  

**Siamak (Sam) Karbassi**

|  |
| --- |
| SUMMARY |

* More than 18 years of experience; leading and managing security projects and teams of up to 12, including testing, risk and vulnerability assessments, a range of components and settings, design, architecture, implementation, and management of security activities. putting in place and maintaining industry and compliance requirements including PCI-DSS, BCDR, and BIA. evaluating and selecting security measures for cloud computing systems. competent to report, make RFPs, business cases, and provide presentations to boards. Additionally capable of managing hands-on implementation and resolving security incidents, including different firewall engines, packet and path analysis with packet analyzers, and SIEM/logging engines for network devices
* Experience and hands on with DFW, VPNs, IDS/IPS, IAM, PAM, ITSEC, SKIP, IPCOMP, ISAKMP, PKI, AAA Servers: RADIUS, TACACS+, ISE, RSA, SIEM/SOAR, EDR, SDLC, IAM, OAuth, SAML, LDAP, Active Directory, Prisma Cloud Container Security, Palo Alto Firewalls and Panorama, Cisco ASA, FTD and FMC, FortiGate and FortiManager, zScaler, Prisma Access
* Cloud design and implementation including private cloud (VMware Cloud Director, OpenStack, OpenShift), public cloud (GCP, AWS, Azure), hybrid cloud and multi-cloud
* Strong understanding of the network components and routing.
* Handling day to day operations including security architecture reviews, incident handling, design and implementation.
* Practical knowledge about different frameworks and compliance including NIST CSF and 800, ISO27001, PCI-DSS, SWIFT, TOGAF, SABSA
* Ability to work independently, lead teams and pursue initiatives and also bring new ideas to the business
* Service and incident tickets handling, escalations and closure
* Ability to analyze packets and find out the security gaps
* Design and delivery of the large projects, including SSL decrypt and service chain
* Experience with datacenter design and security concerns
* Proficient in design and development of SaaS software integration security
* Design of public facing services and communication to the back-end including load balancing, API gateway, WAF and DDoS, front end/public network zoning, tagging traffic and communication to back-end zone, end-to-end encryption
* Design and delivery of IAM including Active Directory LDAP, SSO and federated identity, with SAML and OAuth with various engines, and MFA
* Privilege access management including integration with various IAM engines, and MFA
* Practical knowledge about Active Directory GPO, and public cloud permissions and roles, and structure design of the organization
* Generative AI and LLM security including prompt injections, misinformation production, external tools, data poisoning

|  |
| --- |
| Core Competencies |

* ***Security design and architecture***: Zero trust, CASB, SASE, micro and nano segmentation, trust boundaries and network zones, PAM, IAM, API gateway, PKI, VPN, Cloud networks and components, defense in depth
* ***Security reviews***: Security architecture reviews of various applications including SaaS, PaaS, and IaaS, with on-prem, public cloud tenancy and multi-cloud, compliance, access methods and IAM, data in transit, data at rest, data classification and privacy, privilege access and RBAC, network protection including WAF and DDoS

*Datacenter switches****:*** Nexus 7k, Cisco ACI

* ***Incident management:*** Full incident management lifecycle handling, both technical and non-technical issues including SIEM/SOAR analysis, risk analysis and ranking,
* ***Tools*:** JIRA, Service Now, Active Directory, OKTA, ForgeRock, Google Cloud Identity, IBM verify, DUO MFA

CrowdStrike, NSX-T, Palo Alto, FortiGate, FTD, zScaler and BeyondCorp

* ***Automation*:** PowerShell scripts, Python and Terraform, CI/CD platforms (GitLab, GitHub, Jenkins), REST API, Ansible, JSON
* ***Methodolgies:*** Agile, waterfall, DevSecOps, SSDLC
* ***Frameworks:*** NIST CSF and 800, TOGAF, ISO, SABSA

|  |
| --- |
| Experience |

## Cybersecurity Architect

## *Bell, [Sep 2022 – Present]*

* Delivered 350 inventory security assessments in accordance with the NIST CSF framework
* Defined security controls for 5G and CDN networks
* Designed and delivered Kubernetes security assessments with Prisma Cloud
* Provided security requirements for more various SaaS, PaaS and IaaS platforms
* Lead and delivered IAM SSO platform migration and modernization patterns with GCP and AD
* Designed and build cyber incident response plan (technical and non-technical)

## Cybersecurity Architect

## *TD Bank [Sep 2021 – Sep 2022]*

* Advised security policies along with risk assessment for virtual infrastructure migration of about 4500 VMs by analyzing 300 existing Panorama, Prisma, and NSX policies and Device42 raw data transferring them to Azure and IBM cloud platforms with a 90% success rate
* Delivered SIEM/SOAR log correlation and anomaly detection analysis for the entire network
* Analyzed network anomalies through packet capture tools

## Cybersecurity Architect

## *IBM [Mar 2020 – Sep 2021]*

* Delivered security policy and firewall rules accreditation for performance improvements
* Reviewed and recommended security policies for various applications, systems on-prem and on-cloud including IAM, TLS, Pentest, and compliance
* Developed over 30 security architecture design patterns for cross-domain IAM, cloud API, cloud to -on-prem access
* Delivered gap analysis for current security patterns and updated strategy
* Delivered PoC for various platforms Zero-trust Architecture, micro-segmentation
* Conducted risk assessment for public cloud migration decision support system
* Azure and IBM cloud network security components and design (NSG, ASG, WAF)

## Sr. Security Architect

## *SOCAN [Jun 2019 – Mar 2020]*

* Provided security architectural recommendations for security controls around cloud applications using CASB
* Designed and delivered IAM federated identity deploying SAML for various components
* Redesigned SSLV to take two paths in an Active/Active manner to double the capacity
* Designed vRLI/vRNI SIEM (Collectors, Managers) for advanced traffic analysis
* Completely architected SSL Visibility solution and components including Packet Broker, IPS, IDS, DLP, Malware Protection
* Developed RFP and vendor selection criteria for ZTA platform
* Designed universal policy roll-out for FortiGate UTMs and Palo Alto firewalls
* Developed complete disaster recovery and business continuity plan (BCDR)
* Participated and helped data governance policy development for target maturity level Delivered PKI design, for both internal and public use (CA, RSA)
* Participated and helped data governance policy development for target maturity level Delivered PKI design, for both internal and public use (CA, RSA)

## Sr. Security Architect

## *RBC Bank [Dec 2018 – Jun 2019]*

* Successfully led migration for SSL Visibility project for 15 locations
* Redesigned SSLV to take two paths in an Active/Active manner to double the capacity Completely
* Completely managed and implemented SSL Visibility service chain including Packet Broker, IPS, IDS, MPS and DLP (Symantec, Cisco FP, Niagara PB, FireEye, Bluecoat)
* Delivered rule design, policy staging, hardware refreshes, upgrades, of more than 500 firewalls in heterogeneous environment including Palo Altos, FTDs and FortiGates
* Supervised and rule design for over 300 Check Point firewall domain appliances (R70)
* Standardized routing and policy scheme for firewalls including IDS/IPS, Web URL Filtering

## Sr. Network Security Engineer

## *Mialno Innova Systems (MIS) [Dec 2011 – Dec 2018]*

* Developed Disaster Recovery and Business Impact Analysis for backbone data centers
* Completely managed the payment applications throughout the SDLC lifecycle including SAST, DAST, code reviews, regression testing, unit testing
* Designed and implemented worldwide security policy on Palo Alto firewall clusters
* achieved PCI with guidance and external pen-test results for a payment processor having 500K merchants and 400 TPS
* Integrated Open ID Connect and OAuth federated identity for public applications
* Engineered a massive transaction environment for multi-path Palo Alto firewall and inspection clustering with F5 SSL visibility including RSA design and delivery
* Managed and engineered the project, to deliver a plan for the implementation of VPN mesh among bank branches and ATMs with Juniper and Palo Alto firewalls for 300 locations with detailed change procedures and configurations for devices
* Prepared migration plan from heterogeneous security border firewalls to Cisco ASA-FTD series firewalls
* Fully migrated from Cisco ACS to Cisco ISE with Active Directory integration
* Designed, managed and delivered optimized resources on multiple locations SSL VPN for infrastructure to serve 25,000 desktops over 1,200 locations
* Troubleshoot and fully optimized resources and applied policies with multiple desktops templates to minimize resource allocation duration for a changing environment
* Built and designed 3 levels (HQ, Main, Branch and Kiosk) of baselines security configuration policy for Palo Alto firewalls
* Developed rule base and thread management optimization plan for Palo Alto/Juniper firewalls for over 2 years
* Designed proxy solution for SSL visibility and offloading with bluecoat for both forward and reverse along with WAF capability
* Monitored and supervised Check Point and Palo Alto firewalls and in SOC for more than 3 years in 2 European banks with over 3,000 branches worldwide
* Implemented a wide variety of monitoring SOC tools for more than 5 years using Cisco Prime, Panorama, Juniper NMS, Smart-1, SolarWinds and Manage Engine along with Zenoss and Nagios both in the banking industry and payment providers
* Supervised the implementation of Kaspersky anti-malware for 10,000 devices with centralized Windows patch management and policy distribution for recurring updates, scans, possible threads report etc.
* Managed and script-automated the QRadar and Splunk for minimum false positives and high protection policy match and appropriate actions
* Built multi-layer and multi-context Check Point and Juniper in transparent mode for 3-layer protection at the core along with the Cisco ASA module on the core switch chassis
* Fully generated PCI-DSS compliance for switching and routing environment, including port security, management VLAN and SSH, STP guard, dot1x, Authentication, SNMPv3, Routing protocols authentication
* Implemented Blue Coat devices as a complementary device to Cisco ASA at branches to apply URL/cat Filtering w/wo SSL
* Prepared WAN design and migration from IGRP to OSPF for 12000 nodes using Cisco 7600 at core and 39xx, 29xx, 19xx at branches
* Fully prepared the WBS and over tasks for managing the DC project to meet the milestones and successful completion along with optimized resource allocation
* Fully configured as per instructions networks, including DNS Servers, Clients, DHCP, Active Directory, Cluster
* Implemented vSphere 5.5 to 6.5 infrastructure (ESX, vCenter, vConverter, etc.) with 40 hosts in each data center and disaster recovery site for low-latency storage synchronization
* Backed up virtual infrastructure for bank datacenter using VEEAM and setup, install and configured SRM and replica of VMs on the other hosts
* Security rule base design, conflict resolution and optimization for almost 1200 firewalls in a mixed environment including Juniper, Check Point, ASA, FortiGate
* Provided high-profile consultancy and RFP developer for bank with 2500 branches
* Managed a VoIP design plan for 5 banks in size made up of over 4000 locations and 70 call processing sites

***IT Infrastructure Manager***

***Canadian Advanced Information Technology (CAIT) [Dec 2005 – Dec 2011]***

* Consultant, Supervisor for more than 10 countrywide governmental and banks of variant sites ranging from 2,000 to 10,000 (VoIP, MPLS, Infrastructure, DC, etc.)
* Managed the Architectural, Mechanical and Network Components of TIA-942 tier-3 for the second-largest Bank in the Middle East Region
* Designed and deployed VDI for over 5000 client environments
* Designed a comprehensive self-defense network and application environment for an organization with 3000 locations countrywide
* Designed and implemented Core and WAN block for the second largest bank in the private sector having over 1000 Branches
* Successfully managed a 40$ billion high-critical IT project including DC, network infrastructure
* Successfully integrated the Enterprise Management Infrastructure for a 700 Branch Bank with 99.999% availability and DRP

***Cisco Instructor***

***Ryerson University [May 2001 – Oct 2014]***

* Taught over 500 trainees networking and Internet Security courses
* Outstanding Trainer for Cisco CCNA, CCNP, CCSP
* Prepared the class and lab material for network security courses
* Official Security Trainer for Check Point CCSA, CCSE, CCSE+ and CISSP

|  |
| --- |
| Education |

**Iran University of Science and Technology**

*Bachelor of Science in Industrial Engineering Systems Analysis and Planning, 1992*

*GPA: 3.0/4.0*

*Also Certified CCNA, CCNP, CCIE, CCSA, CCSE, MCSA, MCT*