

# Sheetal Joseph

Email: [sheetal@sheetaljoseph.org](mailto:sheetal@sheetaljoseph.org); [sheetaljo@gmail.com](mailto:sheetaljo@gmail.com)

Phone: +41794523798

Website: <http://sheetaljoseph.org>

LinkedIn Profile: <http://www.linkedin.com/in/sheetaljo>

## OBJECTIVE

Seeking a security consultant position that would utilize my current skills while simultaneously giving me the opportunity to expand my skills into new facets of information security

## SUMMARY

- 6 yrs of professional experience in an information security position with specific focus on:
  - Security Management and Operations, Security Policies, Procedures, System Analysis and Auditing
  - Analyzing Penetration Testing and Vulnerability Assessment reports and creating plans to improve the security posture in the Network, Host and Applications Security Design and Implementation
  - Application Security Testing
  - Hands-on experience in using security tools, techniques and methodologies
  - Operating System, database and network device hardening
  - Linux System Administration
- Strong understanding of regulatory and industry standards (including SOX, ISO17799/27001/2 and PCI DSS) Industry Standards
- Presented in Security Conferences like OWASP ( <http://www.owasp.org/index.php/Mumbai> ) & ClubHack ( <http://clubhack.com/2008/Speakers> ) and promoted security awareness amongst students & general public via lectures/talks in Engineering Colleges & Barcamps ( [http://www.barcampmumbai.org/BCM4\\_Sessions](http://www.barcampmumbai.org/BCM4_Sessions) )
- Developed and implemented information security vulnerability mitigation strategies
- Worked as primary consultant on client engagements and played an instrumental role in securing new projects for the company.
- Worked with Practice Area Leaders on developing and growing the security practice area and related offerings
- Able to identify customer requirements and translate them into an appropriate technical proposal.
- Worked closely with the Sales Team to plan and design a competitive comprehensive business solution.
- Assisted in proposal preparation, time & resource estimation and project implementation.
- Performed technical presentations and demonstrations to corporate clients.
- Mentored and trained consultants on Security Concepts like Server Hardening, Linux Server Security, Rootkits, Firewalls, Wireless Security and other Project activities.
- Was in the technical interview panel while performing recruitment activities for the E-Security dept of TechMahindra

## CERTIFICATIONS:

1. Prince2 Registered Practitioner - APMG
2. CISSP (Certified Information Systems Security Professional)- (ISC)2
3. CEH (Certified Ethical Hacker) – EC Council
4. BS7799 Lead Auditor - STQC
5. ISO 27001 Implementation – British Standards Institute (BSI)
6. IT Project Management – Indian Institute of Technology, Mumbai (DEP)

## EDUCATIONAL SUMMARY

| Degree                           | Duration          | College/School                                | Percentage |
|----------------------------------|-------------------|---|------------|
| B-Tech<br>(Computer Engineering) | Nov '98 - Oct '02 | College of Engineering, Chengannur,<br>Kerala | 70%        |
| Higher Secondary School          | June '97          | Holy Child Auxilium, New Delhi                | 74%        |
| Matriculation                    | June '95          | Holy Child Auxilium, New Delhi                | 81.25%     |

## TECHNICAL SKILLS:

**Operating Systems (OS):** Linux, FreeBSD, Windows, HP-UX, Apple Mac OS X, BackTrack, Knoppix, Open BSD, Helix, Bastile

**Web Servers:** Apache, IIS

**Vulnerability Scanners:** Nessus, Wireshark, Netcat, GFI LANGuard, Retina, X-scan, Sara, Snort

**Application Specific Scanners:** Spike proxy, Paros, WebScarab, Nikto, Whisker, Watchfire's AppScan

**Linux Server Audit/Security Tools:** Nmap, rkhunter, chkrootkit, logwatch, PGP, portsentry, spamassassin, tripwire

**Firewalls:** Netfilter, Openbsd PF, iptables, ipchains

**Programming/Scripting Languages:** C, PHP, Perl, bash scripting, HTML, CGI

## EMPLOYMENT HISTORY

| Company Name  | Duration            | Designation                           |
|---|---------------------|---------------------------------------|
| Tech Mahindra (formerly Mahindra<br>British Telecom ) | Aug 2005 – present  | Security Consultant                   |
| Poornam Info Vision                                   | Dec 2002 – Aug 2005 | Senior Software Engineering, Grade II |

## PROJECT EXPERIENCES:

**Project-1:** TechM Security Compliance in offshore migration of BT's International Billing Plus platform

Role: *Security Consultant and Internal Security Auditor*

On-the-job ACCOMPLISHMENTS:

- Subject matter expert for internal line of business clients and external suppliers for security mitigation and maintenance of their internal control environment over data center operations, system development, change management, incident management and contingency planning
- Conducted security workshops for senior managers in this project for the development, implementation, and auditing of security risk management, governance, and security compliance.

**Project-2:** Security Consultant for the Media & Broadcast wing of British Telecom, E-Security Dept, TechMahindra

Role: *Security Consultant*

On-the-job ACCOMPLISHMENTS:

- BT Security Compliance Management
- Creation of Security Policy Document
- Guidance for implementation of the company security policy in the platform and creating the Implementation Matrix
- Meeting compliance requirements of customer, legal and regulatory aspects in relation to information security governance and processes
- Security Improvement Plan for the platform
- Trained BT's system administrators on Server Hardening in Linux and Microsoft servers and Oracle database
- Configuration Management of Servers and Network Elements
- Ensuring BT Security compliant 3rd Party access to the platform

**Project-3:** Performed Security Standards testing and hardening of Linux servers for all the servers in the Content Processing Capability of British Telecom, E-Security Dept, TechMahindra

Role: *Associate Security Consultant*

On-the-job ACCOMPLISHMENTS:

- Performed Functional Security Testing of the Application.
- Audited the Linux servers to check for compliance to the Security Standards laid down by the client.
- Hardened the Linux and Windows 2k3 servers as per the Security Standards laid down by the client.
- Gave presentations to the client demonstrating the defects, their risks.
- Provided consultancy on how to improve the security of the product.

**Project-4:** Security Requirements for NGN systems of British Telecom, E-Security Dept, TechMahindra

Role: *Associate Security Consultant*

On-the-job ACCOMPLISHMENTS:

- Went onsite to understand the requirements of the Client.
- Created Security Requirements for NGN Systems based on the Clients Security Policies

**Project-5:** Next Generation Network Security- Security Policy Compliance Test Execution for NGN Systems in British Telcom, E-Security Dept, TechMahindra

Role: *Assistant Security consultant*

On-the-job ACCOMPLISHMENTS:

- Create security test case designs for NGN System (consisting of databases, operating systems and applications), against each of the functionally testable Security Policies of the Client.
- Perform test execution for web-based applications to check compliance with Security Policies of the client.
- Perform defect discussions with the client and assign priorities and timelines for the fixes.
- Creation of reports and a Security Improvement Plan.

**Project-6:** Functional Security Testing for NGN Applications in British Telecom, E-Security Dept, TechMahindra

Role: *Assistant Security consultant*

On-the-job ACCOMPLISHMENTS:

- Creation of misuse cases
- Security test execution based on the misuse cases
- Check for privilege escalation, sql injections, cross site scripting vulnerabilities, password strengths etc
- Creation of security defect report

- Providing consultancy services on securing the system

**Project-7:** End-to-End Security Test Designs for NGN Broadband and Transfer Engineering in British Telecom, E-Security Dept, TechMahindra

Role: *Assistant Security consultant*

On-the-job ACCOMPLISHMENTS:

- Creation of End-to-End security test case design document

**Project-8:** Server Security Services – Installations Department, Poornam Info Vision

Role: *Team Lead*

On-the-job ACCOMPLISHMENTS:

- Server Security Audit and Vulnerability assessment and port scanning using tools like Nessus and Nmap
- Creating Vulnerability Assessment Reports detailing all the vulnerabilities found and the best solution for risk mitigation
- Linux Server hardening based on the Vulnerability Assessment Report. This included kernel recompilations, patching the kernel, firewall installations and fixing all server issues.
- Identified major server issues and created scalable solutions from an operations perspective

**Project-9:** Linux Server Administration for a web hosting company named Kiosk – Poornam Info Vision

Role: *Team Admin*

On-the-job ACCOMPLISHMENTS:

- Led a 6-member team as team admin, providing quality Technical Support and Customer care for Network Operation Centers & Dedicated Web Hosting companies.
- Resolved all technical server issues with response time 1 hour and 6 hours resolution
- Securing web servers using Iptables, rkhunter, portsentry, logwatch, nmap, tripwire, tcpdump
- Linux Kernel Recompilations
- Apache recompile , php recompile , Firewall installations

#### **WORKSHOPS/TRAINING PROGRAMS ATTENDED:**

- Prince2 Practitioner Workshop – Global Knowledge London; 5 days; May2008
- ISO 27001 Implementation – British Standards Institute; 3 days; Feb 2008
- Certified Ethical Hacking Training; EC Council; 5 days; July 2006
- IT Project Management; IIT Bombay; 6 months
- SecNet- The Computer and Network Security Workshop; IIT Bombay; 5 days; March 2006
- IT Professionals' Conference 2006- IT Security Track; Microsoft; 2 days Feb 2006
- BS7799 Lead Auditor; STQC; 5 days; Dec 2005
- Linux From Scratch; Poornam Info Vision; 5 days; Jan 2004
- Linux Server Security; Poornam Info Vision; 2 days; Sept 2004

**REFERENCES:** Reference can be provided on request