**Paul G. Amidon**

Lacey, WA 98503 | (360) 339-3735 | paul.amidon@outlook.com | [linkedin.com/in/paul-amidon/](https://www.linkedin.com/in/paul-amidon/)

**Professional Summary**

Recently separated Air Force Veteran with an **ACTIVE SECRECT CLEARENCE** and over a decade of security experience, specializing in Offensive and Defensive Security Operations, Data Analysis, and a wide range of cybersecurity. Proficient in cutting-edge tools and technologies, including Active Directories, Linux, Security information and event management (SIEM) systems, Windows Defender, intrusion detection/prevention systems, packet sniffers, and vulnerability scanners. Demonstrated expertise in identifying and mitigating security risks, data forensics, threat mapping, and security auditing. Adept at leading teams and fostering collaboration, dedicated to enhancing security performance and achieving mission-critical objectives.

**Certifications**

* CompTIA Security +
* TestOut Security Professional
* TestOut Linux Professional
* TestOut Network Professional
* IBM Cybersecurity Analysist
* IBM Data Analysist
* Google Cybersecurity
* Lean Six Sigma Blackbelt
* EC-Council Cybersecurity Attack & Defense Fundamentals

**Education**

**American Military University | Charles Town, WV**

* 2023 - Master of Art’s – Psychology *(Military & Organizational Leadership)*
* 2020 - Bachelor of Art’s – Psychology *(General)*

**Saint Martin’s University | Lacey, WA**

* 2023 - Certificate – Computer Science *(Cybersecurity)*

**Community College of the Air Force | Montgomery, AL**

* 2018 - Applied Associates of Science – Criminal Justice

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Cybersecurity Portfolio Experience**

**CompTIA + TestOut Online Lab Experience:**

* Completed CompTIA’s online TestOut courses in Network Pro, Linux Pro, and Security Pro, demonstrating proficiency in networking fundamentals, Linux administration, and advanced cybersecurity practices and toolsets.
* Developed skills in configuring and troubleshooting network devices, implementing security measures, analyzing data forensics, and conducting risk assessments.
* Acquired extensive hands-on experience in safeguarding business networks against advanced cyber threats, implementing robust security measures, and ensuring the integrity and confidentiality of sensitive data.

**Cybersecurity Challenge Platforms**

* ***Certified Ethical Hacker (CEH) v12:***
  + Engaged in CyberQ Edition Labs aligned with the EC Council’s CEH Course Outline.
  + Navigated solo Capture the Flag style challenges within platform, showcasing practical application.
  + Applied acquired knowledge to real-world scenarios in ethical hacking and cybersecurity though EC Council’s guidlines.
* ***TryHackMe Experience:***
  + Attained a Top 4% ranking with Level 9 achievement.
  + Completed multiple learning paths such as Jr. Penetration Tester, CompTIA PenTest+ prep path, Web Security Fundamentals, and Security Operations Center 1.
  + Engaged in practical application of cybersecurity concepts, covering networking, web application security, and system exploitation/defense.
  + Explored diverse areas in cybersecurity, including threat intelligence, red & blue team roles, and network/data analysis.
* ***HackTheBox Academy & Labs:***
  + Achieved a Top 5% ranking with 117 compromised targets.
  + Highlights include a diverse expertise in Linux, networking, Metasploit, and web application attacks.
  + Emphasized practical understanding of real-world misconfigurations and privilege escalation flaws.
  + Conducted exploration of XSS vulnerabilities and executed vulnerability assessments for web applications.

**Professional Experience**

**Cybersecurity Pipeline Student (Washington Vets 2 Tech)***Lacey, WA August 2023 – December 2023  
Saint Martin’s University*

* Completed an Amazon Approved Training Program, earning an Undergraduate Certificate in Computer Science with a concentration in Cybersecurity Administration.
* Completed comprehensive cybersecurity training under the Washington Vet 2 Tech initiative, gaining proficiency in network security, intrusion detection, and incident response.
* Acquired additional skills through platforms such as HackTheBox labs and academy, TryHackMe Labs, completion of six college courses in network fundamentals, security operations, ethical hacking, penetration testing, Python coding, cloud application development, and AWS training.
* Demonstrated a strong aptitude for understanding and addressing complex cybersecurity threats.

**Manager – Security Operations***Joint Base Lewis-McChord, WA March 2020 – January 2024  
United States Air Force*

* Spearheaded two security teams of 36 personnel, fostering cohesion and efficiency in physical security operations.
* Offered guidance and mentorship to elevate team performance in security operations and limited cybersecurity tasks.
* Formulated and executed security plans, highlighting adherence to regulations and policies.
* Integrated physical security measures seamlessly into overarching operational strategies.
* Conducted comprehensive training programs, emphasizing both physical security and cybersecurity aspects such as social engineering threats.
* Orchestrated responses to security incidents, effectively coordinating communication between multiple departments to effectively move resources for containment and resolution.

**Senior Team Leader – Security Response Team** *December 2017 - March 2020  
Joint Base Lewis-McChord, WA  
United States Air Force*

* + Directed and motivated a team of 18 security personnel, ensuring proactive response training and proficiency in security procedures.
  + Collaborated with superiors to conceptualize and execute security plans, bolstering the overall safety of the installation.
  + Efficiently managed resources, encompassing personnel, equipment, and budgets, ensuring optimal readiness emergency security operations.
  + Engaged with superiors to strategically allocate resources based on evolving security needs.
  + Executed administrative tasks, including personnel management, evaluations, and record-keeping.

**Nuclear Electronic Security Systems Operator***Malmstrom Air Force Base, MT January 2014 – December 2017  
United States Air Force*

* Operated and upheld a diverse suite of electronic security systems critical to nuclear asset protection.
* Ensured the continuous functionality and security of electronic systems, showcasing expertise in safeguarding sensitive assets within the cybersecurity domain.
* Responded to cybersecurity incidents, addressing unauthorized access breaches through swift dispatching of response forces, detainment of individuals, and escorting them out of restricted areas.
* Applied hands-on experience in electronic security operations to enhance cybersecurity practices, leveraging proficiency in managing and troubleshooting complex security systems.