TradeCraft WA: Cyber Talent Pilot

A New Solution for Cyber Talent Development and Access to IT Careers

FAQ

How does TradeCraft WA work?

Recent graduates and current students at Edmonds College's Cyber Defense and Digital Forensics program have been recruited to participate in the first pilot cohort. Over the course of 4 months, TradeCraft WA interns will receive 400 hours of technical and experiential training from the FOUR18 team, gaining the FOUR18 / Silensec Junior SOC Analyst Top 10 Abilities Credential, the MITRE ATT&CK Defender certification and The Cybersecurity Workforce Alliance TradeCraft Program Risk Management Industry Recognized Credential.

In parallel with the training, Employer Hosts will provide a remote Cybersecurity Analyst internship. Employer Hosts can tailor the experience for interns based on their needs and some examples of what they provide are below. The internship will be led by the FOUR18 team's professional cyber analyst coaches emphasizing experiential hands-on learning in live threat hunting, security operations center analyst competencies and cyber risk management.

During the 4-month internship, interns will be engaged primarily in training for the first month and then in months 2-4, interns will have about 20 hours of training and 20 hours of hands-on work, for a total of 40 hours each week. As part of the internship, Employer Hosts have the option to participate in having threats against their people proactively hunted and mitigated through a real-time collective defense approach. This gives interns an opportunity to investigate and preemptively contain threats targeting their Employer Host like new ransomware campaigns.

What are the benefits of being an Employer Host?

There are multiple benefits of participating as an Employer Host, including:

- Exclusive access to qualified cybersecurity talent who complete the program
- Gaining a better understanding of cybersecurity within your organization, including learning about the most recent threats that are targeting organizations like yours
- Collaborative remote team engagement between professional mentors, interns and hosts
- Helping develop career pathways for job seekers with an interest in IT and cybersecurity
- Supporting the protection of your community and local economy
- Additional real-time protection for your organization from emerging cyber threats (optional)

What does it mean to be an Employer Host for a Cybersecurity Analyst intern?

The virtual internship is designed to be a robust learning experience and Employer Hosts will engage with interns in a number of ways, such as:

- Providing opportunities for interns in the program cohort to learn about your organization, your IT department (if you have one) and your industry. This could take the form of informational interviews, guest speaker sessions and/or curated learning materials.

- Meeting weekly on a virtual platform with your intern(s) to follow their work and verify they are developing as new professionals.
- Participating in regular trending threat briefings from interns to supervisors, which can be shared with your people to reduce your exposure and may include briefings about threats targeting your organization, community or industry.
- Integrating the TradeCraft WA program from FOUR18 into your company's response to cyber threats or your cyber talent to leverage the cybersecurity workforce for the future.
- Optionally, providing real-time data from your organization to FOUR18 for your intern(s) to improve your cybersecurity defense against threats proactively and augment your resources
- Considering hiring your intern(s) and optionally extending the proactive threat defense at the conclusion of the internship.

Can Cybersecurity Analyst interns do other work for me?

Yes – as long as the work is related to learning about your organization, your industry, cybersecurity and/or IT more generally. The TradeCraft program can work with you to co-develop the work experience portion of the internship (20 hrs./wk. in months 2-4). You would add any tasks or work assignments you'd like interns to complete to your internship description (see below).

Please note that interns still need to be fully engaged in the TradeCraft WA program and meet the same requirements as other interns in the program. The maximum number of hours per week for interns is 40 hours combined training and work experience over the 4-month program.

Can they work onsite at my organization or in a hybrid arrangement?

Yes – if you would like your interns to be onsite some or all of their work week, please include this in the internship description.

What are the steps to become an Employer Host to a TradeCraft WA intern?

1. Contact Ty Reed and attend an information session. The first session will be Mar 9th, 12-1pm.
2. Fill out a worksite agreement with Workforce Snohomish.
3. Complete an internship description using our template.
4. Set up interviews with potential interns to select your intern(s) in mid-March.
5. Attend an employer orientation.
6. You're on board!

How can I become eligible to host an intern?

There are only a few requirements to be eligible to host interns for the program:

- Your organization or business has operated at your current location for at least 120 days
- Hosting intern(s) will not result in the full or partial displacement of employed workers
- The intern supervisor commits to keeping the employer-of-record (a Workforce Snohomish partner) informed about intern progress, problems, and matters of mutual interest or concern.
- Your organization or business must be current on business and excise taxes

Is there a cost to participate as an Employer Host?

No – the training and wages for the interns are both paid for by Workforce Innovation and Opportunity Act (WIOA) funding. They are paid a prevailing wage for both training and the work

experience portion. Interns are expected to have their own equipment and to work remotely. All you need to do is meet the requirements above and help provide a positive learning experience through engagement with your intern(s) as noted above.

Do I need to be the employer-of-record for the interns?

No – during the internship, Cybersecurity Analyst interns will be employed by a contracted Snohomish County WIOA provider. All payroll and associated liability are covered through this program.

Have they all been vetted as eligible to work in the U.S.?

Yes – but if you require that they are also a U.S. citizen, please let us know.

Do I really need to care about developing the human resources of cyber? Isn't software enough?

Myth #1: IT has it covered. My email security will stop attacks targeting my organization.

Most Likely False. Today's technologies stop less than 50% of the attacks that are the most common and serious. These are attacks such as credential phishing, business email compromise and ransomware that need only one human victim to cause catastrophic loss.

Myth #2: Phishing attacks are always easy to spot.

False. Secure Email Gateways (SEGs) typically fail to identify unknown threats and new or short-lived websites because if a URL isn't on a known blacklist SEGs rarely have reason to not deliver email. The average phishing URL is active for only 19hrs today. Furthermore, today URL based threats are not limited to email – they appear in search engine results, social media, and collaboration chat rooms like those popular with developers, gamers and digital natives in very sophisticated targeted campaigns. These threats need efficient human investigation, but unfortunately the IT industry has been over-dependent on software that is constantly thwarted by creative attackers, and this fact combined with the dearth of talent in an efficient model is a primary contributor to today's ransomware and phishing epidemic.

Myth #3: Only less "tech savvy" users fall for phish.

SERIOUSLY False. Digital natives are the most likely to click on bad links. The recent **Trust Issues survey2** asked how respondents reacted to a suspicious looking email with a link or an attachment. Some 46% percent of Gen Z respondents said they would open the link or attachment, compared to just 1% of Baby Boomers and 4% of Gen X; 29% of Millennials would also take the bait.

Myth #4: Attackers don't target small businesses.

False. Small-medium businesses (SMBs) operating solo and SMBs served by MSPs are just as much at risk as enterprise organizations. The Verizon Data Breach Report3 indicates that **43% of all data breaches involve small and medium-sized businesses**, and 61% of all SMBs have reported at least one cyberattack during the previous year. Recently DHS CISA warned that the "Big Game" targets of 2021's ransomware attacks like the Colonial Pipeline have shifted to smaller midsized companies and their supply chains, including their IT services firms.

Myth #5: Cyber threats can't be found proactively, and my IT team and me are on our own. We're too small to do otherwise.

False. Our program develops intelligence efficiently on threats in real time while they are actively trolling for victims across all the users of a collective set of organizations and proactively blocks any threats seen for all users instantaneously. We anonymize and prioritize the data in stage to train and scale up the cyber workforce to stop the threats that are most likely to target you. It is an ideal solution for smaller organizations where one click can be the end of your company.

Who is involved in TradeCraft WA?

Workforce Snohomish invests government and private funding to continuously increase the global competitiveness and prosperity of our businesses and workforce, to fill current and emerging jobs, and to provide full employment. Our investments are made through effective business, labor, educational, community-based, and service provider organizations for the opportunity, economic well-being, and benefit of our entire community.

FOUR18 Intelligence is creating a new hands-on based approach to cybersecurity human talent development and accessibility through a gamified and collaborative live, real-world cyber threat hunting and incident response platform that connects analysts-in-training with professional coaches and host companies virtually. This solves today's desperate needs of organizations for up-to-date hands-on skills and knowledge of threat intelligence in the face of relentlessly evolving cyberattacks. It's signature workforce development program, TradeCraft, meets the market demand for cyber defense through an intensive training and live-fire internship engagement model.

Edmonds College transforms lives through exemplary, nationally recognized educational and career pathways. It offers multiple opportunities to integrate knowledge and skills throughout its degrees and certificates, such as the Cyber Defense and Digital Forensics program.

If you are interested in becoming an Employer Host, would like to attend an information session or have any questions, please contact Ty Reed at ty.reed@workforcesnohomish.org

Workforce Snohomish FOUR18 INTELLIGENCE EDMONDS COLLEGE