

AUSTIN ATEs

SKILLS

- Languages: Python | Golang | Terraform | Bash | JavaScript
- General: AWS | CI/CD | Git (Github) | Gitflow | Automation | Unit Testing | Integration Testing | Back-End Development | Serverless Architecture | Scripting
- Certifications: CompTIA A+ | CompTIA Network+ | CompTIA Security+ | CompTIA CySA+ | CompTIA Pentest + | CompTIA Project+ | Axelos ITIL4

PROFESSIONAL EXPERIENCE

TRANSAMERICA (January 2023 - Present)

Software Engineer (DevOps - AWS)

- My team's general duties are the **automated** provisioning of AWS accounts using **serverless micro-services**, with specific base requirements like the deployment of Cloud Custodian, specific IAM roles, Guard Duty, and more.
- My general duties include: creating resources in **Terraform**, developing and updating serverless features using **API Gateway, Lambda, State Machines, CodeBuild, CodePipeline, SQS**, and more.
- Some of my important projects:
 - I created the functionality for our Mover-Leaver process, which updates **Org Tags** in AWS accounts, updates a **DynamoDB** table with sailpoint IDs and the user's updated tags, and manages SQS messages and more.
 - I have **created an internal Python library** that can be used to automatically update local **GitHub repos**, do keyword searches across our repos, update deprecated resources and more.
 - I have created a generic **Change Ticket Class** to interact with our Change Ticket Api with opinionated features for my team.
 - I have automated my workflow for new stories (updating my local **git** branch, creating an aptly named feature branch, mapping secrets in AWS, opening VS code, etc.). I have also automated the process of finding deprecated resources across our Terraform, and in many cases I can automatically update them.

- I was recruited to my current team after completing a cross-team project: An important contribution I made was to **prevent a vulnerability in a React App** that would have leaked credentials being stored in a window variable as an attempt to avoid using props.

Information Security Engineer

- My biggest contribution was **automating** the workflow that TA was using to track certificates between TransAmerica and our parent company Aegon/GTS.
- General duties: I participated in Transamerica's Change Advisory Board. I reviewed False Positive and Non-Issue findings in our SAST and DAST, and helped teams **make their code more secure**, usually following the OWASP principles. I also **scripted** out dozens of spreadsheets with data from various sources to be ingested into ServiceNOW, to be turned into a powerpoint, and to create automated emails for app team follow up.

SHELTER MUTUAL INSURANCE (March 2022 - January 2023)

Information Security Analyst 1

- I managed several security products in the midst of massive turnover, including: ZScaler, CrowdStrike, Rapid7 IDR, and Cisco FirePower.
- My biggest contributions were creating a new member onboarding program, creating **45** knowledge base articles on our various tools, implementing SCIM provisioning in ZScaler, moving CrowdStrike to Phase 3, and creating a custom alert using Rapid7's API to monitor Admin accounts (written in Python).
- The onboarding process I created **decreased** the expected uptime of new hires to be "production ready" **from 8-12 weeks down to 2-4 weeks**.

O'REILLY AUTO PARTS (August 2021 - March 2022)

Junior Information Security Analyst

- General duties: Incident Response - QRadar and CrowdStrike | Rule tuning and developing custom IOCs - QRadar | Vulnerability Scan Review - Tenable Nessus.sc (On-Prem)
- Biggest contribution: I was responsible for analyzing servers that may be impacted by known CVEs, especially Log4j. I was also the first person on the team to discover the Reddit post that released the Log4j vulnerability that exploded in 2021.
- I participated in a Threat Hunt and OSINT review of O'Reilly Auto.

Software Developer - Intern

- I used the O'Reilly Tech Stack to complete 12 weeks of projects and to pass 6 in-house exams covering: HTML and CSS, JavaScript, SQL, Java 8, and Spring Boot.

- I was hand-selected by the **Security Operations Center (SOC)** to join their team after the internship was completed. I was one of only three people out of a group of 14 who were specifically requested to join a team after the internship concluded.

DEGREES

- Saint Louis University (SLU), Bachelor of Arts, Philosophy (2015)
- Western Governors University (WGU), Bachelor of Science, Cybersecurity and Information Assurance (2022)