

Jacob Pittman

📞 (919) 555-0148 ✉️ jacob.pittman@protonmail.com

🌐 linkedin.com/example/jacobpittman 📍 Raleigh, NC 27609

SUMMARY

Information security leader with 14 years building and operating programs across cloud infrastructure, customer-facing applications, enterprise endpoints, and regulated environments. More than five years managing teams of up to six security professionals while staying hands-on with WAF policy engineering, DLP, **vulnerability management**, incident response, cloud controls, SIEM content, detection engineering, purple team validation, and **security automation**. Partners with CISO staff, engineering, IT, Compliance, HR, and Legal leaders to turn technical risk into clear decisions and practical roadmaps. Recent work secured **AI-enabled workflows**, built Python and Terraform automation, improved triage, and strengthened response operations across AWS and Azure. Ready to help Blue Ridge Sentinel Systems scale **security operations**, develop its team, and reduce risk through disciplined engineering and clear executive communication.

EXPERIENCE

Director, Security Engineering

September 2024 - Present

Northstar Commerce Group

Raleigh, NC

Leads a six-person **security engineering** and operations team supporting WAF, DLP, cloud controls, vulnerability management, incident response, SIEM content, AI security, and automation across AWS and Azure.

- Set a two-year security roadmap with CISO and engineering leaders, aligning hardening, detection, and remediation priorities.
- Rebuilt WAF governance for customer applications, reducing recurring false positives through telemetry and controlled exception reviews.
- Established **AI security** reviews covering prompt risks, sensitive data, vendor assurances, access controls, and workflow logging.
- Converted **purple team** findings into SIEM detections, **Terraform guardrails**, and tracked remediation plans across application and cloud paths.
- Presented risk posture, incident trends, vulnerability aging, and roadmap progress during executive security reviews.
- Coached six direct reports through **performance reviews**, capacity planning, **career development**, and hands-on technical escalations.

Senior Manager, Cyber Defense

January 2021 - August 2024

HarborPoint Financial Services

Durham, NC

Managed four analysts and engineers delivering vulnerability management, incident response, DLP, cloud monitoring, and detection engineering within a regulated financial environment.

- Managed four analysts and engineers across vulnerability management, **incident response**, DLP, cloud monitoring, and **detection engineering**.
- Coordinated high-severity incidents through containment, eradication, **root cause analysis**, legal input, and **post-incident reporting**.
- Migrated priority detection content into Splunk, adding Python enrichment that removed repetitive asset and identity lookups.
- Governed Qualys scanning and **remediation tracking** across infrastructure and applications using exploitability and asset criticality.
- Tuned AWS and **Azure** controls for identity, storage, networks, and configuration monitoring through documented risk acceptance.
- Led quarterly purple team scenarios with external testers, improving alert quality and response playbook coverage.

Security Engineering Manager

January 2018 - December 2020

Cobalt Ridge Technologies

Greensboro, NC

Supervised three security engineers supporting SaaS applications, AWS workloads, corporate endpoints, email systems, WAF, DLP, incident response, and security tooling.

- Supervised three engineers across SaaS applications, **AWS** workloads, endpoints, email systems, and complex escalations.
- Deployed and tuned a cloud **WAF** for production applications through governed changes, testing evidence, and lifecycle reviews.
- Implemented **DLP** across endpoints, cloud storage, and email while documenting workflows and supporting user education.
- Built **Python** utilities and **Terraform** modules for alert enrichment, cloud checks, access reviews, and repeatable control deployment.
- Created incident playbooks for credential compromise, exposed resources, malicious applications, and data exfiltration scenarios.
- Evaluated vulnerability, **SIEM**, and orchestration vendors, presenting coverage, cost, and operational tradeoffs to senior leaders.

Lead Security Analyst

July 2014 - December 2017

Piedmont Health Network

Winston-Salem, NC

Served as technical lead for a five-analyst cyber defense function monitoring clinical, administrative, and cloud-connected systems through SIEM and endpoint telemetry.

- Led five analysts monitoring clinical, administrative, and cloud-connected systems through continuous SIEM and endpoint telemetry.
- Coordinated vulnerability scans across servers, applications, and medical-support infrastructure, producing monthly risk-aging reports.
- Investigated phishing, malware, suspicious authentication, and data-loss events through evidence preservation and **root cause analysis**.
- Developed SIEM correlation rules and Python scripts linking identity, endpoint, vulnerability, and network investigation data.
- Supported email and endpoint DLP implementation through staged enforcement, exception review, and stakeholder communication.
- Mentored junior analysts and translated technical findings into concise updates for privacy, Compliance, infrastructure, and executives.

Information Security Analyst

January 2012 - June 2014

Oakline Manufacturing

Greenville, SC

- Monitored SIEM, endpoint, firewall, and vulnerability-management alerts across manufacturing, corporate, and remote-access environments while supporting investigations and control improvements.
- Monitored SIEM, endpoint, firewall, and vulnerability alerts across manufacturing, corporate, and remote-access environments.
 - Performed authenticated scans and partnered with infrastructure owners to verify remediation, compensating controls, and aging exceptions.
 - Wrote Python and **PowerShell** scripts that normalized scanner exports and enriched alerts with asset ownership.
 - Tested WAF rules for supplier and customer portals, documenting application behavior and approved exceptions.
 - Preserved evidence and drafted timelines for phishing, malware, and unauthorized access investigations.
 - Updated response checklists and escalation contacts after tabletop exercises and security awareness sessions.

PROJECTS

- AI Workflow Security Program**
- 📅 2025
- Created a review path for business AI workflows covering prompt handling, sensitive data, vendor assurances, access controls, and audit logging.
- Cloud Detection Guardrails**
- 📅 2023
- Converted purple team findings into Terraform guardrails, SIEM detections, and remediation tracking across AWS and Azure environments.

LEADERSHIP & AWARDS

- Recognized by executive leadership for translating security risk, incident trends, and roadmap progress into clear decisions.
- Selected to lead cross-functional purple team exercises that connected offensive findings with defensive engineering improvements.
- Built trusted partnerships with Engineering, IT, Compliance, HR, and Legal teams during high-severity incident response.

EDUCATION

- Bachelor's Degree in Information Technology**
- 2011
- Clemson University
- GPA: 3.5
- Clemson, SC
- Coursework:** Cybersecurity, Network Administration, Database Systems, Systems Analysis*

CERTIFICATIONS

- CISSP 📅 2022
- CISM 📅 2023
- GCIH 📅 2019
- AWS Certified Security - Specialty 📅 2021
- Microsoft Certified: Azure Security Engineer Associate 📅 2024

TECHNICAL SKILLS

- **Web Application Firewalls:** Cloud WAF, WAF policies, WAF tuning
- **Data Loss Prevention:** Endpoint DLP, cloud DLP, email DLP
- **Cloud Platforms:** AWS, Microsoft Azure, cloud controls
- **Vulnerability Management:** Qualys, authenticated scanning, remediation tracking
- **SIEM Platforms:** Splunk, SIEM correlation, security logging
- **Security Automation:** Python, Terraform, PowerShell
- **Incident Response:** Containment, eradication, root cause analysis
- **AI Security:** LLM workflows, prompt risks, sensitive-data reviews
- **Purple Teaming:** Offensive testing, defensive validation, detection gaps
- **Endpoint Security:** Microsoft Defender, endpoint telemetry, malware response
- **Identity Security:** Access reviews, identity enrichment, authentication monitoring
- **Security Governance:** Risk acceptance, executive reporting, security roadmaps

SKILLS

- WAF
- DLP
- Cloud Security
- Incident Response
- Vulnerability Management
- Purple Team
- Security Automation
- Detection Engineering
- Root Cause Analysis
- Post-Incident Reporting
- AI Security Reviews
- Executive Risk Reporting
- Vendor Management
- Security Roadmaps
- Performance Coaching

PROFESSIONAL AFFILIATIONS

- ISC2 member, maintaining active engagement with information security leadership and professional development.
- ISACA member, connecting governance, audit, risk, and security management practices with operational delivery.

LANGUAGES

- English (Native)
- Spanish (Intermediate)

ADDITIONAL INFORMATION

Work Status : Authorized to work in United States. No sponsorship required.

REFERENCES

AVAILABLE ON REQUEST