The PISCES Approach to Cyber Education

Addy Moran
Pacific Northwest National Laboratory Pacific
Richland, WA
0000-0001-6922-5011

Ford Powers
Pacific Northwest National Laboratory Pacific
Richland, WA
0009-0005-9571-3576

Lisa Campbell
Pacific Northwest National Laboratory Pacific
Richland, WA
0000-0002-0599-2884

Melanie Rodriguez
Pacific Northwest National Laboratory Pacific
Richland, WA
0009-0007-5477-3438

***Abstract*—The Public Infrastructure Security Cyber Education System (PISCES) program has had significant impact on the cyber security posture of small municipalities and has helped develop qualified entry-level cyber analysts with real-world experience. Due to the ever-evolving nature of cyber security, adjusting our cyber security educational approach to be just as flexible is of dire importance. This paper will address how the PISCES program educates the students and partners with the municipalities, the aspects of cyber security training that PISCES does not cover and makes suggestions on how cyber security training can be applied to other situations.**

Keywords—cyber security training, talent gap, pedagogy

I. INTRODUCTION: WHY DEVELOPING CYBER SECURITY TRAINING IS SO HARD

Thirty years ago, cyber security was where quantum computing is now. New. A buzz word. It's evolved as rapidly, if not more so, as the rest of the tech industry. Between the constantly evolving base technology, the creativity of the attackers, and that no two systems are the same (due to use case, technology stack, among other reasons), training the technical nuisances of how to secure these systems, ideally, 100% of the time, is hard.

Many cyber security programs today focus on teaching definitions, policy, and controls, and if there is a hands-on element, it is in a simulated environment with cyberattacks that are likely not a realistic representation of defending most "real-world" environments. This type of training is great in developing the next Chief Information Security Officers (CISOs) and cyber security managers, however, for the students that will be boots-on-the-ground, working in a Security Operations Center (SOC) or in another technical cyber security roles, this training isn't enough. It is difficult to go out into the workforce with the necessary skills and confidence if that is the only environment students get taught. The industry needs training that challenges a student's thoughts and problem-solving skills, because our role as educators, is not to teach them to memorize the MITRE ATT&CK framework or every Tactic, Technique, and Procedure (TTP), though that is helpful, it's to teach them to adapt to their situation and handle the attacks no one has seen before[1].

II. WHAT IS PISCES?

The Public Infrastructure Security Cyber Education System (PISCES) program [2] is in-part funded by the Department of Homeland Security's (DHS) Cybersecurity & Infrastructure Agency (CISA). The program focuses on helping the cyber community in two ways; training the future workforce of entry-level cyber analysts, and helping small municipalities monitor their environments for cyber threats. This enables direct experience for the students and adds a layer of security for the organization. PISCES currently partners with thirteen (13) community partners and seventeen (17) academic partners.

As mentioned, PISCES focuses their efforts on training entry-level cyber analysts (synonymous to an Incident Response Analyst or a SOC Analyst) which can be defined as someone who is:

> *"responsible for detecting, investigating, and responding to security incidents within an organization. They work to identify the source of an attack, contain its impact, and prevent future attacks from occurring. Incident Response Analysts are typically part of a larger security team and work closely with other security professionals to ensure that the organization's security posture is strong and effective" [2].*

It was reported that between June 2022 and June 2023, there were over 660,000 cybersecurity job openings [3]. PISCES tries to battle this talent gap by training the students using real-time, real-life data with the oversight of a full time cyber analyst. The students participating in the PISCES program actively monitor and investigate threats and alerts based on the packet header data in a municipality's network/flow data. So far, the program has helped train over 1,200 students. Any student older than 18[3] can participate in the program, including international students.

PISCES partners with small municipalities where it is difficult to obtain funding for dedicated cyber security personnel. If a municipality has less than 150 employees they can sign a no-cost contract for three years, which is renewable if the organization stays below the 150 employee limit. If an organization has more than 150 employees they are eligible for a one year contract with the expectation time will be invested in finding a commercial equivalent. At the beginning of the partnership, PISCES sends a collector with a network tap (at no cost) to the municipality. This collector allows the network traffic to be passively monitored by PISCES' students off of the customer's network and contains

an embedded intrusion detection system (IDS) that monitors the traffic and creates security alerts. For privacy and security, only the packet header/metadata gets copied from the municipality's network, ensuring no content (such as emails, web pages, financial transactions) can be seen by PISCES staff or students[4]. For forensic purposes, the data collected from the municipalities are saved for approximately 90 days and are subject to the defined security standards[5]. If a student finds potentially malicious activity, the student creates a ticket explaining the activity, the full-time cyber analyst validates the finding and then, utilizing a community liaison, contacts the municipality. Internal network scanning, cryptocurrency mining, and malware are examples of some of the activity students have found and reported.

III. EDUCATIONAL APPROACH

Academia is often taught around theory, with little opportunity for application or practice, which continues to perpetuate the "theory-practice gap" [4]. PISCES aims to help close that gap by offering students the opportunity to engage with real data using real tools.

There are multiple approaches to pedagogy[6], some popular approaches are passive learning, active learning, and experiential learning. Passive learning is instructor-centered, and usually consists of lectures and slide decks, and is beneficial when introducing topics. Active learning is student-centered and encourages hands-on activities and interactive engagement with the material that's being taught [6]. The experiential learning cycle requires learners to take a concrete experience, reflect on that experience, think to reach a conclusion, apply meaning, and then act by trying out what they've learned [7]. Experiential learning provides new ways for students to apply the theories they've learned in the classroom [8] and there is evidence that these methods help students learn more than those who participate in courses that only use passive learning methods [9].

PISCES implements a mixture of passive learning (using lecture slides to introduce topics), active learning (hands-on assignments looking through data), and experiential learning (active monitoring and ticket creation on real-time, non-simulated data). The program curriculum is in line with the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) framework which works "to energize, promote, and coordinate a robust community working together to advance an integrated ecosystem of cybersecurity education, training, and workforce development" [10].

The tools used and taught in the PISCES program were chosen because they were more cost-effective and accessible for both the students and the municipalities, while still being widely used across the industry. The data management, searching, and visualization are implemented using Elastic Search[7], LogStash[8], and Kibana[9] (commonly known as the ELK stack). The students use a tool called Mantis Bug Track (MantisBT) [10] to create tickets based on the incidents observed.

IV. IMPACT SO FAR

Between January 2023 and June 2023, the PISCES program processed 8.219514 petabytes of data, with 2,390,930,000 intrusion detection (IDS) alerts generated. Of those alerts, 642 tickets were created and investigated, 152 of them escalated to the community partners, and one of the tickets also going to law enforcement.

Each quarter there are over 132 students participating in the program, and over 1,200 students have graduated from the program so far. Students who have completed the PISCES program have demonstrated a higher level of desired skills to employers compared to other education programs and coursework. Several PISCES alumni have gone on to work at companies such as Google, CI Security, Mandiant, and Crowdstrike, showing a high level of achievement within the short time the program has operated. Other students state that the PISCES program was a large help during the job hunting and interview process.

At the end of each course, the PISCES program requests feedback from the students. Specifically asking what parts of the course were most useful and asking for suggestions on how to improve the course. Based on the feedback from the Winter/Spring 2023 quarter, the students collectively said the course positively contributed to the future career choice by giving them a better understanding of the cybersecurity field and the practical applications that can be found in future job choices. The students highlighted that their favorite parts of the course were "interacting with a professional analyst, working with real world situations, and being able to experience working in a professional environment". The students found the risk management, network security, use of Kibana, working with a professional security analyst, learning how to detect malicious traffic, PISCES team activities, and SOC exposure as the most useful aspects of the course. The students suggested "establishing course expectation structure early on, not only during feedback on dashboards, tickets, etc." and that they would like to collaborate with fellow students more when developing tickets and working on assignments.

A request for feedback was sent in early 2023 to the thirteen community partners, ten of them responded with the following feedback:

- The alerts received from the PISCES team were:
  - all actionable. (2/10)
  - most were actionable. (4/10)
  - some were actionable. (4/10)
- 50% partners said that there have been alerts that resulted in the prevention of serious impacts to their organization.
- 66% of the partners reported that elected officials and government executives were engaged and supported/interested in the program.

One of the community partners said "We really appreciate the service. We have an IT staff of 1 and minimal budget so this service is very valuable".

V. OPPORTUNITIES FOR EXPANSION

There are areas of cyber security training that PISCES does not currently support, whether due scoping, funding/staffing restrictions or lack of community partners. Operational Technology (OT), Internet of Things (IoT), and threat hunting are all areas that are not currently taught in the PISCES curriculum but would be beneficial to both the students and the industry.

A. Operational Technology (OT)

Operational Technology (OT) networks, while similar to typical Information Technology (IT) networks, require more education and training in order to properly assess, monitor, mitigate, and respond to risks within the network [11]. Currently PISCES does not have visibility to OT network traffic but is hoping to develop a new course on OT technology specifically. This would improve the student's overall education and help expose the students to other job opportunities. OT networks utilize other protocols not common in IT networks such as MODBUS and BackNet TCP/IP. Providing students with the exposure to these protocols would allow them opportunities to work on embedded environments such as cars, boats, aircrafts, factories and other physical automation. This course would provide an understanding of the various protocols and their purposes, exposure to cross-network (IT to/from OT) traffic, and the types of simplistic traffic (OT to OT) that can be expected in such an environment. While the hardware and protocols used in OT aren't new (some protocols dating back to the early 1970s), there has been a well-needed urgency in recent years to secure these systems, something not taken into consideration during the protocols creation.

B. Internet of Things (IoT)

The Internet of Things (IoT) industry has been one of the more recent technology advancements, pushing the tech field in the name of making people's lives more automated (specifically through home automation systems [11]. The devices and protocols enabling this functionality are notoriously insecure, the industry driving the technology forward without taking security into consideration. This could lead to anything from inconvenient to life threatening consequences, such as unlocking the doors to a house [12], locking the owner out of their house, making the house temperature uncomfortable enough to scare the residents or force them to leave (allowing a burglary) [13], or spying (and potentially selling the videos) on the residents using security and baby cameras [14].

Like OT systems, the security of IoT systems has become more important. Developing a course to illustrate proper network security behaviors on IoT networks, how IoT devices are often misused or misconfigured, and the unique threats they create in IT networks [15] would be of great impact to the industry. Currently, PISCES uses IT network traffic which, depending on the municipality, contains traffic from IoT devices, however they are not treated differently than normal IT devices. One possibility is to save the traffic to and from the IoT devices as a separate data collection and build a supplemental curriculum based off of it. This course would help in educating students on the importance of network segmentation and device inventory, along with the exposure to the common IoT protocols and traffic patterns.

C. Threat Hunting

Another area that is beneficial to the industry but not currently in the PISCES scope is training the next generation of threat hunters. A threat hunter can be defined as:

> *"a proactive role that involves actively searching for threats within an organization's network. Threat Hunters use a combination of manual and automated techniques to identify and investigate potential threats that may have gone undetected by traditional security measures. Their goal is to identify and neutralize threats before they can cause harm to the organization" [2].*

While there are multiple approaches and methodologies to threat hunting, the two this paper will introduce are: utilizing published indicators of compromise to identify an attacker and utilizing a traffic baseline to look for anomalies.

CISA publishes Structured Threat Information Expression (STIX) files which document Indicators of Compromise (IOC) as part of their alerts and advisories, valuable resources when identifying cutting-edge cyber-attacks [12]. Another resource is the MITRE ATT&CK Framework [13] which documents the common steps in an attack, which systems can be compromised, and the common threat actors that use those attack patterns. This information could provide additional context to the motivations behind the attack, what the attackers are looking for, and potentially allow the defenders to predict the attacker's next steps.

Another approach to threat hunting is to establish a normal baseline of behavior using network diagrams, firewall rules, network traffic, and other system documentation to determine what is expected for the system. For example, determining:

1) How much traffic gets sent across the network per day?
2) Which systems talk to each other (and which ones don't)?
3) What does network communication look like when people aren't in the office?

Answers to these questions give threat hunters a way to quickly see if something isn't working as expected, which could be something as simple as a bad upgrade or power outage or as dangerous as a cyberattack. As an example, if system A never talks to system B and then on Saturday the 4th, it sent 15 GB worth of data, that may have been a data

leak, it could have been a change in system that's now requesting a status ever millisecond, or that could be expected behavior due to a planned change in the infrastructure.

Proactively defending a network is an innovative approach that requires significant understanding of the system, the technology, and the threats. Threat hunting would be a difficult course to develop (because each system is different) but promoting creative problem solving using a seminar-based course with a realistic enterprise scenario (network diagrams and documented procedures and training) may be an option.

VI. OTHER TRAINING OPPORTUNITIES

One of PISCES most promising approaches, is that it provides hands-on training with experienced analysts using real-time, real-life data. While PISCES approaches this by partnering with low personnel, low budget communities, the approach could be transferred to other situations. Privacy is one of the primary concerns organizations have, especially when the most interesting cyber data is also the data that can be the most damaging to the company. PISCES negated this concern by only inspecting packet headers. This could be similarly applied if an organization wanted to hire a summer intern, host a weeklong cyber summer training, or offer a certification, where they only allow the trainees access to the packet headers.

Another opportunity that could be explored when developing a technical cyber security training is to develop a challenge/competition using a simulated network environment and split the students into teams, one defensive (blue) team, one offensive (red) team, and one threat hunting (purple) team. Allowing the students the freedom to try new things and adapt/react to the actions of the other teams, without step by step instructions. Then have three rounds, allowing each student to participate on each team. Not only does this help give them a better understanding and respect for the different cyber security roles (and therefore a better understanding of their own preferred role), it also allows the teacher to grade based on attitude under stress, problem solving and creative thinking, and collaboration with their peers.

VII. CONCLUSION

Each organization and municipality has different customers and requirements, leading to different risks and consequences, and therefore, forcing the cyber security approach to change based on each specific environment. Trying to teach the next generation of defenders the base technology and the cyber security terminology and methodologies, while promoting problem-solving and adaptability is difficult. However, the industry will not be able to adequately defend themselves without producing independent, creative thinkers and problem solvers. This paper addresses the PISCES approach to training entry-level cyber analysts, identifies the areas that PISCES does not support, and provides suggestions on how the industry can continue evolving the PISCES approach to cyber security training to better prepare the industry for the battles ahead.

ACKNOWLEDGEMENT

The authors gratefully acknowledge Amanda Hutton, Pacific Northwest National Laboratory, for sharing her expertise and Amariah Jackson, Pacific Northwest National Laboratory, for her help in garnering the feedback on the PISCES program. The accuracy of the information and the perspectives presented in this report are the responsibility of the authors.

REFERENCES

[1] Lucian Constantin. (2023, March 22). "55 zero-day flaws exploited last year show the importance of security risk management" CSO Online. https://www.csoonline.com/article/574825/55-zero-day-flaws-exploited-last-year-show-the-importance-of-security-risk-management.html (retrieved 2023 Sept 8).

[1] Infosec-Jobs. (2023, August 12). "Incident Response Analyst vs. Threat Hunter" Infosec-Jobs. https://infosec-jobs.com/insights/incident-response-analyst-vs-threat-hunter/(retrieved 2023 Sept 8).

[2] Cambrie Eckert. (2023, June 26). "JUST IN: U.S. Desperately Needs Cyber Talent, Congress Says". National Defense. https://infosec-jobs.com/insights/incident-response-analyst-vs-threat-hunter/ (retrieved 2023 Sept 8).

[3] Ville Björck. (2020). "The idea of academia and the real world and its ironic role in the discourse on Work-integrated Learning". Studies in Continuing Education, vol. 42:1, pp. 1-16, DOI: 10.1080/0158037X.2018.1520210 (retrieved 2023 September 6).

[4] Merriam-Webster. (n.d.). "Pedagogy". https://www.merriam-webster.com/dictionary/pedagogy (retrieved 2023 September 10).

[5] John Hopkins University. (n.d.). "Active Versus Passive Learning". John Hopkins University: Academic Support. https://academicsupport.jhu.edu/resources/study-aids/active-versus-passive-learning/ (retrieved 2023 September 6).

[6] Institute for Experiential Learning (n.d.). "What is Experiential Learning?". Institute for Experiential Learning. https://experientiallearninginstitute.org/what-is-experiential-learning/ (retrieved 6 September 2023).

[7] Kruger JS, Kruger DJ, Suzuki R. (2015). "Assessing the Effectiveness of Experiential Learning in a Student-Run Free Clinic". Pedagogy in Health Promotion. vol. 1:2, pp. 91-94, DOI: 10.1177/2373379915575530 (retrieved 2023 September 6).

[8] Louis Deslauriers, Logan S. McCarty, Kelly Miller, Kristina Callaghan, and Greg Kestin. (2019). "Measuring actual learning versus feeling of learning in response to being actively engaged in the classroom". PNAS, vol: 116:39, pp. 19251-19257, DOI: 10.1073/pnas.1821936116 (retrieved 2023 September 6).

[9] National Institute of Standards and Technology. (n.d.). "NICE". NIST Information Technology Laboratory: Applied Cybersecurity Division. https://www.nist.gov/itl/applied-cybersecurity/nice (retrieved 2023 September 8).

[10] Daniel Ricardo dos Santos, Mario Dagrada, and Elisa Costante. (2021). "Leveraging operational technology and the Internet of things to attack smart buildings". Journal of Computer Virology and Hacking Techniques, vol. 17, pp. 1-20, DOI: 10.1007/s11416-020-00358-8 (retrieved 2023 September 6).

[11] Kevin Townsend. (2019, December 11). "Vulnerability Allows Hackers to Unlock Smart Home Door Locks". SecurityWeek. https://www.securityweek.com/vulnerability-allows-hackers-unlock-smart-home-door-locks/ (retrieved 10 September 2023).

[12] Trend Micro. (2019, September 27). "Hacker Compromised Family's Wi-Fi, Taunted Family With Thermostat, Camera for 24 Hours". Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-

and-digital-threats/hacker-compromised-family-s-wi-fi-taunted-family-with-thermostat-camera-for-24-hours (retrieved 10 September 2023).

[13] Amy Wang. (2018, December 20). "'I'm in your baby's room': A hacker took over a baby monitor and broadcast threats, parents say". Washington Post. https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/ (retrieved 10 September 2023).

[14] Hamed HaddadPajouh, Ali Dehghantanha, Reza M. Parizi, Mohammed Aledhari, Hadis Karimipour. (2021). "A survey on internet of things security: Requirements, challenges, and solutions". Internet of Things, vol. 14. DOI: 10.1016/j.iot.2019.100129 (retrieved 2023 September 6)

Notes

1. There were fifty-five (55) zero-day attacks exploited in 2022 [1].
2. https://pisces-intl.org/
3. Must be of legal adult age to sign the Non-Disclosure Agreement (NDA).
4. The packet headers include the source and destination addresses, port, protocol, and timestamp.
5. PISCES enforces the following security standards: the data is "stored at a participating university, and the data center must maintain security standards for physical security of the facility, network-level access control, time-limited access authorization for students, and data center security monitoring." See the PISCES Community FAQ page for more information.
6. pedagogy: the art, science, or profession of teaching [5]
7. https://www.elastic.co/elasticsearch
8. https://www.elastic.co/logstash
9. https://www.elastic.co/kibana
10. https://www.mantisbt.org/
11. An integrated network of appliances (fridge, oven, thermostats), smart physical systems (bluetooth enabled garage doors or exterior doors), security systems (video doorbells), bluetooth capable sound/music systems, etc.
12. https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/automated-indicator-sharing-ais
13. https://attack.mitre.org/