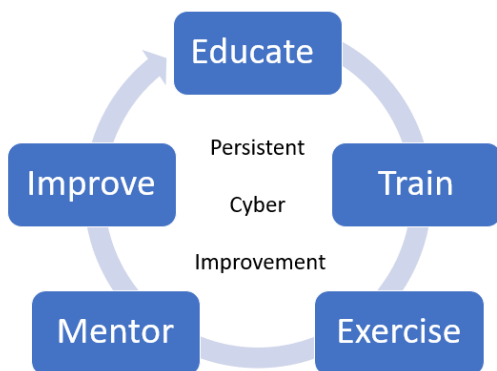
Scalability of OC3 Efforts
Ohio Persistent Cyber Improvement (O-PCI)

Senior Leaders Brief

Gateways

	Gateway 1 (Core)			Gateway 2 (Standard)			Gateway 3 (Advanced)		
	Classes	Products/actions	End Point	Classes	Products/actions	End Point	Classes	Products/actions	End Point
All Users	Cyber Awareness		Annual Cert	Cyber Awareness		Annual Cert	Cyber Awareness		Annual Cert
IT Professionals	Cyber 101	Cyber Inventory Best practices/NIST Internal Auditor	OhCR visit and review AAR	Cyber 102	Cyber anticipation/response recovery plan Continuity of Effort Plan TTX SOP/OPLAN Plan Manager	Usable Plans TTX AAR	Cyber 103	Red on Blue X plan	Complete Red on Blue AAR
Managers	Cyber 101	Cyber Inventory Best practices/NIST Internal Auditor	OhCR visit and review AAR	Cyber 102	Cyber anticipation/response recovery plan Continuity of Effort Plan TTX SOP/OPLAN Plan Manager	Usable Plans TTX AAR	Cyber 103	Red on Blue X plan	Complete Red on Blue AAR
C Suite	Cyber 101 Legal/Risk management	Internal Auditor Review Provide resources	Org. Badge	Cyber 102 Legal/Risk management	Cyber anticipation/response recovery plan Continuity of Effort Plan TTX SOP/OPLAN Plan Manager	Org. Badge	Cyber 103 Legal/Risk management	Red on Blue X plan	Org. Badge

Ohio Cyber Collaboration Committee (OC3)
<u>Resources you can use</u>

- OC3 – https://www.oc3.ohio.gov
- Ohio Cyber Range – https://ohiocyberrangeinstitute.org
- Ohio Cyber Reserve/ONG – Use ema process
- Ohio Homeland Security/CISA – https://www.cisa.gov
- FBI/Department of Public Safety/Secret Service/NSA
- NIST – https://www.nist.gov
- Trusted vendors
- OARnet – Survey - https://oar.net/securitysurvey

Ohio Cyber Collaboration Committee (OC3)

OC3 is supported by a "whole of government" approach to ensure its success. Primary sponsors are the Adjutant General's Department/Ohio National Guard, the Department of Higher Education, The Department of Education, The Department of Administrative Services, The Department of Public Safety, and The Department of Transportation.

OC3 has over 120 organizations who are active members who support the OC3 mission and objectives

https://www.oc3.ohio.gov/

OHIO CYBER COLLABORATION COMMITTEE (OC3)

Ohio's cyber community working together to help Ohio's citizens and organizations achieve world class cyber security

Points of Contact

Primary

Mark Bell
Cyber Security Outreach Coordinator
2825 W Dublin Granville Road
Columbus Ohio 43232-2789
Phone 614-336-4903
Mobile 614-256-2391
Mark.a.bell16.nfg@army.mil

Alternate

Craig Baker
Program Administrator,
Ohio Cyber Reserve (OhCR)
2825 W Dublin Granville Road
Columbus Ohio 43232-2789
O: 614-336-7992
OhioCyberReserve@ucmail.uc.edu