Luke Milby

XSIAM Consultant

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

Profile

Experienced Software Development and Automation Consultant specializing in XDR, SIEM, and Automation integration. Proven ability to streamline processes, develop innovative automation solutions, and enhance endpoint capabilities. Strong background in Agile methodologies, with a focus on building MVPs and exploring multiple use-cases. Committed to leveraging cutting-edge technologies to drive success for organizations and their clients through effective collaboration and continuous improvement.

Experience

Nov 2023 - Present
XSIAM Consultant, *Palo Alto Networks*, Greenville, SC/Remote
Notable Achievements:
- Prioritize clear communication to ensure understanding and alignment.
- Employ an Agile approach to building automation with a focus on time to value.
- Develop environments for Adversary Emulation to test agent capabilities.

Sept 2022 - Nov 2023
SOAR Engineeeer, *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

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`