Teaching SOC (TSOC) @ UO

REZA REJAIE

PROFESSOR & HEAD

DEPARTMENT OF COMPUTER SCIENCE

JOSÉ DOMÍNGUEZ

CHIEF INFORMATION SECURITY OFFICER

Cybersecurity Programs at UO

- Bachelor's degree in cybersecurity (launched in Fall 2023)
- Master's degree in cybersecurity (will start in Fall 2026)
- Grad certificate in cybersecurity (will start in Fall 2026)
- Emphasis on experiential learning: TSOC and RISK Clinic
- TSOC is a fully operational Security Operations Center (SOC) that immerses students in defending partner organizations across the state against evolving cyber threats
  - Initially planned to train students in the UO SOC (CSOC)
  - TSOC was not part of UO's original plan/budget for OCCoE at 2023
- RISK Clinic: training students to conduct cybersecurity assessment
  - Currently focusing on water districts (funded by a SLCGP grant)

UNIVERSITY OF OREGON

Basic Information

- The plan for creating TSOC was conceived in the summer of 2024
- Our team: José Domínguez, Dan Carrere Leland VanBrunt, Reza Rejaie
  - A SOC Engineer (Saran Venugopal) was hired in January 2024
- TSOC is integrated into all cybersecurity programs at UO
- TSOC is funded by OCCoE, UO and industry
- ORTSOC team at OSU has graciously shared their experiences & insights

UNIVERSITY OF OREGON

TSOC Guiding Principles

- Adopting a hybrid service model
  - Relying on XDR services by major partner vendors to ensure **high quality of services**, **rapid scalability** and **manageable cost**
    - Avoid vendor lock-in
    - Some services are on-premise services and integrated with partner services
- Students are supervised by professionals and manage all the services
- Several top-tier vendors have been evaluated. Top two vendors were identified for contracting as TSOC partners
- Vendors' *academic programs* are used for onboarding of students
  - Academic programs can be leveraged for training other groups, e.g., high school students, IT workers

UNIVERSITY OF OREGON

TSOC Services

- Initial Services
  - Risk Assessment
  - Incident Response
  - Vulnerability Scanning (with Attack Surface Management)
  - Threat Intelligence

- Future Offerings
  - Penetration Testing
  - Threat Hunting
  - Compliance Monitoring and Reporting

UNIVERSITY OF OREGON

Progress & Current Status of Key Tasks

- University facing tasks
  - Proper space was designated and has been going through renovation
  - Required equipment and furniture have been identified & ordered
  - Legal, liability, security, privacy issues were explored and addressed
- Vendor facing tasks
  - Evaluating top-tier vendors (concluded)
  - Alpha testing of vendor services at UO (in progress)
  - Contracting with selected partner vendors (in progress)
- Student facing tasks
  - Developing TSOC curriculum, ensuring its proper integration into UO's cybersecurity programs (in progress)
  - Developing student on-boarding and supervision processes (in progress)
- TSOC partner facing tasks
  - Developing prospective partner's onboarding and service processes (in progress)
  - Informing and recruiting prospective partners, e.g. counties, cities

UNIVERSITY OF OREGON

Upcoming Steps

- Finalizing vendor contracts and testing of services (mid June)
- Recruiting and serving our first couple of partners (summer 2025)
- Finalizing TSOC curriculum, student onboarding, supervision processes (summer 2025)
- Offering the first edition to TSOC course (Fall 2025)
- Growing the TSOC team to expand the services, number of served partners & students (from Winter 2026)

UNIVERSITY OF OREGON

Long-term Support for TSOC

- TSOC offers a cost-effective and scalable cybersecurity service to local governments and public institutions while training the next generation of cyber workforce
- TSOC can be supported during the 2025-2027 biennium by using UO's current level of OCCoE funding and carry over savings from the 2023-2025 biennium
- Continuing (and expanding) TSOC operations in the 2027-2029 biennium require a higher level of funding from OCCoE

UNIVERSITY OF OREGON