

PRASHANT KUMAR

CISSP, CISM, CISA, Azure Security

Network/Cloud Security Architect & Consultant, Team Lead

IT & Cloud Security



+974 70926573

prashant.advit@gmail.com

KEY SKILLS

Team management, Mentoring, Performance reviews, Cloud Security, NGFW Palo Alto, PAM, AlgoSec, Azure Security, SSL Certificate Management, F5, Fortinet, Cisco Firepower, Infoblox, FireEye, Cisco ISE, DevSecOps practices, Regulatory adherence, Security audits, Risk management, Cross-team coordination, Stakeholder engagement, Training, process optimization, Adoption of new technologies

EXPERIENCE

Qatar Islamic Bank Qatar – Feb 2017-Present

Senior Security Specialist (IT & Cloud Security Team Lead)

Main Responsibilities:

Lead, mentor, and manage a team of network security engineers or analysts, providing guidance, training, and support to ensure high performance and professional growth

Design, implement, and maintain secure network and cloud architectures, ensuring alignment with business goals and regulatory requirements

Lead cloud security operations for SaaS, IaaS, and PaaS environments, including AWS, Azure, and/or GCP

Provides extensive, in-depth, technical consultation to the clients, partners, and IT Management to develop plans and directions to ensure the integration of corporate business area requirements.

Hands on Experience on Network Security Appliances which includes configuration, management and troubleshooting devices like Palo Alto, Fortinet, Cisco FTD, F5 Web Application Firewall LTM/ASM/GTM, Forcepoint, FireEye NX/EX, Cisco Email Security Appliance, AlgoSec Firewall Analyzer & Fireflow, Beyondtrust Privilege access Management (PAM), and Infoblox DNS Security.

Act as a SME in driving operational and security improvements to the overall Secrets Management program and Beyondtrust Password Safe PAM service.

Strong understanding of PAM solutions and tools CyberArk, BeyondTrust, & Thycotic.

Demonstrate a firm understanding of the concepts of password vaulting, privileged session management, secrets management, and DevSecOps.

Experience with creating credential vaults, defining access control policies/platforms, user provisioning and entitlements, managing applications credentials, key management, and user access policy management.

Experience in setting up segmented privileged access management environments for specific use cases.

Ensure cloud infrastructures comply with legal and industry standards (QCB, GDPR, HIPAA, PCI DSS, ISO 27001) by conducting regular audits and assessments

Evaluates and selects from existing and emerging technologies those options best fitting business/project needs

Experienced, functional expert with technical and/or business knowledge and functional expertise

Displays a balanced, cross-functional perspective, liaising with the business to help improve efficiency, effectiveness, and productivity

Evaluate existing network and security infrastructure, identify vulnerabilities, and recommend enhancements to align with Zero Trust principles.

Expertise in Azure Active Directory (Entra ID), ADFS, Azure AD Connect, and Azure B2C/B2B.

Strong knowledge of Windows Server (2016/2019/2022), DNS, DHCP, and LDAP.

Experience with identity federation protocols (SAML, OAuth, OpenID Connect, Kerberos, NTLM)

INFORMATION AND COMMUNICATION TECHNOLOGY Qatar – JUN 2015-FEB 2017

TECHNICAL SUPPORT ENGINEER

Main Responsibilities:

Diagnose and resolve network connectivity issues, including LAN/WAN, VPN, and firewall-related problems.

Provide advanced troubleshooting for network and firewall incidents, escalating complex issues when necessary.

Partner with stakeholders to evaluate security solutions

- Implementation of security controls and processes
- Low Level Designs
- Firewall configuration and policy management
- Testing
- Documentation and training for transfer of support to Operational Teams
- Deployment of security controls for endpoint and network

Technical Support

- Maintain and improve existing network security
- Network and host Firewall architecture and security policy
- Hardware and software lifecycle
- Security compliance scan result remediation
- Audit policy for security and performance optimization, using automation tools and manual processes, based on logging and other data sources
- IDS/IPS, Anti-virus, Malware detection
- VPN
- Complex maintenances
- Escalation support

Managing firewall technologies, including Cisco, Palo Alto Networks, and Juniper skilled in designing and implementing firewall rules, access controls, and security zones to protect network infrastructure and data. Monitor network traffic for unusual activity and potential security breaches.

Execute operational tasks for network security solutions, including network firewalls, intrusion prevention systems (IPS), proxies and web application firewalls (WAF).

Install, configure, maintain, and upgrade network firewall hardware and software for all environments, including production and test.

Implement, review, and update firewall rules and policies to ensure secure network access and segmentation

Monitor firewall and other network security devices (IDS/IPS, proxies, etc.) for threats, anomalies, and compliance with security standards Conduct vulnerability assessments, penetration tests, and security audits of firewall configurations and network infrastructure

PENTA CONSULTING APRIL 2014-MAY 2015, QATAR

SECURITY ENGINEER

Client: IT Services, Banking & Finance

Main Responsibilities:

Design, deploy, and manage Fortinet solutions (FortiGate, FortiManager, FortiAnalyzer, FortiWeb, FortiAuthenticator) across enterprise and hybrid on-prem / datacenter environments.

Act as a subject matter expert (SME) for Fortinet infrastructure, firewall policy design, VPN configuration (IPSec/SSL), and UTM services.

Manage and maintain the organization's network infrastructure, including routers, switches, wireless access points, Firewalls, and related network equipment. This includes on-site support to manage switch/WiFi Access Points as needed.

Monitor network performance and availability to ensure optimal uptime, identifying and resolving

bottlenecks or performance issues.

Configure and manage VLANs, QoS, load balancing, IPSEC, Remote SSL-VPN, and other network technologies to optimize traffic flow and security.

Perform regular network maintenance, including firmware updates, patches, and configuration backups.

NK NETWORK CHAMPS PVT. LTD.

NETWORK ADMINISTRATOR LEVEL 2 JULY 2011-MARCH 2014, INDIA

Client: HP India, VFS Global, OnMobile Global, GE Healthcare

Main Responsibilities:

Firewall Management: Configure, maintain, and troubleshoot Fortinet, and ASA firewalls to secure the organization's network

Policy Development: Design and implement firewall rules, access control policies, and NAT configurations to ensure compliance with security standards and business requirements

Monitoring & Optimization: Conduct regular performance monitoring, rule base reviews, and policy cleanups to enhance efficiency and eliminate redundancies

Threat Mitigation: Analyze and respond to security incidents, ensuring swift remediation of vulnerabilities and threats

Network Architecture: Collaborate with network architects to design scalable, secure, and highly available network solutions

Compliance & Audits: Ensure firewall configurations align with organizational security frameworks and industry standards includes PCI DSS, ISO 27001

Design, configure, and implement Fortinet-based security solutions, including FortiGate firewalls, FortiAnalyzer, and FortiManager, tailored to organizational or client requirements

Provide technical support and troubleshooting expertise for Fortinet solutions, both remotely and on-site as required

CERTIFICATIONS



**Certified Information
Security Manager
(CISM)**
ISACA



**Certified Information
Systems Security
Professional (CISSP)**
(ISC)²



Azure Security Professional
Microsoft



**Certified Information
Security Auditor (CISA)**
ISACA

TECHNOLOGY USED

Palo Alto NGFW | FortiGate | Microsoft Azure | Infoblox | F5 ASM AWAFF | CrowdStrike | FireEye | Fortiweb | One Identity Safeguard | Cisco Firepower | Cisco Umbrella | F5 LTM | Cisco ESA | Fortinet ADC | Cisco ISE | Akamai Prolexic | Tenable Nessus | Forcepoint Web | Arbor DDoS | McAfee DLP | BeyondTrust Privileged Access Management PAM | Forcepoint Email Security | LogRhythm | Cisco AnyConnect | Azure Key Vault

EDUCATION

Master of Computer Applications (M.C.A.) Computer Application Sep 2008 - Sep 2010- PTU

Bachelor of Computer Applications (B.C.A.) - Computer Application Sep 2004 - Sep 2007, IGNOU, Delhi

Personal Information

Address: Doha, Qatar, Nationality: Indian, DOB: 23-Dec-1986