

Luke Milby

Security Automation Engineer

Austin TX

(309) 319-3442

luke.milby@gmail.com

linkedin.com/in/luke-milby



Profile

Senior Software Engineer with a background in Cyber Security. Passionate about creating and automating processes which reduce toil. Numerous open source contributions and personal projects including a enterprise grade homelab, honeypots, and an internal SIEM.

Experience

Dec 2021 - Present **Senior Software Engineer**, *SumoLogic*, Austin, TX/Remote

Notable Achievements:

- Refactoring legacy code and improving our CI/CD pipeline
- Architecting log and event collection agents for SIEM ingestion

Sept 2017 - Aug 2021 **Senior Software Engineer**, *Rapid7*, Austin, TX/Remote

Notable Achievements:

- Built and maintained over 300+ REST API integrations for our enterprise SOAR solution
- Performed scrum master and software architect responsibilities
- Implemented CI/CD pipelines that delivered tooling to various package management services

Oct 2013 - Sept 2017 **Security Analyst**, *Country Financial*, Bloomington, IL

Notable Achievements:

- Built out and managed an internal red team
- Coordinated and executed penetration testing engagements
- Authored risk assessment profiles following NIST guidelines

Feb 2012 – Oct 2013 **Information Security Analyst**, *Pearl Technology*, Peoria, IL

Notable Achievements:

- Coordinated external network and web applications penetration tests
- Recommended security focused architectural improvements
- Used OSINT tools to perform security posture operations

Education

2006–2010 **Bachelors of Science - Information System Security**, *ITT Technical Institution*, Arnold MO

Technical Summary

Operating Systems Windows, OSX, Linux(Ubuntu/Centos/Redhat/Arch)

Languages Go, Python, Bash

Frameworks GoKit, Goreleaser, Cobra, React, Vue

Devops Tooling Docker, Kubernetes, Spinnaker, Jenkins, Elasticsearch, Ansible

Databases Postgresql, MongoDB, BoltDB, BadgerDB

Collaboration Git, Slack, Miro

Project Management Agile, Scrum, Sprint, JIRA

Security Tooling Nmap, Metasploit, Kali, burp

Security Frameworks & Standards NIST 800-53, OWASP Top 10

Cloud S3, IAM, SQS, SNS, Amazon Cloud Security, Aurora EC2