Raajhesh Kannaa Chidambaram

raajheshkannaa@gmail.com | linkedin.com/in/raajhesh-kannaa-chidambaram | github.com/raajheshkannaa | raajhe.sh
Cloud Security Engineer | DoorDash | Toronto, Canada

SUMMARY

Security engineer with 15 years of experience, from bare metal infrastructure to securing cloud environments at scale. I build security tooling, automation, and enforcement pipelines that make secure defaults the easy path for engineering teams. Offensive security certified (OSCP, OAWSP) with deep AWS security architecture expertise.

CERTIFICATIONS

OSCP Offensive Security Certified Professional

OAWSP Offensive AWS Professional (CloudBreach)

AWS Security AWS Certified Security Specialty

AWS Networking AWS Certified Advanced Networking Specialty

EXPERIENCE

Cloud Security Engineer | DoorDash
July 2023 - Present | Toronto

- Built natural-language querying tool for AWS infrastructure security discovery across all accounts using Steampipe.
- Automated Private Terraform module synchronization across the GitHub Organization.
- Developed SlackBot for automated GitHub PR review and approval in Cloud Security support channel.
- Led full lifecycle evaluation, selection, and integration of a CSPM tool.

Senior Staff Security Engineer | Delphix
June 2022 - April 2023 | Toronto

- Built CDK Pipelines/GitOps delivery for AWS Config Conformance Pack findings with SecurityHub, PagerDuty, Slack, and Jira alerting.
- Built Incident Response Notebooks using Jupyter to query CloudTrail Lake for investigation and GuardDuty response.
- Designed Enforcement Engineering Pipeline deploying SCPs, corrective actions, and Permission Boundaries via CDK.
- Built Detection Engineering Pipeline for IAM credential exposure and Access Denied monitoring via CloudTrail Lake.

Senior Security Engineer | Guidewire Software
May 2021 - May 2022 | Toronto

- Automated AWS Attack Surface Management for 300+ accounts using CDK CI/CD Pipelines.
- Set up AWS Control Tower enrolling 300+ accounts with Security Hub, GuardDuty, SSO/Okta, and SCPs.
- Built Deception Engineering system to detect targeted attacks and prevent lateral movement.

Senior Security Analyst | BoxyCharm
Sept 2019 - April 2021 | Toronto

- Built Security Operations Center using GuardDuty, SecurityHub, CloudTrail, Config with Sumologic and PagerDuty.
- Built ChatOps-driven preventive guardrails for real-time Security Group change approval and revert.
- Operated Palo Alto VM-300 firewall in AWS with Transit Gateway for 300+ users across production and corporate.

Security Engineer | Zuora
Oct 2018 - Sept 2019 | Chennai

- Built Vulnerability Management solution using Qualys API, Lambda, DynamoDB, and Sumologic.
- AWS security operations across 60+ accounts using Organizations, GuardDuty, SecurityHub, and Inspector.

Technical Lead, IT Risk Management R&D | BNY Mellon | Eagle Investment Systems
Oct 2016 - Oct 2018

- Built Application Security Program with static analysis (Coverity), dynamic analysis (Burp Suite, AppScan), and OWASP Dependency Check.
- Developed Secure Development Lifecycle documentation and security awareness programs.

Senior System Administrator | Ebix
Mar 2011 - Sept 2016

- Vulnerability Assessment using Qualys. WAF with ModSecurity. OSINT with Censys.io. FIM with OSSEC HIDS.
- Infrastructure operations, database encryption with LUKS, internal phishing campaigns.

PROJECTS

GHA Scanner scan.defensive.works
GitHub Actions security scanner. 25 checks, 8 categories, graded reports. Open source.

Attack Surface Management github.com/raajheshkannaa/attack-surface-management
Continuous external attack surface discovery and vulnerability scanning across AWS accounts.

Green Stone github.com/raajheshkannaa/green-stone
Real-time Security Group change detection and one-click revert across AWS Organizations.

Fleet Access github.com/raajheshkannaa/fleet-access
Hub and Spoke IAM Roles for AWS multi-account security at scale.

WRITING

Assumed Role
Cloud security thriller. IAM credential theft, lateral movement, incident response. MITRE ATT&CK mapped.

Signed and Sealed
Supply chain attacks, CI/CD compromise, code signing. Parallels to SolarWinds, Codecov, tj-actions.

TECHNICAL SKILLS

Cloud: AWS (IAM, SCPs, Organizations, SecurityHub, GuardDuty, CloudTrail, Config, Control Tower, CDK, Lambda), Azure, Terraform
Languages: Python, TypeScript, Bash, SQL
Security: Penetration Testing, Incident Response, Threat Detection, Vulnerability Management, Security Automation
CI/CD: GitHub Actions, CDK Pipelines, GitOps
Infrastructure: Linux, Docker, Kubernetes, Palo Alto Networks