CAE IN CYBERSECURITY COMMUNITY

PISCES

PISCES

CYBER RANGE POULSBO
WESTERN WASHINGTON UNIVERSITY

CWU

CAE IN CYBERSECURITY COMMUNITY

PISCES Objectives

- Workforce Development
- Infrastructure Protection
- Support Research

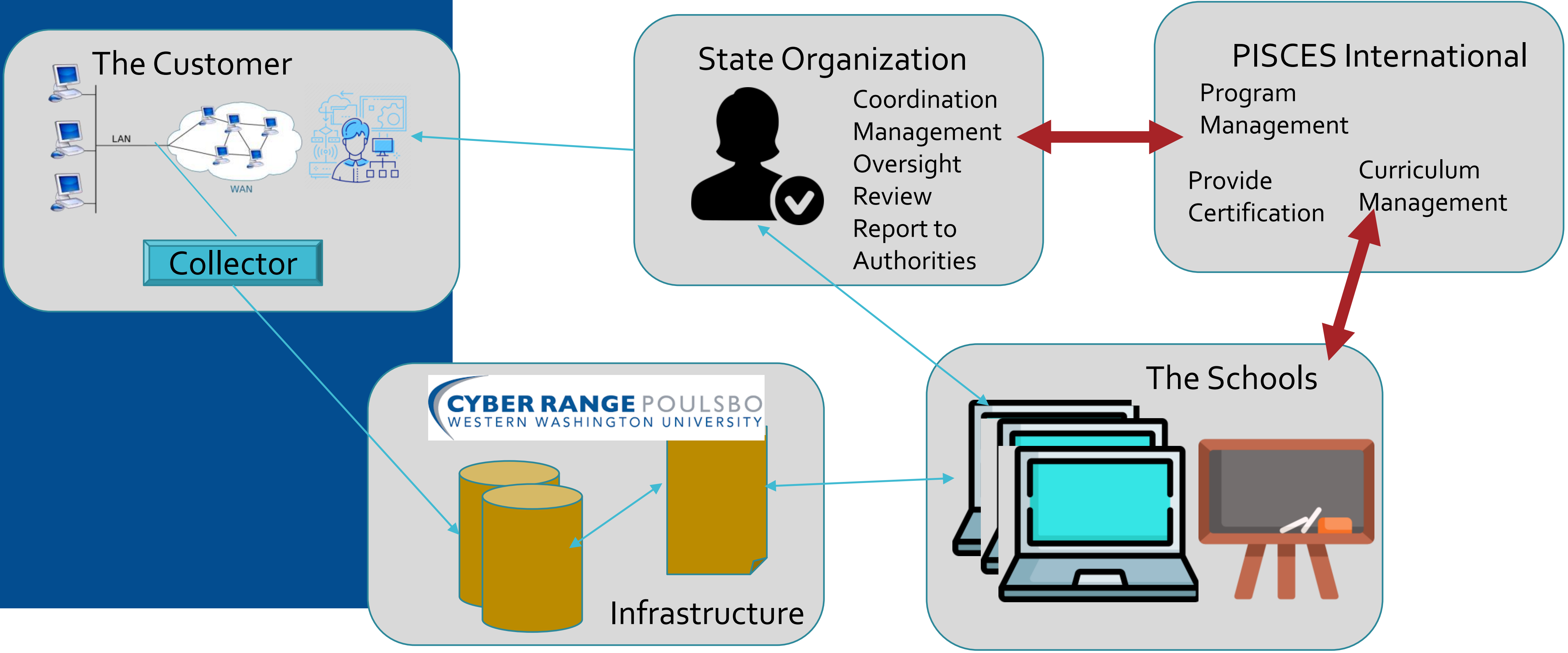
PISCES

CYBER RANGE POULSBO
WESTERN WASHINGTON UNIVERSITY

CWU

No-cost security monitoring for the public sector, using data collected to train university students as cyber analysts

PISCES



The Customer

Collector

State Organization

Coordination
Management
Oversight
Review
Report to
Authorities

PISCES International

Program
Management

Provide
Certification

Curriculum
Management

CYBER RANGE POULSBO
WESTERN WASHINGTON UNIVERSITY

Infrastructure

The Schools

Roles

PISCES International

- Develops and maintains Infrastructure.
- Develops Curriculum
- Train the Trainer
- Sets Guidance and Expectations.
- Manages assessment and certification.
- Works with CISA/PNNL to help with initial funding.

State Responsible Organization

- Recruits and Schedules Schools
- Recruits and manages relationships with local customers.
- Provides customer liaison.
  - Interface to customers
  - Review of Student Tickets
- Develops long-term funding for state.
- Provide periodic reporting
  - Students, etc.
  - Customer Reports

CAE IN CYBERSECURITY COMMUNITY

ROLES

PISCES

Schools

- No cost
- Teach students
  - Use curriculum base
- Ensure students sign NDA
- Ensure students cover assigned customers.
- Ensure Students provide reports.

Customers

- No Cost
- Install Collector
- Provide Network Information
- Provide contact Information
- Respond to notifications
- Gives more peace of mind

CYBER RANGE POULSBO
WESTERN WASHINGTON UNIVERSITY

CWU

Participation

- 2022-23 - 270 Students
- Washington
  - 7 Schools
  - 19 Cities, Counties, etc.
- Colorado
  - 2-3 Schools
  - 6+ Cities, Fire Districts, etc.
- Kentucky
  - 2 Schools
  - 6+ Cities, etc.
- Idaho
  - 2 Counties
- Montana
  - 1 School
  - 4 Customers
- Alabama
  - 1 School

CAE IN CYBERSECURITY COMMUNITY

Successes

- 10/3/2Larval debug attempt detected by USA based IP
- 10/3/22 Possible Mirai botnet activity seen from very high risk foreign address
- 10/4/22 High risk foreign address attempted to scan your network
- 10/4/22 High risk foreign address seen attempting traffic with your critical asset
- 10/4/22 High risk multi-region address attempted traffic to critical asset
- 10/5/22 very high-risk foreign address attempted to http scan critical asset.
- 10/5/22 High risk multi regional address attempted zmap scan on your network. The scanning attempt was successful.
- 10/6/22 high risk foreign address attempting nat stun on assets in your network
- 10/10/22 High risk foreign address attempted to grab .env file

- 2/1/23 Kerberos error flood detected
- 2/1/23 High risk CO-location spambot seen.
- 2/1/23 High risk Russian PHP webshell successful compromise of hvac. Infection beaconing.
- 2/2/23 High risk CO-location spambot seen. 2/3/23 High risk source seen attempting traffic.
- 2/3/23 High risk multi geo domain source seen attempting traffic
- 2/3/23 Network scanning by high-risk source.
- 2/8/23 High risk source communicating with internal host. 2/13/23 High risk source attempting asset compromise
- 2/14/23 Very high-risk spam source and ASN seen 2/23/23 Suspicious phishing email with malware attachment.
- 2/24/23 More spam bots traffic found internal to the community partner 2/27/23 Attempted mirai botnet traffic
- 2/28/23 High risk source unsuccessful in web exploit attempt.

PISCES

CYBER RANGE POULSBO
WESTERN WASHINGTON UNIVERSITY

CWU

Curriculum

- General PISCES Curriculum
  - Basics on Kibana Application
  - Introduction to Suricata
  - Networking monitoring
  - Ticket writing
- SOC Curriculum
  - Setting up Kibana
  - Introduction to honeypots
  - Incident response
  - Red/Blue/Purple Team
  - SOC Operations

Workforce Development Goal: Create “experienced” students

- Curriculum designed to teach skills valuable in cybersecurity.
  - Knowing
- Enforcement of “knowledge” through hands on experience.
  - Doing
- Experience with processes, systems, and actual data.
  - Internalizing
- Unstructured problems with no “correct answers”
  - Exploring
- Requirement to work with “tickets”
  - Communicating

The Experience

- 1/3 1/3 1/3
- Challenging to translate previous classes to the real world.
- Satisfying to work with actual data.
- Good contribution for the resume.
- Contributes to success in hunting.

Infrastructure Protection

Goal: No Cost Monitoring

PISCES

- Small Entities
  - Small budgets
  - Small staff
  - Limited time, resources, etc.
- Critical Links
  - Use the same state and federal services
  - Provide essential services – Water, power, etc.
- Limited Protection
  - Not 24/7, 365
  - Not experienced staff

Infrastructure Experience

- Initial Implementation is challenging
  - Deciding to start can be hard
    - Uncertainty about data
    - Need to bring many on-board
    - Not sure of the value proposition
  - Not a lot of time or talent
    - Simplified implementation
- Initial Monitoring is exciting
  - Lots of real and potential issues
  - Lots of false positives – getting to know the infrastructure.
  - An opportunity for embarrassment.

- The level of excitement drops over time.
  - Initial issues are resolved
  - Network and firewall configuration is refined
  - Better understanding of the network
- Time for more focused monitoring
  - Threat hunting.
  - Watching the ransomware fail.

CAE IN CYBERSECURITY COMMUNITY

Research Goal: Explore What works

- Usefulness and usability of tools.
- Mapping current attack vectors to PISCES tools
- Real world data set.
- Other areas.

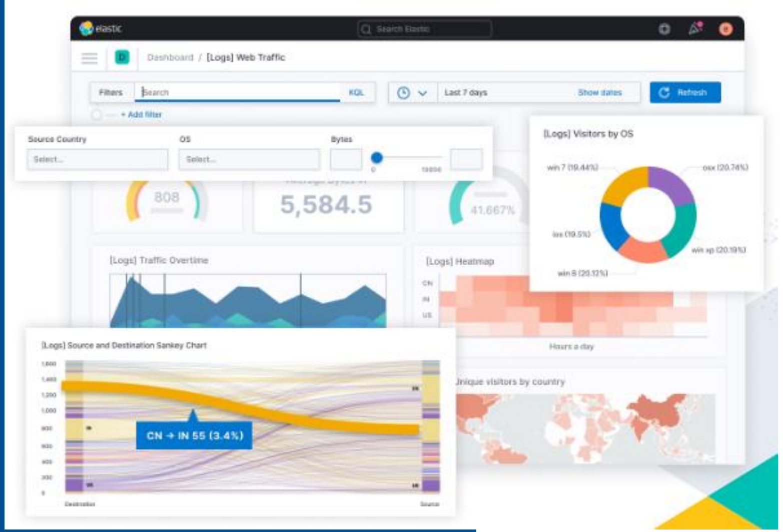
PISCES

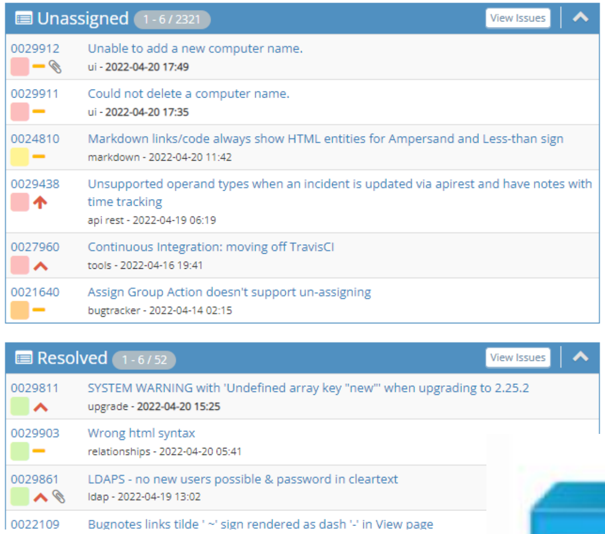
CYBER RANGE POULSBO
WESTERN WASHINGTON UNIVERSITY

CWU

CAE IN CYBERSECURITY COMMUNITY

The Tools





Unassigned 1 - 6 / 2321 View Issues

0029912 Unable to add a new computer name.
ui - **2022-04-20 17:49**

0029911 Could not delete a computer name.
ui - **2022-04-20 17:35**

0024810 Markdown links/code always show HTML entities for Ampersand and Less-than sign
markdown - 2022-04-20 11:42

0029438 Unsupported operand types when an incident is updated via apirest and have notes with time tracking
api rest - 2022-04-19 06:19

0027960 Continuous Integration: moving off TravisCI
tools - 2022-04-16 19:41

0021640 Assign Group Action doesn't support un-assigning
bugtracker - 2022-04-14 02:15

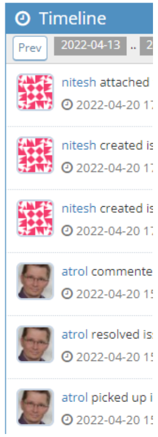
Resolved 1 - 6 / 52 View Issues

0029811 SYSTEM WARNING with 'Undefined array key "new"' when upgrading to 2.25.2
upgrade - **2022-04-20 15:25**

0029903 Wrong html syntax
relationships - 2022-04-20 05:41

0029861 LDAPS - no new users possible & password in cleartext
ldap - 2022-04-19 13:02

0022109 Bugnotes links tilde ' ~' sign rendered as dash '-' in View page



Timeline

Prev 2022-04-13 .. 2

nitesh attached
2022-04-20 1

nitesh created is
2022-04-20 1

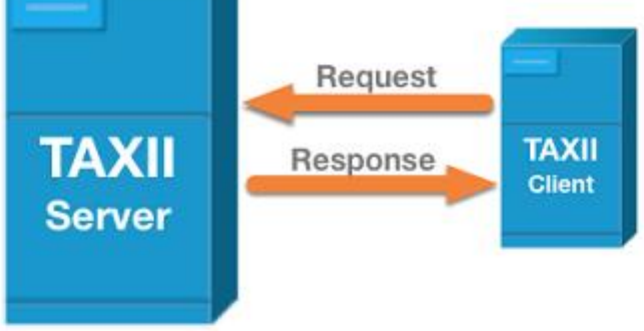
nitesh created is
2022-04-20 1

atrol commente
2022-04-20 1

atrol resolved is
2022-04-20 1

atrol picked up i
2022-04-20 1

PISCES



CYBER RANGE POULSBO
WESTERN WASHINGTON UNIVERSITY

CWU

Questions