Rohit Kumar

Date of Birth: 16/09/1987
PR : House No.- 534A, Road No.- 6, Magadh Colony, Gaya, Bihar, India - 823001
Contact Number: +91-9902521766
Email: rohit.kr.ind@gmail.com , rohit.kr.48@gmail.com

OBJECTIVE

To contribute to the developments in the field of Computer Science and Information Technology by involving myself in continuous learning and research and to build a long-term promising career with a reputed firm, which encourages professional growth through a wide range of challenging assignments, which would use my skills and knowledge and would allow me to gain expertise and enhance my skills.

TECHNICAL PROFICIENCIES

Programming Languages:	Python3.6.1, C, C++, SQL, HTML5, CSS3, Javascript
Software Tools/Packages:	ArcSight(SIEM), Tripwire(FIM), Sourcefire (IDS/IPS), Trend Micro Deep Security (HIDS), Antivirus, Tipping Point SMS (NIPS), Symantec CSP (IDS), Barracuda (WAF), MS Office, MS Visual Studio, Oracle(9i,10g), Adobe family, Network Simulator 2, Eclipse Neon, MySQL
Libraries/APIs Explored:	STL, OpenMP, MPI, jQuery
Platforms Used:	Windows (XP, Vista, 7, 8, 8.1, 10), Linux (Ubuntu, Kali Linux), Macintosh OS.

PROFESSIONAL EXPERIENCE

Organization Name: KPMG India, Mumbai

Designation: Cyber Security Consultant

Industry Type: Information Technology

Duration: August 2018 - Present

Description: Working as Cyber Security Consultant for KPMG, where I perform below tasks:

- Assist, define, implement, operate and improve Information security processes and related to information security standard.
- Establish understanding of the security issues and providing advice to the stakeholders.
- Track, assist and manage to resolution the closure of security risks including review plans and monitor progress or remedial actions.
- Analyzing the results of the security testing conducted and assisting stakeholders with identifying viable remediation solutions for any vulnerability identified.
- Develop and execution of technology risk management, IT and

- information security strategy and processes to ensure compliance with the security policies and risk frameworks.
- Provide effective development and implementation of information security risk and management and security frameworks.
- Delivery of technical Security Testing and Security Assessments.
- Analyze the results of the security testing / assessment conducted and assist stakeholders with identifying viable remediation solutions for any vulnerability / gap identified.
- Track, assist and manage to resolution the closure of security risks including reviewing plans and monitoring progress or remedial actions.
- Delivery of Security Gap Assessments and its closure.
- Establish appropriate metrics in order to have a solid understanding of the operational issues and provide value reporting to the stakeholders.
- Provide an in-depth review of an organization's ability to protect its information assets and its preparedness against cyber threats.
- Proactive assessment of an organization's technical infrastructure including host-based log analysis, and/or network analysis to determine if any unidentified compromise has occurred previously.
- Provide a review of an organization's ability to respond to cyber security incidents.
- Support client in the identification, creation and execution of an IR program after a cyber-incident has occurred.

Organization Name:	Network Intelligence India, Mumbai
Designation:	Senior Cyber Security Analyst
Industry Type:	Information Technology
Duration:	March 2018 – August 2018
Description:	Worked for Network Intelligence India SOC as Senior Cyber Security Analyst, where I performed below tasks:

- Secure multiple clients by performing Security Information and Event Management using ArcSight(SIEM), AlienVault(OSSIM) and Qradar(SIEM).
- Integrating every network devices to SIEM to analyze real time security events using ArcSight ESM and Logger.
- Creating Custom Rules, filters and reports for the events that are generated in ArcSight Console on the basis of client's requirement.
- Configuring ArcSight Smart and Flex connectors for integrating different security devices and servers on the network.
- Creation of new dashboard, reports and rules as per the requirement for the priority events.
- Monitoring and mentoring L1 team and handling/ managing escalations made by them.
- Identification, investigation and resolution of security breaches detected by SIEM tools.
- Review security logs and reports of all operational devices.
- Creating Change Requests and implementing changes accordingly.
- Perform incident management using Spicework and maintaining SLA for each Incident based on its severity.
- Perform threat hunting/incident response for critical incidents and develop and document appropriate troubleshooting techniques.
- Perform email header and malware analysis for relevant incidents.
- Perform configuration reviews of multiple security tools for different clients.

Organization Name: Wipro Technologies, Pune

Designation: Project Engineer

Industry Type: Information Technology

Duration: August 2011 – August 2013

Description: Worked for Wipro SOC as Cyber Security Analyst, where I performed below tasks:

- Security Information and Event Management using ArcSight, Web Application attack analysis using Imperva, File Integrity Monitoring using Tripwire, Network Intrusion Detection and Prevention(IDS/IPS) using Sourcefire, Host intrusion Detection(IPS) using Symantec CSP & Trend Micro Deep Security.
- Analyzing real time Corporate and retail security events using SIEM tool such as ArcSight remotely.
- Creating Custom Rules and filter for the events that are generated in ArcSight Console on the basis of client requirement.
- Configuring ArcSight Smart connectors for different security devices.
- Creation of new dashboard as the requirement for the priority events.
- Analyzing Imperva and Sourcefire logs for web application attacks.
- Identification, investigation and resolution of security breaches detected by ArcSight and Sourcefire.
- Review security logs and reports of all operational devices.
- Understanding and managing PCI compliance using FIM tool such as Tripwire for corporate and retail nodes.
- Analyzing events for network intrusion detection & intrusion prevention on corporate and retail assets using Sourcefire.
- Creation of Rules for firewall events in Deep Security (HIDS).
- User creation & folder access management in AD & DFS as per the user's request.
- Creating Change Requests and implementing changes accordingly.
- Operate within defined ITIL processes for Incident and Change Management.
- Working on ticketing tools like ITSM (BMC Remedy) and Business Verizon Totality.
- Develop and document appropriate troubleshooting techniques.

EDUCATION

M.Tech – Computer Science and Engineering (2015 - 2017)
Birla Institute of Technology, Mesra, Ranchi, India

B.Tech - Information Technology (2007 - 2011)
Indian Institute of Information Technology, Allahabad, India

ACADEMIC PROJECTS / THESIS

Project Title:	Bayesian Spam Filtering
College:	IIIT Allahabad, India
Duration:	January 2011 – May 2011
Status:	Completed
Description:	This project demonstrates the working and implementation of Bayesian Spam Filtering on an Email client.
Project Guide:	Dr. Shirsu Verma, IIIT Allahabad, India.

Thesis Title:	Statistical Analysis of Amir Schoor's Algorithm in Sequential and Parallel Environment
College:	BIT Mesra, Ranchi, India
Duration:	August 2016 – June 2017
Status:	Completed
Description:	In this thesis we calculate the algorithmic time complexity using statistical bound estimate approach for the Amir Schoor's algorithm with different inputs within Sequential and Parallel environment and compare them for the average case analysis.
Thesis Guide:	Dr. Amritanjali & Dr. Soubhik Chakraborty, BIT Mesra, Ranchi, India.

AREAS OF INTEREST

- Cyber Security (Threat Hunting/IR, Digital Forensics, Malware Analysis, VA/PT and SOC)
- Computer Networks
- Data Structure\Algorithms
- Operating System

ACADEMIC AND EXTRA CURRICULAR ACHIEVEMENTS

- Was among top 2.5% students in **AIEEE** (All India Engineering Entrance Examination) for year 2007.
- Volunteer in International Conference on **Wireless Communication and Sensor Networks** (WCSN-2009), Organized by IIIT-Allahabad U.P, India.
- Participated and won several inter and intra school competitions.
- Qualified **GATE** (Graduate Aptitude Test in Engineering) for year 2015.
- Volunteer in National Workshop on **Wireless Network Simulation Using NS2/ NS3** (WNS-2016), Organized by BIT Mesra, Ranchi, India.

HOBBIES

- Surfing Cyber Security websites (e.g. Cyware, Threatpost, Darkreading, SANS, Dshield etc.)
- Reading Computer Magazines
- Watching Movies
- Playing Computer Games / Chess

I hereby declare that the above information is correct to the best of my knowledge.

Rohit Kumar