

Sai Prasad Kesavamatham

Objective: Seeking a full time position as a Security Architect that is challenging and allows me to utilize my extensive skills in the area and grow my expertise further.

Experience: 13+ years experience in System and Network Engineering, Architecture and Security. Experience working in strategic and tactical roles, spanning multiple environments, technologies, and organizational boundaries.

Education:

- B.S (Electronics & Communications).

Certifications:

- ISC2 - **CISSP** Certified.
- SANS **Security** - GIAC Certified Intrusion Analyst

Operating Systems and Enterprise Applications:

- Linux (multiple flavors), Windows 2008/200x, Solaris, HP-UX, Novell Netware 4.x/5.x, Terminal Servers, Citrix, Mail Servers, LDAP – Active Directory, NDS.

Skills:

- **Team Lead/Architect** involving analysis, planning, system design, implementation, performance monitoring, OS tuning, security, capacity planning, hands-on-implementation and management of corporate system infrastructures.
- Excellent **documentation and presentation skills**. Experienced in developing Corporate Standard Operating Procedures (**SOPs**), Service Level Agreements (**SLAs**), and **technical papers**. Will provide samples if asked for.
- Very good experience in Technology Evaluation roles. Worked on projects involving Security tools like BigFix, Blade Servers, IP based SAN storage using **iSCSI** technology, directory services, dynamic DNS/DHCP (BIND), mail servers, web servers.
- **Security – Sarbanes-Oxley, IBM internal security standards**, Vulnerability assessment for systems, networks, application & web infrastructures using tools like **nessus, nmap, Firewalk, SARA, ssh, hping2, httptunnel, ethereal, ettercap** etc.
- Risk evaluation and developing security standards, policies and procedures for infrastructure security as per CIS (Center for internet security) standards.
- **Dynamic DNS (BIND), DHCP (NetID/QIP), WINS, Active Directory Integration, IIS, Apache, and NTP.**
- **Email** systems using Unix Courier mail server, SMTP, Microsoft **Exchange 5.5, 2000/2003. Web and Email security** using OpenSSL and Microsoft **Certificate Servers, PKI, SSL, SSH, sudo, IPsec.**
- **Firewall** filtering using Linux IPTables/IPChains, Microsoft IAS and Cisco **router ACL's.**
- Host based intrusion detection systems (**IDS**) using UNIX, Windows 2000, Netware auditing systems and tools like **sudo, snare, tripwire.**
- **Network IDS (Intrusion Detection)** using **Snort and ACID** (Analysis Console for Intrusion Databases).
- Comfortable with MySQL, Sybase, Oracle and MSSql databases and CGI programming.
- **Monitoring** tools using **Sun SMC, MRTG, Sniffer Pro, Ethereal, SNMP, Perl** scripting.
- Load balancing and fault tolerance using **Sun B1600 B10n** and BigIP/3DNS.
- Proficient in **TCP/IP, UDP, SNMP.** Good understanding of **Routing Protocols, VPN.**
- **Disaster recovery** architecture and run book experience for active directory, enterprise DNS, file servers, network redundancy.
- Research and perform feasibility testing on system architectures, security and future technologies.
- **Published** articles on security at SANS.

Professional Experience:

IBM, Foster City (Information Security Specialist)

March 06 - Present

As part of corporate security team for server security compliance I work as a liaison between corporate business control, local security teams and local admin managing servers and networks.

- Enforce IBM security standards across multiple server platforms.
- Perform security reviews on existing and newly built servers.
- Develop and implement security policies, procedures and system, network audit procedures for local centers.
- Act as subject matter expert on system and application security.
- Work with Business Controls group to perform peer review audits.
- Develop presentations and conduct security awareness trainings for server administrators and business groups.
- Use other security compliance tools like BigFix, Nessus.

Levi's, San Francisco (Sr. SOX Application Remediation Consultant)

Sept 05 – Feb 06

Developed global security policy for applications and created corresponding process and procedure documents. Worked with multiple business units, application architects, internal audit team and IT teams in assessing the business work flow and gap analysis. Conducted presentations to technical and business groups on business processes and other SOX security related processes.

VMWare Inc., Palo Alto, CA USA (Sr. SOX Auditor)

Mar 05 – Aug 05

SOX internal readiness project: Work involved identifying existing IT and business process flows, identifying gaps, creating SOX matrix templates and working with the internal groups for risk remediation to get certified for the external audit. The major domains were IT infrastructure security, Program development, Change control management, operations and IT organization policies and business alignment. Work also involved developing information security best practices, polices, procedures where needed.

Gap Inc., San Bruno, CA USA (Sr. SOX Consultant)

July 04 – Dec 04

Worked on development and implementation of SOX 404 compliance for enterprise IT Security. Worked closely with OS, application and vendor groups.

- Identified and assessed SOX IT controls based on COSO/COBIT framework.
- Worked with business process owners, platform owners and vendors and identified application processes within the financial footprint.
- Conducted risk assessment audits and developed security standards and policies across UNIX, windows active directory, mainframe and intrusion detection platforms.
- Developed policies and procedures where needed to comply with Sarbanes-Oxley standards.
- Conducted risk assessment and created tactical and strategic remediation plans along with self-audit procedures. Developed and implemented remediation plan for security incidents under risk management.

- Worked with identity management group to resolve security issues within the integrated ldap authentication system.

State Street Global Advisors, Boston, MA USA (Sr Consultant)

March 03 – June 04

Worked on multiple projects involving Security, Enterprise DNS/DHCP, Sun B1600 Blade Servers & B10n load balancers, Disaster Recovery, and developing Service Level Agreements (SLA) & SOPs. Worked on technology evaluation projects like UNIX patch management, iSCSI technology, NIS to LDAP migration.

Security

- Involved in creating and reviewing security policies, certification procedures and other security standards for UNIX systems. Actively involved during the IT auditing phase.
- Enterprise DNS/DHCP and DR*
- Implemented DNS/DHCP and disaster recovery migration project on Nortel NetID and Oracle database..
- Active Directory 2003 Services Design*
- Worked with the Windows group and developed active directory services design and implementation plan. Tested certificate servers and digital certificates.
 - Developed Standard Operating Procedures and Service Level Agreements for the Unix group.

Lucent Technologies, NJ, USA (Sr. Security Consultant)

Feb '02 – Jan 03

Worked as a windows NT/2000/IIS server security consultant at Lucent Technologies. Developed and implemented security and disaster recovery procedures for Windows 2000, active directory, IIS and Terminal Servers.

Providian Financial Corporation, CA, USA (Sr. Architect)

Oct '00 - Dec '01

Designed, developed, tested and implemented a high availability Enterprise Dynamic DNS/DHCP infrastructure compatible with the legacy DNS/DHCP systems and Microsoft Active Directory Services using Nortel Network's NetID and Oracle. Integrated legacy DNS, DHCP systems across US, Europe and Argentina.

Arsin Corporation ITS, CA, USA (Team Lead)

Mar '00 - September '00

The work environment consisted of Windows NT 4.0, Sun Solaris, Linux servers and Cisco routers. Designed and implemented corporate VPN. Evaluated, tested, designed and implemented Microsoft Exchange Server 5.5. Evaluated, tested and implemented BIG/IP load balancers from F5 networks for e-commerce web servers.

Bank of America, CA, USA (Consultant)

Sep '98 - Feb '2000

Worked as a Consultant as part of the DNS/DHCP (QIP) design team. Worked on development and integration of corporate DNS domain structure for the Nations Bank and Bank of America merger. Developed Perl scripts for Cisco router configuration and monitoring.

National Semiconductor, ME, USA (Systems Administration)

Feb '97 - August '98

The work environment consisted of Windows NT 4.0, Citrix WinFrame, Novell Netware 4.1, NDS and Lotus Notes. I was involved in the Planning, Design, Implementation and Administration of Windows NT 4.0, WinFrame, Novell Netware 4.1, NDS and Lotus Notes servers.