Objective:

11 years of experience in IT Network/Cyber Security projects and operations, played key role in design & implementation projects, Security operations and migration projects. Performing Security Administrator, Security Consultant, Security Architect, Team Lead, adapted to various roles and opportunities provided to me. Whether leading or managing teams/ or project or technically supporting, I will continue to work hard in achieving goals and objectives in an IT Security for the organizations.

Experience Summary

* Accomplished successfully various Transition, migration and implementation Projects in IT Security both at Onsite and Offshore.
* Insightful knowledge of business process analysis and design, re-engineering, process rationalization, cost control, capacity planning, performance measurement and quality.
* Understanding the problems & requirements, initiating, planning Scheduling, executing, monitoring and control of the project.
* Strategic management of IT Security matters, launching and driving new IT infrastructures project initiatives, negotiations with customers, building good relationship and reputation with customers to create positive business environment.
* Keeping track of the progress of project tasks and deliverables as per schedules and reporting to management stake holders.,
* Managing required skills and resources, work hours calculations and costing as per the project requirement.
* Achieved successful relocation of company Data centre to new building/facility with zero downtime.
* Worked in process management on ITSM tools HP SM 7, VMware SM9 and BMC Remedy as per ITIL.
* Involved in setting up and drafting IT Security Policies and Risk control mechanism for the enterprise.
* Drafted Boundary Standards for reference for all network and security devices policy configurations.
* Documented Detailed Design Specification, Method Statement and Factory Acceptance Test (FAT) for Network Security Project.
* Set a Critical IT assets/facilities security policies management and implementation of safeguard recommendations.
* Security patching, Windows Patch update management &secure access control mechanism.
* Monitoring and providing analysis of logs on various Windows Servers, Security devices and applications in the network.
* Risks, threats, vulnerabilities assessment and cyber attacks by performing security tests investigations.
* F5 Load Balancers LTM/GTM, implementation, configuration, administration and Operations.
* Managed RSA Token Server, authentication issues, replication issues among server clusters.
* Access control mechanisms on Juniper SSL VPN on Juniper SA6500 and Token Authentication.
* Configured Authentication Realms, User Roles and Resource Policies on Juniper SA6500.
* Worked on Skybox and AlgoSec with Firewall assurance, Network Assurance and Risk Control modules.
* Firewalls (including industrial firewall) implementation, configuration, management, administration and Operations.
* IPS/IDS/NIPS/NIDS/HIPS implementation, configuration, management, administration and Operations.
* Anti-Virus Server implementation, configuration, management, administration and Operations.
* Content filter and Web Security tasks like Blacklisting /White listing and URL re-categorization.
* Proxy Servers implementation, configuration, management, administration and Operations.
* Monitoring on various monitoring tools like Nagios, Cacti, etc.
* Monitoring and analysing critical alerts and warnings from SIEM tools, coordinated with teams to resolute against them.
* Installed and configured VMware, virtual box, on Linux and Windows machines.
* Managed DNS, DHCP, Active Directory, Domain Controller and Patch management server WSUS.
* Routers, Switches and VLAN configuration, management and administration.

**Professional Certifications**

* Cisco Certified Network Associate (CCNA)
* Cisco Certified Network Professional (CCNP) – Routing
* ITIL V3 Certified.

Professional Trainings Attended

* Trained in CEH, and CISSP
* Trained in Six Sigma, PMP, Strategic Management & Agile Management.

Achievements

* Successfully completed transition project for the certain Security services for the UK’s leading Bank.
* Achieved successful relocation of company Data centre to new building/facility with zero downtime.
* Successfully implemented the Symantec Endpoint Protection Antivirus server (SEPM) and done migration from 11.0.7 version to 12.1.4 version.
* Successful implementation BIG IP F5 LTM (Local Traffic Management).

Education

* **B.E (Mechanical Engineering),** BVB College of Engineering & Technology, Hubli, India.

Technical Summary

|  |  |
| --- | --- |
| **Skills** |  **Tools/appliances/Software** |
| **Management**  | Project management, IT Security management, IT Security Operations, Team Management, Project Life Cycle. |
| **Security Standards** | PCIDSS, ISO 27001 |
| **Security Appliances** | * Load Balancers: BIG IP F5 LTM/GTM/ASM, Radware LP100, Juniper SA6500
* Firewalls: Cisco PIX, ASA, Checkpoint Firewall, Netscreen (SSG/SRX), Cyberguard, Fortigate Firewall from Fortinet, MCafee Firewall, Palo Alto.
* Industrial Firewalls: Tofino firewalls (for Modbus and OPC)
* IPS: Sourcefire 3D ,TippingPoint, ISS Proventia IPS GX3002, RealSecure Server Sensors, Trend Micro HIPS agents
* NSM for Juniper firewalls version,
* Anti-virus Servers: Symantec Endpoint Protection Servers, Sophos, F-Secure, Trend-Micro and Mcafee EPO.
* Web Proxy/Filter: Mcafee WebWasher, Cisco Scansafe content filter, IronPort.
* Proxy: Bluecoats SG 300, 600.
* Auth. Servers: RSA Token Servers, 4Tress Active Identity two factor authentication servers. Juniper SA6500 (Juniper Pulse Secure Access Service).
* Monitoring: Nagios, Cacti, SolarWinds, Splunk
* SIEM: QRadar, ArcSight
* Servers: Active Directory server, GPO, WSUS server, IIS Web services.
 |
| **Operating Systems** | * Windows XP, 7, 2008, 2012 & Linux Fedora, CentOS, Ubuntu, BackTrack, VMWare
 |
| **Cisco Routers/Switches** | * Routers 2801, Switch 3560, 6509 & 6513-E
 |
| **VAPT/RA Tools** | * Wireshark, QualisGuard, Nmap, Nessus, ColaSoft, Metapoilt, AlgoSec, Skybox
 |
| **ITSM Tools** | * BMC Remedy, HP SM7
 |
| **Other Used Support Tools** | * MS Project 2010, MS Visio
 |

Work History

|  |  |  |
| --- | --- | --- |
| **Duration** | **Organization** | **Designation** |
| Feb 2016 – Till Date | Yokogawa Middle-East and Africa. UAE | Senior Network Security Engineer |
| July 2014 – Feb-2016 | Tech Mahindra Ltd. | Associate Security Architect |
| April 2011 to July-2014 | Wipro Technologies Ltd. | Senior Systems Engineer. |
| Nov-2010 to April-2011 | Software Paradigm Infotech. | Senior Network Engineer |
| March-2009 to Nov-2010 | Stoke Networks Ltd. | Network Administrator |
| May-2008 to March-2009 | Arctern Consulting Pvt .Ltd. | IT Network Engineer. |
| May-2006 to April-2008 | Network Solutions, An IBM Company. |  Network Engineer. |
| June-2005 to March-2006 | Zee Networks. | Technical Support Engineer. |

Work Experience

## Company: Yokogawa Middle East and Africa. (Feb 2016 – Till Date)

**Role : Senior Network Security Engineer**

**Project Client : CBDC-Ruwais/Yokogawa office Musaffah Abu Dhabi - UAE**

Responsibilities:

* Defined the required Skills, resource requirements and schedules deadlines of the project according to the clients’ objectives.
* Created alternative acceptable low-risk strategies for the customers. Coordinated with other teams & stakeholders to list out required tasks and activities in order to ensure the successful completion of the project.
* Led the Project in achieving the objectives and deliverables as per the schedules and contributed in achieving it within the specified budget.
* Documentation of Detailed Design Specification, Method Statement and Factory Acceptance Test.
* Providing Technical Guidance and support to team whenever needed.
* Led the team to perform the tasks of configuring devices and appliances during implementation as per Design.
* Managing weekly meetings with customers and reporting the progress and status of the project work.
* Responsible to complete the Pre-FAT/FAT/SIT and getting closed all the punch points.
* Responsible for planning and executing the implementation as per Design Specification at the site.
* Complete the Site acceptance tests (SAT) after implementation.

## Company : Tech Mahindra (July 2014 – Feb 2016)

**Role : Associate Security Architect**

**Project Client : SOMC (Sony Mobile Corp.), LUND - Sweden**

Responsibilities:

* Successfully accomplished new project transition of Technical Support and Operations Services to Offshore.
* Achieved reduction in the operations cost and achieved high quality of operations and technical support.
* Due Diligence (DD) and DD Report presentation, Knowledge Transfer (KT) Planner and KT completion at LUND, Sweden(Onsite)
* After completion of Knowledge Transfer (KT) trained the Team members at Offshore to set-up the 25 member team to provide 24x7 Support from the Offshore.
* Provided the training on ITIL process as per Sony Sweden environment and also provided hands-on training on technologies F5 load-balancer (LTM and GTM), AlgoSec firewall Analyzer, Bluecoats Proxy, Juniper SRX, Checkpoint and Mcafee Firewalls.

**Project Client : Solenis Inc. (Solenis Security Management), Philadelphia – USA.**

Responsibilities:

* Successfully completed planning, designing, providing various network security architecture options to customer based on the requirements and budgeting/costing involved in Project.
* Accomplished the implementation of Network Security devices for Solenis as separate infrastructure carved out of ASHLAND Corp.
* Accomplished migration of Symantec Endpoint Protection Anti-Virus security at enterprise level for Solenis.
* Completed implementation of Firewalls, Bluecoats Proxy SG, URL filtering, IPS/IDS and WAN Optimization.
* After the implementation is completed, handover to Operations Management team after training the Operations team personals.

## Company : Wipro Technologies (April 2011 - July 2014)

**Role : Senior Systems Engineers**

**Project Client : Affinia Group.**

Responsibilities:

* Symantec End-Point Protection Security Anti-Virus Server (SEP) move from one datacenter to another datacenter and migrated from SEPM 11.0.7 to 12.1.4 version.
* Improvements in existing security policies based on the analysis of existing network and security infrastructure.
* Drafting a Boundary Standards Security Policies reference document for various network and security devices/applications for identifying various vulnerability, threats and possible risks in the network.
* Managing Symantec Endpoint Protection environment complete activities after implementation including new security policies once SEPM server move is completed.
* Monitoring the Antivirus server operations like monitoring critical alerts for infections, new updates on SEP, generation of reports on daily & weekly activities on SEP Servers and forwarding the details of infected host machines with file path and location of non-quarantined or undeleted viruses in the network to L1/local support/desktop engineer to manually delete/remove.
* Implementation of industrial Tofino Firewalls, Active Directory services management and Administration.

## Project Client : LLOYDS BANKING GROUPS, Manchester- United Kingdom

Responsibilities:

* Involved in Transition of certain Security services were after having worked at onsite and then created new team at offshore.
* Skybox risk and network security analytic application
* Firewall Assurance, Risk Control and Network Assurance models of Skybox.
* Involved in identifying possible risks, threats and vulnerabilities on various network and security devices or applications and reporting the same to next level after analysis with possible solution.
* VAPT about Client-Servers, Webservers & WEB Application, & systems in LAN, Sniffing- WireShark, Colasoft packet crafter, Smart Sniffer and monitoring system, etc.
* Skilled in NMAP, Nessus, Wireshark, QualisGuard, scanner, for Scanning a system, network and websites to get the vulnerability.
* Access control mechanisms on Juniper SSL VPN on **Juniper SA6500** and Token Authentication.
* Configured Authentication Realms, User Roles and Resource Policies on **Juniper SA6500.**
* Involved in configuring and implementing Host Checker Policies/ restrictions on **Juniper SA6500.**
* RSA Token Server looking into the issues related to replication among the RSA server’s clusters.
* Troubleshooting the RSA token authentication issues with RSA token users.
* 4Tress Active Identity two factor authentication server used for internet Banking Users.
* Investigations and Security auditing on windows servers, Security applications Devices.
* Monitoring and Analyzing logs on Windows Servers, Security devices and applications in the network.
* IBM IPS appliances Proventia Network IPS GX3002 and HIPS RealSecure Server Sensors.
* Involved in log analysis on NIPS, HIPS and firewalls to identify the unknown sources, destination and services to decide Block/Unblock.
* Process management on ITMS tools HP SM 7

## Project Client : CA-CIB (Credit Agricole Corporate & Investment Bank) Security Operation, Singapore

Responsibilities:

* Monitored security critical alerts & warnings for security devices in the network of CACIB across the globe.
* Managed incidents, requests for changes, service requests, DRP activities & daily routine action against new infections and treats post analysis of logs on various security devices.
* Consolidated rules & policies on the firewalls, guided local teams in various branches across the globe to remove identified infections like malware, Trojan horse, root kits, etc, on Sophos antivirus solution.
* Identified, analyzed & reported various possible treats from critical/blocked traffic on IPS across the network.
* Performed day to day routine activities & security checks of all architectures in the network across the globe.
* Planning/approving/implementing improvements in process, practice and procedures in security operations and reporting RCA (root cause analysis), PM (Post Mortem) for high priority incidents.
* Initiating CAB meetings with all the stake holders to discuss the change related risks, schedule, tasks, teams, etc.
* Assessed threats & vulnerability for critical assets/facilities and implemented safeguard recommendations
* Configured site to site VPN tunnels between new project offices, recommended security policies and processes after evaluation.
* Successful implementation of **BIG IP F5 LTM,** configured QoS and other necessary features for load balancing.
* Configured nodes, load balancing pools, pool members and profile on **F5.**
* Performed various tasks like renewal of SSL certificates for websites, deleting adding pool members on **F5.**
* Managed PROXY services like adding/removing URLs on Blue Coats Proxy servers.
* Managed DRP activities with key role in planning, scheduling & coordinating critical operations in IT security.

**Project Client**  : **COMCAST\_RCM\_CONSULTING (Security consulting), Pune - India**

Responsibilities:

* Involved in mapping, scanning, remediation and reporting on QualysGuard.
* Generated reports of critical & warned alert for hosts post scan and recommended solutions for identified vulnerability assessment and analysis of scan results.
* Assess threats & vulnerabilities for critical hosts and provided safeguard recommendations.
* Critical IT assets/facilities security policies management and implementation of safeguard recommendations.

**Project Client**  : **BRITISH PETROLEUM (Firewall Operations Team), Bangalore-India**

Responsibilities:

* Monitor & analyze logs from security devices, assess vulnerabilities & threats, report to system administrators on possible potential risks and Cyber attacks, suggest and assist for solution to terminate possible threats.
* Making report on Vulnerability Assessment and Penetration Test with the help of scanning & pen test tools like nessus, metasploit framework, specially configuring Clustering & VPN and IDS/IPS SourceFire.
* Access control mechanisms on Juniper SSL VPN on **Juniper SA6500** and Token Authentication.
* Configured Authentication Realms, User Roles and Resource Policies on **Juniper SA6500.**
* Involved in configuring and implementing Host Checker Policies/ restrictions on **Juniper SA6500.**
* Administer Sourcefire IPS DCs & Sensors, upgrade software version of DCs & Sensors, update Sourcefire SNORT Enhanced Updates (SEU) and emerging threats on sensors.
* Add/ delete sensors in network based on requirements, liaise with vendor for hardware/ technical issues, health checkups and maintenance of IPS sensors.
* Manage changes, requests & incidents on various security devices in the BP network.
* Planned/implemented improvements in process, practice and procedures in security operations and reporting RCA (root cause analysis), PM (Post Mortem) for high priority incidents whenever demanded by stakeholders.
* Ensure smooth functioning of HIPS application environment (Manager and Agent state).
* Deploy new version of software (DSM & Agents), install and configure HIPS Agents.
* Update DPI Attack Signature & Integrity Monitoring Signatures; manage remedy ticket management for monthly MS patch updates on Trend Micro HIPS agents.
* Work on McAfee ePolicy Orchestrator as the end point security solution in PCN environment, protecting primarily servers, Microsoft Windows Server Update Service (WSUS), patch management solution for windows system in PCN Environment.
* SaaS based solutions Scansafe (Wired BP Network, old Websense Coverage) & OpenDNS (Wireless Networks).
* Monitor Scansafe, OpenDNS & IronPort events; liaise with vendors for re-categorization, white listing, blacklisting & blocking URLs.
* Monitored and analysed critical alerts/warnings on ArcSight SIEM & coordinated with team to resolve against them
* Documented new architectures & networks, policies, processes and configurations.
* Configure site to site VPN tunnels between new project offices, recommending security policies and processes after evaluation.
* Process management on ITMS tools BMC Remedy.

## Company: Software Paradigm Infotech, Mysore (Nov 2010 – April 2011)

**Role : Senior Network Engineer**

Responsibilities:

* Performed security reviews on system development projects and servers prior to commissioning for production environment.
* Assessed & reviewed existing technology of infrastructure to identify key risk areas, ensured availability of adequate levels of controls.
* Designed & implemented network & connectivity to new client locations, based on requirements without compromising on security.
* Planned critical operations & functioned as primary client liaison for one or more concurrent engagements.
* Configured & managed VPN tunnels to various branches and clients across the Globe on various Cisco devices.
* Worked on local proxy server to control user accessibility to various sensitive data resources, configured managed VLANs and ether-channelling on Cisco Switches 3750, 3560 and 2900 in the network.
* Initiated technical and management documentations of all implementation, configurations, changes and incident management, improvement plans and procedure for IT security team operations.

## Company: Stoke Networks Ltd. Bangalore (March2009 – Nov 2010)

**Role : Network Administrator**

Responsibilities:

* Initiated and scheduled weekly meetings on improvements and progress in various IT management related activities.
* Achieved Asset/Data Security at highest by introducing security policies and its awareness among end-users.
* Vigilantly performed packet analysis and traffic monitoring to avoid DoS/DDoS attacks and network slowdown.
* Responsible as a single point of contact for all communications related to test lab and network management, license management of software and hardware including IT infrastructure related purchasing in India as per the specified budget.
* Spearheaded team efforts in relocation of company to new building with zero down-time with planned, designed and provided guidance to structured cabling teams to complete the network cabling of new datacenter and Test lab as per the drawings.
* Maintained stable internet, Intranet and Lab environment in the network and assisted the Test engineers’ team in facilitating the test-lab environment according to their requirements.
* Managed & configured site to site IPSec VPN tunnels for all branches on Juniper Netscreen Devices like Netscreen 204 and Netscreen 5GT.
* Managed disk space and quota on NAS (Network Attached Storage) from SANAT integrated with NFS.
* Worked on terminal servers like Cyclades & Cisco AS2511to provide SSH console access to Test LAB devices.
* Achieved systematic management of complete enterprise network by maintaining IP network/subnets and proper VLANs on Cisco L3 3560 and 6509, high-end network issues to User-End local workstation issues.
* Managed Symantec Antivirus server, virus count, DNS (FreeBSD), DHCP (Medusa Linux servers in the network).
* Managed Virtual machines installations on both Windows and Linux operating systems.
* Administration in heterogeneous environment of various flavours of Linux OS and Windows OS.

## Company: Arctern Consulting, Bangalore (May 2008 – March 2009)

**Role : IT Network Engineer**

Responsibilities:

* Proven ability to achieve results in very high pressure environments and to keep teams motivated
* Ensured internet connectivity & implemented new equipments for enhanced network performance.
* Created and reported daily status reports of the network-security devices and applications, latest virus infections, bandwidth utilization, possible vulnerability and risks to IT manager.
* Proven ability to achieve results in very high pressure environments to keep teams motivated and coordinated with teams from other branches to resolve network and security related issues during the crunch times.
* Configured site to site IPSec VPN tunnels for all the branches on Cisco 2801 routers, Cisco ASA 5510, for director’s home offices on Cyber Guard Firewall/Routers, Easy-VPN on Cisco ASA 5510 for providing connectivity for end users from anywhere in the world to Head office.
* Managed DSL & leased lines connections from different ISPs on LinkProof Load balancer from Radware for link load balancing, High availability, ISP failover and Bandwidth management.
* Configured Cisco Router 2801 and Cisco ASA 5510 Firewall from the scratch.
* Managing and implementing future plans and decisions on network related matters for new office branches.

## Company: Network Solutions, an IBM Company, Bangalore (May 2006 – April 2008)

**Role : Global Support Engineer**

Responsibilities:

* Coordinated with customers in resolution of connectivity related issues.
* Monitored Network Links and traffic flow at the Interfaces of the core Routers.
* Worked on rules & policies changes on check point NG firewall through Smart Dashboard.
* Focused on system administration with regards to account management, object and password management.
* Rendered technical support for remote laptops with Win XP for onsite users.
* Installed & configured VPN agents, Mail Clients like MS Outlook, on office Laptops & Blackberry device.
* Updating Windows OS patches, Anti-virus version and other office application as per security policies.
* Maintained virus counts in the network, synchronization of RSA Secure Id Token and authentication issues.

## Company: ZEE Networks, Bangalore (June 2005 – March 2006)

**Role : Hardware & Network Engineer**

Responsibilities:

* Lead the sub teams in achieving the reduction in downtimes in cable modem and corporate customers.
* Managed escalated calls from Level 1 engineers and customer support team.
* Liaised with RF team and maintained leased line/fibre link of corporate customers.
* Worked on BGP on Cisco 7200 series, Cisco Routers 7204vxr, 2801series & switches, various WAN.
* Monitored network devices status on WhatsUp Gold, Nagios and MRTG.
* Focused on Bandwidth & User account management using Quipus (Linux) Server.
* Assisted customers in resolution of issues with internet connectivity and restored to normal.