Jake Spillers

St. Johns, FL
732-397-1156 | jake.spillers10@gmail.com | linkedin.com/in/jake-spillers | github.com/jspillers10

Experience

Live Nation Entertainment January 2026 - Present
Cyber Security Specialist *Remote, FL*

- Reduced third-party risk assessment drafting time by 80% by architecting and building an AWS Bedrock agent that turns a verified Slack request into a reviewable assessment document, using Step Functions and Lambda to orchestrate data retrieval, guarded AgentCore execution, encrypted storage, audit logging, and delivery.
- Drove remediation of authentication, data-exposure, injection, and tool-access risks across 40+ pre-deployment integrations by leading security architecture reviews of enterprise cloud, AI/ML, and MCP systems.
- Reduced inconsistencies in third-party JavaScript security assessments by 40% by conducting source-code reviews and designing and enforcing a Third Party Code governance framework with standardized security criteria.

Live Nation Entertainment April 2025 - January 2026
Third Party Risk Analyst *Remote, FL*

- Conducted more than 150 third-party risk assessments, evaluating vendor access controls and security programs against NIST CSF, ISO 27001, and SOC 2.
- Built a risk-scoring methodology and executive dashboards giving C-suite stakeholders visibility into more than $50 million in vendor exposure.

Projects

Secure Agent Gateway | *Python, FastAPI, OPA/Rego, Docker, AI Agent Security* August 2026

- Built a policy-enforced AI agent gateway using delegated RS256 identity, fixed tool registration, strict argument validation, server-computed risk, OPA authorization, single-use approvals, and redacted auditing.
- Tested controls against scope escalation, JWT algorithm confusion, approval replay, client-controlled risk, policy-engine failure, unauthorized approval, and direct policy-service access using 59 tests, 96% source coverage, 26 Rego tests, hardened Docker integration, and cross-version CI.

MCP Security Scanner | *Python, AST Analysis, SARIF, MCP Security* June 2026

- Built an AST-based security scanner for Python MCP servers covering seven vulnerability classes, with text, JSON, and SARIF 2.1.0 output for CI and code-scanning workflows.
- Created a pinned, reproducible benchmark with file hashes, machine-readable ground truth, deterministic matching, and explicit false-positive and false-negative analysis, improving security F1 from 0.843 to 0.989 on the educational corpus.
- Developed isolated FastMCP runtime labs validating command-injection and path-traversal findings inside network-disabled, non-root, read-only containers; maintained 199 tests and nine passing CI jobs across Python 3.10 through 3.13 and Windows.

Authorized AI Red Team Assessment Lab | *Web, API, LLM and MCP Security* May 2026

- Conducted an authorized black-box assessment across web, API, and AI surfaces, validating seven findings involving access control, prompt injection, SQL injection, and command injection.
- Traced a multi-stage path from model-facing input to privileged backend behavior through an exposed MCP integration and documented preconditions, evidence, impact boundaries, and root-cause remediation.

Secure Multi-Tier AWS Infrastructure | *AWS, IAM, CI/CD* December 2025

- Architected a two-AZ AWS environment with private application and database tiers, least-privilege IAM, Secrets Manager, IMDSv2, and automated CodePipeline deployment; independently diagnosed a cross-service deployment failure through IAM, agent, and lifecycle logs.

Education

Florida State University
Bachelor of Science in Cyber Criminology (Computer Science + Cybersecurity), GPA: 3.3 *Tallahassee, FL*

Certifications and Technical Skills

Security Engineering: Application security reviews, threat modeling, API security, cloud security, secure architecture, vulnerability validation
AI Security: LLM application threat modeling, prompt injection testing, agent and tool authorization, MCP security, adversarial ML fundamentals
Languages and Tools: Python, JavaScript, SQL, Bash, AWS, Docker, GitHub Actions, FastAPI, OPA/Rego, SARIF
Frameworks: OWASP LLM Top 10, NIST AI RMF, NIST CSF, ISO 27001, SOC 2
Certifications: AWS Certified Machine Learning Engineer Associate, AWS Solutions Architect Associate, CompTIA Security+, HTB Certified Offensive AI Expert, HTB CDSA