Luke Milby

SOAR Engineer

Austin TX
☎ *(309) 319-3442*
✉ *luke.milby@gmail.com*
🌐 *linkedin.com/in/luke-milby*

Profile

SOAR Engineer with a solid background in Cyber Security and Software Development, specializing in streamlining Security Operations Center processes and enhancing incident response capabilities. Proven track record in leveraging automation solutions, fostering collaboration, and contributing to open-source projects. Committed to driving success for organizations and their clients through innovative approaches, adaptability, and continuous improvement.

Experience

Sept 2022 - Present **SOAR Engineer**, *Entelligence*, Austin, TX/Remote

Notable Achievements:

- Successfully collaborated with the Security Operations Center (SOC) and Incident Responders to reduce time to remediation and enhance focus on critical tasks
- Leveraged Agile methodology and Azure DevOps for effective project management, improving overall team productivity and collaboration
- Provided expert consultation on best practices for XSOAR operations, leading to optimized processes and increased client satisfaction

Dec 2021 - Sept 2022 **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

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`, `XSOAR`
Security Frameworks & Standards	`NIST 800-53`, `OWASP Top 10`	Cloud	`S3`, `IAM`, `SQS,SNS`, `Amazon Cloud Security`, `Aurora EC2`