**Evan Eastwood**

evan@eeastwood.info|evanw.eastwood@gmail.com ❖ (724) 713-2048 ❖ Tampa, FL ❖ https://www.eeastwood.info/

**WORK EXPERIENCE**

**ReliaQuest Aug. 2021 – Present**

*Senior Detection Developer Tier 1 | May, 2023– Present Tampa, FL*

* As a trusted resource, I've successfully resolved numerous high-pressure situations, leveraging my analytical skills to develop effective solutions
* Acted as the lead developer on specific out of band work requested by management and customers
* Assisted more junior developers to help build their knowledge
* Taught others how to use tools in which I have become extremely experienced
* Managed workloads and projects while balancing distribution of work when needed

*Detection Developer Tier 1 | Oct, 2022 – May, 2023*

* Designed and developed logic for detecting threats ranging from insider risks to zero-day exploits
* Built and maintained a functional library of logic in various SIEMs and query languages (Splunk, Azure Sentinel, Devo)

*Associate Detection Developer | Aug, 2021 – Oct, 2022*

* Learned in depth about a variety of SIEMs and security tools, particularly how they log and interact
* Built and deployed logic in customer environments to detect malicious activity

**Textron Systems July 2020 – Aug. 2021**

*Information Systems Security Officer Huntvalley, MD*

* Worked with TS/SCI clearance to plan, secure, and accredit information systems for engineers pursuing classified contracts
* Used various tools and knowledge to harden systems to NIST 800-53 standards for accreditation
* Leveraged expertise in information systems security to effectively manage and prioritize projects for teams working with classified data, ensuring seamless integration with federal security requirements.
* Served as Linux SME for the department

**Bell Flight May 2019 – Aug. 2019**

*IT PMO Intern Dallas/Fort Worth, TX*

* Conducted data science work and dashboarding of project data to determine risk and hiring needs
* Completed a company-wide risk assessment of shop floor computers and controllers

**EDUCATION**

**The Pennsylvania State University May, 2020**

*BS, Cyber Security Analytics and Operations State College, PA*

* Focus: Cyber Threat Intelligence and Analytics
* Competitive Cyber Security Team

**CERTIFICATIONS, SKILLS & INTERESTS**

* **Certifications:** CASP+
* **Skills:** Azure Sentinel, Splunk, Devo, Exabeam, LogRhythm, Qradar, Python, Bash/Shell, KQL, SQL, AQL, Java, Linux, BSD, Windows, Networking, Network Security, Firewalls, system hardening
* **Interests:** Cyber Security, homelab, scale modeling

**Achievements**

* Eagle Scout
* Red Cell Analytics Lab: Open Source Intelligence Gathering and Threat Analytics
* Competitive Cyber Security Team: Treasurer (2019-2020)
* Collegiate Cyber Defense Challenge Team: 2 years
* Cyberforce Team: Fall 2019
* Raymond James CTF Team: Fall 2019
* Keystone Boys State: 2015