Raj Singh

nova.magus@gmail.com 505-603-6389 www.linkedin.com/in/rgsingh01 rajsec.dev

EXPERIENCE

Hudson River Trading *New York, NY*

Security Engineer *March 2025 – Present*

+ Enterprise security – many hats, but currently focused on cloud security and vulnerability management.

AWS *New York, NY*

Security Engineer *December 2023 – March 2025*

+ Embedded security engineer acting as the trusted security voice to deliver end-to-end security reviews for 7 AWS services across industry segments.
  - Acts as a single threaded leader for cross functional teams of software engineers and technical project managers to embed security into products.
  - Leads design review, threat modelling, architecture review, code review, pentest finding mitigation, etc for large scale AWS services.
  - Reduces organizational security risk by helping teams mitigate security findings and influencing product vision with security in mind.
  - Creates golden-path documents which solve ambiguous security problems and helps teams avoid sharp edges.
  - Mentors and cross trains engineers on how to raise the security bar of their products.

Goldman Sachs *New York, NY*

Security Architect (Associate) *October 2022 – December 2023*

+ Security advisor for the firm's fully managed, continuous delivery service for AWS infrastructure
  - Performed threat modelling for the supported resources and services in the platform.
  - Wrote 100+ CDK test cases to validate the efficacy of the platform's security guardrails.
  - Partnered with various business units to increase platform adoption by providing architecture guidance, design patterns, and processes aligned with firm-wide security standards.
+ Performed architecture reviews (AWS native and hybrid with on-prem) for production workloads and core services used by multiple teams across the firm, along with peer reviews for other teammates performing similar assessments.
+ Wrote requirements, design patterns, and runbooks for integrating cloud-native applications managed by different teams with differing security postures and controls.

Millennium Management *New York, NY*

Cloud Security Engineer *June 2020 – October 2022*

+ Enabled various AWS services across the organization (100s of AWS accounts.)
  - End-to-end security feature evaluation of a given AWS service.
  - Security-focused API allow / denylisting in the organization SCPs.
  - Policy/role creation and deployment across the organization through CI/CD pipelines/step functions, etc.
  - Notable services include IAM Access Analyzer, FSx for Windows/NetApp OnTap, and DynamoDB Accelerator.
+ Code owner of the organization's AWS detection/notification/remediation framework.
  - Wrote and deployed Python code to remediate misconfigured VPC endpoints / S3 access points / public Airflow environments / and public Sagemaker resources among other things, code to monitor suspicious API calls, etc.
+ Implemented various GCP security controls via Terraform infrastructure-as-code, including:
  - More than 50 organization policies.
  - Log-based metrics from the Google Logging Service.
  - Alerting policies from the Google Monitoring Service.
  - Updates to VPC Service Control configurations.
+ Platform owner for the company's Hashicorp Vault instance in AWS.
  - Designed a secrets management schema for Vault paths based off of organizational structure.
  - Wrote Terraform code to integrate various Vault authentication backends (LDAP, Kerberos, approle, Nomad) with existing production workloads for secret retrieval/storage.
  - Implemented security features in Vault including token TTLs, CIDR restrictions for tokens, etc.
+ Deployed a third party CSPM tool across the organization in order to gain better visibility into both the AWS and GCP environments in terms of vulnerabilities on VM instances, configurations, overly permissive IAM entities, etc.
+ Onboarded hundreds of AWS accounts to the company's IDP to enable customer usage.
+ Performed security evaluations of various third party vendors (SaaS/PaaS) and coordinated with these vendors to perform proof of concepts.

- Worked with third party security companies to scope/coordinate/monitor penetration tests for both AWS and GCP as well as interviewing potential penetration testers.
- Acted as a project manager to coordinate meetings between the Linux Engineering and Information Security teams to track progress on ongoing projects.
- Actively works on cross-training other parts of the information security team to disperse cloud security knowledge in the form of runbooks, documentation, resource sharing, etc.

SKILLS

- **Cloud Security Skillset:**
  AWS Security: IAM/S3/VPC/KMS/Organizations(SCP)/Lambda/GuardDuty/SecurityHub
  GCP Security: organization policies, VPC (service controls, firewall rules, service perimeter), Alerting/Monitoring services, Cloud Logging/Stackdriver.
- **Cybersecurity Skillset:** computer networking, cryptography, NIST RMF, NIST CSF, OCTAVE FORTE, FAIR, GDPR/CCPA (basics), threat analysis/modeling (MITRE ATT&CK, STRIDE), cyber intelligence (SEI Cyber Tradecraft Report), security baselining, Metasploit, Wireshark, Redis, tcpdump, ELK Stack, nmap, Nessus.
- **Programming Languages:** AWS CDK (Typescript), Python, Terraform, HCL, C, Java, SQL
- **Software Tools:** Linux, Git, Microsoft Office, Windows, OSX
- **Soft Skills:** Fluent in Hindi, Professional Speaking, Technical Writing/Communication

EDUCATION

Carnegie Mellon University — *Pittsburgh, PA*
Master of Science in Information Security, Policy, and Management – GPA: 3.9 — *May 2020*

New Mexico Institute of Mining and Technology — *Socorro, NM*
Bachelor of Science in Computer Science — *May 2018*

PROJECTS

US Army NETCOM Capstone Project — *January 2020 – May 2020*
- Worked in a team of five and created an automated pipeline for ingesting, analyzing, and visualizing threat intelligence data from Symantec.
- Wrote Python code which (1) integrated custom objects with a Redis database, (2) performed graph-based analysis on those objects, and (3) created a rolling data ingestion process.

SSH Honeypot — *January 2020 – May 2020*
- Ran a publicly visible SSH honeypot on a Raspberry Pi. Analyzed packet data and system logs from the honeypot to gain insight into attack vectors, attacker demographics, etc.

Cyber 9/12 Strategy Challenge — *March 2019*
- Represented Carnegie Mellon in a strategy challenge about analyzing the impact of policy during cyber crises. Wrote policies and delivered oral presentations based on threat intelligence reports in a crisis simulation.

Academic Papers — *January 2019 – May 2019*
- Co-authored a paper which analyzed First American's 2019 data leak. Provided policy recommendations and technical mitigations based on OCTAVE Forte and NIST 800-53 control families.
- Wrote a paper which compared and contrasted the NIST RMF and FAIR. Outlined the strengths and weaknesses of both and identified initial steps that organizations could take to implement those frameworks.