JONATHAN L. PEREZ, MS, CISSP, CISM

Active Secret Clearance
Aldie, VA | 703-843-6887 | jleepe@outlook.com | linkedin.com/in/cyberjp | Securitybyjp.com

Diligent and adaptable cybersecurity and risk management professional with over 10 years of experience overseeing the security posture of cloud and on-premises systems. Proficient in leading system authorizations aligned with NIST RMF, FedRAMP, and other compliance frameworks to support ATO readiness. Experienced across AWS environments, leveraging native and third-party tools to identify vulnerabilities, coordinate remediation, and maintain continuous monitoring. Leads enterprise vulnerability management programs, driving risk-based prioritization, remediation tracking, and executive reporting across hybrid environments. Skilled in automating security processes, closing risk gaps, and translating complex technical issues into actionable insights for executives and engineers. Strong background in developing security policies, incident response strategies, and cross-functional team leadership across full project lifecycles.

PROFESSIONAL EXPERIENCE

ASSURIT
Senior Cybersecurity Specialist – September 2018 – Present

- Direct the vulnerability management program; lead cross functional teams in remediating vulnerabilities and partner with engineers to resolve complex vulnerabilities that are not easily fixed from patches or workarounds.
- Serve as SME on RMF, continuous monitoring, security control assessments, and vendor risk reviews; ensure compliance with federal cybersecurity regulations.
- Lead weekly vulnerability management sessions to assess threat landscape relevance, prioritize findings by risk and asset criticality, validate false positives, and coordinate retesting and remediation with stakeholders to ensure remediation meets CVSS-based prioritization standards.
- Drive vulnerability reporting workflows using Qualys, Tenable, and Wiz; track remediation efforts through Jira, ServiceNow, and GRC platforms to ensure accountability and audit readiness.
- Executed and tuned vulnerability scans and scanning policies across hybrid environments using various tools such as Qualys, Wiz, Tenable, and CrowdStrike.
- Provide executive reporting related to vulnerability status, remediation metrics, and regulatory requirements, partnering with Legal, Finance, IT, and Operations to strengthen enterprise-wide risk awareness.
- Develop and implement security awareness and PII/FTI handling training programs.
- Leverage AI-driven capabilities within Qualys, Wiz, Tenable and CrowdStrike to streamline vulnerability triage, accelerate risk analysis, generate contextual security insights, and support the entire security lifecycle.
- Supported vulnerability remediation workflows using AWS Systems Manager for EC2 patching and Amazon ECR for container image analysis; collaborated with DevOps to address CI/CD pipeline risks identified through Wiz.
- Developed and maintained vulnerability metrics dashboards to track Mean Time to Detect (MTTD) and Mean Time to Remediate (MTTR) to enhance executive visibility into vulnerability remediation program.
- Aligned vulnerability management activities with NIST SP 800-53 and PCI DSS 4.0 control objectives, supporting risk-based remediation, risk register updates, audit preparation, and POA&M tracking across cloud and containerized environments.
- Conduct PIAs as part of NIST RMF/ATO, integrating privacy and security into authorizations and during major changes
- Manage and lead the annual contingency plan (CP) test across enterprise tenant environments and AWS platform teams, while continuously updating playbooks and maintaining CP/BCDR policies to align with applicable regulatory standards and industry frameworks.

Selected Achievements:

- Revamped vulnerability management processes for the Federal Election Commission by aligning with the CISA CDM Program and leading the migration from Tenable to Qualys. This improved scan accuracy, alert reliability, and remediation validation, resulting in enhanced federal audit readiness.
- Streamlined remediation processes, reduced response times for critical and legacy vulnerabilities by 30%.
- Spearheaded web application scanning integration using Qualys and Tenable.io, optimizing threat detection, vulnerability identification, and reducing critical vulnerabilities through streamlined workflows
- Evaluated cloud infrastructure and AWS configurations to ensure alignment with regulatory standards; Improved cloud security posture by identifying and resolving vulnerabilities and issues, reducing threat landscape.

Senior Information Security Analyst / Information System Security Officer (ISSO) – April 2014 – September 2018

- Ensured compliance with NIST, FedRAMP, and FISMA standards, supporting audit readiness and security control testing. Utilized NIST SP 800 series, FIPS, ISO 27000, and other frameworks to guide System Security Plan (SSP) development and ensure continuous alignment with regulatory requirements.
- Reviewed federal and COTS configuration documentation to assess potential security vulnerabilities and risks.
- Communicated priorities to stakeholders and presented bi-monthly briefings to review security issues and prioritize remediation efforts.
- Implemented and managed secure baseline configurations for Windows platforms in alignment with CIS Benchmarks, USGCB, and DISA STIGs, reinforced system security and standardization across platforms.
- Led change management initiatives; reviewed change requests and drove product adoption and end-user training.
- Conducted security impact analysis; monitored and researched the potential impact of system modifications.
- Managed vulnerability and compliance scanning in support of independent verification and validation (IV&V), audits, and incident response. Configured scan and audit policies for UNIX, Cisco, and Windows platforms.
- Served as a SME on IDS/IPS, port and vulnerability scanners, network detection, and security requirements.
- Coordinated troubleshooting efforts for problematic scans with OS Support, Database, Networking and VMware.
- Remotely isolated problem targets to fix, performed troubleshooting of access and connectivity issues.
- Coordinated cross-platform troubleshooting across UNIX, Cisco, and Windows environments, resolved vulnerabilities using a variety of tools, including Tenable Nessus. Executed local scans to secure high-value assets.

Selected Achievements:

- Conducted comprehensive vulnerability assessments to map NIST controls, strengthen organizational compliance, and protect intellectual property for the United States Patent and Trademark Office.
- Provided in-depth source code analysis during a short-term contract with the Securities and Exchange Commission; ensured secure coding practices and minimized software vulnerabilities within strict project timelines.
- Developed resolution policies that ensured rapid response to highly visible vulnerabilities identified during continuous monitoring, significantly improved mitigation turnaround times.
- Created an automated scanning workflow that increased productivity and enhanced scan data accuracy.
- Designed and implemented the After-Action Report (AAR) process to enhance tracking of automated scans and standardize reporting across multiple teams, which contributed to the expansion of the scanning team.
- Tailored audit policies and scanning tools to minimize unnecessary data output, streamlined analysis, and improved actionable insights for remediation.

EDUCATIONAL BACKGROUND

- University of Maryland University College: Master of Science (MS), Cybersecurity
- Savannah College of Art and Design: Bachelor of Fine Arts (BFA)

CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Amazon Web Services Solutions Architect (AWS - Associate Level)
- Certified in Governance, Risk and Compliance (CGRC, formerly CAP)
- Certified Ethical Hacker (CEH)
- Certificate of Competence in Zero Trust (CCZT)
- Trusted AI Safety Expert (TAISE) Certificate | CSA
- Certificate of Cloud Security Knowledge (CCSK)
- CompTIA Security+ Certified Professional (SEC+)
- CompTIA Network+ Certified Professional (NET+)
- Certified AI Security Specialist (CAISS)
- AES High Value Asset Technical Lead (TL)
- AES Risk Vulnerability Assessment Lead (AL)

TECHNICAL SKILLS

Tools & Vulnerability Management: Qualys, Tenable, Wiz, CrowdStrike Falcon, AWS Security Hub, Burp Suite, Fortify, Checkmarx, DOJ CSAM, RegScale, SCCM, Splunk, AWS (ECR, Systems Manager), Azure, JIRA, Confluence, ServiceNow GRC; CVSSv4, EPSS, MITRE ATT&CK, container image scanning, CI/CD integration, risk-based triage, and remediation tracking

Frameworks & Compliance Standards: NIST RMF, NIST SP 800-53 / 800-171 / 800-30 / 800-37 / 800-18, ISO/IEC 27001/27002, FIPS 199/200/201, PCI DSS 4.0, HIPAA, GDPR, SOC 2, COBIT, CIS Controls & Benchmarks, CMS MARSE 2.2 and ARC-AMPE, IRS Publication 1075, DISA STIGs, FedRAMP, FISMA, USGCB, CISA Evaluation Standards

Governance & Security Documentation:
System Security Plans (SSP), POA&Ms, Security Assessment Reports (SARs), Security Authorization Packages (SAP), risk assessments, vulnerability scan documentation, remediation tracking workflows, false positive analysis, audit preparedness, security policy development, Agile SDLC