RAAJHESH KANNAA CHIDAMBARAM

OSCP | AWS Security & Networking Specialty

Security Architect and Engineer specializing in multi-cloud environments by utilizing Detective and Preventive controls and applying security at all layers through defense in depth strategies. Regardless of my knowledge and education so far, I would love to unlearn and learn something new every day in the field of Information Security and Technology.

raajheshkannaa@gmail.com

416 992 4946

Toronto, Canada

raajhe.sh

linkedin.com/in/raajhesh-kannaa-chidambaram

github.com/raajheshkannaa

SKILLS

Amazon Web Services | Azure | Infrastructure Security | CDK/ Pipelines | Terraform | Security Automation | Threat & Vulnerability Management | Security Operations | Linux | Incident Response | Logging & Monitoring | Identity & Access Management

INTERESTS

Active Defense | Threat Intelligence | Machine Learning | Malware Analysis | Network Forensics | Network Security & Monitoring | Purple Teaming | Threat Hunting | Open Source Intelligence

WORK EXPERIENCE

Cloud Security Engineer
Doordash

07/2023 - Present

- Developed a product leveraging Streampipe, using natural language for querying AWS infrastructure through a user interface. This tool facilitates the search and discovery of AWS resources and addresses security inquiries, such as identifying publicly exposed resources across accounts.
- Created automation scripts to manage and synchronize Private Terraform module updates across the GitHub Organization, ensuring consistent and up-to-date references.
- Developed a SlackBot powered by AWS Lambda to automate the review and approval of GitHub Pull Requests in the Cloud Security support channel, significantly reducing operational overhead.
- Played a pivotal role in the full lifecycle of the project to identify and integrate a CSPM tool, from proof of concept, through selection and onboarding, to post-implementation support and progression.

Senior Staff Security Engineer
Delphix

06/2022 - 04/2023 *Toronto, Canada*

- Designed and Built an Enforcement Engineering Pipeline to deploy AWS Service Control Policies, corrective actions such as reverting Security Group rule changes, Permission Boundaries.
- Designed and Built Automation to send Azure's Microsoft Defender for Cloud Security Alerts and Recommendations using Azure Functions to Slack, PagerDuty and Jira respectively using Azure Functions.
- Built an automation delivery using GitOps for Customization & Tuning of AWS Config findings imported into SecurityHub and alert escalations using AWS Lambda Functions` through PagerDuty, Slack, Jira.
- Collaboratively working with the DevOps/SRE team to build Incident Response Notebooks using Jupyter Notebooks to query CloudTrail Lake for investigation and respond to GuardDuty events in corresponding AWS Accounts.
- Built a delivery pipeline with GitOps to streamline maintenance and delivery of Roles/Permission Sets to AWS Identity Center(AWS SSO).
- Built a Detection Engineering Pipeline to deploy detections` as code for IAM Credentials exposure, Access Denied Monitoring due to AWS Service Control Policies using AWS Lambda Functions` and CloudTrail Lake.
- Setup Azure Policies to enable Microsoft Defender for Cloud in all Subscriptions across tenants`.

WORK EXPERIENCE

Senior Security Engineer
Guidewire Software

04/2021 - 05/2022 *Toronto, Canada*

- Architected and built an automated solution for attack surface discovery & management for 200+ AWS accounts with daily scans for external facing AWS Services such as Elasticsearch, Redshift, RDS, EC2, ALB/ELB, Lightsail, Cloudfront, Beanstalk, API Gateway.
- Built a solution to detect vulnerable AWS Route53 domains which could be taken over due to missing origins such as deleted S3 buckets.
- Setting up AWS Control Tower, enrolling 300+ accounts, customizing landing zones for Security Hub, GuardDuty, AWS SSO integration with Okta, Service Control Policies for reducing attack surface using AWS Native services.
- Deception Engineering using deceptive techniques to detect targeted attacks and early signs of a breach and prevent lateral movement using fake disallowed entries in robots.txt, developer comments in page source, session cookies, javascript, user accounts, database tables, API endpoints, AWS access/secret keys.

Senior Security Analyst
Boxy Charm

09/2019 - 04/2021 *Toronto, Canada*

- Established visibility across the Enterprise catering to 300+ users and AWS Infrastructure catering to approximately 2Million users for better Detection and Response using multi account strategy to collect telemetry in a central location and built a Logging Architecture using Sumologic and Panther Labs SIEM.
- Built a comprehensive Vulnerability Management solution involving Scanning and Reporting automation using Qualys API, AWS Lambda, DynamoDB and Sumologic.
- Built Security Operations Center using AWS GuardDuty, SecurityHub, CloudTrail, Config, Qualys Vulnerability findings with Sumologic integrated with PagerDuty, Slack and Jira for Security Monitoring & Incident Detection.
- Built Preventive Guardrails using a ChatOps approach with Slack Interaction to revert AWS Security Group changes to specific ports from an IP, which will alert in Slack to approve or disapprove.
- Built automation of Blocking malicious IPs using AWS Lambda with Sumologic with an interactive ChatOps approach to block IPs in Cloudflare from Slack.
- Built AWS Service Control Policies reducing the attack surface across our AWS Infrastructure by up to 90% at scale, along with Tag Policies.
- Built, maintain and operate Palo Alto VM Series 300 in the AWS Cloud for Global Protect VPN for 300+ users, across platforms such production and corporate needs using AWS Networking capabilities such as Transit Gateway and Global Accelerator.

Security Engineer
Zuora

10/2018 - 09/2019 *Chennai, India*

- Security Operations - Responsible for continuous monitoring for anomalous activity with Incident Response and Digital Forensics.
- Sumologic for Log aggregation, Visualization, Security Analytics, Monitoring and Alerting.
- Lacework for monitoring AWS activity using AWS CloudTrail logs.
- Threat Stack for monitoring AWS activity using CloudTrail logs, Virtual Machine & Container agents for user activity and File Integrity monitoring.
- AlertLogic for Intrusion Detection and Monitoring for AWS EC2 using host agents.
- Cisco SourceFire for Intrusion Detection, monitoring network traffic.
- Rapid7 tCell for Web Application Firewall monitoring web traffic from containers and application agents.
- AWS Security using services such as GuardDuty, SecurityHub, Inspector orchestrating using Lambda with Python for automation and enforcements with cross-account IAM roles for managing and orchestrating 60+ AWS Accounts using AWS Organizations along CloudTrail and Config.
- Insider Threat Monitoring using enSilo for Real-time defense against malware in user's machines. Sophos for Anti-Malware Endpoint protection. Cisco OpenDNS for monitoring and blocking of malicious traffic from user's machine. Cisco Cloudlock for monitoring for PII and PCI Data leakage in cloud storage services, Google Drive & Box.
- Vulnerability Management & ASV for PCI External Scanning Requirement using Rapid7 InsightVM & CoalFire and Qualys Guard.

WORK EXPERIENCE

Technical Lead - IT Risk Management R&D
BNY Mellon | Eagle Investment Systems

10/2016 - 10/2018 *Chennai, India*

- Responsible for the Application Security Program on a budget with the philosophy of high returns on Investments.
- Static Code Analysis - Coverity, Cppcheck, VisualCodeGrepper.
- Dynamic Analysis - IBM AppScan, Burp Suite, Zed Attack Proxy.
- SecDevOps using Jenkins for immediate feedback for Agile Teams.
- Elastic Stack and Splunk as the platform for automated pipeline delivery of Static and Dynamic testing reports.
- OWASP Dependency Check for 3rd party/Open Source.
- SonarQube for Quality Analysis in the code base.
- Manual verification of reports provided by 3rd party assessments.
- Secure Development Lifecycle Documentation - Best practices, Policies and Procedures, OWASP Cheat Sheets for each of the Top Ten 2013.
- Security Awareness programs using deliberately vulnerable web applications.

Senior System Administrator
Ebix Software India Pvt LTD

03/2011 - 09/2016 *Chennai, India*

- Cyber Security Team - Responsible for Vulnerability Assessment, Management and Security Operations for the entire infrastructure. Vulnerability Test Assessments using Qualys Scan and remediation plans for Hosting team. Database backups Encryption using LUKS encrypted volumes. Regular perimeter scans for open ports/services. Internal Phishing campaign using the Lucy Framework.
- Operating System Audits using ‘Lynis’ Audit tool. Web Server hardening by removal of weak Cipher Suites/Protocols and implementing stronger alternatives to match industry standards along with enabling HSTS/HTTP Strict Transport Security for all domains. ‘stunnel’ for tiered application involving a Web, App, DB stack to encrypt traffic between the stack components.
- Web Application Firewall using Modsecurity for Apache. Enabling Web Security using HTTPS/TLS using the free CA ‘Let's Encrypt’ for all domains for considerable cost savings to the organization.
- Security Onion as our passive secondary Network Security Monitoring tool, which currently being used to track activity. IDS setup using AlienVault OSSIM for SIEM Open Source IP Reputation Portal by AlienVault Import the database into iptables in linux to better protect our web servers from malicious activities.
- Open Source Intelligence using Censys.io for collection and analysis to review publicly available data about the company that could be used for offensive purposes before threat actors do.
- File Integrity Monitoring using OSSEC HIDS & GitLab to maintain backup copies of mission critical application data.
- Cloud Administrator's Team - Responsible for the Hosting Services Management at Amazon Web Services Design and Architect the first of our initiatives to move to the IAAS cloud. Moved our development environment to AWS EC2/VPC running over Ubuntu with DB’s using RDS.
- Operating Systems team - Responsible for New host setup using HP iLO and Dell DRAC web interfaces for a 3 Tier infrastructure involving Web/Application/Database servers.
- Setup virtual environments involving - VMWare ESXi, Oracle VirtualBox, Citrix Xen.
- Storage Administrator's Team - Responsible for creation and management of virtual volumes on SAN across data centers which include HP P2000, HP P4500, HP 3PAR. Creation and management of volumes on Linux using multipath-utils, LVM, RAID.

CERTIFICATIONS

Offensive Security Certified Professional - OSCP

AWS Certified Security - Specialty

AWS Certified Advanced Networking - Specialty