+91 9043040398

www.linkedin.com/in/archana-sn

archana.n1921@gmail.com

Bangalore, India

EDUCATION

Bachelor of Engineering
R V College of Engineering | 2011 -2015

CERTIFICATIONS

- **AWS Solutions Architect - Associate**
- **AWS Cloud Practitioner**
- **Splunk Power User Certified**
- **Cisco Certified Network Associate Routing and Switching (CCNA)**
- **Certified Ethical Hacker 312-50)**
- **Zscaler Certified Cloud Administrator Internet Access**

TECHNICAL PURVIEW

- **F5 Shape: SSE, Cloud Protection Manager, CAPPI.**
- **Akamai: Bot Management Tool**
- **AWS: ASG, EC2, VPC,DataDog, ALB,NLB, ACM**
- **Logging Tool: SPM, Splunk Monitoring Tool: DataDog**
- **Arbor: SP Peakflow, Sightline, SP Collector, Arbor TMS, Pravail APS, SSL Inspection, Pravail NSI, AED.**
- **Radware:DefensePro, DefenseFlow, APSloute Vision Reporter, Alteon- SSL Inspection and Radware MSSP Reporting Portal.**
- **GenieATM ISP and F5: DDOS Hybride Defender, SSL Orchestrator .**

ARCHANA S NARAYANASWAMY

Cloud Infrastructure and Security Engineer

PROFESSIONAL SUMMARY

Cloud Infrastructure and Security Specialist with 8+ years of technological expertise in the industry. Proven ability to Secure Cloud infrastructures and applications using industry-leading tools and best practices. Experienced in the areas of Cyber Security, Information, Network Security and Cloud Concepts including Deploying and Managing Multi-Vendor Cloud based Anti-DDoS Security Services and Bot Management Services to Mitigate and Securing Perimeter for large scale organisations along with configuration and management of Clients Architecture and migration of workloads to Cloud.

EXPERIENCE

Cloud Infrastructure and Security Specialist
11/2020 to Present JPMorgan Chase & Co.
Bangalore, India.

- Designing the platforms, servers and networks that make it possible to provide service to end customers, clients, and business around the globe each and every day.
- Experience in designing tailored solutions to understand the requirements of a project, test the performance of the infrastructure and verify that the requirements have been successfully met.
- Responsible for driving the results, collecting, and analysing monitoring data in test and production, and managing projects to completion.
- As a member of an engineering team that works closely to mitigate perimeter security risks in an agile fashion.
- Analyse cybersecurity attacks methods and tactics, unauthorised activities leveraged against the firms' mobile and web applications, review/produce technology partners and technology specifications for any changes or improvements to existing technology or purpose entirely new solutions as necessary.
- Work with other engineers on team, global technology partners and technology vendors to ensure that specifications are clearly documented, communicated, and understood, and advise the business on options, risks, and costs.

- Deploy and support perimeter defense solutions and security measures leveraging a combination of vendor and internally developed components, to detect and mitigate automated attack traffic and cyber- attacks.
- Analyse the performance and efficiency of production systems and controls and recommend and deploy enhancements to maintain control effectiveness in response to changing attack patterns and methods.
- Proficient knowledge in the following key areas hardware architecture (performance testing, monitoring, operations), Hardware benchmarking (program management, network management), Design and network engineering(planning, provision).
- Knowledge on one specific infrastructure technology and basic programming languages.
- Intermediate understanding of line of business technology drivers and their impact on architecture design.
- Knowledge on more than one specific infrastructure technology (F5 shape bot- management and Akamai Bot Manager).
- Ability to think creatively to deliver solutions through continuous improvement.
- Understanding of web/http security risks; knowledge of OWASP automated threat category and familiar with OWASP Top Ten
- Experience with http protocols response codes, modern usage, and web scripting/automatio n tools.
- Experience with large-scale/high- volume ecommerce infrastructure and/or consumer mobile applications and associated threats.
- Fundamental understanding of modern TCP/IP network infrastructure and network hardware/software (CCNA Routing & Switching or Network + is a plus).
- Industry recognized security certifications such as Certified Ethical Hacker, CCNA Routing & Switching,
- Industry recognized monitoring
- platforms certifications such as splunk power user certification and Datadog.
- Industry recognized AWS Certification such as AWS Cloud Practitioner and

Senior Information Security Engineer , 04/2017 to 11/2020
Tata Communications Limited, Bangalore, India.

- Responsible for identifying risks associated with organisation information assets related to DDoS attacks.
- Design secure systems, applications, and networks that meet user needs while maintaining the highest level of operational security.
- Designing and co- creating DDOS service solutions along with architecture team for clients to provide defense against distributed denial of service attacks triggered by attackers leveraging compromised bots to initiate the malicious traffic.
- Responsible for planning, coordinating, and implementing application architecture designs and engineering reviews to ensure that new services are secure by design.

- Mapping client's requirements and coordinating, developing, and implementing processes in line with guidelines.
- Demonstrated experience in the practical implementation of detailed project plan, creation of detailed process documentation including risk mitigation documentation.
- Knowledge sharing with 24*7 SOC teams about customer infrastructure and methodology followed in implementing the DDoS solution and providing support by handling customer escalations in case of a security incident.
- Ensures documentation is created for hand off to the Security Operations Center (SOC) Team as part of project handover post implementation and validation of security measures to protect the clients

Information Security Engineer , 06/2015 to 04/2017
Tata Communications Limited, Chennai, India.

- Designing, Validating and Implementing DDoS Solutions for various Client Network Infrastructure to protect from distributed denial of attacks generated by attacker using bots..
- Demonstrating the mDDoS Multi-Vendor Detection and Mitigation platform capabilities to end customers.
- Navigated the use of controls, tools, and best practices for the network security devices to identify unauthorised, anomalous events and security infractions that may exploit system vulnerabilities thereby reducing impact.
- Accountable for installation,
- maintenance of Arbor, Genie, Radware Multi- Vendor DDoS Platforms.
- Provided exceptional support for business via On-site support, travelling and remote support via VPN technologies.
- Exhibited efficiency in executing tasks by doing things within agreed SLA to meet customer requirements.
- Improvised & Standardised the LLD for mDDoS Customer implementations and review with solution architecture team.
- Extensive use of latest networking platforms and security focused appliances.
- Identify and resolve hardware and software related security threats in deployment by implementing suitable security solutions to mitigate the attacker traffic intended to compromise the clients infrastructure.
- Responsible for Creating and maintaining Production devices Inventory.