Sam Sepassi

Senior Security Technical Specialist

samsepassi2@gmail.com • (703) 935-3344
LinkedIn • Sterling, VA

Seasoned Cybersecurity Specialist with progressive experience in enterprise security architecture, vulnerability management, and threat mitigation across government, financial, and technology sectors. Proven expertise in conducting Design Engagement Reviews (DERs), architecting secure systems, leading vulnerability assessments, and driving cross-functional security initiatives. Adept at aligning cybersecurity strategy with business objectives, enhancing system resilience, and ensuring compliance with regulatory frameworks, including NIST 800-53, ISO 27001, GDPR, and HIPAA. Demonstrated success in strengthening incident response capabilities, reducing attack surfaces, and optimizing SIEM and threat-hunting operations using tools such as Splunk and Tenable.io. Skilled in Cloud Security (AWS, Azure) with a strong command of the MITRE ATT&CK framework, firewall/ACL standardization, and continuous security monitoring. Recognized for mentoring technical teams, streamlining risk management processes, and delivering scalable security solutions in complex, hybrid environments.

Areas of Expertise

- Vulnerability Management
- Compliance Scanning
- Threat Hunting & Incident Response
- Risk Assessment & Mitigation
- Continuous Monitoring & Governance
- Data Protection & Privacy Strategy
- Security Tools & Platforms
- Security Architecture & Design
- Cross-Functional Leadership
- Penetration Testing & Ethical Hacking
- Scripting & Automation
- Enterprise Security Architecture

Professional Experience

Senior Security Architecture Specialist | ORACLE | Reston, VA 2025 – Present

Track risks and recommend controls by assessing and reviewing technical security architectures to minimize exposure to potential threats. Administer comprehensive security assessments, including threat modeling, risk analysis, and secure code review to enhance system resilience and reduce vulnerabilities. Prioritize critical vulnerabilities and architectural weaknesses to deliver remediation strategies tailored to risk impact and organizational priorities.

- Advised on data protection, privacy, and compliance best practices, ensuring alignment with regulatory frameworks such as GDPR, HIPAA, NIST, and ISO 27001, strengthening overall governance.
- Standardized ACL firewall rule templates, ensuring alignment with network architecture and maintaining compliance with corporate security assurance frameworks.
- Applied expert-level knowledge of secure architecture design across networks, applications, systems, and cloud platforms, ensuring adherence to internal security policies and business unit goals.
- Developed a vulnerability threat and management prioritization metric to drive focused remediation efforts and accelerate vulnerability burn-down across enterprise system

Cyber Security Senior | Vulnerability Management Freddie Mac | McLean, VA 2023 – 2025

Partnered with internal teams to analyze vulnerabilities and prioritize remediation to ensure focus on the highest-impact security risks. Spearheaded vulnerability and compliance scanning initiatives to identify high-risk gaps across cloud and on-prem environments to drive proactive remediation and improve audit readiness. Executed comprehensive scans across network devices to operate systems, databases, and wireless systems while uncovering critical misconfigurations and high-risk vulnerabilities.

- Reduced 25% scan errors and increased scanning efficiency across enterprise by driving scanner deployment.
- Improved scan accuracy by investigating false positives and collaborating with platform SMEs, resulting in more reliable vulnerability assessments and faster remediation cycles.
- Engineered continuous monitoring solutions while ensuring alignment with published security standards.
- Boosted 35% team technical proficiency and raised 20% productivity in the first quarter by directing cross-functional mentorship and training efforts
- Formulated and rolled out various robust network hardening strategies to strengthen defenses in accordance with evolving threats and cybersecurity best practices.
- Elevated the organization's incident response capability by integrating scan data with threat intelligence feeds, enabling proactive threat mitigation and faster response times.

Cyber Security Engineer | Leidos | Reston, VA 2022 – 2023

Steered Design Engagement Reviews (DERs) across enterprise environments, implementing strategic controls that reduced risk exposure and strengthened overall security posture. Orchestrated collaborative DER sessions with Security Architects and Engineers, delivering comprehensive evaluations and generating actionable insights to enhance cybersecurity frameworks.

- Engineered and deployed robust network defense strategies, fortifying critical assets against advanced persistent threats (APTs) and minimizing potential breach vectors.
- Optimized the organization's SIEM capabilities by developing and refining detection and response mechanisms, improving threat visibility and accelerating incident response times.
- Partnered with external security organizations to ensure Cyber Security Architecture Engineering (CAE) compliance, resulting in improved audit readiness and alignment with evolving regulatory standards.

Cyber Security Risk Management Analyst | Leidos | Reston, VA **2021 – 2022**

Delivered detailed risk assessment reports by conducting security profiling analysis across diverse network security technologies to enhance proactive threat identification. Strengthened enterprise risk management decision-making by reviewing and analyzing third-party COTS and open-source software for potential vulnerabilities and compliance gaps. Identified and assessed risks in complex IT environments while influencing strategic security enhancement initiatives and reducing enterprise-level exposure.

- Improved network defense by evaluating security control effectiveness using industry-standard risk assessment methodologies, leading to early detection of architectural vulnerabilities.
- Reduced potential attack surfaces by implementing continuous monitoring and assessment frameworks, improving overall enterprise security posture.
- Enhanced cybersecurity alignment and regulatory compliance by collaborating with key stakeholders to refine and standardize risk management procedures.

Additional Experience

Information Security Officer (ISSO) / Cyber Security Engineer | The Mitre Corporation | McLean, VA

Education

Master of Engineering in Cybersecurity Analytics | George Washington University | Washington, DC | 2024

Bachelor of Science in Information Technology; Minor in Cybersecurity | George Mason University | Fairfax, VA | 2021

Certifications & Licenses

AWS: AWS Certified SysOps Administrator - Associate (Apr 2024 - Apr 2027) | AWS Certified Security - Specialty (Jul 2021 - Jul 2025) | AWS Certified Cloud Practitioner (Jan 2021 - Jul 2027)

CompTIA: CompTIA Advanced Security Practitioner (CASP+) (Jan 2024 - Jan 2027) | CompTIA Linux+ (May 2023 - Jan 2029) | CompTIA PenTest+ (Jan 2021 - Jan 2027) | CompTIA Security+ (Jan 2020 - Jan 2027) | CompTIA CySA+ (Sep 2020 - Sep 2027)

(ISC)^2: CCSP (Jun 2025 - Feb 2028) | CISSP (Jun 2025 - Apr 2028)

Microsoft: AZ-500 - Azure Security Engineer Associate | SC-900 - Security, Compliance, and Identity Fundamentals

OffSec: OSCP | OSCP+ (Jun 2025 - Jun 2028)

Others: Certified Ethical Hacker (Sep 2021 - Sep 2027) | Junior Penetration Tester (eJPT) (Dec 2024 - Dec 2027) | Practical Network Penetration Tester (PNPT) (Jan 2025) | Oracle Cloud Infrastructure (OCI) Certified AI Foundations Associate | Oracle Cloud Infrastructure (OCI) Certified Security Professional

Interim Top-Secret Clearance

Technical Proficiencies

Programming Languages: MySQL, Java, JavaScript, Python, Bash Scripting, PowerShell

Cybersecurity Tools: Splunk, VirtualBox, Nmap, Wireshark, FlareVM, Burp Suite, Gobuster, Netcat, Metasploit, Tenable.io

Operating Systems: Windows, Linux (Ubuntu, Kali)

Applications: eMASS, ENS/HBSS, ACAS, ServiceNow, Jira

Publications

Co-author: NIST IR 8441: Cybersecurity Framework Profile for Hybrid Sate lite Networks (HSN)