MCCoE

MISSOURI CYBERSECURITY CENTER OF EXCELLENCE

Cybersecurity Trade Craft

"You will be assimilated. Resistance is futile."

501.c.3 Non-Profit www.MCCoE.org

Sensitive - For Official Use Only

Introductions

- Steven Farrar – Executive Director
- Wes Hester – Steering Committee / Tech Committee
- Dr. Shannon McMurtrey – Steering Committee / Education & Training Committee
- Heather Noggle – Steering Committee / Marketing / Donor Relations

As A Nation, State, Region…

- A growing concern over the lack of technically trained individuals in the Cybersecurity field to fill an ever-growing gap of supply and demand (~2M World-Wide).

- Focus on protecting the 16 Critical Infrastructure Sectors:

Why Do We Need Cybersecurity Professionals?

National Security, Espionage

Nation-state actors
Stuxnet, NotPetya, SolarWinds, REvil

Notoriety, Activism, Defamation

Hacktivists
Lulzsec, Anonymous

Monetary Gain

Organized crime
Zeus, ZeroAccess, Ransomware

Nuisance, Curiosity

Insiders, Spam, Script Kiddies
Nigerian 419 Scams, Code Red

Perpetual War!

{* CSO *}

77% of security leaders fear we're in perpetual cyberwar from now on

Also, Charming Kittens from Iran scrape email inboxes, France could fine Google again, and more

Brandon Vigliarolo

Sat 27 Aug 2022 // 07:49 UTC

MCCoE Vision

The MCCoE Secures our regional assets while creating a cybersecurity ready workforce.

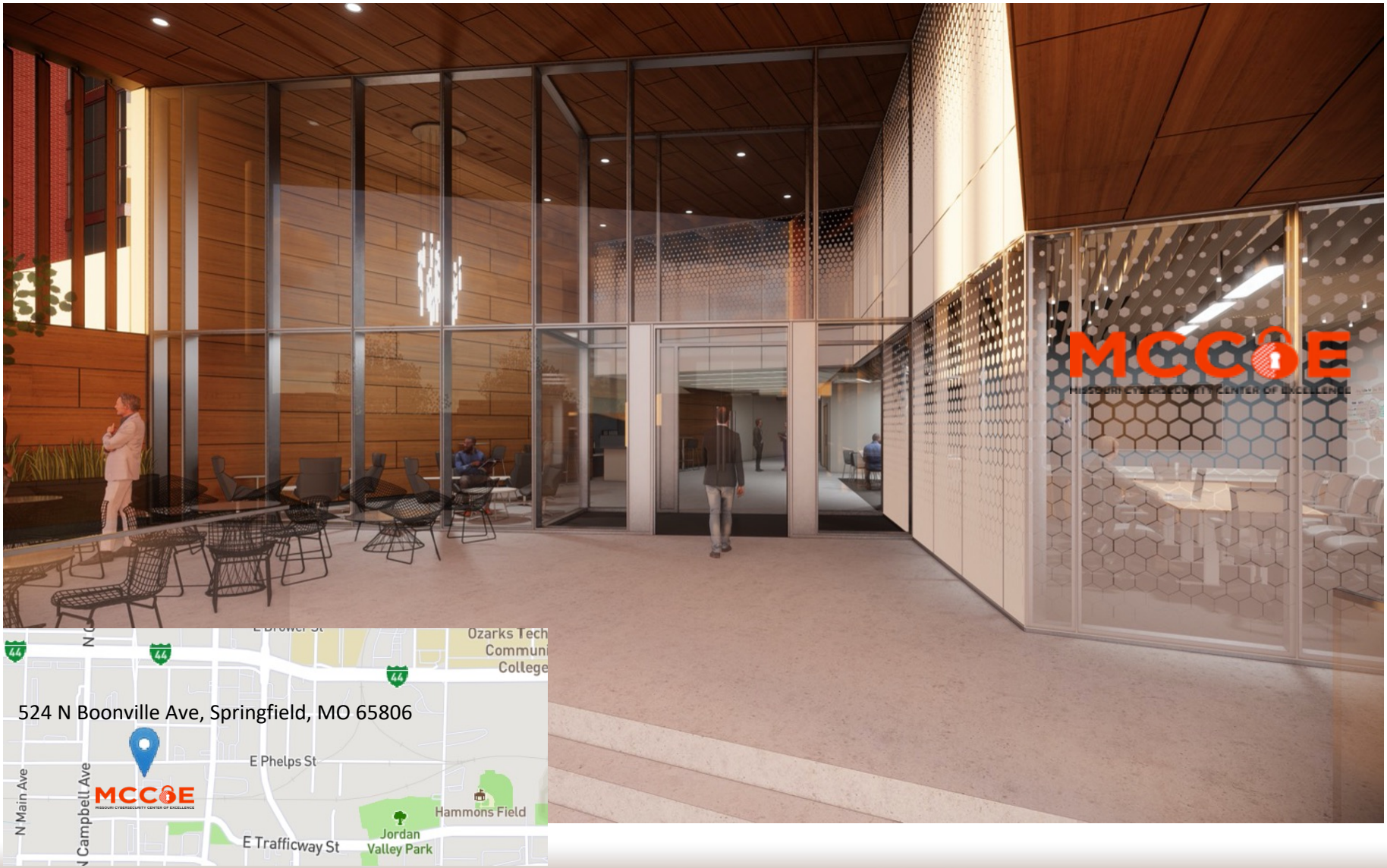
The MCCoE is partnered with other National Centers of Excellence such as:

- San Diego Cybersecurity Center of Excellence (SDCCoE - https://sdccoe.org/)
- Merit (https://www.merit.edu/)
- CyberUp (https://wecyberup.org/)
- MOREnet (www.more.net)
- DHS National Imitative Cybersecurity Careers and Studies (NICCS) https://niccs.us-cert.gov/about-niccs/niccs#

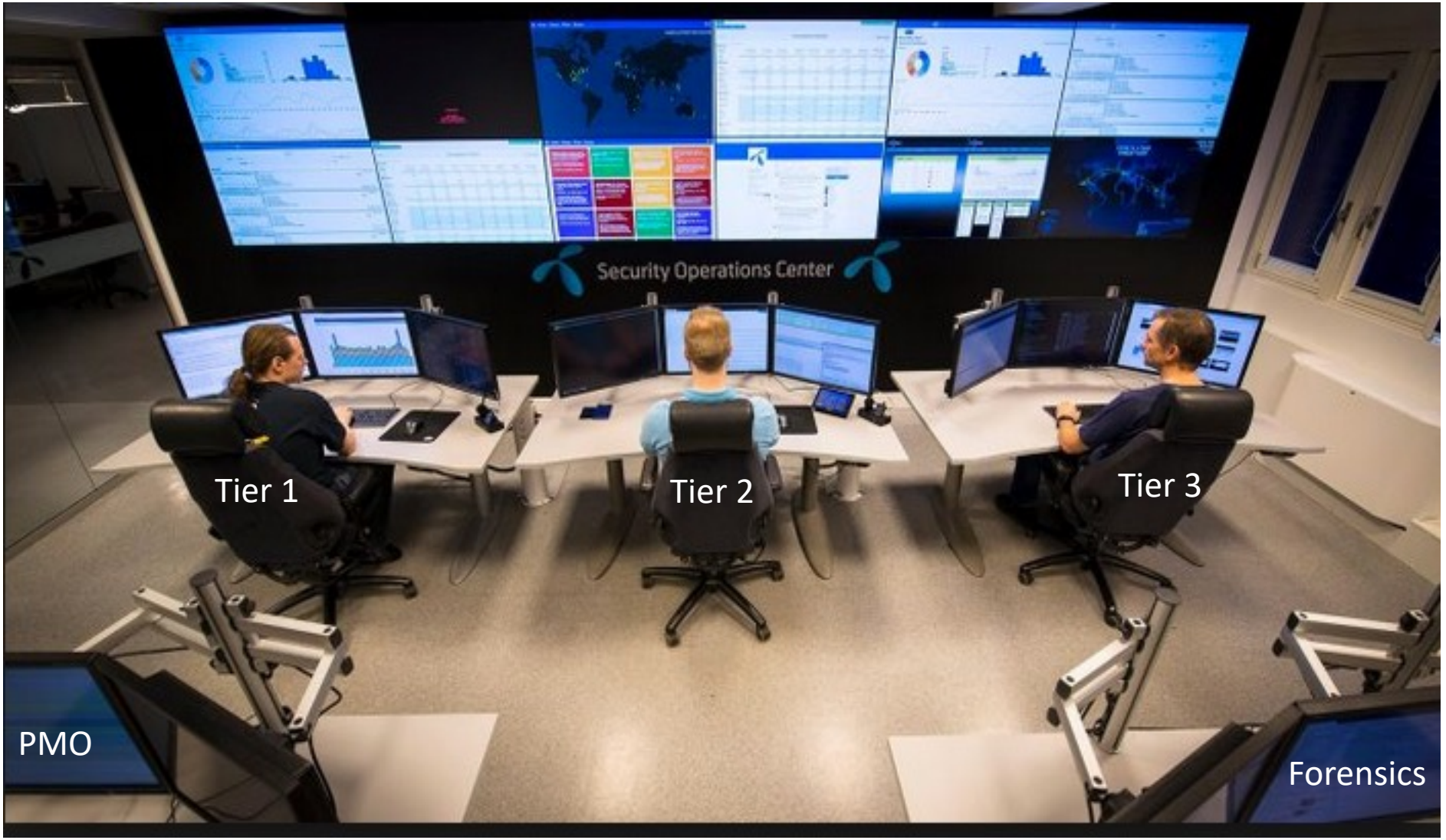
The MCCoE is a non-profit, **public-private partnership between Academia, Industry, Non-Profits, and Government**, dedicated to accelerating the region's cyber economy and positioning it as a State hub of cyber innovation. By capitalizing on Springfield's unique location and strengths in this expanding and future-oriented field, the MCCoE aims to grow the regional economy by:

- Provide Cybersecurity Services to the regional community
- Provide educational and career hands-on training and certifications
- Workforce development
- Accelerate innovation – thought leadership fostering collaboration
- Attract and nurture talent
- Create new business opportunities

Jordan Valley Innovation Center (JVIC) - Entrance Way



MCCoE SOC Floor



”This is a 24 x 7 x 365 Job!”

MCCoE Focus Areas

Public-Private Partnership between Academia, Industry, Non-Profits and Government

Security Operations Center "Protect, Detect, Respond"

Help Non-profits, small-to mid-sized businesses, and government agencies combat and recover from cyber attacks.

Workforce Development

A pipeline for workforce development and placement of University Students into the Cyber Workforce

Accelerate Innovation

A Cyber institute to bring real-time information on the latest cyber trends, security, best practices and resources to better protect the region's systems, networks and critical infrastructure.

Education & Certification

A Cyber Research, Education and Training Center that will conduct research on cybersecurity threats through education programs at MSU, Drury, Evangel, and other schools around the state and nation.

Alignment with Economic Development Office

- Creating and retaining quality jobs
- Increasing Education and Training of Citizens per capita
- Improving the quality of life for all citizens
- Increasing private investment in the community
- Increasing the property tax and sales tax base
- Providing and maintaining public infrastructure

Getting Government Buy In?

Governor Mike Parson @GovParsonMO · 16h

Today, I signed FY22 state operating budget bills that invest in critical infrastructure projects, support stronger communities, fund workforce development priorities, and increase pre-pandemic K-12 and higher education spending levels.

12 8 23

Getting Academia Buy In?

OZARKS TECHNICAL COMMUNITY COLLEGE

Office of the Chancellor

October 26, 2021

DRURY UNIVERSITY

OFFICE OF THE PRESIDENT

September 18, 2018

Dear Business Leader:

This letter is to demonstrate Drury University's interest and commitment to help support a public-private Cybersecurity Center that will serve Springfield and the State of Missouri. The University recognizes the talent and skills shortage in cybersecurity and related technology careers, and the impact this has on local employers. This Center is one example of the University's commitment to elevate our collaboration with business in order to meet the workforce development demands.

This Center will be operated by an independent organization, and is planned to be located at the Jordan Valley Innovation Center (JVIC). The Cybersecurity Center is designed as a center of excellence to provide a number of services, but will primarily focus on workforce training and preparing students with the skills needed to immediately influence your business. In addition, the Cybersecurity Center will include an operations center that will help nonprofit organizations and small businesses combat and recover from cyber-attacks. The Center will also conduct research on cybersecurity threats and bring real-time information on the latest cyber trends, security best practices and education resources to business, nonprofits and public entities.

The Center will be operated by a core leadership team of experienced full-time employees, and will be supported by students in order for them to obtain the skills, training, and certifications needed for this demanding and growing field. Experiential learning and training is often the best career preparation. It is estimated that there are about 1,000,000 cybersecurity-related positions currently unfilled. Drury University is committed to help solve this growing issue.

The Cybersecurity Center is not sustainable without industry leaders like yourself. I encourage you and your management team to learn more about this opportunity, and whether this model is something that will help address your workforce development needs. Regardless of your needs, please let me know how Drury University can best assist your business.

Sincerely,

J. Timothy Lloyd, PhD
President

Missouri State University

August 8, 2018

Dear Business Leader:

This letter is to demonstrate Missouri State University's interest and commitment to help support a public-private CyberSecurity Center that will serve Springfield and the State of Missouri. The University recognizes the talent and skills shortage in cybersecurity and related technology careers, and the impacts this has on local employers. This center is one example of the University's commitment to elevate our collaboration with business in order to meet the workforce development demands.

This Center will be operated by an independent organization, and is planned to be located at the Jordan Valley Innovation Center (JVIC). The Cybersecurity Center is designed as a center of excellence to provide a number of services, but will primarily focus on workforce training and preparing students with the skills needed to immediately influence your business. In addition, the Cybersecurity Center will include an operations center that will help non-profit organizations and small business combat and recover from cyber-attacks. The Center will also conduct research on cybersecurity threats and bring real-time information on the latest cyber trends, security best practices and education resources to business, non-profits and public entities.

The Center will be operated by a core leadership team of experienced full-time employees, and will be supported by students in order for them to obtain the skills, training, and certifications needed to for this demanding and growing field. Experiential learning and training is often the best career preparation. It is estimated that there are about 1,000,000 cybersecurity related positions currently unfilled. Missouri State University is committed to help solve this growing issue.

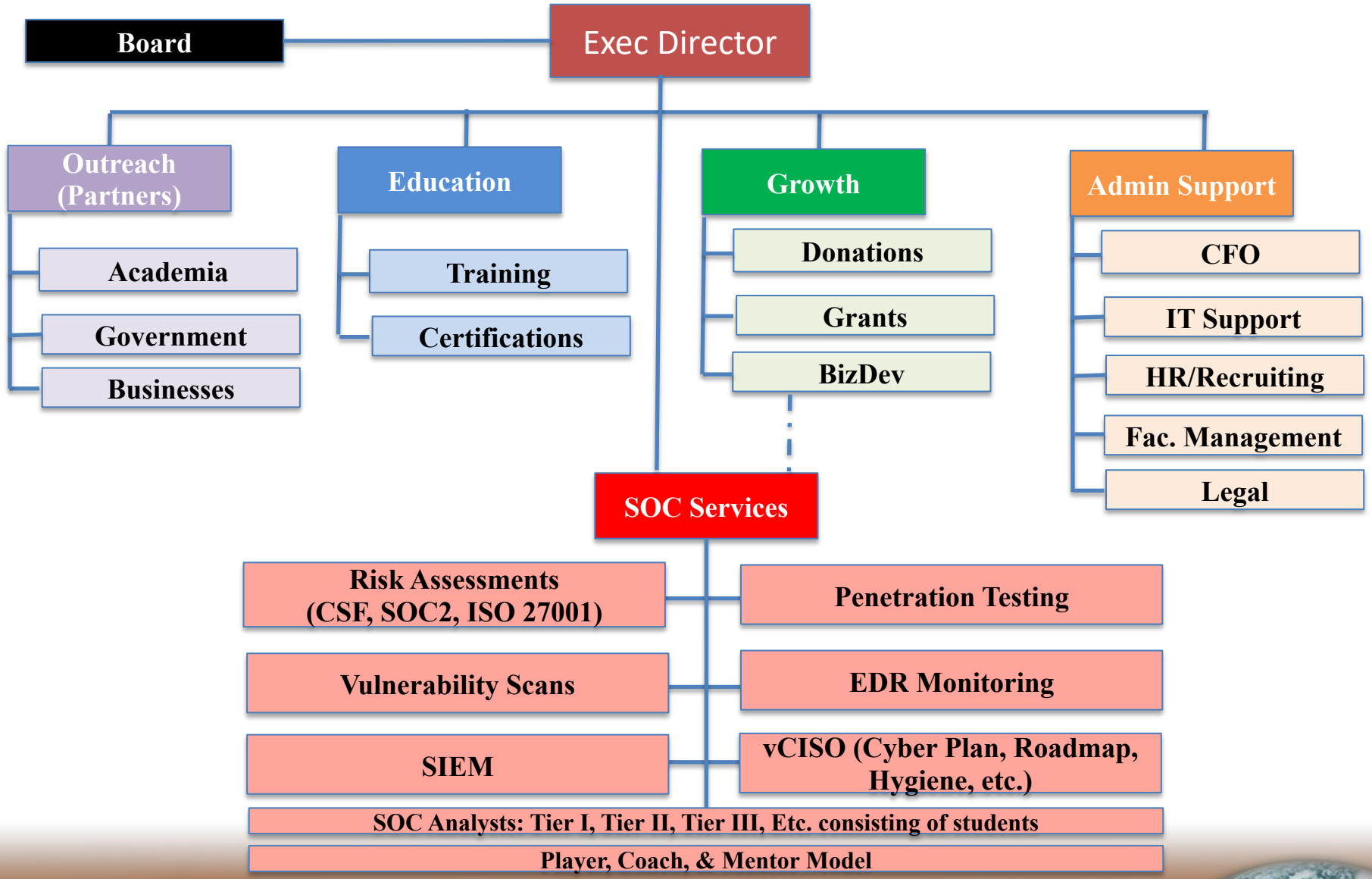
The Cybersecurity Center is not sustainable without industry leaders like yourself. I encourage you and your management team to learn more about this opportunity, and whether this model is something that will help address your workforce development needs. Regardless of your needs, please let me know how Missouri State University can best assist your business.

Very truly yours,

Clifton M. Smart III
President

OFFICE OF THE PRESIDENT

How is MCCoE Organized?

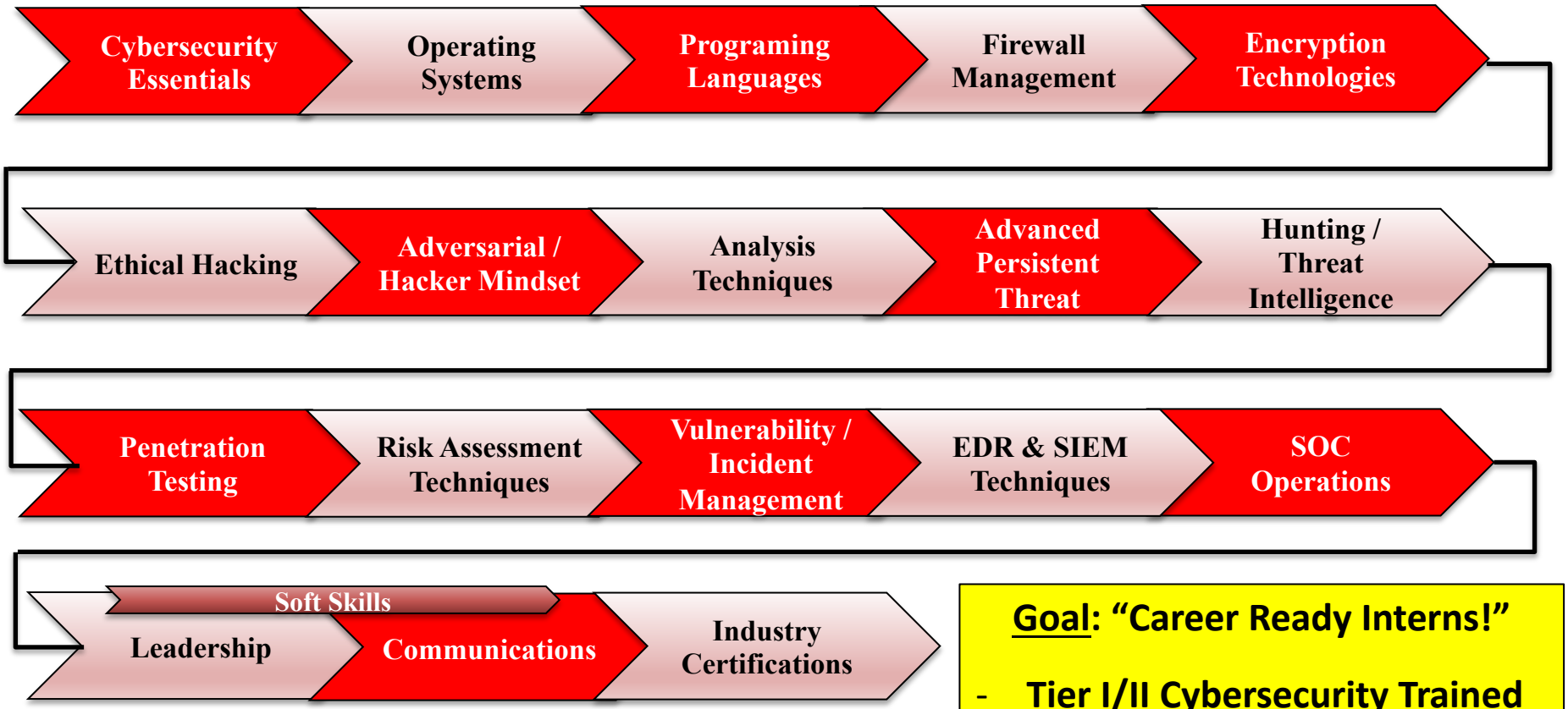


College Journey Map

(Target College Years 3 & 4)

	Aware	Study/Learn	College Fusion Ctr	MCCoE	Internship	Career
Goals	Wants to obtain a College Degree	Learn Technology Fundamentals	Building Blocks Established	Real Work Experience	Career-Ready	Make World Safer Place
Timeframe	Prior to attending college	Years 1 & 2	Years 2 & 3	Years 3 & 4	Years 3 & 4	Post Graduation
Process						
Channels	Google	Laptop	Cyber Fusion Center	MCCoE	Internships	LinkedIn

Internship Training Journey Map



Goal: "Career Ready Interns!"

- **Tier I/II Cybersecurity Trained**
- **Hands On Experience**
- **Certifications (Security+, Etc.)**
- **US Clearance**

Fellowship/Internship Methodology

Purpose and vision: Provide a tailored, flexible and purposely designed program to support our Regions students, while focused on equipping students with the tools, skills, and opportunities to successfully succeed in the professional cybersecurity workforce.

- Our vision of success in our Fellowship program is the continual re-investment of experienced, talented and driven students back into the Missouri communities and region.
- To accomplish this, the program must be designed to appeal to a wide-range of candidates and able to adjust in real-time to the needs of our individual fellowship participants.

Methodology:

- Employ a deliberate but flexible approach to each student's experience with MCCoE.
- Establish a baseline of MCCoE and cybersecurity industry knowledge for each intern.
- Utilize a tailored and phased process to identify and match each intern with focus areas and expose them to areas, processes and challenges that are unique to their experience, interest and specific talent set.
- Develop and utilize customizable timelines and transition gates for each phase.
- Assign primary mentors to provide guidance and direction during each phase of internship.

0-14 days;

PHASE I: Onboarding / Corporate Introduction

- **Emphasis:**
  - **Integration into Team MCCoE**
  - **Introductions to MCCoE Leadership, mission and organization**
  - **General knowledge of MCCoE structure, Mission, functional areas and processes**
  - **Direct Mentorship by Workforce Modernization Lead**

14-60 days

PHASE II: Focus Areas Observation / General Support

- **Emphasis:**
  - **Initial identification and integration into potential Focus Areas**
  - **Detailed exposure to MCCoE functional areas and Cybersecurity Essentials Course**
  - **Assignment of responsibilities and tasks within Focus Areas / Begin Training**
  - **Assignment and Direct mentorship by Program Manager, Director, or functional lead**

60-365 days

PHASE III: Focus Position Observation / Direct Support

- **Emphasis:**
  - **Refinement, finalization and integration of a specific Focus area**
  - **Training and Certifications**
  - **Shadow specific positions and potential employment opportunities**
  - **Review and consider reassignment of Direct Mentorship as required**

Success!

PHASE IV: Transition

- **Emphasis:**
  - **Successful Transition to Civilian Workforce**

Focus Area Definition: Functional area for Cybersecurity Professional

Phase I: Onboarding / Corporate Introduction

- **Start point: NLT 30 days prior to Start of Internship**
- Expected duration: 0-14 days after internship start date
- Key milestones/actions:
  - NLT 30 days prior: Initial contact with Sponsor (Senior intern if available)
  - 7-10 days prior to start date: Internship Onboard preparations
    - Provide intern onboard paperwork and day one check-in instructions
    - Begin administrative onboarding process where able (i.e. email account, TEAMs access)
    - Schedule onboarding meetings and administrative actions (Utilize MCCoE Intern roundtable)
  - Day 1-3: Complete Administrative Onboard and initial leadership introductions
    - Non-Disclosure Agreement and badging must be completed Day 1
  - Day 4-14: Complete Introduction and Functional area overviews with key MCCoE HQ personnel and leadership. (Timelines variable based on availability)
    - To include Resume Workshop, Interview training and other Job Placement training with Recruiting Directorate
  - Minimum bi-weekly progress / mentorship sessions with Senior Mentor- Director of Federal Strategic Relations (A.C. Coley)
- Phase I Transition Gate:
  - Determination of at least one (or more if appropriate) Potential Focus area within MCCoE based on outcomes of Progress / Mentorship sessions and evaluation of intern interests, experiences, and initial assessed fit within MCCoE.
  - Assignment of PM/Director level Mentor based on determined Focus Areas

Phase II: Focus Areas Observation / General Support

- **Start point: Completion of Phase I Transition Gate**
- Expected duration: 14-60 days
- Key milestones/actions:
  - Initial meeting with Focus Area Mentor with focus area to provide in depth understanding of job responsibilities and efforts and provide initial guidance
    - Secondary meetings with mentors in other focus areas as required
  - Assignment of standing responsibilities / tasks within focus area as determined by Focus Area mentor
    - Intent is to provide general support to Focus Area Mentor in performance of their duties while increasing level of knowledge and providing exposure within each focus area.
  - Weekly progress / mentorship sessions with Focus Area Mentor (via Stand alone or already existing events)
  - Weekly meetings with Recruiting Directorate to discuss Job placement progress and Hiring Opportunities
  - Bi-weekly progress / mentorship sessions with Senior Mentor-Director of Federal Strategic Relations (A.C. Coley)
- Phase II Transition Gate:
  - Determination / decision by Focus Area Mentor and Senior Mentor to finalize focus area based on assessment of best possible fit and opportunity within MCCoE
    - Consider assignment to shadow, mirror specific position within MCCoE
    - Develop and Sign Training Plan
  - Re-assign Senior Mentor if required based on finalized focus area or position

Phase III: Focus Area / Position Observation / Direct Support

- **Start point: Completion of Phase II Transition Gate**
- Expected duration: 60-180 days (or completion of Internship)
- Key milestones/actions:
  - Continued Assignment of standing responsibilities / tasks within focus area as determined by Focus Area mentor
    - Intent is to provide more direct support to requirements and more detailed tasks within focus area
  - If applicable, assign specific positions / team members to shadow and support
  - Bi-Weekly progress / mentorship sessions with Focus Area Mentor (via Stand alone or already existing events)
  - Weekly meetings with Recruiting Directorate to discuss Job placement progress and Hiring Opportunities
  - Monthly progress / mentorship sessions with Senior Mentor-Director of Federal Strategic Relations (A.C. Coley)
- Phase III Transition Gate:
  - ~30-60 days prior to end of internship:
    - Hiring Opportunity Meeting with Senior Mentor, Director of Recruiting to determine hiring opportunities within Spathe and / or opportunities with corporate partners.
    - This meeting provides a candid assessment of potential employment for each Intern with Spathe Systems and their intent/desires for employment. Thereby allowing interns to fully understand their opportunities and begin to make decisions on future employment.

Phase III - SOC Analyst Training Program

- **What is involved and who is targeted?**
  - College Students and Select High School Seniors
  - 2nd Career Transitions
  - DoD SkillBridge for Military Transitions

- **Structure training around Comptia Security+:**
  - 1 Year training program - College students attend the first 6 months as internship in college and the last half after graduation.
  - Anyone taking certification pays for it up front but if they pass they are reimbursed

- **Requirements:**
  - Ability to obtain security clearance
  - Must be able to pass a background check
  - Someone who has basic familiarity with computers and networking and be able to email and use Microsoft Office
  - Speaks fluent English
  - Commit to 36-week program and be regularly attended

Phase III - SOC Analyst Training Program (Con't)

- **Timeframe:**
  - Semester runs August – May with Winter and summer break
  - If we have a training staff member then summers would be additional voluntary time as well

- **Final Output -** Students will have…
  - Security Clearance
  - SOC Experience (At Least 128 Hours)
    - First 16 weeks in T1
    - Second 16 weeks in T2
  - CompTIA Security+ Certification
    - Each week align to material for the exam

Phase IV: Transition

- **Start point: Completion of Phase III Transition Gate**
- Expected duration: NLT 30 days prior to end of Internship
- Key milestones/actions:
  - Placement within MCCoE HQ.
    - Complete required administrative and onboarding for transition to MCCoE employ
  - Placement within MCCoE Partner company
  - Notification of successful employment outside of MCCoE.
  - Closeout meeting with Senior Mentor and Director of Federal Strategic Relations (A.C. Coley) to provide feedback and lessons learned on program
  - If not transitioning to employment at MCCoE, complete administrative checkout/clearance items
- Phase IV Transition Gate:
  - End of Internship and transition to civilian employment

Internship Methodology Flow Chart

MCCoE
MISSOURI CYBERSECURITY CENTER OF EXCELLENCE

PH 0 - Application & Vetting

Partner Companies Submit

Retiring / Separating DoD member

DoD SkillBridge

College Student or Civilian

College Internship

Program Application

DoD = Service Specific
College = Handshake Portal

MCCoE Intern Application Portal

MCCoE ICIMS Database

Intern Interviews with Senior Mentor / Dir of Recruiting

Assessment of MCCoE Requirements and potential Intern Fit

Qtrly Internship Update and Decision Board

- Senior MCCoE Representation
- Status update for current Interns
- Discussion of Intern Applicants
- Decision on Intern Acceptance

PH I - Onboarding

Notification of Acceptance (Senior Mentor / Dir of Recruiting)

Finalization of Internship Dates / Welcome aboard Email

DAY 1 | Initial Check-in / Onboarding

Includes
- HR (NDA)
- Security/Badging
- IT systems/ Account access

DAY 0-14 | Introductions and Baseline Training

Includes
- Senior Leader Introductions
- Functional Area 101 briefs
- Senior Mentorship Sessions
- Recruiting Job Placement Deep Dive
- Tailored training (PM / Job Placement)

DAY ~14 | PH I Transition Gate

Includes
- Focus Area & Training Determination
- Focus Area Mentor Assignment

PH II / III-Integration

Focus Area Observation / Training / Support

Includes
- Senior Mentor Updates/meetings
- Basic Cybersecurity Essentials
- Focused Training
- Focus Area mentor Meetings
- Job Placement and Hiring Opportunities Updates
- Tailored training (SOC Analyst)

NLT 30 Days before end of Internship | PH III Transition Gate

Hiring Opportunity Meeting Senior Mentor and Dir of Recruiting)

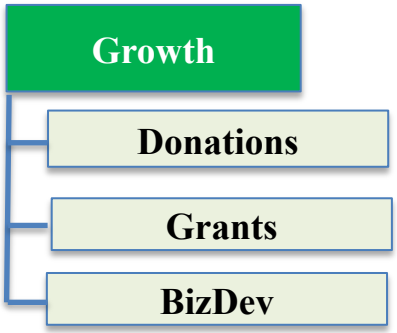
NOTE: Transition between PH II and III will be flexible and specific to each Intern.

PH IV – Transition

Includes
- Administrative Checkout/Clearance items
- Specific to Job Placement results (MCCoE Systems vs Other employer)
- Final Closeout with Senior Mentor
- Completion of Intern Exit Survey and Testimonial Interview Video (Optional)

How is MCCoE Funded?

Funding comes from three (3) Sources:



- **Donations - Individual & Corporate**. We have hired a company to assist with a goal of $250K annually. It is costing us about $5K. As to date we have averaged only about $20K a year.

- **Grants.** We have hired a company to assist with a goal of $500K annually. It is costing us about $8K. Over past two years we have won $1.6M for the SOC Build-out (Building, Furniture, and HW/SW).

- **BizDev**. We have a part-time BizDev person. So far, we have spent $2,000 and have six (6) clients and one (1) Five-year contract with a City. Goal is to generate $500K with 10 Contracts annually; but we are not there now with only $18K last year.

Students in the News

Drury University student attempts to hack city of Springfield in cybersecurity partnership

By Shoshana Stahl
Published: May. 20, 2022 at 8:08 PM CDT

SPRINGFIELD, Mo. (KY3) - Drury University partnered with the city of Springfield to ensure its network is guarded against malicious hackers.

Is Staff Paid or Volunteer?

We have adopted a **Player, Coach, Mentor Strategy** consisting of:

1. **Paid Staff** (Full Time (FT) and Part Time (PT) Mix): ($168K for 2024)
    1. Exec Director (PT)
    2. SOC Manager (FT)
    3. Penetration Test Lead (PT)
    4. Vulnerability Scan Lead (PT)
    5. IT Support Lead (PT)
    6. Assessment Lead (PT)
    7. SIEM/EDR Lead (FT)

2. **Unpaid Staff** – AKA Volunteers consisting of Students, Industry and Academia partners.

Notes:

1. Crawl, Walk, & Run (CWR) Strategy
2. As a 501.c.3 we do not have to pay Interns. However, we want to attract talent, so we pay:
    a. Entry Level – Unpaid to Paid at $12.30/hr (Min Wage)
    b. Mid Level – $15/hr
    c. Sr Level – $15-$20/hr

Sample MCCoE Budget

	2024	2025	2026	2027	2028
Total Students Served	9	25	55	65	75
Total Clients Served	15	35	48	65	90
Expenses					
Comercial/Payment Processing Fees	3,398	7,661	11,710	12,694	16,290
Rent Expesne	40,080	48,060	48,060	48,060	48,060
Utilities Expense	3,000	3,750	4,688	5,859	7,324
Labor Expense	168,992	388,361	640,740	694,325	761,060
Student Certification	0	12,100	22,000	22,000	22,000
Marketing	24,695	21,715	21,514	30,000	30,000
Phone/Internet	1,750	2,100	2,100	2,100	2,100
Software and Licensing	12,000	13,200	14,520	15,972	17,569
Insurance	1,500	1,650	1,815	1,997	2,196
Tax and Licences	100	100	100	100	100
Additional Expenses	8,000	10,000	12,000	14,000	16,000
Total Expense	263,515	508,697	779,247	847,107	922,699
** Interns receive 144 Hours Per Semester; Paid Interns receive $15/hr pay for internships*					
** Interns are eligible to receive paid certifactions for CompTIA Security+*					
** Budget Maps to Goals*					
** Volunteers from Industry, Gov,, and Academia used to agument Mentors and Coaches*					
** Years 1-3 require increased Donations and Grants and declines Years 4-5*					

Discussion & Questions

Contact Info:

524 N Boonville Ave, Springfield, MO 65806

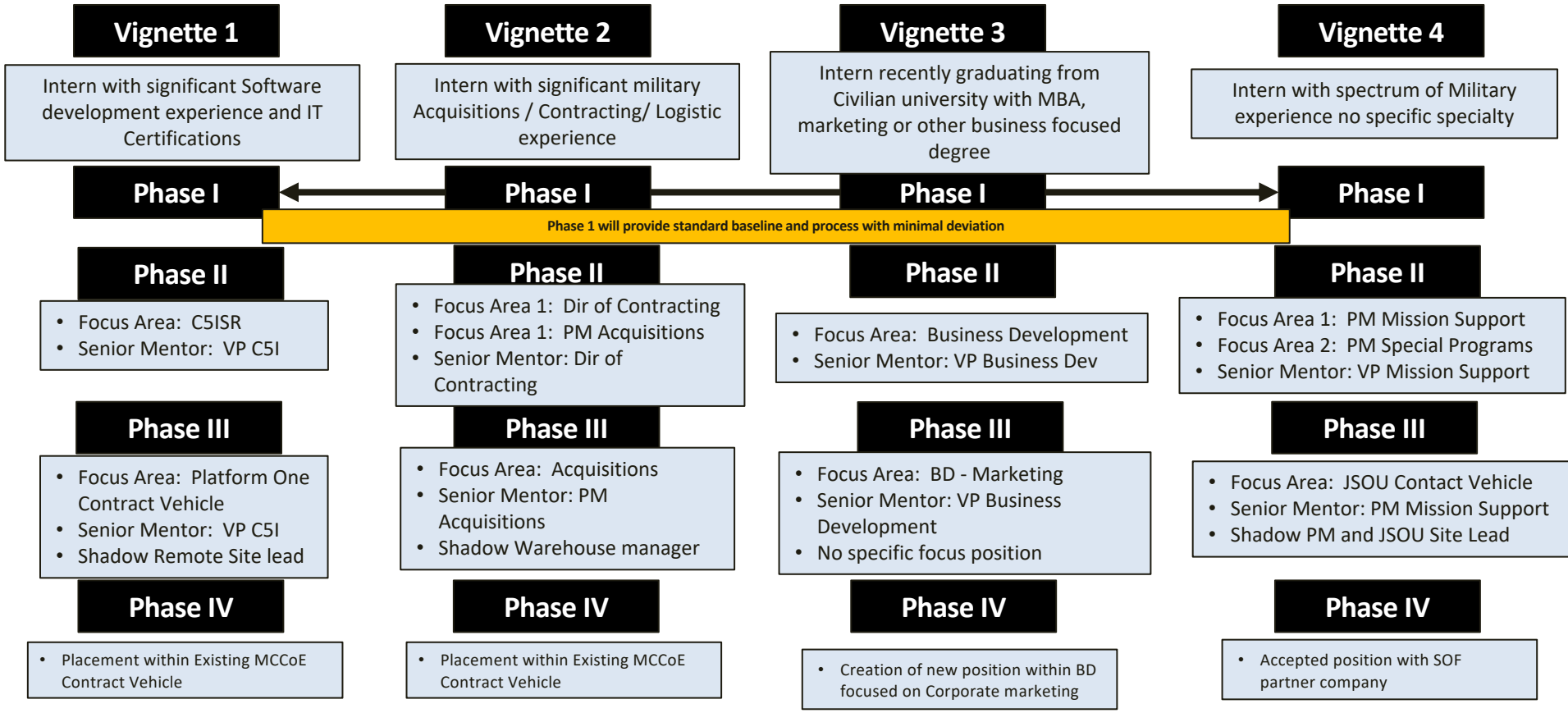
P: (417) 553-1020

F: (417) 763-3214

501.c.3 Non-Profit **www.MCCoE.org**

BackUp Slides

Intern / Fellowship Vignettes



Phase III - SOC Analyst Training Program

- **Tier 1 SOC Analyst Training Program**

  Week 1 - Onboarding

  Week 1 – Learning ReflexSOAR

  Week 2 – Cybersecurity Analyst

  Week 3 thru 16 – Internship

- **Tier 2 SOC Analyst Training Program**

  Week 17 – Incident Response Lifecycle

  Week 18 thru 32 – Internship

Phase III - SOC Analyst Training Program (Con't)

MCCoE Security+ Training Program

Week 1 and 2 - Today's Security Professional
Week 3 and 4 - Cybersecurity Threat Landscape
Week 5 and 6 - Malicious Code
Week 7 and 8 - Social Engineering, Physical, and Password Attacks
Week 9 and 10 - Security Assessment and Testing
Week 11 and 12 - Secure Coding
Week 13 and 14 - Cryptography and the Public Key Infrastructure
Week 15 and 16 - Identity and Access Management
Week 17 and 18 - Resilience and Physical Security
Week 19 and 20 - Cloud and Virtualization Security
Week 21 and 22 - Endpoint Security
Week 23 and 24 - Network Security
Week 25 - Wireless and Mobile Security
Week 26 and 27 - Incident Response
Week 28 and 29 - Digital Forensics
Week 30 - Security Policies, Standards, and Compliance
Week 31 - Risk Management and Privacy
Week 32 - Final Security+ Exam Review Week

SOC Training Program

- **SOC Training Program**
  - What training will be included outside the hands-on SOC work?
    - How to use SOC Solution
    - Basic evacuation procedures
    - When will we provide this (times/days)?
    - Where will we provide this?
    - What staffing will provide this?
  - Use CompTIA for Security+ training

- **SOC Lab Program**
  - Processes for analysis, triage, and escalation
  - Processes for escalation and who to escalate it to
  - When will we provide this (times/days)?
  - Where will we provide this?
  - What staffing will provide this?
  - User Experience Training 1 – 2 hours per week and work with clients plus Google Certificate course

SOC Training Program (Con't)

Requirements
To become a Cybersecurity SOC Analyst, it will take a combination of skills, education, and hands-on work experience, with an option of certification. Some of the skills that you will want to have before starting a new career are listed below.

1. Cybersecurity Essentials (2 days)
An accessible introduction to cybersecurity concepts and practices guided by NIST CSF and CISA Concepts. Cybersecurity Essentials provides a comprehensive introduction to the field, with expert coverage of essential topics required for entry-level cybersecurity certifications.

Learning Objective: Identify the Cybersecurity Essentials?

2. Operating systems (5 days)
You will need at least an intermediate level of familiarity with Windows, macOS, Linux and other operating systems to be competitive. Not all organizations use the same operating system so diversify your skill set to include as many relevant operating systems as you can.

Learning Objective: What is an Operating System (Windows, macOS, Linus and others)? How to install, and how to maintain.

SOC Training Program (Con't)

3. Firewall management (4 days)
Cybersecurity consultants are expected to have proficient firewall management skills. Specific skills related to this position include breach detecting, backups and fail-safe features.

Learning Objective: How to conduct Firewall Management?

4. Encryption technologies (3 days)
Encryption is increasingly being used as a key line of defense against data theft and destruction. Cybersecurity consultants should have a good understanding of how encryption will impact the organization's operations and have experience implementing an encryption solution.

Learning Objective: What are Encryption Technologies and howe to implement?

5. Advanced Persistent Threat management (3 days)
Advanced Persistent Threats, or APTs, are multi-stage attacks that may proceed through a variety of different attack vectors. Examples of the knowledge required include network access control, phishing and social engineering.

Learning Objective: What is Persistent Threat Management and how to implement?

SOC Training Program (Con't)

7. Principles of ethical hacking and coding practices (5 days)
When you think like a hacker you can better stop them in their dirty deeds. The skills required include a firm understanding of threat modeling and configuration.

Learning Objective: What is ethical hacking and coding practices? How to use ethical hacking to strength an organizations cyber hygiene.

Penetration testing (10 days)
This position will require you to act as both the attacker and defender with regard to your client's network and security environments. One example of real-life penetration testing skills is the ability to measure the vulnerability of a client's applications and software.

Learning Objective: How to conduct Penetration Testing?

SOC Training Program (Con't)

8. Adversarial/Hacker Mindset (2 days)
The other side of the proverbial coin is knowing how hackers/attackers think. Knowing how hackers think will help a cybersecurity consultant better predict the strategies used and where attacks are more likely to be focused. It's almost more important to be able to think like a hacker than to think from a more defensive mindset.

Learning Objectives: How to think like an adversary/hacker? What are the types of hacker attack trajectories?

9. Programming languages used in raw data storage and processing (20 days)
The same rule applies here as it does with the operating system skills from above. The more programming languages you know that are used in raw data storage and processing, the better off you will be.

Learning Objective: Understand programing languages used in raw data storage and processing. Be able to develop and execute a program on raw data files and show how they can be processed as part of the cybersecurity mission.

SOC Training Program (Con't)

10. Analysis Techniques (5 days)
SOC Analysts need to have solid analysis skills. This includes the application of industry standard analysis criteria where necessary, such as when analyzing organization security solutions.

Learning Objective: Demonstrate industry standard understanding of data and problem analysis as relates to an organizations security solution. Demonstrate use of tools to assist in the analysis of data.

11. Soft skills - There are a range of soft skills SOC Analysts rely on daily, consisting of:

11.a. Leadership skills (1 day)
Working as a consultant requires leadership skills. A SOC Analysts will often have to take a leadership initiative in solving potential organization cybersecurity issues proactively; in the most involved of situations, you will even be responsible for a security team that reports to you. This takes a high level of leadership skills, especially managing a security.

Learning Objective: Demonstrate ability to engage with client, peers, and supervisors in an effective and professional way. Demonstrate ability to work with limited to no supervision

SOC Training Program (Con't)

11.b. Communication skills (1 day)

Effective communication is required to manage security teams but even with clients that do not have a security team you will have to have regular effective communication with executives, department heads, and sometimes even the end user. Without strong communication skills, it's nearly impossible to be a successful cybersecurity consultant.

Learning Objective: Demonstrate ability to communicate (written and verbal) with clients, peers, and supervisors in an effective and professional way. Demonstrate ability use administrative communication tools such as MS Powerpoint, MS Excel, MS Project, MS Word, email, text, MS Teams, MS Zoom, and social platforms.

12. Education (TBD)

There are no set education requirements for becoming a SOC Analysts. That said, there are some common ways for professionals to demonstrate that they possess the right education level — mostly by earning a bachelor's degree. Many earn a bachelor's degree in information technology, computer science, cybersecurity and related fields. Others satisfy this requirement by gaining the equivalent work experience with relevant certifications.

SOC Training Program (Con't)

13. Work experience (Goal to Obtain 1 year)

There is no set-in-stone progression of work experience necessary to become a SOC Analysts. With this said, cybersecurity consultants in the United States are expected to have three to five years of professional experience.

What would a career path for a cybersecurity consultant look like? Below is one example of a realistic work experience path to becoming a consultant:

- Enter an entry-level IT or information security role
- Earn the role of security administrator, analyst, engineer or auditor
- Acquire some relevant information security certifications
- Begin role of cybersecurity consultant

This may take you longer than three to five years. The position is not one-size-fits-all, and this extends to the length of time needed to gain enough experience.

SOC Training Program (Con't)

14. Certifications (Self Paced)

There is no one specific certification that you need to earn for this position, but the more you have, the better. Certifications you can use to help earn this position span the whole range of information security certifications — from beginner to expert. While our training will align with various Industry Standards (ref. below), and we will pay for "select" students taking the Certification tests, students will have to engage with an Industry Standard partner highlighted by following industry certifications:

- CompTIA Security+
- Cybersecurity Analyst (CySA+)
- Certified Ethical Hacker (CEH)
- EC-Council Certified Security Analyst (ECSA)
- Certified Information Security Manager (CISM)
- Certified Information Systems Security Professional (CISSP)
- Offensive Security Certified Professional (OSCP)

SOC Training Program (Con't)

15. Competency Definition: The career path of a cyber security consultant is similar to that of any other cyber security professional in some ways but diverges in others. There is no "entry level" cyber security consultant role; in order to work as an in-demand consultant, you'll need training, education, and years of experience. In fact, a consultancy can be seen as the pinnacle of a cyber security career — a role in which you choose your clients, name your prices, and determine your own hours.

16. Competency Assessment: When evaluating the proficiency following Cybersecurity Training, we will conduct proficiency evaluations through various assessment methods, such as self-assessment, manager assessments, 360-degree feedback, hands on exercise, and performance appraisals.

- Our Rubrics criteria are used for grading/assessing the students and are clearly spelled out along a continuum. We will utilize an **Analytic Rubrics:** Separate scales for each trait, or learning outcome, being assessed within the assignment (e.g., separate scales for "Argument," "Organization," "Use of Evidence," etc.). whereby letters are assigned certain percentage values out of 100% or are given a named value such as Excellent, Good, Fair, Poor, & Failure.

17. Gap Analysis: Our Gap Analysis will compare the current competency levels of employees with the desired levels for Cybersecurity Consultant roles, highlighting areas where improvement or development is needed.