

NCyTE FACULTY EXTERNSHIP PROGRAM:
2024 ANNUAL
REPORT

Connecting Cybersecurity Faculty with Industry

PROGRAM YEAR 2024

Kyle Jones

Department of Information Technology,
Sinclair Community College

Prepared from participant final reports, program records, and applicant data.

Table of Contents

01.	EXECUTIVE SUMMARY	3
02.	PROGRAM OVERVIEW	4
03.	THE 2024 COHORT	5
04.	EXTERNSHIP HIGHLIGHTS	6
05.	WHAT THE COHORT LEARNED: CROSS-CUTTING THEMES	9
06.	CURRICULUM IMPACT 2024-25	11
07.	PARTNERSHIPS & NETWORKING	12
08.	PROGRAM EVOLUTION & FUTURE DIRECTIONS	13

ABOUT THIS REPORT

The NCyTE Faculty Externship Program Annual Report summarizes the accomplishments and impact of the 2024 program year. Developed from participant final reports, program records, and application data, it showcases how faculty externships bridge education and industry by fostering professional growth, strengthening curriculum, expanding strategic partnerships, and aligning cybersecurity education with evolving workforce needs. The report also captures emerging trends, best practices, and program outcomes that continue to guide the externship's growth and long-term impact.



Executive Summary

In 2024, the NCyTE Faculty Externship Program placed eleven cybersecurity, information technology, and engineering technology faculty members inside working industry and enterprise environments for a minimum of 80 on-site hours each. Drawn from an applicant pool of 24 faculty across 13 states, the completing cohort represented institutions in ten states and worked with hosts spanning an unusually wide range of sectors: industrial automation, community banking, coatings manufacturing, defense contracting, cybersecurity consulting, enterprise campus IT, quantum-computing research, a professional governance association, and the maritime industry.

The 2024 cohort’s findings converged on a consistent message: there is a real gap between what students expect of cybersecurity careers and what employers actually need, and closing it requires early and frequent industry exposure, hands-on work with real equipment, and deliberate instruction in soft skills, documentation, teamwork, and compliance. Every completing participant returned with concrete curriculum plans — from new Industrial IoT labs built on donated hardware to quantum-cryptography modules, MSSP evaluation exercises, tabletop scenarios, and team-based projects — and several placements produced immediate, tangible wins for students, including hires, internship pipelines, donated equipment, and a proposed annual student training stipend.

24	11	13	10	80+
Applicants	Participants	Applicant States	Participant States	On-Site Hours Each

Program Overview

The Faculty Externship Program connects educational institutions with industry partners to give instructors direct, hands-on exposure to real-world cybersecurity and IT operations. Faculty commit to a minimum of 80 on-site hours during the summer — through group meetings, one-on-one interviews, facility tours, research, and project contributions — and are frequently encouraged to arrange placements through advisory boards, local business networks, or their state’s Manufacturing Extension Partnership (MEP) offices. Each participant documents the experience in a comprehensive final report with clear recommendations for new processes, procedures, or curricula, to be implemented in the following academic year, and shares the experience with departmental colleagues through a fall presentation.

2024 Selection Pipeline

Applications Received	24 faculty from 13 states (Ohio led with 5 applicants)
Applicant Profile	20 of 24 were full-time faculty; all 24 could commit 80 hours and had administration support; 13 were already familiar with their state’s MEP system
Demographics Tracked	Gender and race data collected across the applicant pool to monitor program reach
Cohort Completing	11 faculty from 10 states, placed with hosts spanning industrial automation, banking, coatings manufacturing, defense contracting, consulting, higher-education IT, a professional association, and the maritime sector
Reporting	Final narrative reports and supporting documentation collected and synthesized into program-level summary documents

The 24 applicants came from California, Colorado, Florida, Georgia, Illinois, Indiana, Maryland, Missouri, New Jersey, North Carolina, Ohio, Tennessee, and Washington, with Ohio contributing the largest share. Program administration in 2024 maintained detailed applicant records — including qualifying-question responses, statements of fit, and demographic data — along with color-coded review lists and a check against prior-year applicants who had not completed, groundwork that shaped the more formalized ranking process adopted in 2025.

The 2024 Cohort

Eleven faculty members completed externships and submitted final reports. The cohort and placements were as follows:

Cohort Placements

Faculty Participant	Home Institution	Externship Host	Host Location
Ulku Clark	University of North Carolina Wilmington (NC)	Maritime sector — multiple locations	Various
Jason Edmondson	Augusta Technical College (GA)	Scientific Research Corporation	Augusta, GA
Carmela Gonzales	Capitol Technology University (MD)	ISACA Greater Washington DC Area	Arlington, VA
Brian Hurley	Metropolitan Community College–Kansas City (MO)	Blue Ridge Bank and Trust Company	Independence, MO
Jiri Jirik	Moraine Valley Community College (IL)	Keller Schroeder and Associates	Evansville, IN
Nelly Mulleneaux	Purdue Global (IN)	Purdue Global, School of Behavioral Science	West Lafayette, IN
Andrew Rettig	Sinclair Community College (OH)	Opto 22 Headquarters	Temecula, CA
Nathan Roskop	Pikes Peak State College (CO)	Confidential manufacturing company	Colorado Springs, CO
Mohammad Shanehsaz	Brookdale Community College (NJ)	Brookdale Office of Information Technology	Lincroft, NJ
Joel Shaw	Metropolitan Community College–Kansas City (MO)	Tnemec Company, Inc.	N. Kansas City, MO
Khalid Tantawi	University of Tennessee at Chattanooga (TN)	UTC Information Technology Services	Chattanooga, TN

One host organization requested that its identity remain confidential and is therefore identified above only by sector and location.

Externship Highlights

Industrial IoT, Hands-On: Andrew Rettig at Opto 22

Andrew Rettig, Assistant Professor and IoT Coordinator at Sinclair Community College, completed his externship with Opto 22, a leader in the Industrial Internet of Things (IIoT) space, at its Temecula, California headquarters. His goal was to understand how companies are bridging the OT/IT divide — and the experience exceeded expectations. Through comprehensive training on the groov EPIC system, groov Manage and View, PAC Control, Ignition Edge, MQTT/Sparkplug, and Node-RED, he gained the foundational knowledge to activate five recently purchased devices in Sinclair’s advanced IoT course, complete with vendor-provided introductory labs. The partnership continues to grow: Opto 22 has connected Sinclair with a California community college on IoT controls curriculum, invited follow-on training with partner Inductive Automation, and is exploring an annual stipend award sending one Sinclair student to Opto 22 training each year.

Securing a Manufacturer: Joel Shaw at Tnemec Company

Joel Shaw, full-time CSIS faculty at Metropolitan Community College–Kansas City, embedded with the IT leadership of Tnemec Company, a coatings manufacturer in North Kansas City, as they searched for a new Managed Security Service Provider (MSSP). Working directly with the company’s IT Director and Vice President, he drafted proposed Service Level Agreements for MSSP/MDR services, documented vendor evaluations, and researched ideal MSSP contract terms — producing deliverables the company used in selecting its partner. The experience yielded candid lessons about small and mid-size business security: vendor quality depends on onboarding, communication, and transparency; IT staff are often assumed to have security expertise they were never trained for; and policy only works with employee compliance. The relationship has already paid off for students — one MCC graduate was hired by the company, with a second under consideration — and Tnemec employees are engaging with MCC’s Cyber Security Club.

Additional Placements Across the Cohort

- **Khalid Tantawi (UT Chattanooga)** — Shadowed the installation of network switches in a university data center and confronted the reality of securing a campus network of more than 43,000 connected devices; he plans to present his findings at the CyAD conference and to propose institutional funding for student and faculty externships.
- **Jiri Jirik (Moraine Valley CC)** — At Keller Schroeder and Associates, gained hands-on Governance, Risk, and Compliance (GRC) consulting experience that validated and exceeded expectations, and will now emphasize business acumen, report writing, ethics scenarios, and team-based projects culminating in oral and written deliverables.
- **Brian Hurley (Metropolitan CC–Kansas City)** — At Blue Ridge Bank and Trust, documented the gap between student expectations and actual job duties, added new members to his industry advisory board, and is discussing a standing intern/shadow role for students at the bank — which has a history of hiring the college’s graduates.
- **Jason Edmondson (Augusta Tech)** — At Scientific Research Corporation, which builds cybersecurity training environments for TRADOC, learned that roughly 75% of the work was collaborative planning and design — prompting a shift away from “cookbook-style” labs toward guided exploration, team roles, and after-action reviews, while SRC internships are promoted to students.
- **Mohammad Shanehsaz (Brookdale CC)** — Worked alongside her college’s Office of Information Technology on a live upgrade of more than 64 IDF closets to Cisco 3850/9000-series switches — VLANs, port security, port channels, stacking, and Meraki cloud management — with replaced equipment repurposed directly into her classroom labs.
- **Nelly Mulleneaux (Purdue Global)** — Researched quantum key distribution (QKD) and post-quantum cryptography (PQC) with Purdue Global colleagues and is proposing a specialized quantum cybersecurity track, bringing quantum-resilient encryption into computing coursework.

Additional Placements Across the Cohort

- **Carmela Gonzales (Capitol Technology University)** — Embedded with ISACA’s Greater Washington DC chapter, mapping industry programming — zero trust, AI-driven threat detection, IoT/cloud security, governance frameworks — against her graduate research curriculum, and planning “meet the industry” events and ethics workshops.
- **Ulku Clark (UNC Wilmington)** — Explored maritime-sector cybersecurity across multiple locations, including IMO-driven international standards, IT/OT security differences, and the port-security implications of GPS blockers.
- **Nathan Roskop (Pikes Peak State College)** — Completed his externship with a Colorado Springs manufacturing company, strengthening his college’s connection to regional manufacturing and DoD-adjacent employers, with plans for advisory sessions, MSP networking, and student internships.

2024 Host Sectors



What the Cohort Learned

- Cross-Cutting Themes -

Synthesis of the eleven final reports surfaced consistent themes across very different host environments:

- **Early and Frequent Industry Exposure** — Participants repeatedly stressed that students need exposure to employers and industry practices early and often — through internships, shadowing, site visits, guest speakers, and case studies — to align expectations with real job roles.
- **Certifications Alone Are Not Readiness** — The most cited gap: graduates hold certifications yet still face a readiness deficit, because employer expectations and technologies vary widely and substantial on-the-job learning is always required. Curricula should teach students to work with and troubleshoot technology, not only build it from scratch.
- **Soft Skills Decide Hiring Outcomes** — Employers consistently prefer candidates with strong critical thinking, communication, professionalism, and teamwork — sometimes over stronger technical skills — driving plans for team projects, presentations, documentation exercises, and tabletop scenarios.
- **Real Equipment Changes Teaching** — Hands-on experience with actual equipment — from IIoT controllers to enterprise switches, network testers, and SIEM interfaces — was the single most valued takeaway, and faculty plan to integrate real devices and industry tools directly into labs.
- **Scale, Documentation, and Compliance Are the Daily Reality** — From a 43,000-device campus network to a mid-size manufacturer's MSSP search, participants saw that effective security depends on collaboration, meticulous documentation, compliance, and coordination across teams and vendors.

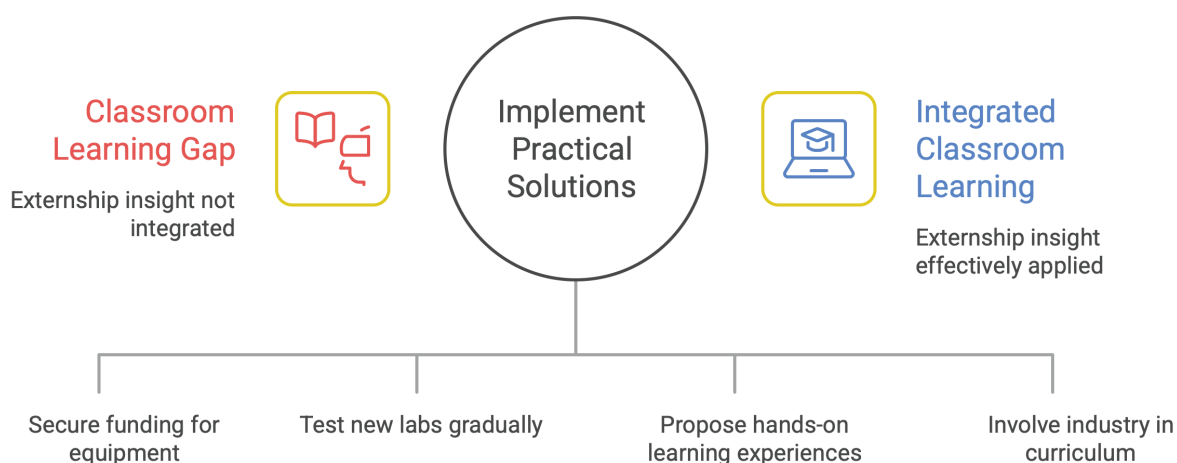
Challenges Identified

Participants identified several practical constraints to translating externship insights into the classroom:

- Curriculum changes require administrative approval and lengthy implementation processes.
- Students often lack access to the devices, professional platforms, and resources needed for realistic, hands-on learning.
- Graduates frequently enter the workforce with underdeveloped soft skills.
- IT professionals in industry often juggle broad, multi-role responsibilities that are not reflected in narrowly focused academic courses.

Responses include pursuing grant funding for equipment, piloting new laboratory experiences, proposing practicum courses, and increasing advisory board involvement in curriculum design.

Bridging Externship and Classroom Learning



Curriculum Impact 2024-25

Every completing participant returned with specific curriculum commitments. Representative plans include:

- **Sinclair College** will add a full week of IIoT content to its advanced IoT course — built on Opto 22 devices, Ignition Edge, MQTT, and Node-RED — with foundation labs serving as the launchpad for advanced student projects.
- **Metropolitan CC–Kansas City** will add SIEM evaluation, logging, backup, and documentation assignments to IT Fundamentals and Linux courses, expand tabletop exercises with realistic scenarios, and propose a dedicated practicum course.
- **Augusta Tech** will convert step-by-step Microsoft Client labs into collaborative, plan-first team projects with randomly assigned team leads and after-action reviews, plus a new lab on troubleshooting misapplied NTFS/share permissions.
- **UT Chattanooga** will bring network testers and data-center infrastructure content into troubleshooting instruction, using real cases — including a costly cabling-pathway decision — to teach planning and IT assessment.
- **Moraine Valley CC** will implement team-based GRC project scenarios that culminate in oral and written reports, enriched with real consulting case studies and ethical dilemmas.
- **Purdue Global** will integrate QKD and post-quantum cryptography content into computing courses and pursue a specialized quantum cybersecurity track.
- **Brookdale CC** will expand individualized hands-on training using donated layer-3 switches, stackable cables, and UPS units from the campus infrastructure upgrade, alongside cloud-management, AWS/Azure, and Palo Alto firewall content.

Faculty will measure impact through lab rubrics and test items tied to new content, pre/post student surveys, project outcomes and engagement, qualitative feedback from hiring managers and recent graduates, and ongoing advisory-board input — with several participants explicitly weighing both tangible results and intangible benefits.

Partnerships & Networking

The 2024 externships generated concrete, continuing benefits for students and programs:

- **Tnemec Company** hired one MCC graduate, with a second under consideration for entry-level work, and company staff are engaging with the college's Cyber Security Club and student Q&A sessions.
- **Blue Ridge Bank and Trust** is discussing a regular intern/shadow role for students and contributed new members to the program's industry advisory board.
- **Opto 22** is exploring an annual stipend award to send a Sinclair student to its training program, facilitated a curriculum collaboration with a California community college, and opened follow-on training with partner Inductive Automation.
- **Scientific Research Corporation** deepened its relationship with Augusta Tech, supporting competitive internship opportunities for students.
- **UT Chattanooga's** participant plans a joint proposal with IT Services for institutional funding to create student and faculty externships, and will present results at the CyAD conference.
- **Brookdale's** participant secured donated enterprise equipment for classroom labs and positioned students for job openings within the campus IT organization.
- Consulting, association, and maritime placements produced standing contacts for guest lectures, advisory boards, case studies, and student networking through professional organizations.



Program Evolution & Future Directions

The 2024 program year demonstrated the program’s flexibility. While rooted in manufacturing through the MEP network, successful placements also occurred in banking, defense, consulting, professional associations, campus-enterprise IT, and research environments, each producing classroom-ready outcomes.

Administrative practices introduced in 2024—including demographic tracking, prior-completion checks, and structured applicant review—laid the foundation for the formal eight-member ranking panel and standardized selection process adopted in 2025.

Combined with the strong applicant-to-seat ratio and the tangible curriculum, partnership, and student outcomes documented throughout this report, the 2024 program affirmed the externship as one of NCyTE’s most effective strategies for keeping cybersecurity education aligned with workforce needs.

NCYTE CENTER

National Cybersecurity Training & Education Center

The **National Cybersecurity Training and Education Center (NCyTE)** at Whatcom Community College, funded by the NSF, enhances U.S. cybersecurity education by supporting faculty, developing resources, and strengthening industry partnerships to build the cybersecurity workforce.



The National Cybersecurity Training and Education Center is funded by the National Science Foundation grant #2054724.