Prashant Kumar

974 70926573
prashant.advit@gmail.com

Executive Profile

Cybersecurity professional with 12 years of experience in developing and implementing complex Cyber security programs. Expertise in solving complex technical challenges, driving effective systems planning, engineering, and operations. Analytical problem-solver who delivers cutting-edge security solutions that protect enterprise communications, systems, and assets from both external and internal threats.

Key Responsibilities

- Designs the enterprise security infrastructure and architectural topology including recommending hardware, operating system, software, and information security requirements to ensure the confidentiality, integrity, availability, and privacy of information systems. Ensure consistency and sufficient integration with existing infrastructure.
- Designs more complex application security architecture. Coordinates technical design/review activities with various groups including application development, enterprise architecture, information security, systems, network, and database groups to develop secure frameworks and enterprise applications.
- Design, Detect Internet Banking, Swift, NETS, ATM, HSM and Payment Gateways from a network and security perspective.
- Stayed up to date with the latest threats (exa-MITRE ATT&CK) methods and developed protection plans to prevent cybersecurity incidents.
- Managed internal and external stakeholders, including IT teams, business units, and vendors, to ensure alignment and coordination of cybersecurity efforts.
- Detected insecure features and malicious activities within networks and infrastructure using security monitoring tools.
- Conducted security awareness campaigns to educate employees on cybersecurity best practices.
- Developed and maintained close working and technical relationships with internal and external technology stakeholders, including government agencies and industry associations. Researches, recommends and implements changes to procedures and systems to enhance security.
- Creates incident response plans, including coordination with appropriate departments, other business units, and appropriate authorities.
- Responsible for the design and evaluation of a broad range of Network security technologies in Op-Prem and Cloud, processes and best practices. Solid understanding of various security tools such as NGIPS, WAF, Load balancers, Proxy, APT, DNS Security, DDOS Solutions, SSL VA, Tapping Solutions, DLP, EDR, PAM.
- Hands on experience in various Network Security products such as Next Generation Firewalls, IPS/IDS, Anti-APT, Web Proxy, End Point Security Solutions, Secure Access Control Servers, Web Application Firewalls, Cloud Security, DNS Security etc.
- Forward-focused Security Consultant and act as a subject matter expert in the cybersecurity areas of Data Loss Prevention, Data Classification and Rights Management, Data Discovery, Data Access Governance, Data Retention and Destruction, Web Security, Cloud Data Protection through CASB, Next Generation Antivirus and Endpoint Detection and Remediation (EDR), Key and SSL/TLS Certificate Lifecycle Management, Data Encryption, Public Key Infrastructure, etc. and other data protection related technologies.
- Knowledge of internal and external IT security standards, SOX, PCI-DSS, SOC2/1, ISO27001 standards and relevant legal compliance aspects.

Soft Skills

Customer Focused
Proactive Attitude
Problem Solving
Excellent Communication - Verbal & Written
Team player
Take initiative

Technical Experience

Firewalls Products- Palo Alto, Fortinet, Cisco ASA, Forcepoint
End Point Security- McAfee AV, DLP, Crowdstrike
APT- FireEye
IDS/IPS –Sourcefire, Tipping Point
Cloud Platforms: AWS, Microsoft Azure, Google GCP.
DevOps- Jenkins, Ansible, GIT
Content Delivery Systems - f5 LTM, GTM
Content Filtering-Websense, IronPort WSA, Bluecoat
Email gateway – Cisco ESA, Websense
Multifactor Authentication – RSA, Vasco
Web Application Firewall – F5 ASM, FortiWeb
IPSEC/SSL VPN: FortiGate, ASA, Pulse Secure, Global Protect
Privilege Access Management- One Identity, Thycotic now Delinea, CyberArk
SSL Decryption- f5 SSL Orchestrator
DNS Security- Infoblox
Vulnerability Scanning/Management- Nessus

Academic Details

Masters in computer application (MCA) from Punjab Technical University in 2010

Bachelors in computer application (BCA) from Indira Gandhi National Open University in 2008

Certifications

CISSP ISC2-578207
Certified Ethical Hacker (CEH)
ISC2 CC
Palo Alto ACE
Certified Information Systems Auditor (CISA)
Certified Information Security Manager (CISM)
Project Management Professional (PMP)
Microsoft Certified: Azure Security Engineer Associate (AZ-500)

Projects

(Role: Lead Consultant)

- Apple Pay
- Himyan Card
- Bank Core Banking temenos products
- Swift Payment Gateway
- Next Generation Firewall Migration from Cisco ASA to Palo Alto NGFW
- Infoblox DNS Migration
- Privilege Access Management Implementation
- Forcepoint Email Security Implementation
- Crowdstrike EDR deployment
- FireEye NX and EX APT Implementation
- F5 WAF migration from Fortiweb
- F5 LTM migration from Fortinet ADC
- F5 GTM implementation
- Cisco ESA tech refresh
- Microsoft Office 365 Migration from on prem Exchange
- Cloud F5 WAF deployment

Organizational Experience

Mar'17- present with Qatar Islamic Bank Group, Doha, Qatar

Security Officer (L3-Architecture and Digital Transformation)

Key Result Areas

- Providing engineering support to architect, design, implement, administer for all QIB Palo Alto Firewalls and Panorama Management Appliance and documents final enterprise architecture, network diagrams, security best practices
- Responsible for Design, build and periodic review of enterprise-class security system
- Align standards, frameworks and security with overall business and technology strategy that include all legal, physical and technical controls involved in organization's risk management
- Extensive experience in information security and/or IT risk management with a focus on security, performance and reliability
- Expertise across variety of security products including Next Generation firewalls, URL filtering, End point Security and Incident Analysis
- Review existing security architecture for On-prem and Cloud, identify security design gaps in existing architecture, and recommend changes or enhancements
- Consulting and engineering in the development and design of security best practices and implementation of solid security principles across the organization, to meet business goals along with customer and regulatory requirements
- Understanding on Security considerations of cloud computing: They include data breaches, broken authentication, hacking, account hijacking, malicious insiders, third parties, APTs, data loss and DoS attacks
- Good working knowledge on Identity and access management (IAM) and best practices.
- Solid understanding of security protocols, cryptography, authentication, authorization and security
- Experience in implementing multi-factor authentication, single sign-on, identity management or related technologies
- Maintains security by monitoring and ensuring compliance to standards, policies, and procedures, developing and conducting training programs
- Prepare comprehensive reports including assessment-based findings and propositions for further system security enhancement
- Assist in resolving technical challenges, provide solutions to Operational Team, and document the findings
- Identify and communicate current and emerging security threats/vulnerabilities and remediate them within environment
- Ability to identify risks associated with business processes, operations, information security programs and technology projects
- Sound knowledge on cloud technologies like SaaS, IaaS and PaaS, exposure to AWS, GCP and Azure Cloud stack
- Define the security control metrics for evaluating the efficiency of existing controls
- Prepare and document standard operating procedures and protocols
- As technical SME within the Data Security domain responsible for designing and implementing enterprise technology and procedural controls. Extensive experience with system security concepts, tools, implementation, DLP, CASB, and integration with various data sources and application stacks.

Jun'15- Feb'17 with Information and Communication Technology, Doha, Qatar

Technical Support Engineer

Key Result Areas

- Assist in the hands-on implementation of multiple DLP solutions.
- Working with vendors to implement and support DLP technology, including troubleshooting and upgrading.
- Maintaining DLP technology, configuring policies, and compiling reports for analytics.
- Monitoring and responding to alerts generated from DLP systems and other technologies.
- Working with the Incident Response team to escalate and respond to potential or real threats.
- Serving as a DLP subject matter expert within the organization.
- Collaborating on the DLP rule development lifecycle including policy development, response rules, and maintenance.
- Provide DLP subject matter expertise and thought leadership as an extended member of a customer team.
- Provide guidance, recommendations, best practices, etc. for DLP operations.
- Assist with DLP component upgrades, installs, testing and configuration.
- Liaise with Symantec Support, Engineering, Product Management, and others within Symantec on behalf of the customer.
- Provide single point of contact and hands-on escalation and remediation for critical issues.
- Respond rapidly to unplanned events, including after hours for Severity 1 issues.
- Proactively communicate relevant technical information and alerts on known issues, hot fixes, new releases, etc.
- Provide regular status reports for critical incidents, projects and proactive services.
- Communicate professionally and effectively at all organizational levels.
- Keep the Account Team informed of major issues or new opportunities.
- Coordinated the incident response activity in case of a cybersecurity event, as per Information Security Incident Management Standard
- Collaborated with all stakeholders involved, and provided the communication required in the process

April 14-May'15: Penta Consulting, Doha Qatar

Security Engineer

Key Result Areas

- Design, configure, implement and maintain all security platforms and their associated software, such as routers, switches, firewalls, intrusion detection/intrusion prevention, anti-virus, cryptography systems, SIEM, Anti-SPAM, and MDM.
- Working with vendors to implement and support DLP technology, including troubleshooting and upgrading.
- DLP Agent Deployment and troubleshooting.
- Maintaining DLP technology, configuring policies, and compiling reports for analytics.
- Monitoring and responding to alerts generated from DLP systems and other technologies.
- Working with the Incident Response team to escalate and respond to potential or real threats.
- Serving as a DLP subject matter expert within the organization.
- Collaborating on the DLP rule development lifecycle including policy development, response rules, and maintenance.
- Proven effective verbal and written communication skills
- Ability to independently research and solve technical issues
- Demonstrated integrity in a professional environment
- Knowledge of core Information Security concepts related to Governance, Risk & Compliance
- Data Loss Prevention (DLP) Technology support and Event Handling

July 11- Mar'14: NK Network Champs Pvt. Ltd.

Network Administrator- L2

Client: HP India Sales Pvt. Ltd, Bangalore, India

Key Result Areas

- Manages and configures security devices such as firewall, IPS/IDS, Proxy, VPN, and provides fault resolution and escalation.
- Document's security incidents via ITD-E Service Desk system. Respond to the functional units of the security incidents per the guidelines of the information security policy.
- Provide second level support and work closely with other team members in IT projects that need network/security/hardware installation and configuration.
- Troubleshoots and diagnoses network security problems and corrects identified problems.

Personal Details

Date of Birth: 23rd December 1986
Languages Known: English and Hindi
Present Address: Al Hitmi, Doha. Qatar 559