**AMITJAISWAL**

**Email : jaiswalamit1242@gmail.comA picture containing text, clipart

Description automatically generated**

**Mobile : +91-7045361311**

**Experience : 8+ Years**

CAREER VISION

An IT Security professional with 8+ years of experience in Information Security with core competencies in design & planning, implementation, custom content development and consulting. An excellent communicator with exceptional analytical, relationship management and coordination skills and has consistently met project delivery targets and exceeded customer expectations.

TECHNICAL SKILL

Area of expertise includes NGFW (Checkpoint, Fortinet, Palo Alto, Cisco ASA, etc.), Sand-Boxing, IPS(Trend Micro,McAfee ) VPN, F5 LTM/ASM/APM and Radware SLB, Proxy (Bluecoat, Z-Scaler), Networking Monitoring tools, SIEM and is also well exposed to other areas like ISO-27001(ISMS,Auditor),NIST(Cyber Security Framework),PCIDSS Standard, HIPAA ,CMM-L5,ITIL Process Management, Threat analysis using Mitre Attack,Unit-42 ,FireEye Mandiant tools and well under usnder stand GRC,GDPR.

* Router& Switch - Cisco ASR& ISR cisco1800, 1900, Cisco Switch 3750, 2960, 2950.
* NGFW: - Checkpoint 12200,4600,4800, Cisco ASA 5555 5020, 5010, Palo Alto 3050,500,200, CYBER OM, FortiGate FIREWALL.
* Protocol: - TCP/IP, DHCP, DNS, WINS, MPLS, NNTP, POP3, TELNET, IPsec, IKE, AH, ESP, SMTP, RIP, OSPF, BGP, IPSEC, FTP, HTTP, HTTPS

Technologies: - F5 Load Balancer LTM, F5 SSL VPN APM, Blue Coat Forward Proxy ASG-S400, F5-ASM(WAF), Imperva WAF, Trend Micro IPS McAfee NIPS, Cisco Source Fire, McAfee HIPS (ePO), McAfee DAM, PIM Arcos,FIREEYE HX & EX , SMOKESCREEN Technolgy

* OS: Linux. Tools – Basic knowledge on Algosec, Basic Knowledge on Splunk
* CISSP Training Competed andpursuing CISSP Exams

**Experience Summary**

**KEY PROJECTS Implementation:**

**Project: Palo Alto & F5,Bluecoat Implementation, Upgradation and Migration**.

Kotak Life Insurance: Migration as well as new installation Firewall.

Kotak Life Insurance: Remote access VPN Migration on F5 APM SSL VPN

Kotak Life Insurance:LB Migation on F5 LTM from Bluecoat .

Central Bank of India (RRB): Checkpoint deployment and Migrate checkpoint from CISCO ASA

Central Bank of India (RRB):PIM Implementation( Arocss)

Credit Agricoal(French Bank): Security Gateway, Management server,

**Experience on Oprerations Project :**

**CHECKPOINT, CISCO ASA, PALO ALTO, FORTIGATE FIREWALL:**

* I have hands experience on multiple firewall technology for example creating access rule ,type of nat rule on multiple firewall, creating site to site VPN and remote access VPN on multiple firewall, configuring device setup and os upgradation and Hotfix ,high availability configuration and troubleshoot ing on mentioned firewall.

**F5 TECHNOLOGY & IMPERVA WAF:**

**F5 LTM**: Configuring the multiple method for load balancing the traffic and creating policy for redirection the traffic and configuring required multiple types of profiles (SSL Profile, Persistence Profile) and device setup configuration and os upgradtion and Hotfix.

**F5 APM**: Configuring the SSL VPN based on customer requirement and changing the visual Policy editor on demand client and also configuring the application tunnel device setup and os upgradation and Hotfix.

**F5 ASM/ Imperva WAF:**configuring custom security policy and integration certificate according to application and customer requirement and analyse the traffic logs base on signature and configured policy based on different required action Mode ( Simulation and Production) and protecting the application.

**BLUECOAT PROXY: SG-300, ASG-S400 & Zscaler Proxy:**

* Changing the configuration on Proxy based on Customer requirement (DNS Configuration, Authentication Method, interception the traffic, host forwarding, intelligent inspection of Bluecoat) and configuration VPM policy based on user requirement and Upgration device.

**IPS TECHNOLOGY: McAfee NIPS, CISCO SOURCE FIRE, PALO ALTO THREAT PREVENTION, CHECKPOINT THREAT PREVENTION TREND MICRO IPS:**

* Creating IPS Policy or Security Profile based on customer requirement and working and changing the Signature action based on security requirement and analysis the logs and making report of on demand.

**DATA LEAK PREVENTION (McAfee DLP) and DATABASE ACTIVITY MONITORING (McAfee DAM):**

* Creating custom Policy or applied default policy based on customer requirement and generating the report.
* Creating the custom Rule for DBMS group or applied default DBMS Group and integrating the install sensor with DBMS Server and analysis the logs and generating report for user activity on database.

**PRIVILEGED IDENTITY MANAGEMENT (ARCOS PIM)**

* Creating the user or user group on PIM and Providing the access for specific server or server group created.
* Created password vaulting on PIM
* Providing the role for user to accessing the server based on demand customer.
* Analysis the text logs or video logs on PIM.

**CYBER SECURITY EXP : MITRE ATT&CK, FIREEYE EDR SOLUTION SMOKESCREEN,GITHUB, MANDIANT AND ELASTIC & VT SCAN AND MULTIPLE TOOLS FOR Threat Intelligence**

* Analysis the Malicious file or Malware ,Trojan Virus based on hash value ,file extension with muliple tools and work with Fireeye Tac and Symantec Tac for detection.
* Analysis the various types of Cyber Attack using Mitre att&ck navigator (TTP) Method and research on Elastic site and github attomic site and many more open source for code of executions and attack method and creating indicator of comromise (IOC) also Using Mandiant Technology for IOC Creation and applied on FireEye HX and Symantec AV .
* Analysis Phising email attack anlysis the attachment or link on multiple open re-source and fix on FireEye EX or Malicious URL fix on Bluecoat Proxy .
* Working on SMOKESCREEN Deception technolgy and creating Decoys in network on demand of customer requirement for prevent the attack on basis of multiple types of decoys in network .
* Understand ISO 27001 ISMS and follow Framework and their Clouse and Security Controls for Compliance.

PROFESSIONAL QUALIFICATIONS & TRAINING

* **Training attempted** :CISCO CCIE SECURITY V-4, Checkpoint CCSA & CCSE . Palo Alto PCNSA Zscaler ZIA Certified
* **Project Exp**: Tricky Solution Dec-13-Jun-15 as support engineer. Dimension Dara-Jul-15-Dec-17 as Security Engineer in Andhra Bank- Project-July-15-Apr-16, Kotak General Insurance May-16-Aug-16,Kotak Life Insurance Sep-16-Dec-17.Wipro Dec-17-Oct-18 Sr Security Engineer in Central Bank of India Project. Capgemini-Oct-18-May-20 as security consultant in a Project Credit Agricol French Bank.
* **Current Company Softcell Technologies global Ltd. (Jun-20-Present): Client is HDFC Bank as Security Engineer.**

**Current Job Profile: BAS operation team & Zscaler Proxy migration from Bluecoat** – Work on FireEYE APT to configured the IOC (Indicator of compromise), To get the alert of Malicious activity. QRadar SIEM for monitoring the logs and investigate.

* Coordinating with Red Team to block the malicious file with the help of Hashes and files.
* Audit purpose IOC and Threat Intelligence.
* Team Lead for Cyber Hygiene team, configuration review, product like Firewall, WAF, IPS, Proxy and Security Analytic.
* Firewall Rule Lifecycle management ,compliance and reporting against firewall rules using Algosec Tools.
* Audit firewall changes for completeness and correctness and ensuring rules are compliant to architecture design and Policies and execute post change review for firewall performing quality checks and reporting to management team and project team.
* and is also well exposed to other areas like

EDUCATIONAL DETAILS

|  |  |  |  |
| --- | --- | --- | --- |
| Education | University | Percentage | Years |
| B.Tech (IT) | SRM University | 66 | 2009-2013(July) |
| HSC | Sarvodaya Inter college (SB) | 70 | 2005-2006 |
| SSC | Sarvodaya Inter college (SB) | 52 | 2003-2004 |

PERSONAL DETAILS

Date of Birth :03-Jan-1989

Nationality : Indian

Passport NO :

Gender : Male

Marital Status : married

Languages Known : English, Hindi ,French(Basics )

Hobbies : Watching Movies, Playing Cricket ,

Place : Mumbai

Date: AMIT JAISWAL