Shakti Prateek Gyan Prakash Sharma

Cell: 91.8130402828 | 91.9718176116

Mail: Shaktigps@gmail.com

Linked in: in.linkedin.com/in/shaktiii

DOB: 28/02/1981

Contact: +91.8130402828 /+91.9718176116

Present Location and Permanent Address :

H.No 1719, Sector 45, Urban Estate, Gurgaon, Haryana, India – 122003.

Profile and Summary of Experience

With over 10+ Years of I.T experience oriented towards security (5 years Security Operations and 5 Years of Information Security) presently perform complex level professional internal auditing work, Conducting Internal audits for project’s compliance towards MSA, Security policies and best practices, Privacy Impact Assessments, SSAE 16, ISO 27001, I.T.G.C Audits, Risk Assessment, Security Incident Investigations and such consulting aligned work for HCL Internal projects and HCL Corporate.

Education

MSC - Information Technology from SMU, Gurgaon, in the year 2014

MBA – Information Systems Management/I.T from SMU, Gurgaon, in the year 2012.

Bachelor’s Degree in Commerce from University Of Rajasthan, Jaipur, in the year 2002.

Certifications

* CPISI from SISA Information Security
* ISO 27001:2005 to ISO 27001:2013 Lead Auditor transition from BSI.
* ISO 27001:2005 Lead Auditor trained @ Intertek/Moody International.
* Certified Ethical Hacker (CEH).
* Certified Hacking and Forensics Investigator (CHFI).
* EC-Council Certified Security Analyst (ECSA).
* Juniper Networks Certified Internet Associate – FWV & VPN.
* Juniper Networks Certified Internet Associate – SSL VPN.
* Juniper Networks Sales Associate.
* Juniper Networks Sales Specialist.
* ITIL V2 Foundation.
* DOEACC ‘O’ Level.

Tools

**Compliance, Audits & Risk Assessment:**95/46/EC (EU data protection Directive).  
2002/58/EC and 2006/24/EC (E-Privacy Directive and Amendments to E-Privacy)

ITGC, SAS 70, SSAE 16 - SOC1 and SOC2, ISO 27001, PCI-DSS, HIPAA, GLBA, SOX 404, and COBIT.  
Risk Assessment: Qualitative, Quantitative and CRAMM.

Security Controls: SANS Top 20, NIST SP800 and SOGP.

Information Security Policies and Procedure Writing.

**Security Testing Frameworks:** OWASP, OSSTM, ISSAF.

**Penetration Testing and Ethical Hacking:**

**Fingerprinting:** Nmap

**Vulnerability Assessment:** Nessus, Retina, Openvas.

**Web Vulnerability Scanners:** Nikto, Nstalker, Paros, Webscarab, BurpSuite, Acunetix.

**Password Cracking**: Rainbowtables, Ohpcrack, Cain and Able, LC5, John & Hydra.

**Database Auditing**: OAT, Winsid, Orabf, SQLDict, SQLping, Forcesql, Impreva, AppDetective Pro.

**Firewall:** Hping, Firewalk, tcp-Traceroute.

**Sniffers:** Wireshark, TCPDump, Snoop.  
**Packet Generators:** Hping2, Hping3 and Colasoft.  
**Denial Of Service:** Hping, TFN2K, Stacheldhrat, Trinoo, Idswakeup.

**Exploiters and Professional Tools:** Metasploit.

**SIEM (Security Information Event Management):** RSA Envision, LogLogic, and Juniper STRM.

**HoneyPots (low interaction Honeypots only):** Virtual honeyd deployments and log analysis.

**Digital Forensics:** FTK and FTK Imager, Encase 4.2, DD, DCFLDD, Sleuthkit, HexWorkShop, Winhex, photorec & Helix.  
  
**IPS and IDS:** Tippingpoint IPS, and Snort.

**Firewalls:** ISA Server 2004 and 2006, Checkpoint FW1, Juniper/Netscreen.

**Virtualization:** VMWare Workstation, Microsoft Virtual PC.  
  
**Linux and Unix:** FreeBSD, NetBSD, OpenBSD, Redhat, OpenSuse, CentOS, Ubuntu.  
  
**Windows Technologies:** DOS, Windows 9x, Windows 2000 Prof/Servers, Windows XP, 2003, 2008 Server, Windows 7.

**Antivirus:** Trend Micro, Symantec & MacAfee EPO.  
  
Experience on cisco routers and switches.

Employment History

HCL Technologies, Manesar & Noida, India  
14th May 2012 – Present

Current Role *2****:*** Deputy Manager – Information Security.

* Responsible for MSA and Security compliance of few assigned projects. (MSA, Security policy, SSAE 16, ISO 27001 and PCI-DSS)
* Risk Assessment Implementation for Finnish customer
* DLP Auditing project for Finnish customer
* Corporate Information Security Team for SSAE16/SAS70
* Travelled to Finland for Data Privacy - PIA (Privacy Impact Assessment) for a Finnish customer – Ongoing Project which includes compliance with EU Data protection for Infrastructure, Applications and Operational Privacy.
* Lead Security Incident investigations.

Role 1: Lead Information Security, Corporate Information Security team till September 13.

* Supporting Vertical: Banking Sector, Retail and Healthcare along with HCL Corporate.
* Lead audit team for Process and Technology clauses for SSAE 16(SAS 70) SOC1 and SOC2 (Service Organizational controls for HCL as well as User Organizational Control’s for various projects), PCI DSS for Banking Projects and Merchant clients, ISO27001, and HIIPA Security rule - audit covers the following domains as per Internal ITGC checklist’s (Physical security and Access Control, Logical security, BCP/DR, MSA Review’s, Human Resources, Project, Maintenance and I.T Audits).
* Responsible for driving regular Internal shadow audits for the SSAE16 and ISO27001, publishing audit Internal audit plans and reports, also driving the respective Information Security Officers for the closure of findings, thus ensuring smooth and regular compliance for all the controls in SSAE 16 and ISMS.
* Suggesting Complementary/Compensatory controls where ever applicable in case the primary control is not meeting the objective it has been designed for.
* Security Incident Investigation and reporting includes forensics as and when required.
* Implementation, GAP Analysis and Audit of SSAE 16 SOC2 compliance across few HCL projects. Mapped the SSAE 16 Controls with existing SSAE 16/ SAS 70 SOC 1 controls and ISO 27001 controls.
* Speaker at Induction and Various Security Awareness Trainings within HCL.

Alternatively/other than my KRA and assisted the project team thus enhancing my knowledge in current job: -

* Revised Internal SSAE 16 SOC1 checklist aligning with internal process within 8 months of my joining a one of my significant achievement.
* Designed the DISO (Delivery Aligned security officer) Framework for Project level compliance from security baselines point of view.
* Assisting Projects with Risk Assessment, Risk Register, designing of compensatory controls, GAP Analysis, Server hardening, Application security audit, Infosec trainings, etc. (Not under my KRA).

Wipro Infotech, Gurgaon, India  
13th July 2009 – 11th May 2012.

Role: Senior Engineer - Security Operations Centre (Telecom Domain)

Project 1:

* Overall Security Operations Centre In-charge for SOC Services delivery from Team Wipro to Client. Managed SOC Services and overall Operations specific delivery of routine functions for SOC, Key responsibility for the delivery and management of the SOC CSV’s Critical Success factors, defined procedures and practice of SOC.
* Facilitate in regular ISMS Audit and external audits, including ISO 27001, SAS 70 and PCI additionally hands on experience facing various Internal and External Security Audits.
* Define key baselines and Secure Configuration documents for I.T and telecom devices.
* Sophisticated Tracking and Forward-looking Reporting of issues specific to ISO27001, Internal SAS controls and other general compliance using multiple SIEM and using manual Correlation. Showcasing such reports on regular basis to top management, viz: CISO.
* Creation of reports and a Security Improvement Plan & Risk Tracker of known and unknown potential threats.
* Owner of Several KPI’s including Antivirus, SOC and security devices compliance (SCD’s/device hardening), Server Hardening, ensuring secure devices delivery before go-live.
* Proactively executed audit and assess threats, risks, and vulnerabilities from emerging security issues, publishing security Advisory, newsletter for technical groups and domain leaders and updating them on daily basis for the latest vulnerabilities.
* Identifying the Risk and Information Security requirement of the Organization, Designing Information Security framework for the organization, identifying the current risks and bringing about mitigating controls through process and technology.
* I was responsible for Designing, setup and Leading SOC team members through the distribution of requirements, managing project requirements, and establishes development time lines. Managed process and acted in the lead role for computer security incident response team and suggested appropriate countermeasures in Incident cases.
* Designed architecture level Internet filtering solutions “Websense” for Internet Infrastructure and gateway security.
* Leading team for Vulnerability Assessment for the entire server infrastructure of datacenter included host OS like Unix, Sun Solaris, Linux and Microsoft Windows OS, Identified and recommended remedial measures to mitigate the findings, like unpatched servers, Server and service misconfigurations, and secure firewall configurations on network end to protect the Infrastructure.
* Mentored and trained engineers on security concepts like server hardening, Linux Server Security, Rootkits, firewalls, wireless security and other project activities.

Project 2:

Consulting Project for African clients regarding Security and Hardening of Wintel and UNIX servers for telecom project along with secure configuration of deployment for Juniper and Websense gateways.

Saudi Paramount Computer Systems, Riyadh, Saudi Arabia

June 2007 – 13th May 2009

Role: Information Security Consultant, Project Management - Professional Services Vulnerability & Risk Management.

Company website www.pcssaudi.com

GIP- General Intelligence Presidency – Information Security, Riyadh, Saudi Arabia

* Procedural Qualitative Risk analysis for GIP Infrastructure and applications using CRAMM tool (CCTA Risk Analysis and Management Method).
* Technical Risk Assessment of the Entire GIP identifying Vulnerabilities in GIP Infrastructure, Threat modeling, conducting Threat and Vulnerability Assessment for organizational information and technological assets.
* Penetration Testing of various LAN, WAN components of GIP.
* Comprehensive Risk Assessment using CRAMM software, assisted in translation of procedural questionnaire to Arabic language for the local teams to understand based on which periodic audits and GAP Analysis where carried out.
* Designing Information Security framework for the GIP, Identifying the current risks and bringing about mitigating controls through process and technology.
* Identifying new security solutions applicable to the GIP to enhance the security posture of the organization.
* Assess, recommend and coordinate Compliance, Legal and regulatory requirements related to IT Systems.
* Framing of policy, procedures, guidelines and baselines with reference to GIP infra.

Others:

* Checklist based audits and GAP analysis for various clients.
* Penetrating projects for Servers, Network Infra, Web Applications, etc.
* Preparing power presentations for management using SIEM and threat reports.

Wipro Technologies Ltd India, Bangalore & UK.

August 2006 – June 2007

Last Client: Security Testing of EVDO and Telecom infrastructure of US’s Leading EVDO Company

Role: Information Security Analyst

Assignment 1: Coventry, UK.

* Executed a Blackbox and Whitebox Penetration testing project in Coventry, UK for a Tourism agency, identifying major security loopholes in external and internal applications.

Assignment 2: Coventry, UK.

* Consulting and deployment for large scale PAN-America and PAN-Europe patch management solution, Designing KPI and solution documentations post the tool go live.

Assignment 3: London, UK and Bangalore, India.

* Security testing(Ethical Hacking) of Telecom data networks – EVDO (Evolution data only networks)
* Release lab testing of various EVDO device from security point of view.
* Security Audits of the EVDO LAB, each and every single component form BTS, TP, AP to IP Backhaul backbone.
* Vulnerability scanning and exploiting the vulnerable services.
* Service Fuzzing to find vulnerabilities in the device.
* DOS and DDOS attacks on the lab components.
* Review of post attack logs.
* Writing and developing test cases as a part of DTFT (design testing and future testing) team.
* Lab monitoring and alerting in real-time, packet captures for analysis of devices if they would have gone down during testing phases.
* Several other such activities involved in Data testing.

Tools and Technologies:

Nessus, Nmap, Nikto, Acunetix, Appscan, TFN2K, Stacheldhrat, Trinoo, IDSwakeup. Any available tool that we can lay our hands on for ethical hacking purposes.

Foresight Software Solutions, New Delhi, India

June 2005 to August 2006

Role: Technical Specialist, (Technical presales role for Security solutions)

Client: Various (HCL, Career, Mastek DSM Anti-infective, etc.)

For more information please visit: www.foresightho.com

Key Technologies: Checkpoint, SurfControl, Microsoft ISA Server, CRAMM, Vulnerability Assessment.

Key focused area: Key technical presales for SurfControl and content filtering and other solutions mentioned above, single handedly handled the entire operation for North region.

Bees Infotech as System Admin/Network Administrator – 2004 – 2005

CMS Computers Chandigarh as Trainee Systems Engineer – 2003 - 2004

Freelance Hardware and network solutions provider 2000 - 2003