**Walter Stoichevski** [**wstoy1@gmail.com**](mailto:wstoy1@gmail.com)

Senior Technical Professional with 15 years hands-on skills with AWS, Azure & GCP experience working with DevSecOps, Data Engineering, Security, IoT. Hands on team leader and contributor with AWS, Azure and GCP environments.

**PROFESSIONAL EXPERIENCE**

**Fortune 500 (Digital Startup) New York**  **05/2017 - Date**

Work with 4 global cloud teams in partnership with Product/Solution owners teams to deliver reliable, security and scalable solutions.

Design and implement DevSecOps, Data Pipeline IoT streaming, mobile & cloud applications in AWS/Azure/GCP environments.

Develop RFI/RFP to support business stakeholder on, sales strategies, project priorities, risk, compliance and governance capabilities.

* Standardize AWS, Azure and GCP Security architectures, accounts, policies, roles, federation, Audit, Risk/Compliance.
* Design data pipelines to extract data from a variety of data sources (Snowflake Cloud, Data Lake, Data Bricks, Data Factory)
* Develop key event streaming, messaging, and DB services such as Cassandra, Kafka, BigTable, DynamoDB, Kinesis.
* Drive DevSecOps for delivering AWS/Azure/GCP solutions through automation, integration, and distribution.
* Create data pipelines by assembling large, complex data sets to meet functional reqs with DataBricks and Snowflake.
* Develop IaC modules for GCP leveraging Google Cloud Foundation Toolkit (CFT), Data protection toolkit(DPT).

**Hands-on Skills:**

* Configure VPC, SCP, CloudTrails, IAM, EC2/EBS/ALB, S3, R53, CloudFront, Subnets, Route Tables and RDS provisioning, NSG, Application Insights, traffic management, workloads, monitoring and logging.
* Implementing AWS Lambda Architecture, Elastic search, API build platforms, AWS datastores in Agile environment.
* Design and deploy containers (ECS, EKS) and SAM, FarGate, Lambda AWS cloud to develop secure cloud capabilities.
* Architect and implement Big Data Infrastructure on AWS using Kafka, Kinesis, Glue, Athena, Redshift, DynamoDB
* Design and build Azure Cloud Services: Snowflake, Data Factory, Data Lake, Databricks, Logic Apps, and Azure Automation.
* Implement Aqua Security, SonarQube, Devo in AWS CI/CD pipeline to secure VM, Containers and Workloads.
* Script IaC with Terraform, Cloud Formation, ARM templates; develop Ansible configuration mgmt. and writing playbooks
* Hands on with GCP BigQuery, Composer, Storage, Functions, BigTable, DataProc, Dataflow and Transfer services.
* Implement pipelines using GCP composer, Kubernetes, Dataproc and storing analytical data in BigQuery.
* Migrate On-Prem data warehouse to GCP cloud native (BigQuery, Composer, Storage and BigQuery Transfer Service)
* Create API integration solutions with internal/external systems from Salesforce, NetSuite and ServiceNOW cloud solutions
* Implement AWS Security: LZ, GuardDuty, Guardrails, DevOps, SecurityHub, IAM (SCP, ABAC/RBAC)
* Configure and implement Security Center for custom policies for: Azure CIS, NIST SP 800-53 and FedRAMP.
* Design & implement (Azure AD IdP), Authorization (AD OAuth 2.0 and Token endpoints for access and ID tokens.
* Develop process and automation across IAM/PIM, CI/CD, Incident Response, Malware, DLP, and Threat Modeling.
* Implement GCP security (VPC Service Control, Cloud KMS, Cloud Armor, GCP Network, Identity Aware Proxy (IAP).
* Lead large-scale migrations to GCP (Cloud LB, DNS, Compute, Networking, Storage, DR, Security, Monitoring)
* Implement Azure Group Membership, Custom attribute, Azure B2C Policy, MFA, SSO and AAD with Azure ADFS.
* Information Protection (AIP) Azure Key Vault, Azure Security Center. Configure F5 WAF and Load Balancers.
* **Security Tools**: Aqua Security, CloudGuard (Dome9), Devo, Netskope, Orca, Qualys, PRISMA, Sentinel One.

**AWS and GCP Skills:**

* Implement Azure Security Center Tools and AIP - including (AAD, ADFS, VM, WAF, VNET, NSG, VPN, LB)
* Implement AWS Landing Zone, VPC, SecurityHub, Guard Duty AWS Shield, AWS Inspector, and configure IAM role, group, permission attributes with business rules and policies with custom rules and policies.
* Configure GCP Cloud IAM for internal/external entities and secure multi-tenancy by defining a tenant-per-namespace model to ensure that Pods and Services in a given namespace cannot access other Pods or Services in a different namespace.
* Automate tasks using ARM templates, Cloud Formation Terraform and workflows with Jenkins and GitHub.
* Implement GCP Binary Authorization for GKE) to be signed by trusted parties in the development phase and enforce signatures.
* Implement GCP security configurations into CI/CD pipelines with Cloud Armor, Shielded VMs, and Binary Authorization.
* Design Network security controls; WAF (F5), malware detection, IDS / IPS and DLP, CASB, Cloud Proxy, DLP, XDR (Sentinel One)MFA, management tools. Setup F5, Fortinet and NetScaler cloud security services.

**Azure Skills:**

**AKS:** Azure Container Registry (ACR), AKS, configure endpoints (properties) in VSTS, Repos, Test Plans, Pipelines to access Azure and AKS, Modify DB with connection string & ACR config the source code. Configure AD for cluster and workload security.

**IoT:** Sensors, Controllers, Trackers, SoC, Agents, Azure IoT DPS, Azure Hub, Azure IoT DA v2, IoT Registration

**Compute**: AKS, App Service, Azure Functions, Batch and Service Fabric.

**DevOps Tools:** Azure Pipelines, Azure Boards, Azure Artifacts, Azure Repos, Azure Monitor

**Security:** Azure AD, Azure DNS, Azure HSM, MS-CAS, Security Center/Security Playbooks, Azure Key Vault

**Database:** Azure DMS, Azure Cosmos DB, Azure SQL, Azure cache for Redis

**App Integration:** Logic Apps, Stream Analytics, Service Bus, API Management, Event Grid.

**Networking:** Express Route, Traffic manager, Azure FW, Network Watcher, Azure Front Door.

**Director – Amazon AWS – (Frankfurt, Germany and London, U.K) 01/2014 – 05/2017**

Work with CTO/CISO to establish the design, implementation and integration of AWS Cloud Security Infrastructure.

Responsible for establishing the long-term plan to build highly scalable projects in a cross-matrix environment.

Work with the executive committee to help define the roadmap, budget & project plan. Steered Audit Committee for clients.

• Establish and sustain AWS standards, process improvements, governance processes and performance metrics to ensure that people, processes and technology mitigate persistent threats and meet reliability standards to protect the client’s information assets in AWS.  
  
•Identify Information Security needs and risks, and establish operational plans that align with client’s vision, mission and objectives, and support long-term Information Security growth and sustainability.  
  
•Direct the assessment of business and technology risks to ensure such risks are appropriately identified and evaluated. Oversee the development and implementation of appropriate measures to identify risks associated with applications/business functions.

**Technical Product Manager – Amazon AWS - (Seattle, WA, Dublin, Ireland and Singapore) 10/06 - 01/2014**

Support the delivery of AWS products related to cloud security, including security governance (security policies and procedures), security strategy (security planning), risk (risk assessments and management), cloud data protection (classification, encryption, and KMS), cloud-based IdM, and technology/provider-specific cloud architecture.

* Develop architectural leadership on Client’s engineered platforms, tech stacks and infrastructure that power our AWS, vendor and customer facing products and services
* Provide architecture assurance on Cloud security initiatives and compliance of existing security standards interfacing with infrastructure and development teams.
* Develop key event streaming, messaging and DB services such as Cassandra, Kafka, BigTable, DynamoDB, Kinesis.
* Design and manage architecture roadmap at multiple levels (high-level to detailed) and across multiple views (conceptual, logical, physical, data flow and sequence diagrams) providing active “hands-on” guidance.
* Implement PCI, GDRP, HIPAA compliance with policy as code and enforcing policy as code via DevOps pipelines.
* Connect AWS architecture to business needs of the client by working closely with stakeholders and partners.
* Build and maintain the current-state and future-state systems architecture views for the enterprise.
* Develop artifacts for; network/infrastructure diagrams, reference implementations, best practices, and roadmaps.
* Participate in the architecture council to provide governance and build processes to guide critical architectures.
* Develop, document, and present proposals, RFP/RFI, including selection, evaluation, analysis of options.
* Lead selected efforts to craft, build, and develop rapid Proof-of-Concept (POC) solutions and services.
* Provide design and best practices and mentorship for the rollout, and implementation during the 'pre-sales' process for strategic opportunities, including 'proof of concept', Prepare RFP, RFI and proposals for US/Europe/Asia customer base.
* Design EC2 services with ELB (On-Demand, Reserved Instances, Spot Instances) utilizing Lambda and ECS.
* Implement the S3 & Glacier service for storage and archiving/backup in excess of 3 PB on Amazon Redshift.
* Migrated data from MS-SQL into Snowflake and RDS Postgres for ingestion, processing, transforming, and loading.
* Design DB structure and schema, data modeling and forecasting for increased processing of large files (20TB+).
* Implement CloudFront for content delivery web services to distribute low-latency applications in 14 countries.
* Design highly scalable multiple DBs on Aurora, Oracle, MS-SQL, MariaDB, and DynamoDB with Redshift.
* Design VPC on Route 53 (DNS Service) for custom Web-enabled Applications spanning 50 custom apps.
* Implement AWS TrustedAdvisor to provision resources and improve performance, reliability and security.
* Implement AWS Machine Learning tools to detect fraudulent and suspicious financial transactions across multiple applications. This work was in conjunction with IAM utilizing fine-grained attributes and custom code.
* Design and implement Docker containers for use across hybrid cloud (on prem and AWS) using Jenkins.
* Develop and architect applications using Spring Security, Microservices Architecture, Spring MVC, Java Code Refactoring, SOA Architecture and Web Services (SOAP), and Spring Security.

**AWS Skills:**

**Compute:** EC2, Lambda Services, LightSail, ECS, ELB, FarGate,

**DevOps:** CodePipeline, AWS SAM, Cloud9, CodeCommit, X-ray, (Ansible Tower, Jenkins)

**Security:** IAM, Inspector, Security Hub, Cert Manager, AWS-SSO, GuardDuty, CloudHSM, AWS Cloud Compliance

**Management:** CloudTrail, CloudFormation, CloudWatch, Trusted Advisor, Service Catalog, Organizations, Auto Scaling

**Database:** Dynamo, RDS, RedShift, Maria, MongoDB, AWS ElasticCache, AWS DB Migration Service

**App Integration:** AppSync, SQS, SNS, Step Functions, Amazon MQ

**Networking:** Direct Connect, VPC, Route 53, API Gateway, ELB, CloudFront

**Security Manager – Northrop Grumman 12/93 – 10/06**

Developed the Identity/Access Management (IAM) practice and promoted methodologies and engineering standards.

**Technical Skills:**

* Manage encryption policy configuration, key and certificate life-cycle management, configuration (OCSP, CRLs).
* Implement PKI, SSL, HSM, Smart cards, Symmetric/Asymmetric (Public/Private-PKI), subordinate CAs, and MFA.
* Identify and map AD users/groups into IAM and Policy Server to ensure application integration. Create functional workflow design based on user/group profiles identified in LDAP schema. Customized templates for SSO.
* Create functional workflow design based on user/group profiles identified in LDAP schema.
* Designed and implemented military grade RBAC/LDAP infrastructure spanning 8 countries with 1M+ users by consolidating civilian, consular, diplomat, and military officer’s credentials with Top Secret/Secret data.
* Implemented Data Access with DSML over HTTP, Filtering, Indexing and Searching, and Replication.
* Designed the Gateway, Control & Data Layer components for SUN servers in a multi-master tier.
* Implement Access Controls, Access with DSML over HTTP, Filtering, Indexing/Searching, Replication.
* Setup indexes at the OU level, setup change control monitoring, & setup authentication to LDAP.

**Protocols:** DNS-Sec, DSML, HTTPS,HSRP, IPsec, L2F, L2TP, LDAP, MPLS, SAML, SSH, SPML, SSL, TLS

**Networking:** ATM, Ethernet, ISDN, SONET, Gigabit, Wireless, Cable, Optical, Satellite, DWDM.

* Cisco Catalyst Switches 6xxx, 5xxx, 4xxx, 29xx, 19xx: Routers 7200, 4000, 3600, 3000(VPN), 2600.
* Configuration of Switching (Layers: 2, 3, 4);OSPF, BGP4, MPLS, CIDR, VRRP, HSRP, IGMPv2, DNS.

**Cryptography**: AES-256/1024, Blowfish, CAST, ECC, IDEA, Lucifer, MARS, RSA, RC5, Serpent.

**Blockchain Projects:**

* Write Policies and procedures for Mobile and Cloud Encryption from PoC to PoS/PoE.
* Develop blockchain product specs and policy for Mobile and Cloud Platforms (AWS, Azure and GCP)
* Design and build the back-end blockchain functionality for our online/mobile applications using AES-CCM.
* Leverage experience with Hyperledger Fabric platform for Proof of Stake, Proof of Existence.
* Design and implement Ethereum (Solidity), Hyperledger Fabric (Java), and Corda(Kotlin) ledgers for global apps.
* Document best practices and act as a knowledgeable resource for blockchain engineering and problem-solving.
* Implement Permission Blockchain applications to verify authenticity of parts used in financial contracts.
* Leveraging Hyperledger fabric to develop and test mobile platforms for IoT embedded sensors in soldiers’ uniform
* Isolate the ledger from the general cloud environment, building a security container for the ledger to prevent unauthorized  access, and provide tamper-responsive hardware, which shut itself down if it detects a threat.
* Develop framework of linked data records (an immutable ledge )that preserves vital information in a distributed, highly available form based on trust and transparency using SecureKey for RP and CSP.

**EDUCATION (Certifications)**

* Certified: F5 Solutions Architect 04/2020 – 04/2020
* Certified: Blockchain Expert 01/2020 - 01/2020
* Certified: OPSWAT Critical Infrastructure Security 11/2019 - 01/2020
* Certified: CyberArk v11 (Trustee and Guardian) 05/2019 – 05/2019
* Certified: AWS Solutions Architect, ML, Networking and Security 07/2018 - 08/2018
* Certified Application and Data Security/Privacy (GDRP) 07/2018 - 09/2018
* Certified: Azure Solutions Architect and Azure Networking and Security 03/2018 - 03/2018
* Coursework: Cloud Security Implementation (IDM, KMS, HSM) 01/2015 - 01/2016
* Coursework: Cloud Design and Implementation (IaaS, PaaS, SaaS) 07/2010 - 12/2012
* Coursework: Cyber Threat and Intelligence Warfare 05/2005 - 09/2006
* Coursework: Identity Management and Access Controls 01/2005 - 03/2005