Andrew Antles

andrewantles.net / Spokane, WA / andrew.antles@outlook.com / +1 (509) 255-3012

Summary

Security Engineer with 10+ years of experience; 6+ years in Application Security. Skilled in AI Security, Cloud Security and DevSecOps. Known for attention to detail, clean, concise solutions, and excellent communication skills.

Skills

Application Security: Secure Code Review, SAST/DAST, Vulnerability Management, OWASP Top 10

AI/ML Security: GenAI Risk Assessment, LLM Security, MCP Server Security

Cloud & Container Security: AWS, Kubernetes, Identity & Access Management (IAM)

Automation & Scripting: Python, PowerShell, Bash, Terraform, API Integrations, Security Automation

Penetration Testing: Web Application, API, Mobile, LLM

DevSecOps: GitLab, CI/CD Pipeline Security, Infrastructure as Code (IaC), VCS Security

Network Security: VPN, DNS, VLAN, Wireless, SSH Tunneling

Technical Leadership: Cross-functional Collaboration, Security Standards and Process Development, Team Mentoring

Experience

Flatiron Health

Senior Security Architecture Engineer, New York, NY - Remote
06/2023 - Present

Developed and implemented AWS root user management strategy across 40+ accounts in two organizations, eliminating shared credentials and reducing number of admins by 70%

Identified pervasive SQL injection vulnerability pattern in new AI application scheduled for immediate go-live; submitted remediation pull request, eliminating unintended PHI access

Discovered 8-year-old vulnerable authorization pattern affecting dozens of internal systems with PHI access; collaborated on and supported remediation deployment efforts

Averted PHI exposure in AI-powered feature deployment scheduled 3 days out; coordinated with owning team for immediate remediation before launch

Established MCP server security review process and delivered training; created supporting documentation for secure AI tool integration

Automated deployment of Tenable Kubernetes Security Posture Management (KSPM) across 50+ Kubernetes clusters, establishing continuous compliance monitoring and reducing manual security audits by 80%

Discovered and stopped private GitLab exposure to Internet due to improperly configured third-party integration; led SEV 5 incident response and post-mortem

Developed organizational security policies for GenAI technologies; delivered five knowledge-sharing sessions to upskill security team on emerging AI threats

Flatiron Health

Senior Application Security Engineer, New York, NY - Remote

07/2022 - 06/2023

Discovered widespread internal PHI exposure across multiple systems; developed executive reporting, remediation plan, and worked directly with development teams to eliminate the critical exposure

Developed AI security training and organizational AI security standards documentation, providing guidance and structure in a time of rapid change and high ambiguity

Conducted manual secure code reviews and application penetration tests on internal systems; developed and implemented remediation strategies to resolve all discovered gaps

Optiv Security

Senior Application Security Engineer, Denver, CO - Remote

06/2021 - 07/2022

Discovered critical vulnerabilities in Fortune 500 apps including pervasive online banking customer info exposure, authentication bypass in mobile apps, eCommerce checkout bypass; and provided actionable remediation steps

Developed custom security tools in Python and JavaScript including CAPTCHA bypass automation and BurpSuite extensions, expanding testing capabilities and attack surface coverage

Developed internal trainings: Attacking CORS Mis-Configurations, CSRF Exploitation; delivered to team of 40 penetration testers

Optiv Security

Application Security Consultant, Denver, CO - Remote

07/2019 - 06/2021

Conducted comprehensive application security testing for web, API, and mobile platforms, customized for maximum risk reduction against dozens of environments annually

Delivered clear, actionable risk reports with rapid vulnerability classification for technical and executive audiences, reducing complexity and time to resolution for customers

Led project teams of 6+ testers, mentored junior consultants, and refined internal processes resulting in organizational upskilling

Optiv Security

SIEM Security Consultant, Denver, CO - Remote

04/2018 - 07/2019

Partnered with technical and management teams to architect and implement LogRhythm and Exabeam SIEM deployments aligned to compliance requirements

Spearheaded Optiv's Exabeam UEBA delivery practice as one of three engineers selected to launch the program"

Developed custom asset inventory automation using PowerShell empowering customer's Attack Surface Management (ASM) program

NDM Technologies

Security Operations, Spokane, WA - On-site

12/2014 - 04/2018

Led MSSP practice development including SOC procedures, runbooks, and junior engineer mentorship

LogRhythm SIEM Deployment: Scoping and design, implementation, tuning and validation, and provided customer training

Maintained annual vendor certifications for WatchGuard network firewall and LogRhythm SIEM products

Community

Coach, Spokane Cyber Cup CTF: Feb 2021 - Present

Educate and mentor high school and college students in this CTF-style cybersecurity competition

Organizer, DefCon 509; local cybersecurity meetup: May 2017 - Oct 2021

Mentor, AFA CyberPatriot; high school student competition preparation: Oct 2017 - Sep 2018