ABHISHEK SHARMA

Senior Manager Cyber Risk & Security Practice

CONTACT

Greater Noida, India

882-627-2754

abhisheksharmasec@gmail.co

https://www.linkedin.com/in/abhishek-sharma-pmp-cism-173876b9/

SKILLS

- Leadership
- Solutioning & Designing
- Compliance
- Consulting
- Teamwork
- Engineering & Implementation
- Public Communication
- Estimation

Technical SKILLS

Tools: - Wireshark, Firemon, Solar winds, PRTG, JIRA, Qradar, ArcSight. Splunk, Qradar, Azure Sentinel.

Security/ET:- Cisco ASA 5500 series, Palo Alto, Checkpoint R71 &R77,Juniper Net screen, SSL VPN, SRX, F5 LTM Bluecoat Proxy, Websense Gateway, McAfee NSM IPS and IDS, EPO 5.3.1, Nokia checkpoint Firewall & management server; Creating rule base policy as per organization requirement; VPN tunnel, AES, IPSEC, and SSL; Smart defense - IP spoofing, DOS attack, Content security- URL filtering; Context based security RSA Auth Manager 7.1,Symantec DLP, Websense DLP, Microsoft DLP, ZScalar DLP and proxy , Azure, cisco ISE 2.6 One trust, Varonis ,Netskope CASB, MIP, Big ID, MCAS, AIP,AWS , Azure, ATP, Encryption, data protection solutions, Azure ,AWS, GCP.

ABOUT ME

Offering 17.6+ years of imperative Industrial Experience into Cyber security domain for Consulting, Solutioning, Designing, Implementation and project Delivery. Consistently commended by company executives, colleagues, and peers for strong work ethic and ability to finish extremely complex jobs on time.

WORK EXPERIENCE

Sr. MANAGER Wipro Tech. JUL-21 till Now

Job Responsibilities: Worked as Senior manager for cyber risk security practice. Responsible for End-to-End cyber security tools designing, Solutioning and implementation, performing assessment, due diligence & POC ‘s., assessment, proposal with OEM/sales team and senior management.

- ✓ Working on SOW, RFPs, RFI, RFQ, Estimation, POCs, POV, white papers related to cyber security tools under security practice.
- ✓ Active involvement in reading through customer requirement from RFP and drafting solution inline to customer need. Security Risk identification, analysis, assessment, risk mitigation and Gap analysis.
- ✓ Assisting the Global DPO to align the new Wipro business in diverse territories.
- ✓ Experience in Windows Defender ATP and Windows Information Protection, and Cloud hosting services SaaS solution such as Forcepoint, varonis, Big ID, MS DLP, McAfee DLP, Symantec DLP, DAM tools, Proxies, Web Filters, Email gateway, Antivirus, DLP, two factor authentication & Security Compliance.
- ✓ Designing security solutions for Hybrid Cloud and Multi-Cloud platform solution for infra and data security.
- ✓ Responsible for implementation of data protection tools – DLP (Symantec, Microsoft), Data Discovery and classification, Database Activity Monitoring, Static Data Masking for new and existing customers, Data Classification (Azure Information Protection, Titus, Boldon James), Data Access Governance (Varonis, Stealth bits) & CASB (Symantec CloudSOC, MCAS, MVISION, Netskope).
- ✓ Drive customer engagements on Technical Scope meeting/call and develops statement of work and proposal with the relevant work breakdown structures based on customers' requirements.

Consultant Security HCL Tech. JAN-19 to JUL-21

Job Responsibilities: Worked in Cyber security Practice team, day-to-day responsibilities was to Manage the Transition ad transformation for the different customers. Providing support on technical issues, performing Due diligence, assessment, recommending migration approach, designing the security solution and implementation.

- ✓ Working on SOW, assessment, Proposal response based on active RFP, RFQ, RFI ad Effort estimation.
- ✓ Conducting meetings with PM and sales team to discuss the assessments, Conduct the meetings with Vendors, Vendor Relationship Owners.
- ✓ Creating Knowledge base for the Security solutions, playback sessions, playback feedback, runbook etc.

Compliance: - GDPR, CCPA, HIPPA, PCI DSS, PDPA, ISO27017, ISO27018, ISO29100, COPAA, NIST 800-53

Server: - Implementation of DHCP and DNS Servers; Managing AD users and Accounts; Managing Group Policy; Implementation of IIS, Implementation of Routing and Remote Access; Implementation of Terminal Services.

ORGANIZATION

Wipro Tech.	JUL-2021 to Till Now
HCL Tech.	JAN-2019 to JUL-2021
TECH Mahindra	JAN-2018 to JAN-2019
BT Global	NOV-2016 to NOV-2017
Accenture	JUN-2015 to OCT-2016
HCL Tech	FEB-2014 to MAY-2015
Wipro Infotech	SEP-2011 to JAN-2014
IBM NETSOL	DEC-2010 to SEP-2011
CMS Infosystems	SEP-2010 to DEC-2010
Network Bulls	FEB-2008 to SEP-2010
Accel Frontline	DEC-2005 to FEB-2008

AWARDS

- ❖ Ideapreneurship Certificate.
- ❖ Pat on back Award in TechM
- ❖ Role Model Award in BT
- ❖ Idea Value Creator Award in HCL
- ❖ Employee of the month Award in HCL
- ❖ Best North Customer Support Engineer Award in Wipro.

ACADEMICS

- ❖ MASTER OF BUSINESS ADMINISTRATION from Sikkim Manipal University, Delhi in 2011
- ❖ BACHELOR OF ARTS in English Language from Kanpur University (U.P.) in 2009.
- ❖ DIPLOMA IN ELECTRONICS ENGINEERING from B.T.E.U.P.in 2005

ACHIEVEMENTS

- ❖ Successfully added revenue to practice for managed $3 million.
- ❖ Developed and implemented new MSSP strategy for the data security practice.

- ✓ Responsible for implementation of data protection tools – SIEM tools such as Qradar and Splunk ES, DLP, Data Classification & CASB, firewall, proxies, Azure cloud hosting. Deploying cisco ISE solution for wired and wireless authentication, BYOD, guest portal and self-registration portal.
- ✓ Defining project onboarding document for each client including various docs such as Runbook, detailed Sample reports, assisting for VPN setup, onboarding completion certificate, RCA, SLA, welcome email, KT sheet etc.
- ✓ Preparing escalation matrix, SOW mapping, Rules creation for reports generation, Alarms creation, Fine-tuning of logs and alarms, Log validation., Security Connected Platform Approach Solutions - EDR, Perimeter, SIEM, SOAR, Threat Hunting
- ✓ Covering complete service in scope, Event source list, HLD and LLD for each client, post implementation document, SOP, operation risk logs, use cases etc.
- ✓ Cloud hunting with SIEM/SOAR/Threat Hunting / Deception and emerging solutions - azure sentinel, AWS/Azure native security solutions and integrated orchestration design with cloud cyber solutions - many capture the flag scenarios.
- ✓ Identify the in-efficiencies in the operations and identify potential solutions to improve efficiency.

Security Consultant Tech Mahindra JAN-18 to JAN-19

Job Responsibilities: Creation of POV, white papers, RFQ, RFI, RLS & defense with clients. Managing complete GSOC Setup for multiple clients in TechM as SOC Head, Handling a team of 24 subordinates for shared service model for day-to-day operation.

- ✓ Actively participating for proposal creation, POV, white papers, RFQ, RFI, RLS & defense with clients.
- ✓ Worked for Implementing Splunk Enterprise security for Indonesian client with 6 TB log license.
- ✓ Being a part of ESRM practice team in TechM, work closely with our bid manager, sales team and vendors and provide support and guidance through to deal closure.
- ✓ Develop and deliver scope of works, hour/cost estimates shared and dedicated model, professional proposals and design documentation.
- ✓ Covering complete service in scope, Event source list, HLD and LLD for each client, post implementation document, SOP, operation risk logs, use cases etc.
- ✓ Responsible for providing Security Solution and architectural expertise to the System Integrator.
- ✓ Develop detailed equipment list (BoM), build presentations and RFP answers.
- ✓ Analyze and define client's business strategy and determine system architecture requirements to achieve business goals.
- ✓ Provide deep SW / HW technical architecture expertise to ensure proper solution design.
- ✓ Collaborate with other MSS Security Solution Architects and management to grow and evolve Managed Security Service offerings.
- ✓ Interacting with customer for WSR, Scrum, weekly, Steering meeting, service improvement, QM checker and escalations.
- ✓ Working for ISMS policy for projects and implementing process to smooth the operations.
- ✓ Conduct proof of concept activities with key business users in support of advanced use cases

CERTIFICATIONS & TRAININGS

- Core Technical Trainings
  - PaloAltoFirewallEssentials1 (201),Essentials2(205)
  - Websense DLP 7.7
  - Symantec DLP 14.0
  - McAfee EPO 5.1
  - Cisco ISE 2.6
  - Aruba ClearPass training.
  - AZURE MIP
- Core Technical Certifications
  - CISM certified.
  - CISA certified.
  - PMP certified.
  - Prince2 certified.
  - ISO 27001 LA.
  - ZScalar Certified- ZCAA-IA & ZCSS
  - MS Azure
  - AWS-AWS Certified Solutions Architect - Associate
  - PCNSE6- Palo Alto Certified Network Security Engineer
  - CEHv9 – Certified Ethical Hacker
  - Symantec SSE+SSL Visibility
  - Symantec SSE+ ProxySG
  - Symantec SSE+ DLP
  - Implementing Cisco IOS Network Security –IINS
  - Cisco Certified Security Professional-CCSP
  - CCSA - Checkpoint Certified Security Administrator
  - ITIL V3 Foundation
  - CCNA - Cisco Certified Network Associate
  - MCSA – Microsoft Certified System Administrator
  - Spunk fundamentals
- Core functional Trainings
  - PMP
  - ITILV3
  - CISSP
- Pursuing Courses
  - CISSP, exam booked for Sep 2023.

LANGUAGES

ENGLISH

HINDI

Technical Manager BT Global NOV-16 to NOV-17

Job Responsibilities: Managing team of 8 subordinates of implementation team. Working on new proposal and solution based on RFP.

- ✓ Responsible to produce technical related documents diagrams, High-Level Design (HLD), Low-Level Design (LLD).
- ✓ Working on new proposal and solution based on RFP. Contribute to proposals and bids by determining scope of work, completing bills of material, and writing Proposals and responses to tender.
- ✓ Working on Data Center and Site Migration, Transition, and Transformation Projects, and Methods of Procedures to ensure the accurate, complete, and structured approach for implementation.
- ✓ Plan to design on requirements review, objectives, project scope, business, and technical requirements to ensure expectations are met.
- ✓ Proved successful working within tight deadlines and fast-paced atmosphere. Used coordination and planning skills to achieve results according to schedule. Collaborated with Operation, Implementation and account team to achieve result
- ✓ Successfully Migration in customer DC location
- ✓ Fixing the identified root causes, evaluate optimal solutions, and
- ✓ Reviews peer documents for technical accuracy, quality assurance and ensure design compliance. Contribute to team processes and highlight to management any risk to projects and knowledge shared to new engineers.

Security Team Lead Accenture JUN-15 To OCT-16

Job Responsibilities: Worked as team lead managing Project with team in shared service model for daily incident support. Planning and designing security tools migration and implementation.

- ✓ Handling Team of 5 subordinates under my supervision for executing daily tasks for customers in SOC, approving their claims, leave and roster management.
- ✓ Working on incident management on Firewalls, Proxies, Web Filters, IPS, Antivirus, DLP, two factor authentication & Security Compliance
- ✓ Working on problem/change mgmt. on Firewalls, Proxies, Web Filters, IPS, Antivirus, DLP & two factor authentication.
- ✓ Implemented Splunk SIEM solution and operation support for Saudi based client.
- ✓ Designing & Implementation of various Network Security solution for cloud security with one of our customers in Australia.
- ✓ Reviewing daily dashboards for P1, P2 and P3 incident and the follow-up. Reviewing major activity planned for client. Joining bridges for on call support for any major escalated issues.
- ✓ Interacting internally for Lead meetings and with Client for weekly firewall touchpoints. Evaluating new products /technologies to support/ simplify the growth path of the client in a secure manner.
- ✓ Manage Security operations handling various security technologies (firewalls, proxy, intrusion detection/prevention, load balancing, web gateway, endpoint security etc.).
- ✓ Prepare Root Cause Analysis (RCA) for major Problems in the network and provide the necessary corrective and preventive measures.

SAMA Onsite Project Details:

Key Responsibilities includes:

- ✓ Preparing Technical Documents for the customer once implementation ends and asking for sign-off.

HOBBIES

Music

Movie

Sport

Travel

Reading

Internet

PERSONAL DETAILS

DATE OF BIRTH: 30 December 1983

PASSPORT NUMBER: Available on Request

REFERENCES

Available on Request

- ✓ Worked for HLD and LLD for deploying network products. Implementation and Support of information security solutions – IronPort, Websense, McAfee EPO, Juniper SSL, Cisco/McAfee IPS and IDS, F5 LTM and ASM, Firewall-ASA 5585, Palo Alto, FortiGate, Juniper SRX.
- ✓ Worked DNS, DHCP and Riverbed for wan optimizing.
- ✓ Troubleshooting on Websense and Bluecoat, troubleshooting daily sev1 and sev2 issues for global sites.
- ✓ Maintaining security infrastructure, installation, migration and configuration, reviewing Firewall rules.
- ✓ Providing Weekly & Monthly Security Reports to various stake holders.

Technical Specialist HCL Tech. FEB-14 to MAY-15

Job Responsibilities: Responsible for managing a team of 7 engineers and supporting the offshore network and security support.

- ✓ Firewall site migration from ASA to Palo Alto.
- ✓ Responsible for creation, maintenance, update, and review of security documentation like policy, procedure, standards, and guidelines.
- ✓ Designing the security infra and planning and analysis security of threats & traffic. Responsible for managing a team of 7 engineers and supporting the offshore.
- ✓ Handled Splunk, Checkpoint Firewall R75, Bluecoat Proxy, Juniper Net Screen, Juniper SA4000 SSL VPN, and Cisco ASA 5540.
- ✓ Work on Splunk solution for enabling logging for all network and security devices for SIEM monitoring in operations.
- ✓ Managing FortiGate firewall with Forti manager, Implementing and migrating Checkpoint Firewall R77, RSA envision, Bluecoat Proxy, Websense, Juniper Net screen, Juniper SA6500 SSL VPN, and Cisco ASA 5540, juniper with NSM, ASA, Palo Alto PA-200, PA-500, PA-2050, and PA- 5060 through Palo Panorama
- ✓ Managed trouble tickets for the RCA of the problem and live troubleshooting on cases with other teams.

Sr. Eng. NW & Sec Wipro Infotech SEP-11 to JAN-14

Job Responsibilities: Primary project contact for India’s Telecom Service Provider and internal groups, provide continuous project feedback and status updates to key stakeholders. Develop project plans and related task lists as necessary, update plans accordingly.

- ✓ Manage multiple implementation tasks for network security devices with other internal groups to ensure project completion in accordance with client requirements, provide occasional after hour support of client implementations.
- ✓ Develop and maintain professional client relationships and manage expectations with respect to live dates and other key timelines.
- ✓ Maintain accurate and complete documentation including parameters, network paperwork, and documentation for all client interaction and addressing performance bottlenecks and ensuring maximum security services uptime.
- ✓ Designing the security infra and planning and analysis for security threats & traffic.
- ✓ Assisting in the design and implementation of the security, troubleshooting security incidents & conflicts.
- ✓ Implemented change requests of Network and security domain. Did Impact analysis before any deployment or validate change in network, and validate POA to minimize outage.
- ✓ Planning and Upgrading IOS and upgrades on site firewall devices.

Sr. Sec. Eng. IBM Network Solution DEC-10 to SEP-11

Job Responsibilities: Worked for Govt client known as CBDT India for support.

- ✓ Creating & working on change requests raised for updating ACL on Firewalls.
- ✓ Virus Remediation.
- ✓ Monitoring the correlated events and log analysis of firewalls, NIDS, HIDS & Juniper VPN.
- ✓ Ticket creation and handle them within SLA
- ✓ Scheduling, configuring, verifying & backing up jobs and worked on Level 2 escalations.
- ✓ Building Configuration & installation of new WAN circuits and devices.
- ✓ Meeting the prerequisites for updating the configuration.
- ✓ Prepared the change documents including device configurations for site migrations

Sr. FMS Engineer NW. CMS Infosystems SEP-10 to DEC-10

Job Responsibilities: Worked CMS various clients as Support Engineer

- ✓ Responsible for resolving trouble-tickets raised by users of the client’s product/service through phone, email or remote access.
- ✓ Responsible for managing, configuration and monitoring of all customer’s network devices
- ✓ Upgrading firmware for network and security devices.
- ✓ Handled day to day operation on client configuration problem and giving remote support by configuring, managing and troubleshooting OSPF, STATIC routing.

Sr. network Engineer Network bulls FEB-08 to SEP-10

Job Responsibilities: Worked as Sr. Network Support Engineer

- ✓ Managing IT infrastructure such as network, firewall and MacAfee epo antivirus support.
- ✓ Monitoring the correlated events and log analysis of firewalls, NIDS, HIDS & Juniper VPN.
- ✓ Ticket creation and handling them within SLA.

Customer support Engg Accel Frontline DEC-05 to FEB 08

Job Responsibilities: Worked as Customer Support Engineer

- ✓ Ticket creation and handling them within SLA.
- ✓ Monitoring the correlated events and log analysis of firewalls, NIDS HIDS & Juniper VPN.
- ✓ Firmware upgrades and network device configuration.