JOB DESCRIPTION

Product Security Engineer Trainee

Location: Utah **Department:** Engineering **Employment Type:** Full-Time / Paid Training Program

About the Role

We are looking for a motivated, curious Product Security Engineer Trainee to join our organization. This entry-level role is designed for aspiring security professionals who want hands-on experience protecting modern web applications, cloud infrastructure, and customer-facing software products.

Through a structured, mentor-led self-paced training program, you will learn the fundamentals of developing, deploying, and maintaining secure software products—with a heavy emphasis on white hat hacking (ethical hacking) techniques to proactively identify and remediate vulnerabilities before they can be exploited.

What You Will Learn & Do

- **Ethical Hacking & Offensive Security:** Learn and apply white hat hacking methodologies—including reconnaissance, vulnerability scanning, and manual web application penetration testing—to uncover security flaws across websites, APIs, and underlying systems.
- **Secure Software Development:** Understand common software vulnerabilities (such as the OWASP Top 10) and collaborate with software developers to review code and ensure unsafe code is caught before deployment.
- **Infrastructure & Perimeter Hardening:** Assist in configuring, testing, and maintaining Web Application Firewalls (WAFs), geo-fencing policies, SSL/TLS certificates, and network access controls.
- **Automated Security Pipelines (DevSecOps):** Learn how to integrate automated security testing tools (SAST/DAST) into CI/CD deployment pipelines to continuously validate software safety.
- **Incident Response & Remediation:** Participate in analyzing security alerts, triaging reported vulnerabilities, and verifying that security patches effectively resolve underlying weaknesses.

Qualifications & Skills

- **Educational Background:** A bachelor's degree in Computer Science, Cybersecurity, Information Technology, or a related field from a reputed educational institution in the United States.
- **Technical Curiosity:** A strong interest in how websites, networks, and software systems work under the hood—and how attackers attempt to break them.
- **Foundational Knowledge:** Basic familiarity with web technologies (HTTP/HTTPS, HTML, JavaScript, APIs), Linux command-line environments, and at least one scripting or programming language (e.g., Python, Java, or Bash).

- **Problem-Solving Mindset:** Analytical thinker who enjoys puzzles, troubleshooting, and learning new defensive and offensive security tools.
- **Bonus / Nice-to-Have:** Participation in Capture the Flag (CTF) competitions, bug bounty programs, or foundational certifications (e.g., CompTIA Security+, Network+, or CEH).

What We Offer

- **Hands-On Mentorship:** Direct guidance from experienced Product Security and Offensive Security Engineers.
- **Real-World Impact:** Opportunity to test, break, and secure live production environments in a safe, controlled capacity.
- **Career Growth:** Clear pathway to transition into a full-time Product Security Engineer role upon successful completion of the training program.