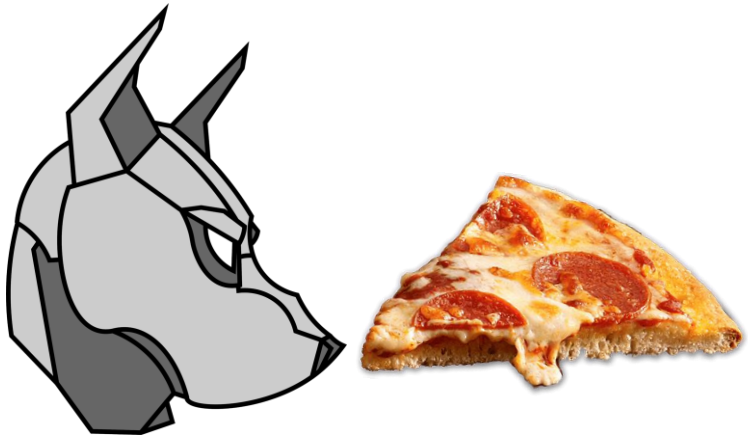
Cyber Defense Organization

Fall 2019 - Intro to CDO



Before We Begin..

Word of the Week

Word of the week

NIST 800-181

NIST Special Publication 800-181

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

William Newhouse
Stephanie Keith
Benjamin Scribner
Greg Witte

This publication is availab
https://doi.org/10.

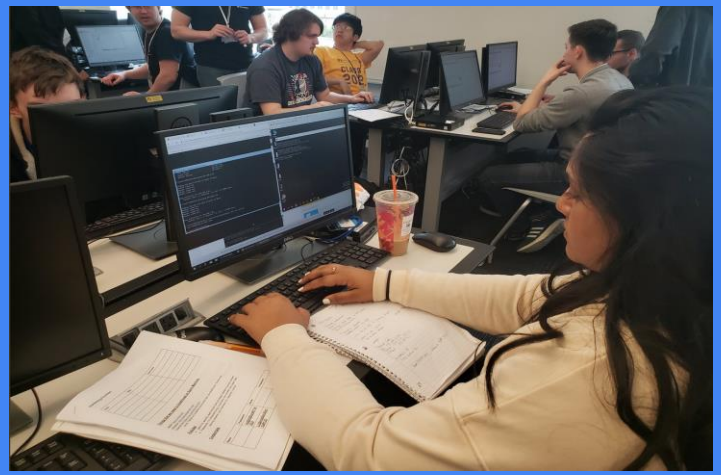
https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework

Security Provision	Information Assurance Compliance	Software Engineering	Enterprise Architecture	Technology Demonstration	Systems Requirements Planning	Test and Evaluation	Systems Development			
Operate & Maintain	Data Administration	System Security Analysis	Knowledge Management	Customer & Technical Support	Network Services	System Administration	Systems Security Analysis	Radio Frequency Teleport	Telephony / Telecoms Management	Space Payload Operation
Protect & Defend	Computer Network Defense (CND) Analysis	Incident Response	CND Infrastructure Support	Security Program Management	Vulnerability Assessment & Management					
Analyze	Threat Analysis	Exploitation Analysis	All Source Intelligence	Targets						
Collect and Operate	Collection Operations	Cyber Operations Planning	Cyber Operations							
Oversee and Govern	Legal Advice & Advocacy	Strategic Planning & Policy	Education & Training	Cyberspace Program/ Project Manager	Cyberspace Supervision, Management, and Leadership					
Investigate	Investigation	Digital Forensics								

Who are you again?

Who We Are

- Premiere campus technical computer security club
- Practical Skills for Practical Situations
- Enhance classroom knowledge & topics
- A place to share and collaborate with people who have passion for cybersecurity like you.



NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION

UB

ENY HACKATHON

Workshops

- Weekly workshops of technical aspects in the field of Cybersecurity.
- No prior knowledge required!
- Learn how to secure infrastructure and build out a defensive architecture step by step!
- Work to educate yourself with InfoSec terminology and standard practices.
- Topics include:
  - Windows Security
  - Linux Security
  - Computer Forensics
  - Security Automation
  - Log Analysis

Competitions

- Simulate an IRL point of view of CyberSecurity.
- Red vs Blue - AKA: Hackers vs You
- Weekly practices to strengthen your skills for the competitions.
- Defend services and work together to fortify your network.
- Specialities include:
  - Linux
  - Firewall
  - Windows
- Travel Upstate or even across state to multi-collegiate competitions, full of opportunities to network and get pwned.

Guest Speakers

People talk to us sometimes, here are some upcoming/past presenters:

Gartner

GreyCastle security

BlueCross BlueShield

amazon

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

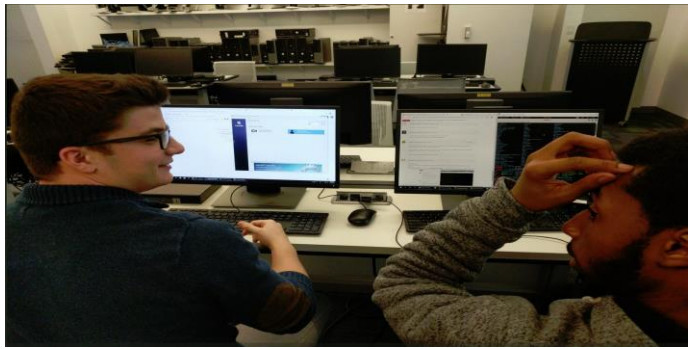
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY BRAVERY INTEGRITY

Interest Groups

New thing this year!

We have a space on the downtown campus. It is perfect for small-medium sized groups.

- Hack the Box
- Web Application Pentesting
- What you guys want more of!
- Anything you want to share with the rest of the organization!



Growth of the Club

Before: 2017

Present: 2019

Eboard Introductions..

Disclaimer:

(Just in case you are new to the InfoSec world).

There are a couple of unspoken rules when “talking shop” in InfoSec.

1. None of what we say is endorsed/sponsored/cleared by any employer or department.
2. Don’t blab about the stack.
3. Don’t talk about clients.
4. And listen. =)

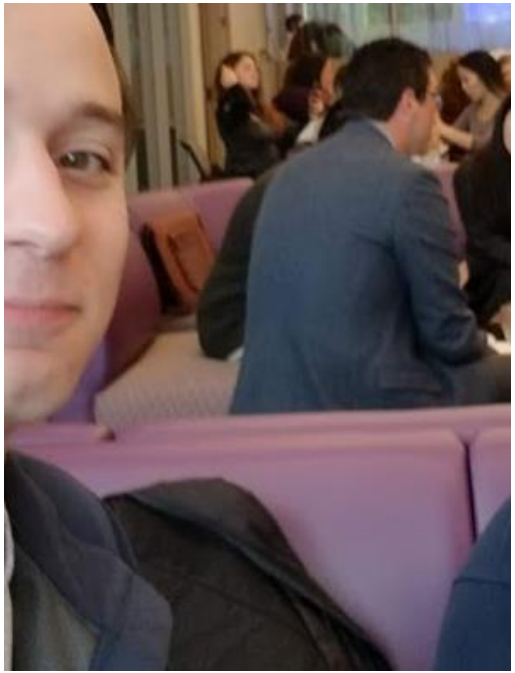
$env:Username
Liam Smith

President, Senior, Digital Forensics.

Consulting Intern at Mandiant™ (a© Fireeye™ Company®)©.

50/50 IR and Proactive Functions. Dead box and live Forensics/Incident Response. (All real cases, which was fun). Report writing. Payload delivery and Active Directory lateral movement.

Talk to me about: Windows (Pen/Forensics/Operation), Homelabing, Web App Security, Rust, beekeeping.



Selfie with Michael Christakis.
Yeah, I got street cred.

Anthony Capece

- Vice President
- Senior, Digital Forensics
- Security Consultant for Waffle House
  Good Food Fast™

Talk to me about:
Linux, Pentesting, Reverse Engineering
Network Engineering, Waffles

Jonathan Matza

- One of the two CTOs
  - One of the most important role is to make workshops for the club, if there is something you want to see or present to the club please approach Me or Tyler Blanco.
- Majors: Digital Forensics & Accounting
- Internship over the summer: Liquidnet
  - A dark pool for trading stocks, liquid assets, etc
  - Responsible for SIEM maintenance and figuring out a solution to forward logs to the SIEM
  - Did day to day operations such as responding to incidents, phishing emails, physical security, etc.
- Talk to me about: firewalls, firewall position for competitions, networking, SIEMS, workshop ideas

Liquidnet

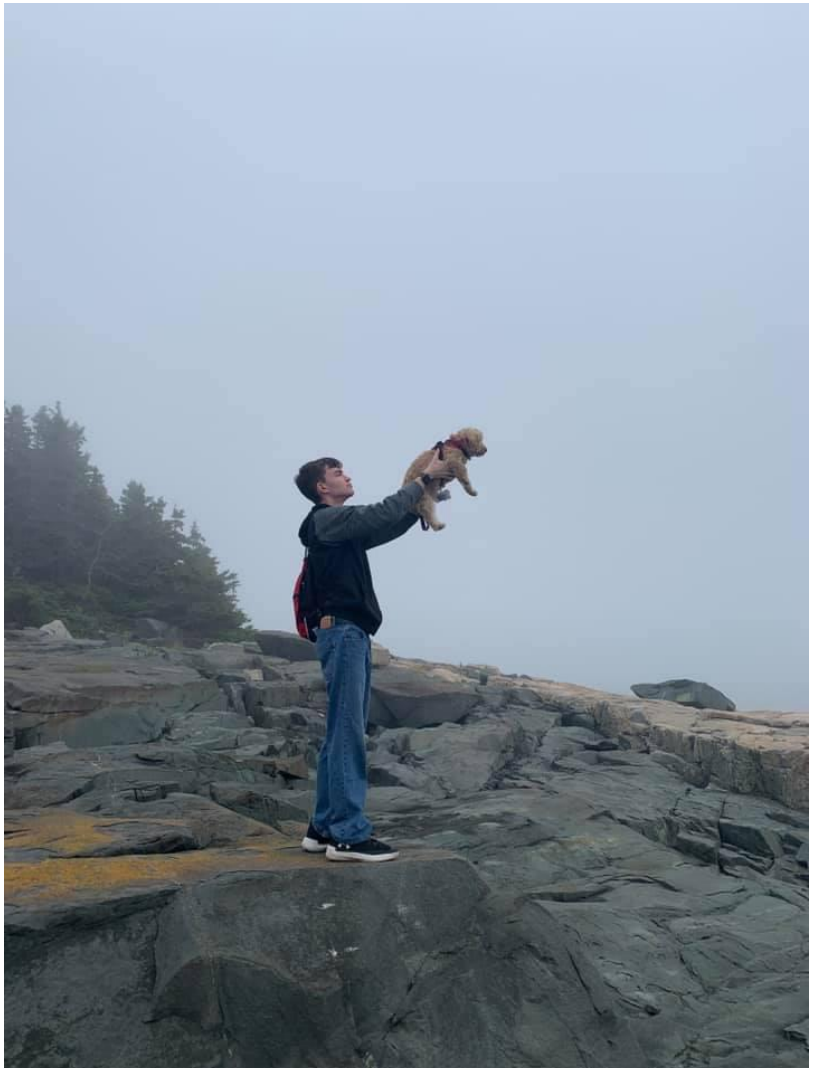
Tyler Ritchie

Major: Digital Forensics

Position: IT-CTO (one of two)

Internships: Stony Brook Hospital IT

Three Village Central School District IT



Tyler Blanco

The other **Chief Technology Officer (CTO)**

Threat Detection Intern at Synchrony Financial

50/50 SOC Analyst and DevSecOps Automation

- Leading projects on Cloud Security automation as well as Endpoint Security with SOAR technology.
- Responsible for detecting unauthorized devices on the SYF network.
- Monitoring **User Behavioral Analytics.**
- Stop phishing and data exfiltration in the company using DLP software.

Talk to me about: Cloud Computing (Automation/Deployment, AWS, Redteaming), SOAR, CDO Workshops this year

synchrony FINANCIAL

Alec Ridgway

- Major- Informatics, concentration in CyberSec
- Position - IT-CTO
- Spent the summer working on...
  - A Networking Primer
  - Windows Security skills
- Talk to me about...
  - Windows security
  - CyberSec in ICS and SCADA systems
  - Warhammer 40k

Me, every night ➔

William Kimler V

Position: Secretary

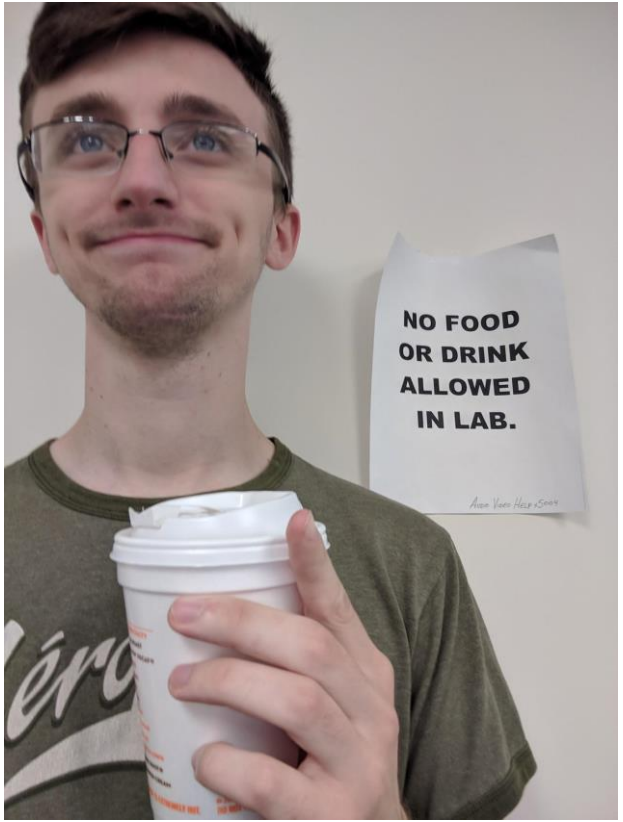
Major: Cehc Cybersecurity

Spent Summer: working on Python projects

Studying for Security+

Interests: python, Java, JavaScript, html, scratch

Talk to me about: programing



Max Kirby

- Year - Sophomore
- Major - Digital Forensics
- Position - Team Captain
- Interests - Linux, Networking, Server Administration, Programming, and Long walks on the beach.

P.S. - If you can't make Monday night practices, but still want to be on the team, speak to me after.

Daunte Kinsey

- **Competition Team Co-Captain**
  - Liason for external marketing
  - Other cool things
- Major: Digital Fowensics
- Talk to me about: Linux Sys Admin stuff, HackTheBox/ Penetration Testing

Mark Tretyak

Marketing Officer

Junior, Digital Forensics major

Information Security intern at Willkie Farr & Gallagher

- Used a vulnerability manager to configure, schedule and review map scans as well as investigate new found devices and add them to the scanning subscription when deemed appropriate
- Re-structured the organization's asset tag system using ~150 location based tags to improve the accuracy and speed of scans
- Used a SIEM to create rules to trigger on events, monitor log and network activity and investigate alerts triggered by rules
- Created and executed several phishing campaigns and educated offending users on the dangers of phishing emails

Talk to me about: Cyber Security certifications, General cyber security, Cyber Security after graduation

Kayla Ibrahim

Treasurer

Junior, Digital Forensics Major

Internship: Research Intern at National Defense University

- Conducted research and produced a publication regarding a policy memo on **<COUNTRY REDACTED>** 5G, AI Technologies and Digital Authoritarianism

Almost Done Here.

All,

CDO is excited to announce that we will be hosting guest speakers from the **National Security Agency on Tuesday the 24th, at 6:30 pm in BB151.**

Jeff Watkins serves as the Communications Director for NSA's Commercial Cybersecurity Strategy, and will speak to students about career opportunities at NSA.

We will also be having an alumnus of the university who works for the Agency speak to their experience aswell.

This will be an opportunity for students to hear from a long-time NSA'er about what it's like to work at the Agency as well as hear from one of our own about their personal experiences.

We hope to see you all there.

<Call to Action Here>

Server Infrastructure / Black Team:

1. Did you ever manage your own minecraft server?
2. Like Linux?
3. Want to play around with a $5k server?

If you answered yes to any of these... you might want to **join our server team!**

Interest Groups:

1. Do you have a cyber/tech related interest/hobby?
2. Want to have us to the boring “club” stuff while you can just do your tech thing?
3. Want to have a small club without having to go through the pain of SA?

Start an interest group!

CTF

- Trying a new thing: Capture the flag
- Every week we will put up questions for you guys to try based on workshops
- The forms will be under our website's CTF tab (uacyber.org)
- Let's see if this works!

Kahoot Time!

- We created a Kahoot go to Kahoot.it to play
- If you place 1st, 2nd, or 3rd come up to us to get the CTF code and potentially a T-shirt

Add us on Social Media!

Twitter: **@ualbanyCDO**

Instagram: **ualbany_cdo**

Website: **uacyber.org**

Myinvolvement: **Cyber Defense Org**

We have a discord!

Cya Next Time!

Next Week's Workshop will be an Intro to **Windows Security** taught by **Alec** and **Liam**!