Salman **Wajid**

Security Engineer

Boston, MA 02119.

salmanwajid@proton.me | Salmanwz?tab=repositories | salmanwz

Summary

Security Engineer with 4+ years securing cloud infrastructure, applications, and enterprise networks across AWS, GCP, and hybrid environments. Experienced in threat modeling, detection engineering, IAM governance, secure SDLC integration, and AI/ML security. MS Cybersecurity (4.0 GPA), certified in CySA+, Security+, AWS Solutions Architect.

Skills

Programming & Scripting	Python, Go, Bash, PowerShell, C/C++, JavaScript, Assembly, YARA/YARA-L
Security Tools	Burp Suite, OWASP ZAP, Metasploit, Nmap, Wireshark, Nessus, Qualys, SentinelOne
SIEM & SOAR	Splunk, Google Chronicle/SecOps, Tines, ServiceNow, Axonius
Cloud Platforms	AWS (EC2, IAM, Lambda, S3, Security Hub, GuardDuty, KMS), GCP (GCE, SCC, Chronicle, Vertex AI, BigQuery)
Infrastructure & IaC	Docker, Kubernetes, Terraform, Ansible, CI/CD Pipelines
Security Specializations	Threat Modeling, Secure Code Review, VAPT, Detection Engineering, IAM Governance, IR, SAST/DAST Integration
AI/ML Security	LLM Security, Adversarial Analysis, Model Fine-Tuning, Prompt Engineering, MITRE ATLAS
Network Security	NGFWs (Palo Alto, Fortinet, Checkpoint), IDS/IPS (Suricata, Snort), VPN, Zero Trust, Network Segmentation
Frameworks	MITRE ATT&CK, OWASP Web Top 10, OWASP LLM Top 10, NIST 800-53, CIS Benchmarks, ISO 27001, PCI-DSS
Certifications	CompTIA CySA+, CompTIA Security+, AWS Solutions Architect, CCNA, CAPIE.

Experience

Khoury College of Computer Sciences, Northeastern University
Boston, MA

TEACHING ASSISTANT
January 2025 - December 2025

- Designed and deployed cloud-based infrastructure with CI/CD pipelines (Terraform, GitHub Actions) to automate grading and performance monitoring, reducing manual effort by 60% and accelerating feedback loops.
- Integrated static code analysis and automated test suites into the CI/CD pipeline, proactively identifying bugs and security flaws in student submissions and improving overall code reliability.
- Mentored 50+ undergraduate students on socket programming, TCP/IP protocols, and client-server architectures through hands-on labs, improving comprehension of network security fundamentals.

Broad Institute of MIT and Harvard
Cambridge, MA

INFORMATION SECURITY ENGINEER COOP
May 2024 - November 2024

- Built and maintained comprehensive threat models for GCP workloads; performed secure code reviews in Python and JavaScript, uncovering vulnerabilities that reduced application risk exposure by 35%.
- Automated cloud-native detection pipelines by integrating Google Chronicle with AWS/GCP logs and Terraform-based SIEM rules; reduced mean time to detect (MTTD) and respond (MTTR) by 45%.
- Developed reusable Terraform modules to enforce IAM least-privilege, VPC segmentation, WAF policies, and CIS compliance across multi-cloud deployments, improving DevSecOps delivery speed by 30%.
- Designed and deployed an AI-augmented vendor risk scoring system using Google Vertex AI and Gemini APIs, accelerating security reviews for third-party integrations by 75%.
- Tuned and validated behavioral detections against MITRE ATT&CK techniques within Google SecOps and SentinelOne, ensuring resilience against insider and advanced persistent threats.

Check Point Software Technologies Ltd.
Bengaluru, India

ASSOCIATE SECURITY ENGINEER
July 2021 - June 2023

- Partnered with global engineering teams to design and enforce secure cloud architectures across AWS and GCP; applied threat modeling and code reviews to eliminate recurring misconfigurations and strengthen defense-in-depth.
- Built Python and Go utilities to scan Check Point CloudGuard and Quantum-managed workloads for misconfigurations against CIS Benchmarks and OWASP Cloud Top 10.
- Deployed and optimized Checkpoint Quantum IoT Protect in manufacturing and healthcare environments; collaborated with R&D to implement lightweight encryption and data validation suitable for IoT/OT networks.
- Integrated SAST/DAST tools into CI/CD pipelines and developed reusable Terraform modules for secure-by-default deployments, accelerating release cycles while ensuring compliance.
- Created correlation rules and dashboards in SmartEvent SIEM to detect data exfiltration, malware, and zero-day threats; validated rule efficacy through adversary emulation mapped to MITRE ATT&CK.

Nutanix Inc. *Bengaluru, India*

SITE RELIABILITY ENGINEER INTERN *January 2021 - June 2021*

- Built Docker-based lab environment to reproduce customer failures, enabling faster root-cause analysis and patch validation; reduced time-to-fix by 50%.
- Automated log parsing and anomaly detection using Python and BigQuery, accelerating incident triage and reducing manual analysis effort by 40%.
- Developed monitoring scripts and health checks to proactively detect node failures and misconfigurations, increasing cluster uptime and customer satisfaction.
- Collaborated with SREs to design firewall and endpoint automation, eliminating repetitive triage tasks and freeing engineers to focus on higher-value reliability improvements.

Education

Khoury College of Computer Science - Northeastern University *Boston , US*

M.Sc in Cybersecurity *Sept. 2023 - Dec. 2025*

- GPA 4.0
- Relevant Courses: Software Vulnerability & Security, Application Security, Network Security, Digital Forensics, Offensive Security

NMIT (Nitte Meenakshi Institute of Technology) *Bengaluru, India*

B.E. in Computer Science and Engineering *Aug. 2017 - Jul. 2021*

- Distinction with Cumulative GPA is 8.52
- Relevant Courses: Software Engineering, Networking , Python Programming, Web Development.

Projects

1. **Wazuh + Threat Intelligence + AI Integration** *Jan 2025*
   - Built an AI-augmented Wazuh threat detection pipeline leveraging MCP-LLM for automated IOC triage, contextual enrichment, and predictive threat scoring.
   - Integrated real-time threat intelligence feeds to reduce false positives by 40% and accelerate incident response.
   - *Tools: Wazuh, MCP-LLM, Python, Threat Intelligence Feeds, Docker*
2. **AI Security Vendor Review Pipeline [Broad Institute]** *Oct 2024*
   - Designed and implemented an automated vendor risk scoring system using Google Vertex AI and Gemini APIs that accelerated security review for third-party integrations by 75%.
   - Deployed the solution as a CI/CD pipeline with Terraform, GitHub Actions, Docker, and GCP Services (Cloud Run, Artifact Registry, Pub/Sub, GCS).
   - *Tools: Python, GCP Vertex AI, Gemini API, Terraform, Docker*
3. **Google Chronicle Alert Pipeline [Broad Institute]** *Jun - Aug 2024*
   - Automated alert pipeline with Google SecOps API and Tines (SOAR) to route Chronicle SIEM alerts into Slack and auto-generate incident tickets.
   - Enhanced situational awareness and reduced mean time to acknowledge (MTTA) by 50% through real-time notifications and automatic assignment.
   - *Tools: Google SecOps API, GCP, Tines, Slack API, Python*
4. **Software Vulnerabilities & Security - AppSec/Binary Exploitation Labs** *Aug 2024*
   - Conducted penetration tests on web platforms, identifying and responsibly disclosing SQL injection, CSRF, cache-poisoning (CPDoS), and other OWASP-class vulnerabilities.
   - Reverse-engineered and exploited 15+ x86-64 Linux binaries, crafting custom shellcode and ROP chains that bypassed ASLR, canaries, DEP, RELRO, and PIE.
   - *Tools: Burp Suite, Ghidra, Binary Ninja, Python, C*