Cloud Security Architect

AWS | Google Cloud Platform (GCP) | Azure

+44 (0) 7863 110553 | cloud@big-technology.co.uk

Email me for fast response!!!!

Executive Summary

A highly experienced **Cloud Security Architect** with experience of Google Cloud Plaform(GCP), AWS and Azure. 5 years security experience with over 10 years architectural experience.

ISO27001, Cloud Security Alliance (CSA), PCI DSS, SABSA and NIST experience in an Agile SecDevOps environment. Multi Cloud expertise in AWS, Google, Azure and OpenShift, alongside IaaS, SaaS, PaaS and Office 365 services.

Container security (Docker, Kubernetes, AWS Fargate, Google Cloud Run. Azure Container Instances, OpenShift Container Platform OCP, AWS ECS, Google GKE, Azure AKS) and Microservices, API security (API Gateway, Google Apigee Edge, Azure API Management).

2 years' security experience working in Agile **Digital** Transformation projects.

Application Security

- OWASP Top 10, Secure SDLC, Application Security Verification Standard, Threat Modelling
- Continuous Integration/Deployment (CI/CD) Nexus, Jenkins, SonarQube, AWS Code Pipeline
- Static Application Security Testing (SAST) - SonarQube
- Dynamic Application Security Testing (DAST) – OWASP ZAP, BurpSuite, Rapid7

Cloud Identity & Access Management (IdAM)

- Role Based Access Control (RBAC) and Host Based Access Control (HBAC)
- AWS, Google GCP, Azure Active Directory, IAM, SSO
- Privileged Access Management (PAM) – CyberArk, BeyondTrust
- IDaaS – OAuth, SAML, OpenID, OKTA, iWelcome, Ping

Cloud Infrastructure & Network Security

- IPS and IDS including NIDS, HIDS, OSSEC and AlienVault
- Threat & Vulnerability Management (TVM)
    - Inspector, Qualys, Retina, Nessus
    - Containers (Twistlock, AquaSec, Layered Insight)
    - Mobile (AppSpider)
- Data Loss Prevention (DLP), Web Application Firewalls (WAF), CDN and Anti-DDoS
- Network Access Control (NAC), VPN and Mobile Device Management (MDM)
- End Point Security (CrowdStrike Falcon), ZScaler, Threat Intelligence & Behavior Analytics
- AWS API Gateway, Google Apigee Edge, Azure API Management

Security Operations

- Security Operations Centre (SOC) - Security Intelligence, Security Analytics, Computer Security Incident Response Team (CSIRT), Threat Monitoring, Threat Triage and Threat Response
- Security Incident Event Management (SIEM)
- AWS CloudTrail/CloudWatch, Google GCP Stackdriver, Azure Monitor
- Office 365 and Azure Identity Secure Score

Data Security & Information Lifecycle Management

- Data at Rest encryption – Databases, block storage and file storage
- Data in Transit encryption – SSL/TLS

Governance, Risk & Compliance

- PCI DSS, UK DPA, ISO 27001:2013 GDPR, HIPAA
- NIST, CSA, SABSA, NCSC Cyber Essentials
- TOGAF, Zachman, MODAF

Cloud Security Architect

AWS | Google Cloud Platform (GCP) | Azure

+44 (0) 7863 110553 | cloud@big-technology.co.uk

Career History

Insurance *Cloud Security Architect*

- Engaged to develop Enterprise Framework for new Cloud (Google Cloud, AWS and Azure) projects including Cloud Capabilities, Security Patterns, Governance, Risk and Compliance.
- Established Enterprise Cloud Capability for security tooling from vulnerability management to identity and access management with strategic and tactical views. Allowing projects to conform to the strategic roadmap with a clear understanding of any tactical usage of tools, with any exceptions requiring a full risk and impact assessment, with CISO signoff.
- Defined minimum SOC capability compliance for Cloud based projects including Security Intelligence, Security Analytics, Incident management, Threat Monitoring, Threat Triage and Threat Response, with exceptions requiring full impact and risk assessment.
- Established compliance framework for AppSec (OWASP Application Security Verification Level 2 and 3) and initiated threat modelling workshops with developers and architects using STRIDE to determine design issues.
- Established mandatory compliance requirements for Secure SDLC (Trunk based Development and Git Flow) including security from code repositories (GitLab, Bitbucket), CI/CD (Jenkins, AWS Code Pipeline) to code coverage analysis (SAST based on SonarQube).
- Expanded Information Security Mandatory Requirements (ISMRs) for Cloud use cases, with additional granularity for avoidance of doubt to reduce probability of projects increasing security risks by deviating from using Enterprise tooling and services and not using Cloud native tools which fail to meet requirements.
- Assessed proposed new Enterprise services from SIEM, Vulnerability Management, Anti-Virus, CASB, Ingress/Egress transit services (WAF, UTM, URL Filtering, SSL Inspection), Logging, Monitoring and Alerting.
- Reviewed DevSecOps function including IaC, InfraOps (Terraform approvals), DAST for websites/APIs using OWASP ZAP and vulnerability management embedded in Pipelines, scanning of docker images (including incorporating multi stage builds to reduce production threat footprint).
- Assessed reference architectures for Big Data platforms including data pipelines for Fraud, MI, Analytics and Data Science models (scoring, rating and pricing) to determine security risks including levels of risk with data (secret and confidential) storage and integration with third parties.
- Increased security of serverless (Lambda and AWS Fargate) by incorporating Twistlock Runtime Application Self Protection (RASP) security.
- Escalated projects to Risk Management team for analysis where projects deviated from strategic pathways, with any exceptions reported to the exceptions team, allowing for full CISO visibility of any risks and exceptions.
- Created security criteria for tactical tooling selection including gap analysis (from strategic), acceptance criteria, impact assessment, support models and third party assurance. Tactical tooling assessments included Rapid 7, AquaSec, Dome9, Redlock, AWS Cognito (instead of OKTA) and AWS SSO (instead of OKTA).
- Review Cyber Resilience capabilities of the Cloud environments to ensure the capability to operate under cyber-attack was not compromised.
- Attended Design Authority, Project Steering, Architectural Steering meetings as well as Solution Design Forums to determine compliance and any joint decisions requiring collaboration from other stakeholders.
- Assessed options for project compliance including how to evidence mandatory security requirements for regulatory and auditing compliance.

Cloud Security Architect

AWS | Google Cloud Platform (GCP) | Azure

+44 (0) 7863 110553 | cloud@big-technology.co.uk

Fintech *Cloud Security Architect*

- Engaged to enhance security for Application development, DevOps, AWS, Office 365, EUC and for insurance (ROAM Insurance), payment (Lyk Mastercard) and Forex (Money) parts of the business.
- Reviewed Insurance processes for security compliance and risk, including processes around data management, access, authorisation, storage and for third party organisations such as Revolut.
- Ran Threat Modelling workshops with development teams to ensure planning activities included security stories for newly established threats, application secure development and any risks where legacy systems were used.
- Recommended changes to the management and usage of SSH keys, CLI user keys, AWS KMS encryption keys, AWS parameter store secrets and AWS Secrets Management to reduce risk of malicious/inappropriate access.
- Reviewed compliance of Containers as a Service (CaaS) AWS Fargate to security requirements including reviewing security tooling such as Qualys and Layered Insight. Looked at alternative measures of using ECS in staging to meet compliance for AWS Fargate.
- Reviewed dependency checking across development pipelines for application vulnerabilities from GitHub, to the AWS Code Pipeline, in the registry (ECR) and on the container platforms.
- Assessed the pipelines for the incorporation static code analysis (SAST) for Elixir, ELM and NodeJS development along with Qualys WAS integration into staging for Dynamic Application Security Testing (DAST) to get an early view on any security issues such as Clickjack threats to header misconfigurations.
- Worked with DevOps team to prioritise security stories for AWS as part of regular Backlog refinement sessions to ensure high priority (high risk) stories were completed quickly.
- Completed PCI Compliance documentation including SAQ-A completion and reviewed compliance to ensure PCI data was not being stored, such as call recording software recording card information.
- Validated Big Data requirements around Tableau integration to S3 data using Amazon Athena as part of Data Lake project along with current temporary options being used.
- Increased progressively the Office 365 Secure Score and Azure Identity Secure Score, to reduce the risk to the business primarily Data Loss.
- Advised on implementation of document classification controls, integration of Office 365 into QRadar SIEM (User Behaviour Analytics for Data Exfiltration protection), rules to stop email forwarding, to restrict anonymous access.
- Created security assessments for EUC management of Apple MacBook's (JAMF and NOMAD Azure Integration), including vulnerability management, application management and data loss prevention measures such as reducing data loss.
- Reviewed applications being developed for data leakage, capacity for Personally Identifiable Information (PII), storage of PII and usage of PII.
- Evaluated application process flows for authentication, authorisation (including KYC) and accounting as part of identity and access management requirements.
- Reviewed regularly process documentation for ROAM insurance to ensure compliance with GDPR Article 30. Assessed effectiveness of restrictions on employees like managers accessing employees data without first going through HR or Security.
- Provided monthly Attestation of Compliance (AoC) reports for all services with the system owner and liaised with Group for services provided by them.
- Established a robust Joiners/Movers/Leavers process whilst the strategic consolidation of identity providers was being planned and implemented. Strategically advised the use of a single identity provider for all services including GitHub, AWS, Jira, Confluence as well as with Office 365.

Cloud Security Architect

AWS | Google Cloud Platform (GCP) | Azure

+44 (0) 7863 110553 | cloud@big-technology.co.uk

Insurance *Security Architect*

- Engaged to define and assess Security Requirements (High Level and Detailed), Security Principles/Controls, Security Policies and potential threats by Threat Modelling exercises.
- Established Top 10 Security Principles to allow for smoother and quicker transition to new 'Cloud First' platforms for new applications to replace existing legacy applications.
- Validated Office 365 privileged access capabilities including Multi-Factor Authentication and Role Based Access Control (RBAC) for administrative access.
- Reviewed access control and identity management capabilities for Office 365 cloud services using Azure Active Directory and AWS Microsoft AD, including single sign-on using Federation Services and App Password (for legacy versions of applications).
- Created Threat Posture assessment security requirements for non-trusted device access using wireless access points managed by a Cisco ISE and Meraki solution. Alongside assessing posturing capabilities of Azure Active Directory (Azure AD) enforcement of conditional access policies based on group membership, location, and device platform.
- Assessed Office 365 Security and Compliance Centre and Microsoft Threat Analytics for alerting, policy scope, reporting, auditing (audit logs activity & sign-ins activity) and advance reporting.
- Defined CI/CD security requirements for application development pipelines including SonarQube and OWASP dependency checking.
- Risk assessed Azure Kubernetes Service (AKS) and Azure Container Registry (ACR) as a comparable Azure based solution for OpenShift, including checking compliance with security requirements around environment segregation, access control (push/pull, service principals) and vulnerability management.
- Ensured Egress security requirements including whitelisting and malware were met with a dynamic filtering and malware signature detection solution.
- Verified Ingress security requirements based on Deny All Default and use of a Trusted Path across from the on-premise data centre to Azure (Express Route) and AWS (Direct Connect), with external Ingress routed through Incapsula Anti-DDoS, with Web Application Firewall (WAF) protection for internet facing applications.
- Defined Linux Host Hardening security requirements based on CIS Templates (implemented using Ansible), OSSEC for HIDS (Rootkits and File Integrity Monitoring), along with ensuring processes were developed for vulnerability management.
- Assessed residual risk for secrets management, using Kubernetes, Hashi Corp Vault, BeyondTrust, AWS Secrets Manager, Azure Key Vault, RedHat IDM Secrets Management and through using image management solutions.
- Evaluated Docker container image vulnerability solutions which provided automatic vulnerability assessment of images coming into the registry, leaving the registry and when run over a period of 24 hours to detect run-time vulnerabilities and malware. RFI Security input to gather further information from vendors. Part of the final selection process.
- Recommended Data encryption options for Data at Rest and Data in Transit. Encryption options included block level encryption (volume and boot), file system encryption, database level encryption (TDE) and Application level encryption. Assessed dependencies against Data Loss Prevention (DLP) and Data Obfuscation projects.
- Defined Privileged Access Management (PAM), Privileged Identity Management (PIM), Break Glass Root account, MFA requirements including assessing BeyondTrust PAM tools, Role Based Access Controls (RBAC) and Host Based Access Controls (HBAC).
- Introduced Threat Modelling workshops for Cloud First applications using STRIDE with developers, Solution/Application architects to determine threats and come up with security controls to mitigate threats found.

Cloud Security Architect

AWS | Google Cloud Platform (GCP) | Azure

+44 (0) 7863 110553 | cloud@big-technology.co.uk

Banking *Cloud Security Delivery*

- Engaged to determine PCI DSS compliance for new Digital Transformation service based on a hybrid OpenShift (on-premise) and AWS (public cloud) environment.
- Reviewed security of AWS, Azure and Google Cloud Continuous Integration (CI) environments including source code management (Git), automated builds (Jenkins), code repository management (Nexus), code scanning (Sonar) and issue management (Jira) including the use of asymmetric authentication and Privileged Access Management using CyberArk.
- Assessed Continuous Deployment (CD) from AWS and Azure non-production to On-Premise OpenShift cloud including processes involved in the pipeline from RFC management, incident management, security monitoring, event management to service introduction.
- Developed best practice enterprise security strategies to manage risks in cloud and DevOps operating environments, ensuring protection against the latest vulnerabilities and emerging cyber threats.
- Documented cloud requirements for information protection including classification, tagging, data loss prevention (DLP) and encryption standards including identifying projects using SHA1 and raising these has high risk for PCI DSS compliance due to TLS1.2 incompatibility.
- Provided oversight to incident response activities (triage, root cause analysis, escalations, notifications, communication, etc.) and developed strategies to contain and eradicate the incident. Assessed cloud security capabilities and gaps during proof of concept engagements including securing cloud technologies against internal and external information and cyber security threats.
- Determined Microservice security requirements for authentication (OAuth2) and authorisation (JWT) using IBM DataPower for external Gateway communications to internal Core Gateway services.

Insurance *Cloud Security Architect*

- Engaged (Agile environment) to assess Azure and AWS cloud providers for IS0270001
- Assessed ISO27001 compliance for new proposed hybrid cloud platform from on-premise to Azure for Digital Transformation and to AWS for development.
- Defined Security Design principles including how on-premise systems and desktops would access Azure PaaS and IaaS instances.
- Developed network architecture to ensure on-premise connectivity via Azure Express Route with F5 ASM/AFM virtual appliance to restrict access to Azure provisioned services and internal resources.
- Determined data risk profile for data at rest, data in transit and data in use to establish conformity with security standards and policies.

Additional CV details

Available on request

Personal Details

Name	Jas Singh
Mobile	+44 (0)7863 110553
Email	cloud@big-technology.co.uk
Nationality	British