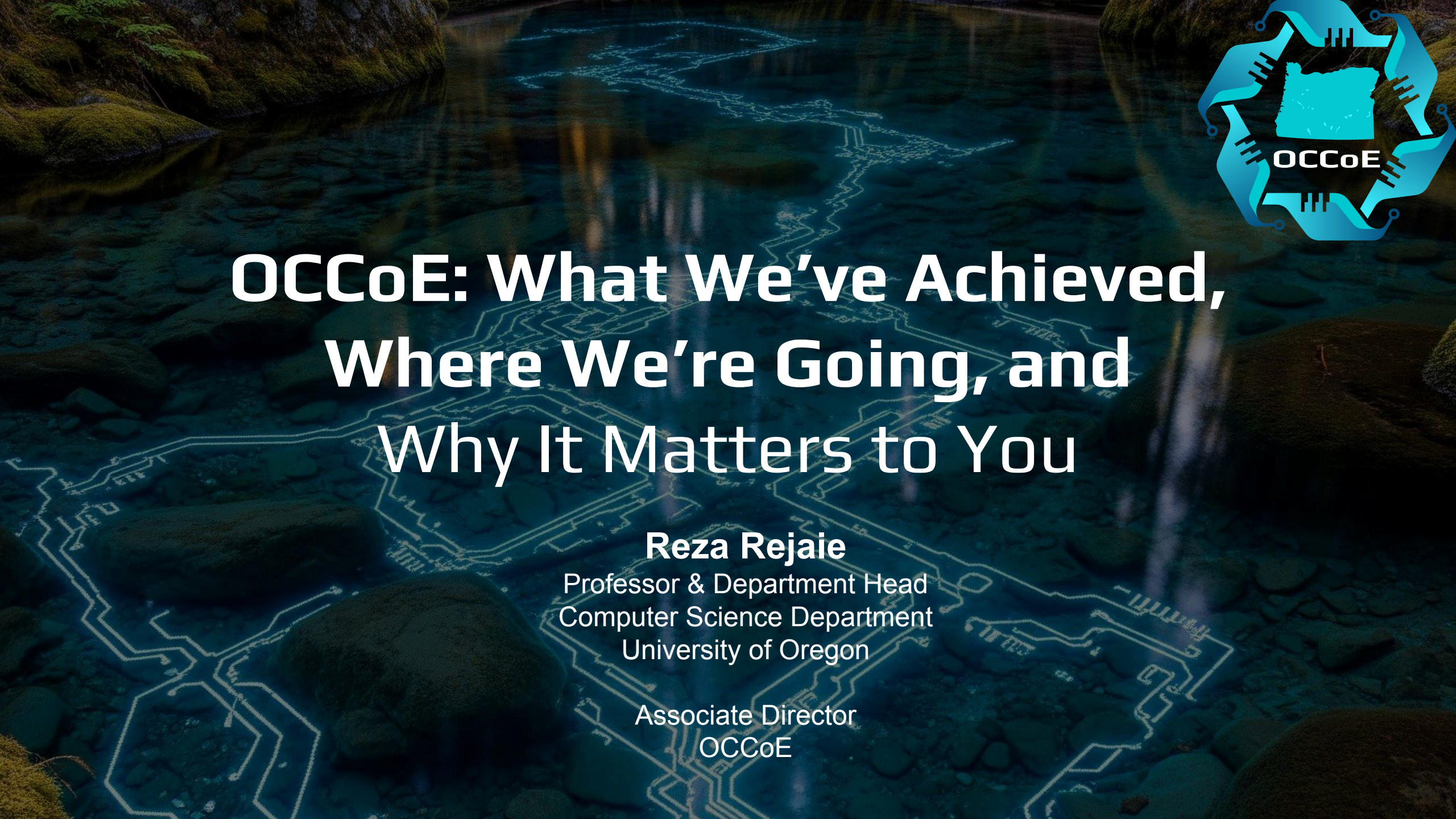


OCCoE: What We've Achieved, Where We're Going, and Why It Matters to You

Reza Rejaie
Professor & Department Head
Computer Science Department
University of Oregon

Associate Director
OCCoE

Purpose of This Presentation

OCCoE was created to enhance Oregon's cybersecurity posture statewide.

This presentation provides:

- A brief overview of OCCoE
- A summary of progress made during the first biennium (2023–2025)
- A preview of plans for the second biennium (2025–2027)

Why it matters to you:

- OCCoE's activities directly or indirectly impact your organization
- There are many opportunities for you to engage, collaborate, and benefit

A Brief Overview of OCCoE

- OCCoE was established in Fall 2023 through the passage of HB2049.
- OCCoE's mandate includes coordinating, funding, and providing:
    - Workforce development, goods and services, advising, outreach, awareness, research, information sharing, assessment, and industry partnerships — all related to cybersecurity.
- Workforce development has been a central focus.
- Strong partnerships with high schools and industry are essential.
- OCCoE is co-present and co-led by PSU, OSU, and UO.
    - Each university brings a complementary set of strengths and capabilities.
- Our Advisory Council includes representatives from local and regional governments, special districts, and other key stakeholders.

Key Activities: 1st Biennium (2023–2025)

Program Development

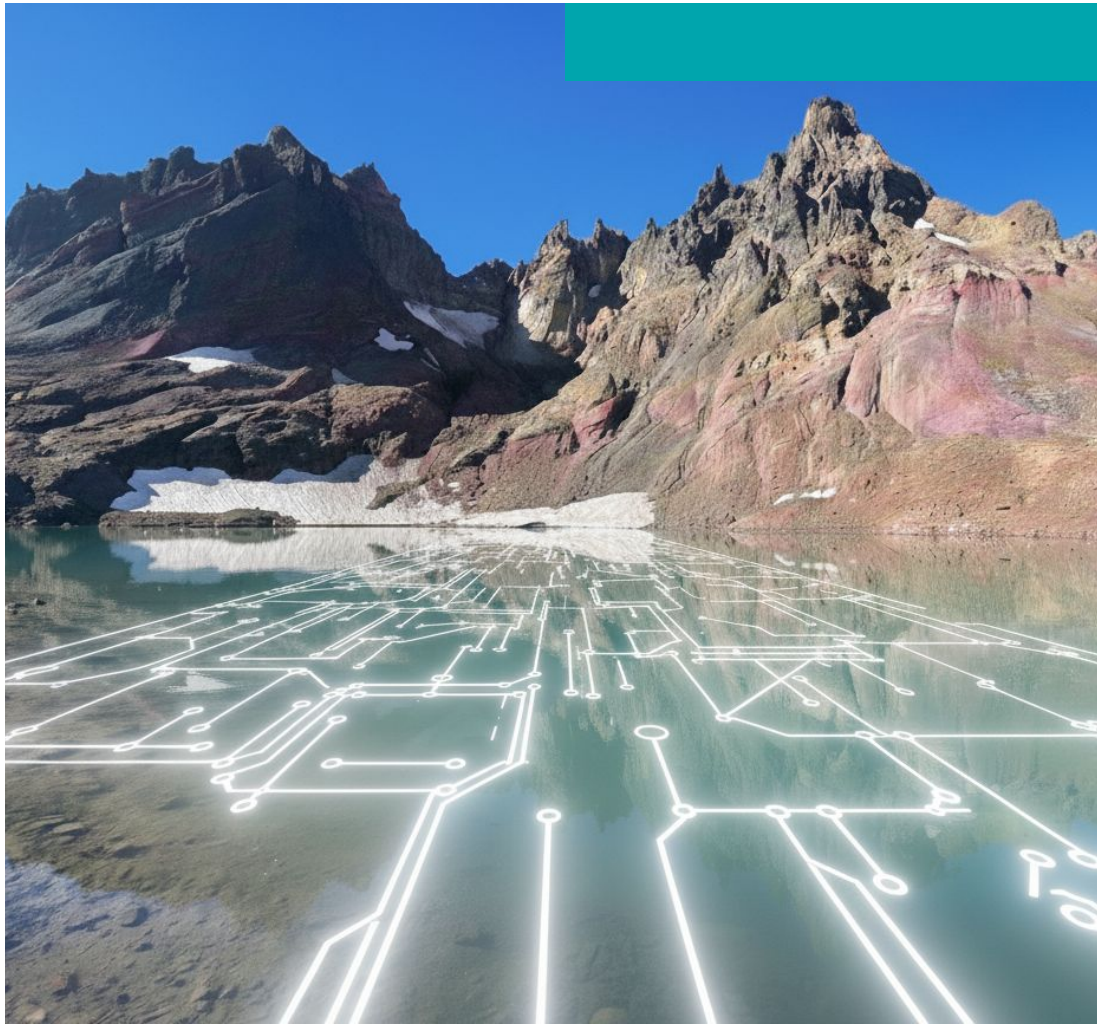
- Bachelor’s Degree in Cybersecurity (UO)
- Cybersecurity Concentration (OSU)
- Non-credit Certificate in Building Cyber Resilience (PSU)

Security Operations Centers (SOCs)

- ORTSOC @ OSU
- TSOC @ UO (starting operation in Fall 2025)

Research

- e.g. Developing AI-based technique to detect DDoS attack at scale (UO)



Key Activities: 1st Biennium (2023–2025)

Outreach

- NW Summer Cyber Camp for high school students
- Training the Trainers:
  - Workshop for high school teachers to deliver a cybersecurity curriculum (NICE/UO)
  - Workshop for middle school teachers (OSU)
- High school visits to promote cybersecurity education (NICE/UO)
- Campus tours to foster a sense of belonging (NICE/UO)
- Cybersecurity resilience initiatives for tribal communities (HECC/PSU)

Industry Partnerships

- UO joined (OSU is joining) Fortinet's Academic Partner Program
- PSU partnered with Cisco to offer training to tribal communities

Visit ***OCCoE.org*** to explore impact map for some of these activities.

Key Activities: 2nd Biennium (2025–2027)

Workforce Development Programs

- MS in Cybersecurity (UO, OSU) and Graduate Certificate (UO)
    - Co-op placements in MS programs and internships in BS programs (UO)
- Exploring interdisciplinary dimensions of cybersecurity (UO)
    - e.g., Law, Public Policy, Business, Psychology
- Expanding the non-credit certificate to serve Oregon’s nine tribal communities (PSU)

SOC Expansion

- Scaling ORTSOC and TSOC capacity and services
- Developing a "Living Lab" for AI-driven analytics at TSOC (AI-SOC) (UO)

Key Activities: 2nd Biennium (2025–2027)

Cybersecurity Assessment

- Cyber Risk Clinic: Assessing cybersecurity risk for 100+ water districts in Oregon (UO, SLCGP-funded)
- Risk assessments for 100+ special districts (OSU)

Awareness Training

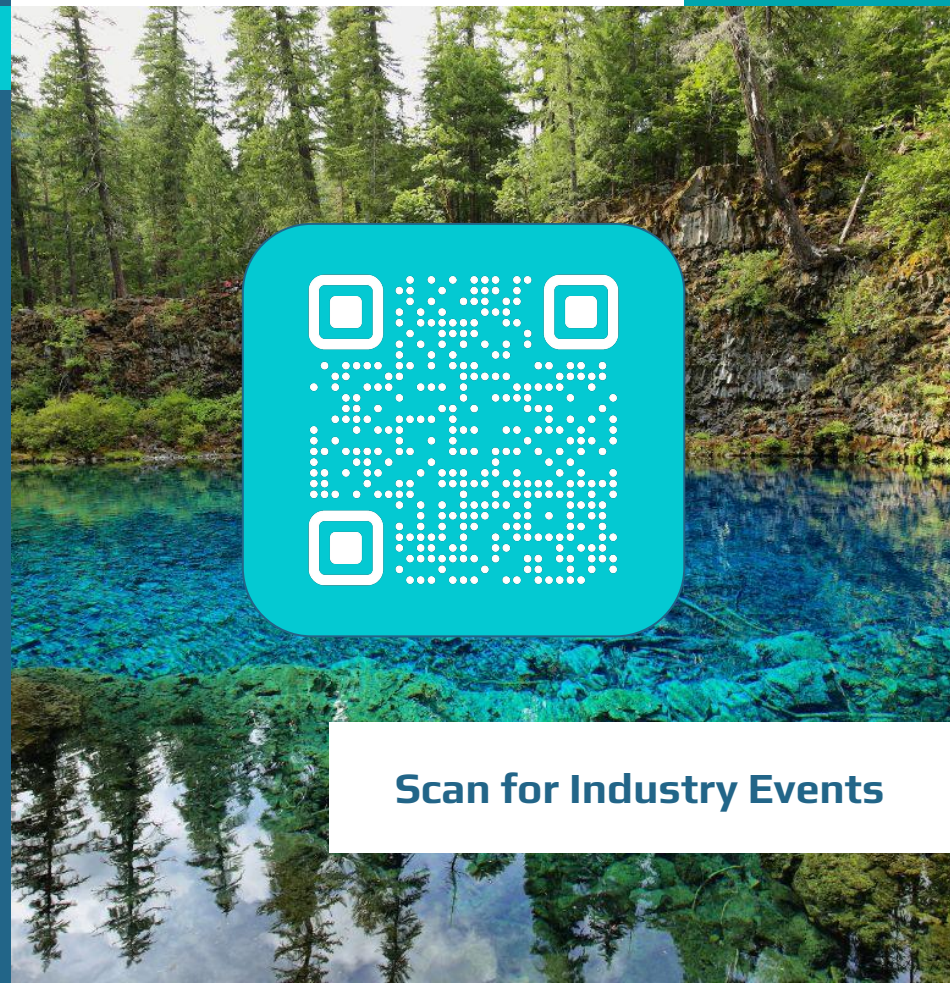
- For executives (UO), senior citizens (OSU), and other groups

Outreach (NICE/UO)

- Cybersecurity training workshops for high school teachers
- Cyber range exercises for high school students
- Cybersecurity competition for high school students
- Coordinating educational pathways with community colleges

Industry Partners Network (IPN) – UO

- UO is building a network of industry partners for our cybersecurity (and other) programs
- Areas of partnership with industry include
  - Hosting curriculum-integrated co-ops and interns
  - Supporting/enhancing experiential learning elements
  - Mentoring UO or high school students
    - capstone projects, cybersecurity clubs, competitions
  - Collaborating on research and development projects
- Co-op and internship programs provide a low-cost, low-risk opportunity to build a ***local talent pipeline for your organization***



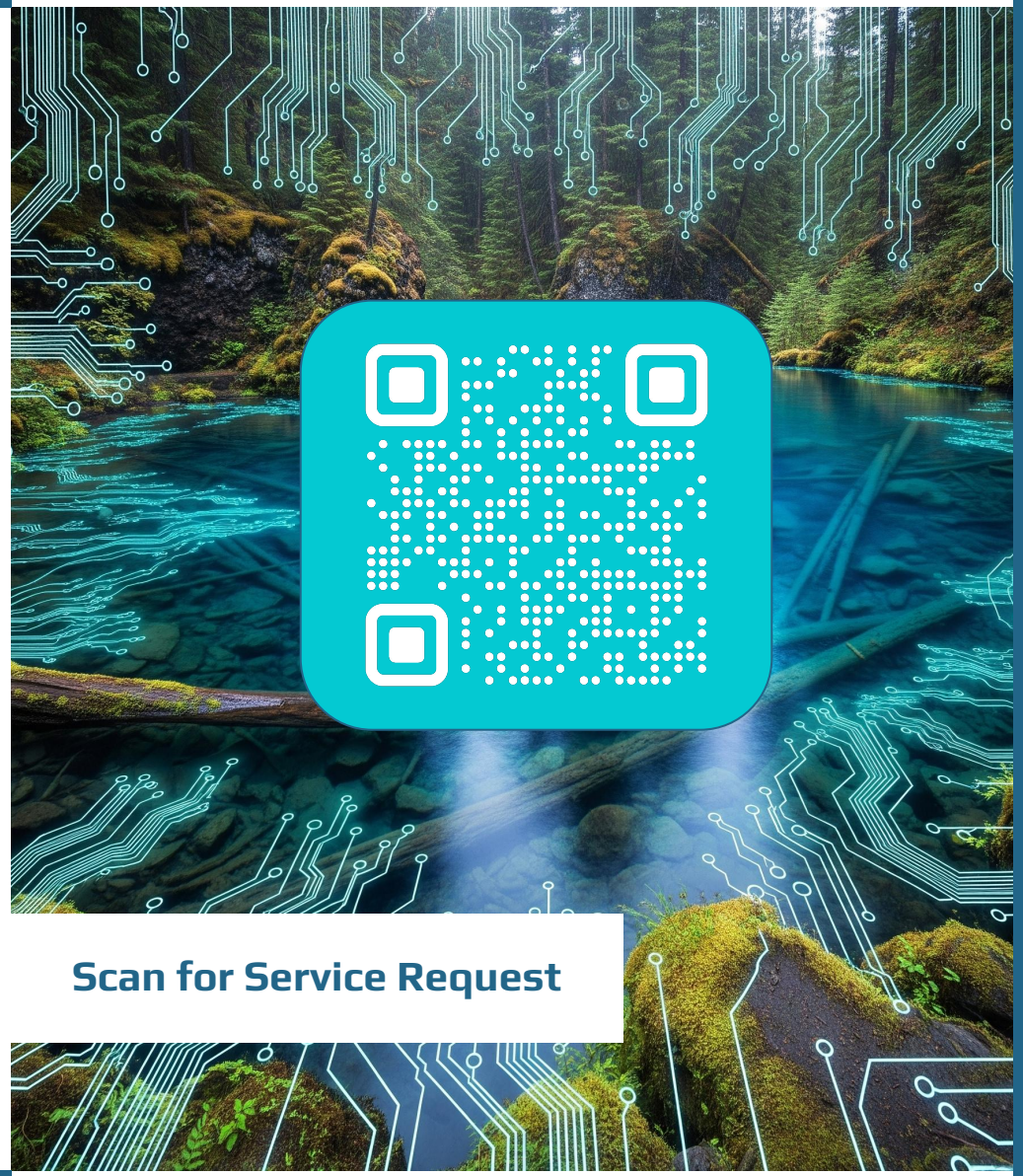
Scan for Industry Events

TSOC (Teaching Security Operations Center)

Starting in Fall 2025

- Fully operational SOC serving state agencies and nonprofits at no cost.
- It is managed by dedicated engineers and provides hands-on training to cybersecurity students.
- TSOC offers monitoring, analysis, containment, eradication and recovery actions, reporting on the incident's nature, response actions and recommendations for improvement.
- TSOC leverages XDR services from major cybersecurity vendors, combined with open-source tools. This service model:
    - Minimizes maintenance overhead
    - Ensures access to cutting-edge tools and capabilities
    - Enables agility, scalability, and remote delivery

TSOC (Teaching Security Operations Center)



Scan for Service Request

- Core Services
  - Log & Network Monitoring
  - Incident Response
  - Vulnerability Management
  - Attack Surface Management
  - Threat Intelligence
- A "Living Lab" is being developed to enable AI-driven analytics (AI-SOC).
- More information at TSOC.uoregon.edu
- We are currently recruiting clients for TSOC
  - Interested client should **complete the service request form**

Thank You