

GINO PEPENELLA, CISSP

Senior Platform Security Engineer & Architect | Cloud Security

Orlando, FL | (352) 650-0088 | g.pepenella@gmail.com

[Portfolio](#)

PROFESSIONAL SUMMARY

Senior Cybersecurity Engineer with 8+ years securing large-scale cloud, distributed, and multi-tenant infrastructure. Specializes in zero-trust architecture, DevSecOps, application security, and security automation. Recent work includes a compliance pipeline that cut scan time from 8 hours to under 30 minutes (94% reduction) and Ansible automation that eliminated roughly 40 hours per week of manual scanning. CISSP-certified, with hands-on experience across SIEM, WAF/IPS, microsegmentation, vulnerability management, container hardening, and CI/CD security gates.

PROFESSIONAL EXPERIENCE

Cole Engineering Services Inc., Orlando, FL

October 2024 - Present

Senior Platform Security Engineer

- Architected zero-trust security controls for a multi-tenant VMware Cloud Foundation platform supporting the world's largest cyber range under on a multi-cloud architecture.
- Lead the enterprise vulnerability management program with risk-prioritized remediation (CVSS plus asset criticality), on VCF and Amazon Web Services platforms.
- Engineered Ansible-driven compliance automation across Linux and Cisco infrastructure, replacing a manual scanning process and saving the team roughly 40 hours per week.
- Built a containerized, PKI-secured compliance platform consolidating thousands of STIG/CKL artifacts into a single auditable interface, accelerating pre-audit prep by 70%.
- Operate a defense-in-depth detection stack (Elastic SIEM, Tenable, NSX-T microsegmentation, F5 WAF/IPS) delivering real-time threat visibility across distributed workloads.
- Harden VM and container workloads against NIST 800-53 and CIS benchmarks, keeping the environment audit-ready for third-party security assessments.
- Mentor junior engineers and author incident-response runbooks adopted as the team's standard operating playbook.

ECPI University, Orlando, FL

November 2024 - March 2026

Adjunct Professor of Cyber and Network Security

- Designed and delivered undergraduate cybersecurity curriculum (network defense, secure infrastructure, applied threat analysis) to 20+ students per term.
- Built hands-on offensive labs simulating phishing, lateral movement, and privilege escalation mapped to MITRE ATT&CK techniques.
- Mentored students through Security+, CISSP, and CGRC certification tracks via structured study plans and mock assessments.

Scientific Research Corporation, Charleston, SC

October 2023 - September 2024

Cybersecurity Systems Engineer (L2)

- Promoted within 6 months for engineering a compliance scanning pipeline that cut execution time from 8 hours to under 30 minutes (94% reduction), via Ansible.
- Embedded shift-left security gates into CI/CD pipelines (SAST, secrets scanning, dependency analysis), reducing post-release vulnerability counts.
- Owned security compliance across multiple concurrent system authorization (ATO) cycles, coordinating evidence collection and remediation with cross-functional engineering teams.
- Automated security Body-of-Evidence (BOE) collection workflows, reducing pre-audit preparation by over 30% and saving hundreds of engineering hours per quarter.

United States Air Force, Oklahoma City, OK
Cybersecurity Engineer, Network Control Squadron

January 2020 - January 2024

- Engineered network and host security controls to protect a multi-site enterprise environment spanning classified and unclassified systems.
- Built Tenable-driven vulnerability detection automation across the network and application stack, cutting manual triage time and accelerating remediation cycles.
- Conducted 750+ security control inspections across mission-critical systems, identifying gaps that shaped organization-wide hardening standards.
- Contributed to security architecture decisions for mission-critical infrastructure that became hardening baselines across the organization.

PEO Exchange (acq. Alkeme Insurance), Tampa, FL
Business Risk Consultant

July 2018 - November 2019

- Conducted third-party risk assessments across 200+ enterprise vendors, evaluating data-protection controls, regulatory posture, and breach exposure.
- Advised clients on vendor risk strategy, reducing supply-chain risk exposure across their portfolios.

TECHNICAL SKILLS

Cloud & Infrastructure Security: AWS, VMware vSphere/VCF, NSX-T, Kubernetes, Docker, Red Hat Enterprise Linux, Infrastructure as Code (Terraform, Ansible), CI/CD security

Application & Network Security: OWASP Top 10, Threat Modeling, SAST/DAST/SCA, API Security, F5 WAF/IPS, Zero Trust Architecture, Microsegmentation, PKI, LDAP, SSO, mTLS

Detection & Response: Elastic SIEM, Splunk, Tenable Security Center / Nessus, Microsoft Defender, CrowdStrike, MITRE ATT&CK, Threat Hunting, Incident Response, Vulnerability Management

Automation & DevSecOps: Ansible, Terraform, Python, Bash, PowerShell, Shift-Left Security, Security-as-Code, GitOps, AI-assisted security workflows

Frameworks & Compliance: NIST CSF, NIST 800-53 (RMF), NIST 800-207 (Zero Trust), SOC 2, ISO 27001, FedRAMP, Third-Party Risk Management (TPRM)

CERTIFICATIONS

- **CISSP**, Certified Information Systems Security Professional (ISC²)
- **CGRC**, Certified in Governance, Risk and Compliance (ISC², formerly CAP)
- **CompTIA Security+ CE**

EDUCATION

M.Sc. in Cybersecurity Intelligence and Information Security University of South Florida
B.Sc. in Business Administration, IT Management Western Governors University