SUNIL KUMAR
Mobile: XXX
Email: sunil1.kumar@hotmail.com

Senior Cyber Security Professional

 # Information Security #Cyber Security # Enterprise Security #MSS #SOC #SIEM # Networking & Systems Administration # Infrastructure Management #Cloud Security

Career Summary

⇒ A "**Performance Driven Professional**" with 20+ years of widespread experience in the domain of Information Security, Enterprise security, Networking, Systems Integration, and Infrastructure Management.

⇒ **Presently associated with Tata Communications as SOC Lead while driving the Security Operations for multiple clients.**

⇒ Adept in **analyzing information system needs**, evaluating **end-user requirements**, custom designing information security solutions, troubleshooting for complex network systems.

⇒ Proficient in **IT Security Operations, Cloud Security, Security Service Delivery, Change, Release, Incident** and **Problem Management**.

⇒ Specialized in **End-to-End Service Delivery, Transition & Migration** for Enterprise **security projects (SOC)** and **Enterprise level Security** Consulting for large Infra Projects.

⇒ Gained exposure while **working closely with global customers, skilled in architecting, documenting, and implementing** various infrastructure solutions, processes, and risk-based controls.

⇒ Implemented project plans within **pre-set budgets** and **deadlines**; refocusing the department's priorities and engagement methods from a **process bound to delivery focused**, thereby **streamlining the program** management process.

⇒ Comprehensive experience in diversified technology areas including in **System /Network /Cloud Security, VA/PT, Auditing & reporting environment** etc. with extensive knowledge on **ITIL** and **IT Security Processes**.

⇒ Effective in working closely with **third-party vendors** and **contractors** to manage and coordinate projects with the business units and other IT departments, where necessary.

⇒ Strong believer of 30-60-90 days, planned and executed 30-60-90 days plan successfully.

⇒ Skilled in **problem-solving** coupled with **assertive decision-making** for enabling **effective solutions** leading to high **customer satisfaction** & low operational costs.

Technology Skills

IS Security Tools	Data Loss Prevention, SIEM, VPN, Anti-Virus, Content Filtering, EDR, IDS/ IPS
Security Tools (VA/PT)	Retina, Nessus, BackTrack, Metasploit, Burp Proxy, Wireshark, Nmap
Firewall	NetScreen, SonicWall, Checkpoint, Fortinet, Huawei
Operating Systems/ Software	Windows, Linux and other office productivity tools
Hardware	CISCO Routers, Cisco Switches, HP Network Devices, NetScreen, SonicWall Firewall, Fortinet IBM & HP Servers
Processes/ Standards	ISMS, ISO27001, NIST, PCI, ITSM Framework based on ITIL and other standards

Career Sketch

As a SOC Lead, my prime responsibilities are to lead and manage the Security Operation Center & Capabilities: Security Information and Event Management (SIEM), Vulnerability Management & Penetration Testing (VA PT, Infrastructure and Application Security Testing)), Identity & Access Management (IAM), Governance Risk and Compliance (GRC), Network Security and Endpoint Security.

Key Deliverables:

⇒ Operations & Leadership Management, Security Service Delivery, Team Building & Management,

⇒ Review of RFP, SOW, SLA, KPI management and collaboration with other teams for defining the optimum solutions.

⇒ Weekly, Monthly & Quarterly reports, presentation to the client and leadership and to ensure all solutions defined are operating in a secure configuration and healthy on an ongoing basis.

⇒ Coordinate with multiple different teams at client location and MSS teams to get the customer queries and concerns addressed in a timely manner.

⇒ Project Finance Management: Forecasting, Budgeting, Profit Margins and Cost Saving.

⇒ Leading the Company Priorities in Innovation, Automation, Analytics and Cost Reduction.

⇒ Identify and help implement continuous process enhancements/improvements in the project.

⇒ Perform People Management Roles: Hiring, Transferring, Promoting and Appraisals.

⇒ Demonstrate Leadership Abilities: Provide directions, checkpoints, and constant feedbacks.

⇒ Lead security & risk related projects from initiation through implementation, transition to support clients' security needs.

⇒ Design, coordinate and oversee security testing procedures to verify the security of systems, networks and applications, and manage the remediation of identified risks.

⇒ Develop and implement the response management processes and recovery plans for detecting, identifying and analysing IT security incident and manage post-event reviews to identify corrective actions required.

⇒ Provide security consultation services, audit support, escalation management, and reporting security service to client Leadership and Board members and stakeholders.

⇒ Perform tasks related to:

- Security Operations Management
- Managing client expectations and requirements
- Service Level and Performance Management
- Types of threats, sources of threats, attack vectors.
- Network vulnerabilities and attacks, IP spoofing, Hijacking, DOS protection.
- User authentication, permissions, password policies, audit policies, encryption.
- Physical security, internet security, wireless security, and core security principles.
- Vulnerability assessment & remediation, Penetration testing.
- Information security, risk management, business continuity.
- Define and deploy the policies for AV, IDS/IPS & firewalls and other in-scope security products.
- Periodically update the policies based on client requirements.
- Incident response and communications to stakeholders

Project: MSS Shared Security Services

Key Deliverables:

⇒ Providing information security services to multiple clients of diverse industry sectors such as financial, hotel, travel, health care etc. across multiple geographies.

⇒ People Manager – Managing a team of Security Team Leads, Sr. Security Analysts and Associates.

⇒ Active participation in Client Visits, RFP review and Due diligence for new deal.

⇒ Driving upsells in Southeast Asia market clients and could add $2M based on impeccable client delivery.

⇒ Successfully Delivery led transitions of multiple projects and streamlining of the SOC processes.

⇒ Spearhead independent review of enterprise security products for encryption, secure messaging, privacy data monitoring, intrusion detection, end point and gateway security, system/network security.

⇒ Security and Compliance Leader for the project teams delivering Managed Security Services support, Malware Defense, Data Loss Prevention, Anti-Virus, VA/PT, IDS and URL Filtering.

⇒ Responsible for managing the infrastructure security tools and day to day operations as per the agreed SLA.

⇒ Responsible for risk identification of compliance requirements and mapping to the business; compliance risk assessment; third party risk assessment; control assessment including self-assessment; and risk-issue tracking.

⇒ Plan specific audits to determine whether information systems are protected, controlled and provide value to the organization. Conduct & report audit findings and make recommendations to key stakeholders.

⇒ Prepare and establish implementation of necessary information security policies, standards, procedures and guidelines, in conjunction with the Business & Security Committee.

⇒ Liaison with related governance functions such as Physical Security / Facilities, Risk Management, IT, HR, Compliance, plus middle managers throughout the organization, on information security matters.

⇒ Periodically review information security metrics and publishing weekly/monthly executive dashboards with senior management for information security posture of the infrastructure.

⇒ Establish & lead activities relating to contingency planning, business continuity management and IT disaster recovery in conjunction with relevant functions and third parties.

Key Deliverables:

⇒ Conducting information security risk assessment, audits and regulatory compliance audits.

⇒ Application security testing/ vulnerability assessment/ Network security assessment and vendor assessments reviews and BCP/DR plan for critical applications.

⇒ Conducting IT Risk assessments, BIA and IT systems recovery analysis.

⇒ Understand the business processes in Operations to identify information security risks and suggesting effective mitigating control measures to manage such risks.

⇒ SDL for reporting performance, escalation handling, clarifying concerns, seeking feedback, monthly evaluation of performance and support.

Dec'2009 – Nov' 2011 **OSCO (OHI Group Company), Muscat, Oman**
Assistant Manager - Information Technology Network & Security

Key Deliverables:

⇒ Defining company's IT Security Policies, Architecture and Procedures for IT related operations.

⇒ Establish, review and enforcement of various information security processes to maintain Confidentiality, Integrity & Availability (CIA).

⇒ Conduct risk assessments based on ISO27001 standards and as per industry's best practices.

⇒ Perform self-assessments to assess the effectiveness of IT Security controls and prepare audit plans.

⇒ Established Data Classification process in the organization and launched data classification execution across the organization as a new IT Security initiative.

⇒ Responsible for Vulnerability Assessment, performing PT and plan corrective actions.

⇒ Actively involved in Business Continuity Planning /Disaster Recovery Planning (BCP/DRP).

⇒ Supervision of preventive and corrective maintenance activities performed.

⇒ Obtain needful compliance to the system audit observation.

⇒ Review the IT Infrastructure architecture i.e. Network architecture, computing architecture.

⇒ Participating in the meeting with Senior Management once a month and ensuring healthy relationship.

Key Deliverables:

⇒ Serving as the primary focal point for all IT security requirements and audits for Accenture in Delhi NCR including Software Development centre and BPO centre.

⇒ Understand the business processes in Operations to identify information security risks and implement effective mitigating control measures to manage such risks.

⇒ Provide assistance to the Security Policy and Security Architecture and Standard Operating Procedures (SOP) for security related operations.

⇒ Responsible for planning & execution of Vulnerability Assessment and plan corrective actions, Third Party Risk Assessment and prepare and review risk mitigation strategies.

⇒ Responsible for regional security incident management and reporting to the concern team.

⇒ Provide consulting support regarding Physical, Administrative, and Technical Security controls and processes that safeguard the Confidentiality, Availability and Integrity of the Infrastructure.

⇒ Verify that all systems & networking devices have been configured as per Accenture Baseline Standards and as per Client Security Standards.

⇒ Evaluation of new security tools, products proactively to overcome with emerging IT Security threats as well as to automate the Security compliance activities.

⇒ Monitoring BCP plan documented & available for Accenture IT facilities & projects.

⇒ Ensuring that all Accenture Delhi-NCR locations sustain certification (ISO20000 /IS027001 /BS25999).

Key Deliverables:

⇒ Process owner of the management team i.e. SLA's, Asset Management, Problem Management, Recovery Management and Change Management.

⇒ Implementation of IBM global security policies, processes and procedures and serve as a focal point for regional security planning and execution.

⇒ Conduct Risk Assessments and Compliance Audits as per IBM standards & Security policies.

⇒ Responsible for security incident management and reporting to the senior management.

⇒ Responsible for Business Continuity Planning /Disaster Recovery Planning (BCP/DRP).

⇒ Creating a formal process of seeking client feedback on a monthly /quarterly basis (internal / External) and dashboard that reflects quality of service delivery.

⇒ Managing a heterogeneous network environment having different Domains and Sites configured.

⇒ Administration and Troubleshooting of all WAN connectivity across Haryana circle E1 Links, ISDN PRI & BRI, VPN connectivity and monitoring the bandwidth.

⇒ Responsible for providing Internet access to users for different domains using Linux Squid proxy server, ISA server.

⇒ Antivirus Server Administration, Server OS Hardening (Windows & Linux), Administrating DNS, DHCP server.

Key Deliverables:

⇒ Primarily deputed at client MMTC and managing their heterogeneous systems and servers.

⇒ Responsible for Vulnerability management for desktops, servers and networking equipment.

⇒ Responsible for Managing and Administering of Windows 2000 Domain, DHCP, DNS, Backup servers.

ACADEMIC DETAILS

⇒ **Executive MBA (EPGDM) form Alliance University, Bangalore in 2023**

⇒ **PG Dip in CYBER LAWS & IPR from Hyderabad University in 2008.**

⇒ **B.Sc. from CCS University Meerut in 1999.**

CERTIFICATIONS ACHIEVED

⇒ **CISSP – Certified Information Systems Security Professional**

⇒ **CCSP – Certified Cloud Security Professional**

⇒ **AZ-900 – Microsoft Azure Fundamentals**

⇒ **SC-900: Microsoft Security, Compliance, and Identity Fundamentals**

⇒ **ITILv3 Foundation Certified**

⇒ **ISO 27001:2013 Lead Auditor**

⇒ **Trained on PMP, AWS Sol. Arch.**

⇒ CISM – Certified Information Security Manager (expired)

⇒ CISA – Certified Information Systems Auditor (expired)

⇒ GIAC Certified Incident Handler – GCIH (expired)

⇒ Other expired certifications – MCE, MCSA, CCNA

OTHER DETAILS

Please feel free to contact in order get other details including references.

(Sunil Kumar)