Satyajeet Sendha

Cloud & AI – Security Consultant

linkedin.com/in/satyajeet-sendha +91-8249789932
satyajeetsendha@gmail.com 8457092055

About Me

Security professional with 9+ years of experience in strengthening cloud and AI-driven environments through both defensive and offensive practices. Skilled in designing resilient architectures, embedding security throughout the software development lifecycle, and conducting adversarial simulations to uncover weaknesses before they can be exploited.

Education History

Masters in Software Engineering
Birla Institute of Technology & Science, Pilani
Class of 2020

Bachelor of Science in Computer Science
Utkal University, Odisha
Class of 2016

Professional Summary

- Proficient in advanced security and AI risk frameworks including **OWASP Top 10 for LLMs, NIST AI RMF 1.0**, **MITRE ATLAS**, **Cyber kill-chain Model**, **MITRE ATT&CK framework**, and Secure Software Development Lifecycle (**SSDLC)**, applying them to design, assess, and strengthen resilient cloud and AI-driven architectures.
- Actively engaged in offensive security skill development through Capture the Flag (**CTF**) competitions, **HackTheBox** challenges, and solving **TryHackMe** machines, gaining hands-on expertise in vulnerability exploitation.
- Specialized in cloud security operations across both **defensive** and **offensive** domains, including architecting layered defense mechanisms, implementing proactive monitoring and **guardrails**.
- Good knowledge of standards and compliances such as **GDPR**, **HIPAA**,**ISO 27001**, **PCI DSS 3.2.1**, and the **NIST** cyber security framework.
- Proven track record of delivering cloud security and compliance solutions for Swiss-based healthcare and fintech clients, with successful engagements across **APAC**, **EMEA**, and **Americas** regions, and currently securing logistics operations at FedEx to protect mission-critical **supply-chain** systems.

Skills

- Cloud Security (Azure, AWS, GCP ,OCI)
- CNAPP (Wiz, Prisma Cloud & Aqua Sec.)
- Scripting (Python & Bash)
- Security Architecture Review
- Source Code Review
- Vulnerability Management (Qualys & Kenna)
- AI Security & Threat Modeling
- Governance & Risk Management
- AI IDE (Google Antigravity)
- DevSecOps
  (Docker, Kubernetes, Jenkins, Maven, Terraform, Ansible, SonarQube, Trivy, Prowler, Grafana and Prometheus)

Certifications

- Palo Alto Networks Certified:
  - Cloud Security Engineer
  - Cyberforce Defender
- Microsoft Certified:
  - Azure Security Eng.
  - Security, Compliance & Identity Funda.
  - Azure AI fundamentals
  - Azure Fundamentals
- AWS Certified:
  - Security Specialist
  - AI practitioner
- Google Cloud Certified Cloud Security Eng.
- MITRE Certified :
  - Cyber Threat Intelligence
  - Security Ops. Center Assessment
  - Attack Fundamentals

Work Experience

Cyber Security Analyst - Senior 2 | Fedex

Nov 2024 to Present

- Developed a comprehensive **GenAI Security Evaluation Framework** to assess model vulnerabilities and data leakage risks; served as a key security contributor to the **Google AgentSpace** POC, defining the trust boundaries and access controls required for autonomous AI agents.
- Authored enterprise-grade **Secure Configuration Guidelines** and **Architectural Design Patterns** for RAG-based and GenAI applications.
- Engineered an automated **Threat Modeling tool** using Python and RAG to revolutionize application security assessments; integrated **OpenAI** and **SSO** with advanced prompt engineering to ingest architectural data and generate high-fidelity risk profiles, reducing manual assessment time while increasing finding accuracy.
- Architected and executed a comprehensive multi-cloud security transformation by deploying **Wiz Cloud** across **AWS**, **Azure**, **GCP**, and **OCI** environment; established a multi-year roadmap that transitioned the organization from reactive scanning to a proactive, context-aware risk posture.
- Managed daily triage of high-priority Wiz alerts across a multi-cloud estate, To scale these efforts, I developed a **Power Automate workflow** that aggregated real-time alert metadata into a centralized tracking hub, reducing manual reporting time by **70%** and ensuring **100%** visibility into remediation progress.
- Authored and enforced the **Wiz Operations SOP** alongside a comprehensive **Multi-Cloud Health Check framework**; established daily standardized procedures to verify the integrity of multi-cloud environment, ensuring 100% visibility and platform uptime.
- Worked on daily **Threat Advisories** and CSP **security bulletins**, analysing emerging **CVEs** to identify impacted resources and briefing cross-functional & product teams on prioritized remediation steps.

Data Governance & Privacy Engineer | Finastra

Oct 2023 to Nov 2024

- Led the implementation of **Dig Security** to safeguard over 3 million sensitive records across 60+ Azure-based products. Achieved instant visibility into data risk and implemented robust data security posture management.
- Develop and enforce cloud security policies to align with organizational and regulatory requirements and address identified vulnerabilities.
- Spearheaded the technical assessment of **CSPM/DSPM** solutions in a cloud security RFP, ensuring alignment with organizational needs through in-depth feature, pricing, and integration analysis.
- Create and enforce security policies for endpoints and Integrated **CrowdStrike Falcon** with other security tools and systems.
- In order to enable data-driven decision-making and an enhanced data protection posture, I have designed a **product data security dashboard** that offers critical insights and real- time visibility on data access, abnormalities, and possible breaches.

Work Experience

Global-SOC Team Lead (Assistant Manager) | KPMG India

March 2022 to Oct 2023

- I have worked on **Prisma Cloud** CSPM module to continuously monitor cloud environments for misconfigurations, vulnerabilities, and compliance deviations and analyze security posture reports to identify trends and potential risks.
- I have used **Dockle** & **Trivy** to perform a meticulous analysis of **container images**, focusing on security aspects. It adeptly identifies potential vulnerabilities, insecure configurations, and other elements that may expose the image to security risks.
- Enhanced cloud security posture by employing **Prowler** to identify and remediate misconfigurations.
- Used **SonarQube** to continuously inspect and analyze the quality of code to identify and remediate issues, enforce coding standards, and ensure code maintainability.
- Leveraged the **MITRE ATT&CK** framework to rigorously evaluate threat detection and response capabilities, guaranteeing selection of tools that effectively address real-world security challenges.
- Implemented **50+** critical security controls across **Azure cloud** infrastructure using Prisma Cloud, significantly reducing vulnerability exposure.

Senior Project Engineer | Wipro Technologies

December 2016 to March 2022

- Managed various cloud security operations with the team, created general and suppression rules in **Azure Monitor** based on the requirements, and assisted in the implementation of regulatory compliance.
- Deployed **Azure Sentinel** and its components. I worked on the data collection part through data connectors (Azure AD, Security Events).
- Created Azure Sentinel **Playbooks** using the logic app, which will disconnect VMs automatically on-basis of Sentinel alerts.
- Assisted in creation of ASG (**Application Support Group**) and assigned it to specified vm as per the requirement in-order to make the maintenance hassle-free.
- Configured Azure AD with the Azure SQL DB, knowledge on transparent data encryption and always encrypted features.
- I worked on the **Azure Security Center** and enabled Azure Defender, advanced protection on resources, and configured **anti-malware extension**.
- Developed and implemented robust monitoring and defense mechanisms, successfully mitigating **DoS attacks**, **MITM** attempts, and other security threats.
- Configured and fixed alert rules based on security requirements, and helped the clients upgrade their **defenders**.