



Rahul Rakshit

Solution Consultant II (SOC)

 Bangalore, Karnataka, 560094

 889 220 7759

 rrakshit86@gmail.com

Experienced Security+/ITIL V3 Certified Senior Solution Consultant (SOC and Network Managed Services) with close to 7 years of experience in Information/Network Security supporting projects for EMEA, AMERICAS, and ASIA PACIFIC Clients looking for a position of (Senior/Lead) SOC Analyst.

Excellent reputation for resolving problems, improving customer satisfaction, and driving overall operational improvements in a very cost-effective manner.

Worked as a Lead in multiple MNCs handling a maximum size of 25 engineers
Worked as an Individual Contributor with onsite management and technical L3 Engineers

Expertise in providing technical solutions to large-sized and mid-sized networks via installation, configuration, continuous monitoring, migration, tool/network upgrade, performance tuning and administration

Strong monitoring, analytical and problem-solving skills, with the ability to recommend scalable, resilient and cost-effective solutions according to company standards

Articulate communicator with excellent collaborative skills to manage and resolve project infrastructure issues, and ensure service delivery excellence



Skills

- Incident, Change and Problem Management
- Security Policies and Management
- SIEM Solutions
- Endpoint Detection and Response
- Asset Management
- Infrastructure Security
- Team Management



Work History

- **Solution Consultant II (SOC)**
Hewlett Packard Enterprise, Bangalore, Karnataka

2017-05 - Current

Cyber security incident management (NIST framework) | | Problem management | | Change management | | Continuous Service Improvement | | PCI DSS compliant scan | | Endpoint Detection and Response | | PAS administration

- Own end to end Cybersecurity Incident Response for computer-based security events and incidents such as ransomware (Wannacry, Loki(formbook), China Chopper, Dog call), malware infections, potential compromise, Distributed Denial of Service (DDoS), etc.
- Provide SIEM (Splunk) Solutions involves appropriate tuning, correlation of critical logs, connection to our incident response process, and reporting of relevant metrics.
- Lead escalation teams to close with a response, containment, and remediation.
- Create, maintain, and promote a set of CSIRT operation SOP's to execute the security incident response process.
- Endpoint point detection and response (Trend Micro Officescan and Symantec EDR) - Conducted detailed analytical queries and investigations, identify indicators of compromise (IOC) or Indicators of Attack (IoA), Threat detection and response
- Vulnerability Assessment/Management (Qualys VS) - Creating asset tags, asset groups, running external and internal scans, creating a scan template, performing PCI DSS compliant scans
- Hands-on Cyberark Privileged Access Security administration for Windows, Linux and DB servers (Oracle) - PAS administration (Creating Platforms, onboarded accounts and creating and linking safely to the accounts)
- Communicate and build effective relationships with all stakeholders
- Plan and execute annual Security Incident Response tabletop exercises

Tools used:

EDR - Symantec EDR and Trend Micro ApexCentral/Office scan

VA - Qualys

SIEM - Splunk

Privileged Access Management and Security - Cyberark PAS

CSIRT tool - ServiceNow, (Salesforce)SFDC

MS Office - Word, Excel, Powerpoint

Project: AT&T McDonalds, Volvo

● **Consultant - Lead for L1 Team**

Capgemini, Bangalore, Karnataka

Incident management (ITIL) | | Problem management | | Change management | | Continuous Service Improvement | | SIEM | | EDR

Deployed at Societe Generale Global Solution Center

- Was part of the transition phase and was a critical resource in setting up the Service Desk and Monitoring Team
- Was a part of the Managed Security Services Team at the Global Solution Center
- Worked on Splunk SIEM -

- o Creating, maintain, support, repair, customizing System & Splunk applications, search queries, and dashboards.
- o Configuring Indexers, Forwarders (Universal and Heavy), Search Heads, Deployment/Management Servers
- o Running Splunk Queries
- o Manage Splunk user accounts (create, delete, modify, etc.)
- o Event Processing, Timestamps, Indexed Field Extraction, Host Values, Source Types, Event Segmentation
- o Review security events
 - Experience in static and dynamic malware analysis using Trend Micro OfficeScan/Symantec EDR
 - Experience in event and log analysis on Symantec/Trend Micro Endpoints
 - Creating and reviewing Policies (ACL, NAT, and VPN) on Check Point Next-Generation Firewall and Cisco Firewall, troubleshot VPN issues (Remote and Site to Site)
 - Responsible to manage and drive to closure all Audit issues to the Incident Response and Management process
 - Analyzed and initiated a P1/P2 bridge and worked closely with different stakeholders concerned for resolution of related issues

Tools Used:

EDR - Symantec EDR 4.2 and Trend Micro ApexCentral/Office scan

SIEM - Splunk

ITSM tool - BMC Remedy, ServiceNow

MS Office - Word, Excel, Powerpoint, SharePoint

Monitoring Tools - Spectrum, Nagios, PRTG, eON

Firewall - Check Point Next Generation Firewall, Cisco 55xx series

Project - AmCare, Societe Generale

2015-01 - 2016-08

IT Specialist

Gensuite LLC - A GE Company, Bangalore, Karnataka

- Worked on Critical Incident(s) and Service request for Network (LAN/WAN), Wireless and Security (Firewall Solutions, Web Filter) related issues
- Network Bandwidth Management and Testing new project implementations for multiple clients (for projects including Yamaha, Nike, GE EHS)
- Worked on RSA SecureID issues
- Initiate a P1/P2 Bridge and engaged the appropriate resolver teams.
- Played a major role in commencing the Network Operation Center for India GL (Bengaluru)

Tools Used:

Monitoring Tool: Aruba APC, PRTG, Nagios

ITSM tool - ServiceNow

MS Office - Word, Excel, Powerpoint

Routing and Switching -Cisco L2 and L3 Switches (2960,3560, 4500 series),

Aruba 7005 Controller, Aruba 2930f Switches

Firewall: Cisco 5505,5510

Wireless - Aruba 275,315 Access Points

Web Filter - Cyberoam

Project: Yamaha, Nike, and GE EHS

IT Executive

Maier And Vidorno GmbH, Bangalore, Karnataka

- Was a part of Global IT operations - Provided L0 and L1 level network support (per ITIL incident response process) to internal and external clients. (Organizational Business to Business) maintaining the SLA and OLA.
- Maintained network infrastructure consisting of Windows, Linux, and Virtual products.
- Worked closely with responsible stakeholders to determine the planning, implementation, and integration of system-oriented projects.

Tools Used:

Monitoring Tool: PRTG, Nagios

ITSM tool - BMC Remedy

MS Office - Word, Excel, PowerPoint, Sharepoint

Networking devices - Cisco 5505, Cisco routers and Cisco switches, HP Switches

Endpoint Security - McAfee

Project: Maier and Vidorno



Education

Bachelor of Technology: Electronics And Communications Engineering

Rajasthan Technical University - Rajasthan



Accomplishments

Professional:

- Received top Performer for FY18 in HPE
- Received top Performer for Q4 FY18 in HPE
- Technical Ninja FY16 at Gensuite LLC
- Best Employee Award FY16 at Gensuite LLC
- Best Dressed Employee FY14 at Maier and Vidorno GmbH
- Commended by the management for working 72 hours non-stop to ensure the uptime of the network infrastructure and provide support for the implementation of business continuity plans at Societe Generale
- Recognized and received many appreciation emails from clients for providing technical expertise and resolving complex issues under strict deadlines

Academic:

- Winner of State Level Quiz Champion
- Winner of State Level Technical Seminar Champion
- Certified by Govt. of Rajasthan for leading entrepreneurship camp held in the city of Bikaner



Languages

- English - Fluent (Speaking, Reading, Writing)
- Hindi - Fluent (Speaking, Reading, Writing)



Certifications

- Cisco Certified Network Associate (CCNA)
- ITIL v3
- Comptia Security+
- Trend Micro OfficeScan XG Certified Professional