Dhanesh Babu

Security Engineer

Chennai, IN

https://dhanesh.info

dhanesh0909@gmail.com

https://www.linkedin.com/in/dhaneshb/

Proven track record in excelling in AWS disaster recovery, cost optimization, and leadership in cloud security. Expertise in AWS Security Best Practices combined with hands-on administration of DLP tools to configure policies, analyze event/alert patterns, and prioritize threats. Demonstrates technical acumen by effectively monitoring and responding to security alerts, ensuring comprehensive protection of networks, systems, and applications through systematic event analysis.

Technical Skills

- Linux Distribution - Ubuntu, CentOS, Kali.
- Cloud - AWS Proficiency, Partial with Azure, Minimal with GCP.
- Security Tools- Cloud Security Scanning Tools(Scout, Prowler, Greenbone).
- Security Audit Standards - ISO 27001, CIS Benchmark, Fisma.
- Security Administration - Linux Server Hardening, IAM, WAF, Security Hub, Config, GuardDuty, Inspector,AWS Organisation, ACM, etc..
- Monitoring - Zabbix, AWS Security Hub, ISMS.
- Application Code Security Scanning - Burp Suite, SonarCube.
- Scripting - Shell Scripting, Bash.

Certifications

2024-06	AWS Certified Security - Specialty - (SCS-C02)
2023-01	AWS Certified SysOps Administrator - Associate - (SOA-C02)
2022-05	AWS Certified Cloud Practitioner - (CLF-C02)
2022-03	Azure Fundamentals - (AZ-900)

Work History

2025-01 - Present

Security Delivery Senior Analyst

Accenture, Bengaluru

- Implemented and managed cloud security controls across AWS, Azure, and GCP, ensuring compliance with industry standards such as ISO 27001, SOC 2, and GDPR.
- Conducted cloud risk assessments, identified vulnerabilities, and implemented mitigation strategies to enhance cloud infrastructure security.
- Designed and enforced access control policies using Role-Based Access Control (RBAC) and fine-grained IAM configurations across multi-cloud environments.
- Monitored cloud environments using AWS CloudWatch, Azure Monitor, and Google Cloud Operations Suite, ensuring real-time detection and response to security incidents.
- Deployed and configured cloud-native security tools such as AWS WAF, GuardDuty, Azure Security Center, and Google Cloud Armor to protect against cyber threats.
- Spearheaded the implementation of data encryption mechanisms, including server-side and client-side encryption for S3 buckets and databases, ensuring data integrity and confidentiality.
- Conducted incident response for cloud-based systems, using tools like AWS Security Hub and SIEM platforms, to minimize downtime and mitigate risks.
- Collaborated with DevOps teams to integrate security best practices into CI/CD pipelines, ensuring secure code deployment across cloud platforms.
- Managed disaster recovery plans and conducted regular simulations to validate backup and recovery processes for cloud workloads.
- Optimized cloud infrastructure costs through rightsizing resources, reserved instances, and cost monitoring tools, while maintaining robust security postures.
- Led cloud security awareness programs for cross-functional teams to align on best practices and improve organizational security culture.
- Conducted penetration testing on cloud-hosted applications and systems, providing actionable recommendations to remediate vulnerabilities.

- Reviewed and enforced security baselines for virtual machines, containers, and serverless functions across AWS, Azure, and GCP.
- Audited cloud environments to ensure compliance with internal policies and external regulations, preparing for SOC 2 and SOX audits.
- Leveraged tools like Datadog, Splunk, and Prometheus for advanced security monitoring and analysis.
- Acted as a liaison between technical teams and business stakeholders, translating security risks into actionable business insights.

2022-07 - 2024-07

Senior Engineer

CTG, Chennai

- Implemented AWS Config to track changes to AWS resources, enforce compliance, and maintain an audit trail of resource configurations to enhance security and governance.
- Implemented AWS GuardDuty to continuously monitor for malicious activity and unauthorized behavior to protect AWS accounts and workloads.
- Managed and rotated secrets and credentials securely using AWS Secrets Manager, ensuring sensitive data protection.
- Implemented centralized management of AWS WAF rules and AWS Shield protections across AWS Organizations and Accounts.
- Configured data security and data privacy service that uses machine learning and pattern matching to discover and protect sensitive data in AWS with Amazon Macie.
- Managed SSL/TLS certificates with AWS Certificate Manager to ensure secure communication between services and clients.
- Conducted automated security assessments using AWS Inspector to identify security vulnerabilities and compliance issues within AWS environments, ensuring proactive remediation and improved security posture.
- Utilized AWS Systems Manager for operational insights, automation, and maintenance of AWS resources securely.
- Improved application availability by designing and implementing effective disaster recovery strategies using AWS backup services.
- Streamlined deployment processes with AWS CloudFormation templates for infrastructure automation.
- Provided prompt support during on-call rotations to address critical incidents involving AWS infrastructure, ensuring minimal downtime and rapid resolution.
- Optimized costs by identifying unused resources, recommending right-sizing instances, and leveraging reserved instances or spot pricing on AWS.
- Implemented budget monitoring, resource tagging, and cost allocation strategies across AWS services.
- Assessed existing infrastructure to identify improvements and implemented cloud-based solutions using AWS services.

- Managed container orchestration with Kubernetes on Amazon EKS for highly available applications in microservices architecture.
- Enhanced cloud infrastructure efficiency by optimizing AWS services and automating routine tasks.
- Trained team members in AWS tools and services for increased efficiency in cloud management.
- Aligned business objectives and technical requirements during planning phases for cloud migrations and deployments.
- Ensured high data security by enforcing encryption methods, policy management, and network access control within AWS.
- Regularly monitored, troubleshooted, and fine-tuned AWS resources to boost system performance.
- Implemented monitoring solutions using Amazon CloudWatch for real-time system performance insights.
- Deployed Lambda functions for serverless computing in response to event triggers in Amazon API Gateway.
- Regularly audited configurations against industry standards such as CIS benchmarks or NIST guidelines to strengthen infrastructure security.
- Developed comprehensive cloud migration plans with cross-functional teams for seamless transitions to AWS.
- Resolved technical problems quickly by monitoring networks and network devices.

  Led server infrastructure development, quality assurance, staging, and production systems.
- Evaluated software products for compatibility with existing systems.

  Implemented robust encryption methods and access control techniques to enhance cloud security.
- Established comprehensive risk management policies to reduce exposure to cyber threats.
- Identified and remediated potential security risks in cloud environments with cross-functional teams.
- Ensured GDPR compliance by implementing stringent data protection measures.

  Conducted vulnerability assessments for cloud applications, recommending updates and patches for security.
- Facilitated smooth migrations of legacy systems to secure cloud platforms, minimizing potential risks.
- Delivered regular reports on cloud security measures to key stakeholders for informed decision-making.
- Implemented multi-factor authentication systems for improved user access management.
- Reduced vulnerabilities through regular security audits and penetration testing for cloud infrastructure.

System Engineer

2018-11 - 2021-11

Full Creative, Chennai

- Installed, configured, and maintained Linux servers, including web and mail servers, ensuring optimal performance and reliability.

- Conducted software installations and upgrades on Linux systems, adhering to established policies, procedures, and service level agreements.
- Implemented and maintained robust security measures, safeguarding servers against unauthorized access and potential threats.
- Deployed new systems and applications, seamlessly integrating them with existing infrastructure, minimizing operational disruptions.
- Collaborated with cross-functional teams to troubleshoot and resolve server-related issues, minimizing downtime and optimizing system performance.
- Documented server configurations, procedures, and troubleshooting steps, facilitating knowledge sharing and ensuring consistency in system management.
- Stayed updated with latest advancements in Linux technologies and best practices, continuously enhancing skills and knowledge in system engineering.
- Proofread all documentation and reports, ensuring accuracy, clarity, and error-free communication.
- Designed and implemented Amazon Connect Contact flow architecture, enhancing customer experience and streamlining call routing processes.
- Managed Twilio platform, including IVR setup for Twilio numbers, ensuring efficient call handling and effective customer interactions.
- Managed WordPress sites and hosted environment in both GCP and AWS, ensuring smooth operation and optimal performance.
- Managed Google Workspace for users, including domain management, data migration, and distribution email group creation.
- Enforced multi-factor authentication (MFA) for Google accounts, enhancing security and protecting sensitive information.
- Generated weekly reports for Sokolove Services, providing valuable insights and updates on key metrics.
- Configured Twilio IVR systems according to client requirements, improving customer experience and streamlining communication processes.
- Troubleshoot computer hardware and software issues, resolving technical problems and ensuring smooth operations.

Education

2014-03 - 2018-06

Bachelors of Engineering: Electronics And Communication Engineering

Sri Krishna College Of Engineering And Technology - Coimbatore, India