OREGON22 – CYBERSECURITY IS A TEAM SPORT

Groan! - No security staff were harmed in the generation of this presentation title.

WHO WE ARE

- Duncan Barth – Interim Director Security Services & Information Assurance
- Jon Miyake – Cyber Security Operations Center Manager
- Information Security Office (https://infosec.uoregon.edu)

UO Information Security Office Mission: To empower the UO community to leverage digital assets and capabilities, and defend our cyber environment through proactive measures .

WORLD ATHLETICS CHAMPIONSHIPS

- First time held in the United States
- Hosted at the iconic Hayward Field at the University of Oregon in Eugene
- 10-day event
- 2,000 athletes
- 200 nations participating
- 13 World Athletics Championships Records Broken
- 3 World Records Broken
- Broadcast to over 190 territories
- "One billion worldwide viewers"

CORE THEME

Collaboration and Mentorship

"Information Security is a team sport"
— Most people doing a cybersecurity job

“Mentoring is a brain to pick, an ear to listen, and a push in the right direction.”
— John C. Crosby

AREAS OF CONCERN

- Areas of concern (leading into and during the event)
  - Denial of Service Attack
  - Interruption of University Business
  - Interruption to the live event
  - Ransomware
  - Site Defacement
  - Reputational Risk

RULES OF ENGAGEMENT

- Do not negatively impact critical assets/partners during event
  - Timing / Scoring
  - Broadcasters & Key Media

- What was consider potentially negatively impactful
  - Active Intrusion Prevention
  - Vulnerability Scanning
  - Mitigating detected malware
    - Disabling network access / quarantine

COLLABORATIONS

LINK OREGON

UNIVERSITY OF OREGON

WORLD ATHLETICS CHAMPIONSHIPS OREGON22

ENTERPRISE information services

DHS CISA TABLETOP

- CISA tabletop – example of fed/state/local partners
  - Partners work together to address cybersecurity scenarios representing threats to the games
  - Exercise stressed process identification and communication (non technical)
- Findings
  - Identified weakness: many stakeholders, communication channels were unclear.
- Outcomes
  - Table gave stakeholders a chance to work together ahead of the championships
  - UO worked on addressing potential process and communication issues related to the championships
    - Create a common understanding
    - Solidified incident management process

ASSET INVENTORY

- Engaged key UO IT stake holders
- Asset Inventory
  - Identify campus technology resources used by the event
    - Identify & triage risks
    - Understand mitigations
  - Take aways
    - Dependencies are deep and often shared
    - Service owners have a good sense of impact, but don't always perceive cybersecurity risk
    - Talk to operational staff, they have tactical insights into service operation
- World Athletics Vendor Inventory
  - Vendors not used to this process, but data was still valuable

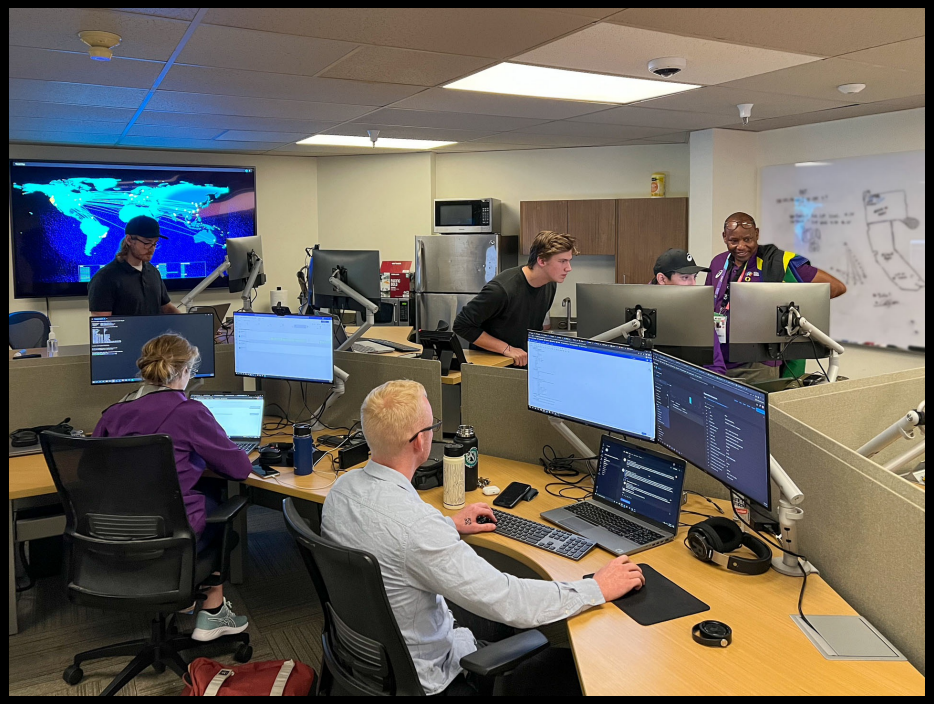
MITIGATIONS

- Denial of Service Mitigation
  - Signature based locally
  - Volumetric deployed upstream
- Digital Risk Protection
- 3rd Party Pentest

- Communication strategies
  - Lines of communications from event technical staff
  - Line of continuous communication with event organizers

WORLD ATHLETICS CHAMPIONSHIP CSOC

- WA CSOC
  - Hiring
    - College Students
      - Multiple Disciplines
  - Training
    - Training via Teams Video Calls
      - Recordings
    - Day to Day Operations
    - Investigations
  - Playbooks
    - Ransomware
    - Phishing
    - DDos
  - Tooling



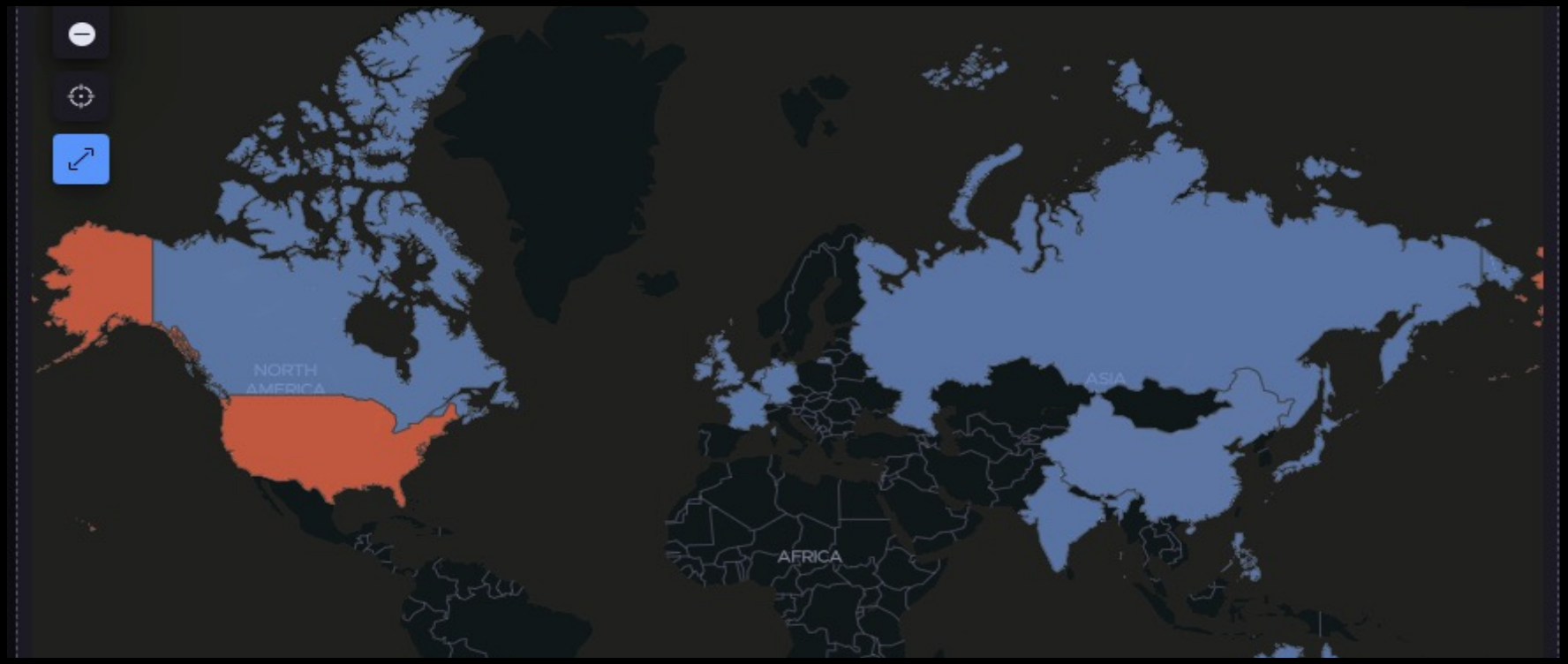
WHAT WE SAW

- Traffic
  - Global
  - Quantity
  - Breakdown
    - by Zones
  - Segmentation
- Detections
  - Type
  - Issues
- Number of Systems
  - ~5,000 Daily

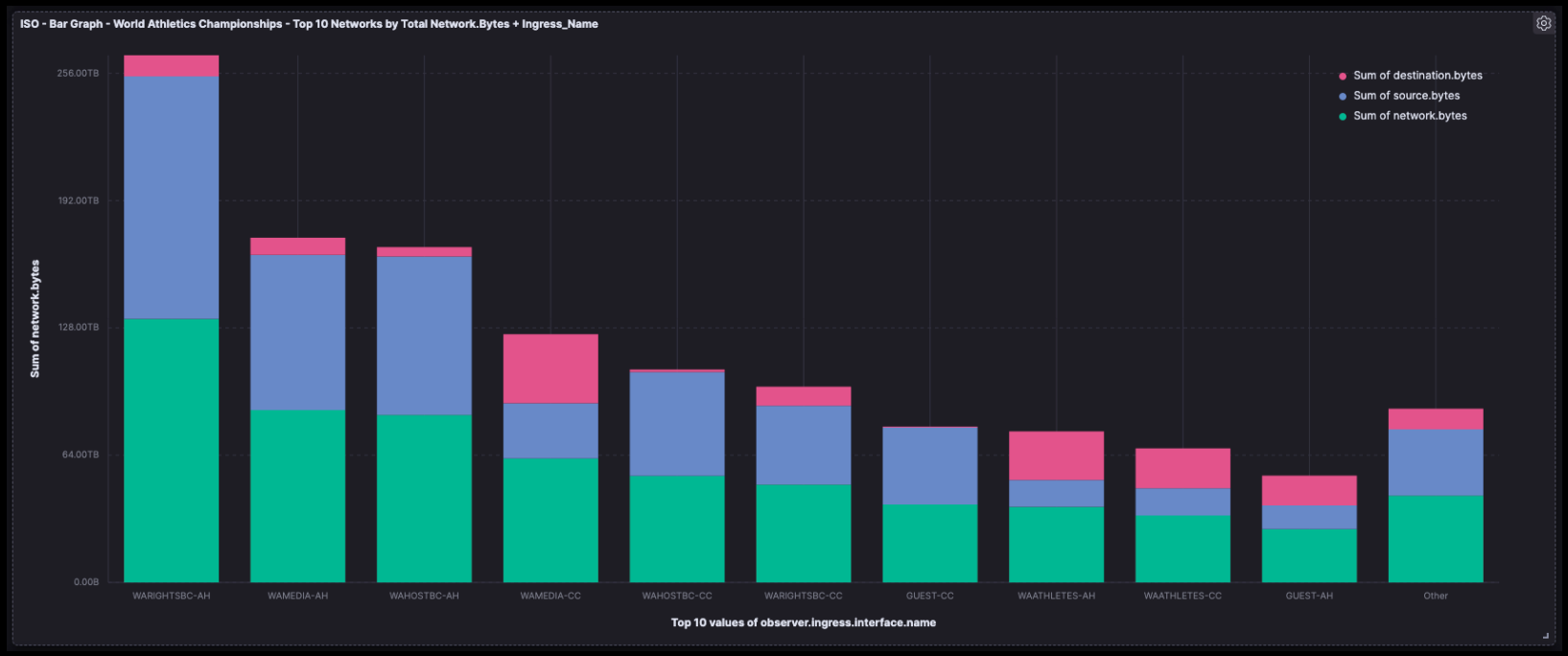
TRAFFIC QUANTITY

649.77TB

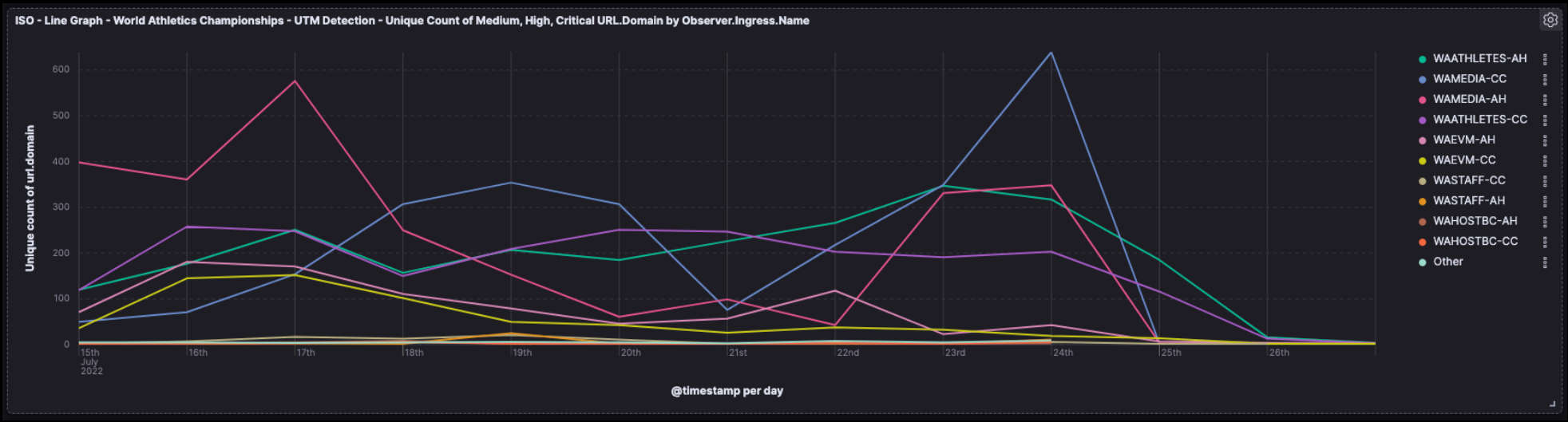
Sum of network.bytes



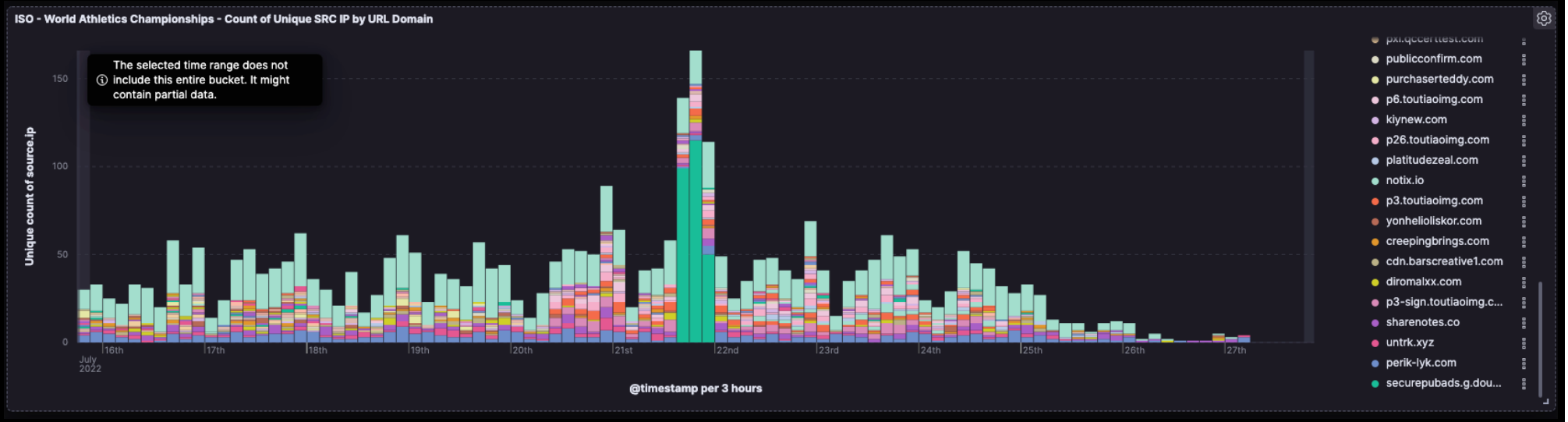
TRAFFIC BREAKDOWN



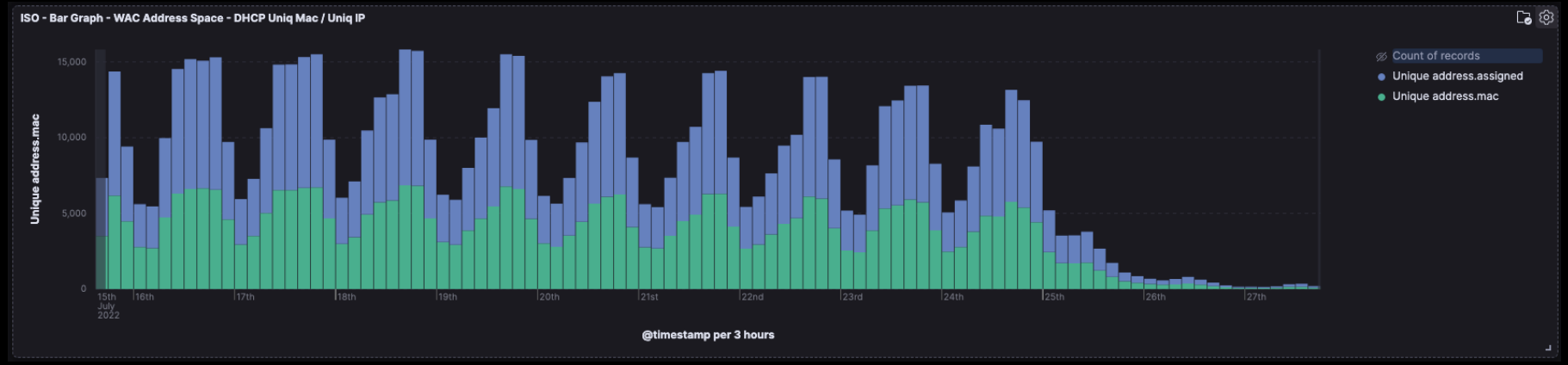
SEGMENTED NETWORK



THREAT DETECTIONS



UNIQUE DEVICES



LESSONS LEARNED

1. Define your communication paths and specific responsibilities in advance
   - CISA Tabletop
2. You can't successfully defend unless you know what you're defending
   - Asset Inventory
3. Demonstrate flexibility and willingness to change course
   - Student CSOC

TAKEAWAYS

- Desires vs capabilities mismatch
  - Resource constraints will always exist
  - Continuously evaluate your needs
  - Choose your battles
- Leverage Opportunities Gained
  - CSOC processes
  - Hired students longer term
- Continue to grow partnerships

WHAT CAN YOU DO

- Make use of your community
  - Other Cyber-Security Practitioners
  - Service Owners
  - Information Sharing and Analysis Centers (ISAC)
  - Communities of Practice

"America needs well trained professionals working in cybersecurity roles. These professionals are critical in both private industry and the government for the security of individuals and the nation." - CISA

THANK YOU

LINK OREGON

UNIVERSITY OF OREGON

WORLD ATHLETICS CHAMPIONSHIPS OREGON22

ENTERPRISE information services

QUESTIONS?

Coming together is a beginning,
staying together is progress,
and working together is success.

Henry Ford

- Federal Government Resources
  - DHS CISA (contact: central@cisa.dhs.gov)
  - Federal Bureau of Investigation (FBI)
    - Internet Crime Complain Center (IC3) (contact: http://www.ic3.gov)
- State Level Resources
  - Multi-State Information Sharing and Analysis Center (MS-ISAC) (contact: info@msisac.org)
  - Oregon TITAN Fusion Center (https://justice.oregon.gov/ortitan/)
- Private Sector/Business Resources
  - InfraGard (https://www.infragard.org/)
  - Internet Security Alliance (http://www.isalliance.org/)
  - Information Sharing and Analysis Centers (ISACs)
    - National Council of ISACs (https://www.nationalisacs.org)