**GAURAV RAMTEKE**

Ghala 2, Flat No. 301, Behind Sheffield School, Al Nahada 2 , Dubai , Dubai  ◆  H: +91 8879675353  ◆  M: +971 501762481  ◆ gaurav.358@gmail.com

 **Objective**

Passionate Thirteen plus years of post-sales, presales and project management experience. Seeking a position that will be beneficial from my strong technical and pre-sales engineering experience to create sales business strategies and develop customer base.
Creative business development and result oriented professional offering, strong decisive executive participation for managing clients with different network topologies, developing customer security environment, SIEM solution architect, professional services, and security operations.

 **Professional summary**

* Lastly associated with Accenture Solution Limited, as Associate Manager. Leading transformational projects in Splunk Enterprise Security and as well involved in the presales activity.
* Technically sophisticated, passionate & result-driven professional working as a presales consultant in Redington Gulf and Certified Splunk Architect handling MEA region.
* Extensive background in complex and challenging environments with proven ability to represent the company with customers and channel partners.
* Other experiences in vulnerability assessment, product level security metrics – Technical Audits, Network Audits, and Datacenters, etc.
* Enthusiastically raise awareness and be able to communicate relevant information, vision, process, and results of the risk at management level in an organization.
* Ability to think independently analyze, troubleshoot and resolve complex technical and administrative problems on any operational level and technology products.

 **Skills**

|  |  |
| --- | --- |
| * Certified Splunk Architect
* Data science - ML and AI - Intermediate
* Phantom SOAR platform - Intermediate
* AWS Cloud and Azure Cloud Services
* Project management, Team liaison, conflict resolution, strong verbal communication, team leadership, customer assessment, and strategic analysis
* Administer all types of Operating Systems mainly Linux and Windows Servers
 | * Administer and manage to troubleshoot complex networking issues
* Shell scripting, Python scripting, Ansible tech
* Firewalls, VPN, Endpoint security, Email - gateway security, gateway proxies etc..
* Database technologies MSSQL, MySQL,and Oracle - Intermediate
* Microsoft IIS and Apache server
 |

 **Work history**

Sr. Presales Consultant, 06/2018 to Current

Redington Gulf Limited – Dubai, Dubai

* Working as a Sr. Presales consultant for Splunk for MEA Region.
* My primary task is to enable local & regional partners, recognize their strengths, build case studies and support them to convert leads and work with them on different opportunities.
* Working on RFP's, designing architecture, filling in compliance sheets, and designing technical proposal for SIEM, ITOPS & Phantom SOAR
* Executing PoC's on Splunk ITSI & ES (SIEM), executing demos\presentation as per the customer requirement, also executing different Splunk partner workshops for their tech hands-on.
* Developing Internal Use cases on Phantom SOAR platform

Associate Manager, 03/2016 to 04/2018

Accenture Solutions – Bangalore, India

* Supported Chief Operating Officer with daily operational functions.
* Managed team of 4 employees, overseeing the hiring, training, and professional growth of employees.
* Associated with the consulting team and working on to deliver \ deploy Splunk Enterprise Security. In a reputed garments brand customer.
* **Client** – Leader in Oil Industries, working as a developer in a (DevOps Team). The solution consists of AWS services, Splunk 6.5, Visual Studio, Ansible - a fully automated solution on AWS using CloudFormation and different types of scripts. Under Agile Scrum methodology.
* Scripting Languages used to design the solution in Python, PowerShell (windows), Linus Bash Shell, PHP, Java, & C++.
* Supported engineers in improving operations and resolving issues to deliver top-notch customer service.

Senior Consultant, 08/2012 to 02/2016

AGC Networks Pvt. Ltd – Mumbai, India

* All projects were offshore (post-sales & pre-sales) projects carried out mainly in the East Africa Region. All projects were single-handedly operated and managed.
* **First Successful Project**: URA – Uganda Revenue Authority (ArcSight 3.0 Express and Connector Appliance 6.3 Implementation and Configuration). Deployed & Implemented in 25 days
* **Second Successful PoC**: Nairobi Waters (Imperva Secure Sphere 9.5 Implementation and configuration). Took 20 days to finalize the PoC. With an appreciation from Director.
* **Third Project Completed**: Imperva Implementation @ URA – Uganda Revenue Authority (Imperva Secure Sphere 9.5 Implementation and Configuration for DAM and WAF).
* **Fourth Project**: PwC Kenya (ArcSight SIEM Implementation) – A total of 9 sites across East Africa Region needed to integrate centrally from Kenya. Completed the project within Project Timelines.
* **Fifth Successful Project**: Imperva virtual appliances Implementation @ Zanaco Bank (Zambia) completed remotely with client appreciation. Concentrated on Database Activity Monitoring.
* **Sixth Successful Project:** Equity Bank Kenya (ArcSight Express Implementation with HA capability): Development of two Flex Connectors required for Banking Applications, End to End Implementation with appreciation from the client. Completed the project within the project Timeline.
* **DTB Kenya**: Complete development of SOC project having ArcSight Express as an SIEM tool, ArcSight Logger as a log management tool and ArcSight Management center as a collector all this environment is configured in HA. Involved in the development of complete security policies and procedures for SOC and took 3 months to complete the project.

Senior Analyst, 09/2011 to 02/2012

Deutsche Bank, DBOI Global Services Pvt. Ltd – Mumbai, India

* An Arcsight Administrator was responsible for maintaining and managing a complete global SIEM solution all the tools like Connector Appliance and ArcSight Software Logger Consulting, ArcSight Flex Connectors Development, Implementation, Security Monitoring, Security Log Analysis, and BCPDR activities.
* Supporting and Maintainance of Arcsight Infrastructure.
* Onboarding of different devices into Arcsight for Security Monitoring.
* Arcsight Infrastructure Enhancement.
* Client Query/Issue Resolution.

Security Engineer, 08/2010 to 09/2011

Paladion Networks Pvt. Ltd – Mumbai, India

* L2 in Managed Security Services (MSS). The client was SBI Life.
* Enable auditing on end devices like ASA, Checkpoint, Oracle DB, Symantec Antivirus, MSSQL DB and Windows 2k3 and 2k8 Servers,etc.
* Conduct root-cause analysis and advise SBIL on corrective action.
* Provide telephonic & onsite support for resolution of the alerts and implementation of the corrective actions.
* Weekly call with management team on the work done.
* Tracking new global threats (attacks, worms & viruses).
* Advisories on trend, threats, vulnerabilities and security patches.

Senior Security Engineer, 03/2008 to 02/2010

MIEL e-Security Pvt. Ltd – Mumbai, India

* Handled multiple client-side projects on different products like Antivirus, Email Security Gateway, Firewalls, NIDS & HIDS.
* Doing health audits for security products and submitting reports for management view.
* Selected as a team lead in evaluating different SIEM Solutions for best fit into MIEL newly formed SOC department. After 3 Months of research done on Symantec SIEM, RSA Envision SIEM, Open SIEM we have decided to go ahead with ArcSight ESM 4.5 SP1 SIEM tool for MSSP Services.
* Monitoring and reporting of critical security incidents on perimeter devices and mitigate them with the proper clearance and SLA.
* Good Knowledge in multi-threaded FortiGate-620B Firewall.
* Excellent knowledge in security products such as •Antivirus: Trend Micro OfficeScan 10, Symantec Endpoint protection 11, McAfee ePO 4.0 and Trend Micro Control Manager (TMCM).
* Gateway level products: Trend Micro IMSS, Trend Micro SMEX, ISA 2005 and Firewall.
* Good knowledge of VMware ESX 4.5 server – Installation, Configuration of LAN and familiar with commands.
* Ability to do a vulnerability assessment and penetration testing for both internal and external stand-alone systems as well as a network of Windows Server, Linux server and IIS Web Servers.
* Well versed with installation and advance level troubleshooting for Microsoft flavor and Linux flavor operating systems.

Senior Technical Executive, 03/2005 to 11/2006

Rincon India Solution Pvt. Ltd – Mumbai, India

* Third-Party Software Solution firm of Captaris, Products like RightFax, Alchemy (Document Management) and supporting software.
* Supervised field engineer and handled customer problems related to software, servers, and hardware.
* Responsible for managing an administrative task and implement them on the client-side. Manage installation, configuration, troubleshoot and executing customer training.
* Worked with Active Directory, Lotus Domino and Exchange server 2003.
* Projects Undertaken - More than 15 projects managed on RightFax.

System Admin, 04/2004 to 11/2004

Wipro – Mumbai, India

* Franchise Support Engineer in Wipro from MACRO Academy. (No documents available to support this experience only have an ID card as proof)
* **Help Desk Support**:- All problems related to the system and other resources on the network were logged with me.
* Responsible for managing, maintaining and configuring all network systems like printers, scanners, computers, servers, and its hardware.
* Responsible for Exchange server, proxy server and network devices like switches and routers for any issues.

 **Accomplishments**

* Sales - Increased sales by doing presales activities over a year's period in Redington Gulf
* Project Development - Collaborated with a team of 4 developers in the development of Splunk in Dev-Ops and Agile environment.
* Creative Problem Solving: - Resolved any technical issues with any security products.
* Delivered presentation \ workshops \ improved overall processes and trained 15 - 20 staff members system.

 **Education**

Certificate of Higher Education: Post Graduation Certificate in Information Security, Jan, 2008

K. J. Somaiya Institute Of Management Studies & Research - Mumbai

BCA - Bachelor's of Computer Applications: Computer Applications, Apr, 2007

Madurai Kamraj University - Mumbai

Polytechnic Diploma: Instrumentation Engineering, Jan, 2004

Vivekananda College Of Engineering - Mumbai

Training Done:

In House Training - Mumbai

* Certified Ethical Hacker (CEH), Trend Appliance Network Access Controller (NAC).
* Attended in house technical training on Application Security

 **Certifications**

Splunk Certified Architect & SE II – working towards Core Consultant and then – ES SME

AWS Technical Accreditation

AWS Certified Cloud Practitioner

AWS Associate Architect

Technical Specialist in Symantec Security Information Manager 4.5 (SSIM).

Pursuing\Preparing CISSP (Target Year - 2020)