Salman Wajid

Boston, MA

✉ salmanwajid@proton.me • **in** salmanwz • ⚙ Salmanwz

Education

Khoury College of Computer Science, Northeastern University   **Boston, US**
M.Sc. in Cybersecurity GPA: 4.0
Relevant Coursework: Network Security, Authentication and Authorization Techniques, Encryption Protocols and Standards, Web and Application Security.

NMIT (Nitte Meenakshi Institute of Technology)   **Bengaluru, India**
B.E. in Computer Science and Engineering GPA: *8.52 (Distinction)*
Relevant Coursework: Networking, Software Engineering, Web Development, Mobile Development, Python Programming.

Experience

Broad Institute of MIT and Harvard   **Cambridge, US**
Information Security Engineer Coop   *May 2024 – Nov 2024*
○ Designed and maintained security pipelines, SIEM tools, and detection systems to actively monitor and protect Broad's GCP environment and web applications.
○ Performed incident response, risk management, vulnerability assessments, and implemented security measures in compliance with federal security standards.
○ Developed solutions to enhance data security, focusing on network design and vulnerability scanning.

Check Point Software Technologies Ltd.   **Bengaluru, India**
Associate Security Engineer   *July 2021 – Jun 2023*
○ Led security assessments and implemented Secure Access Service Edge (SASE) solutions for clients across various industries.
○ Deployed Cloud Guard CNAPP and Harmony EDR solutions to protect critical infrastructure and ensure compliance.
○ Conducted vulnerability assessments and risk management in customer environments, providing consultation on security solutions.
○ Optimized IoT security solutions for healthcare and manufacturing environments, focusing on encryption protocols and network security.

Technical Skills

Programming & Scripting: Python, C++, C, Java, JavaScript, Bash, Go, Ruby, C, HTML/CSS.

Networking & Security: TCP/IP, DNS, DHCP, VPN (IPSec), SSL/TLS, IDS/IPS, DDoS Mitigation, SASE, MITRE ATT&CK, Zero Trust, Anomaly Detection, Vulnerability Scanning.

Cloud & Infrastructure: AWS (EC2, Lambda, S3, DynamoDB), GCP (GCE, Cloud Function, BigQuery), Redis, Docker, Terraform, Ansible, Kubernetes.

DevSecOps & Monitoring: GitLab, GitHub, Jenkins, Splunk, Google Chronicle, Tines, Prometheus, ELK Stack.

Security Tools: Nmap, Wireshark, Metasploit, SentinelOne, TCPdump, Qualys, Axonius, Snort.

Operating Systems: Windows, Linux/Unix, MacOS.

Certifications

CompTIA Security+ (SY0-701)

AWS Cloud Practitioner

Cisco Certified Network Associate (CCNA)

Projects

Secure Chat Application (Feb 2025): Designed and implemented a security-focused chat application with end-to-end encryption, leveraging TLS, Perfect Forward Secrecy (PFS), and modern authentication protocols (OAuth 2.0, OpenID Connect).

AI-based Security Vendor Review [Broad Institute] (Oct 2024): Developed an AI-driven security vendor review automation pipeline using Google Document AI, PaLM2, Terraform, and GCP, with a focus on network security and risk management.

Google Chronicle Alert Pipeline [Broad Institute] (Aug 2024): Built an automated alert pipeline using Google Sec Ops API, Chronicle SIEM, and Tines for real-time Slack notifications, focusing on threat management and security operations.