Sarang Ambotkar *Phone: 8169533870*

Email:
sarangambotkar@gmail.com

ASSOCIATE SECURITY ENGINEER

Current Organization: Saint Gobain India Pvt Ltd
Current Team: Cyber Security INDEC
Experience: 2 years and 11 months
Experience Type: Cyber security Analyst, EDR Admin and Vulnerability Assessment.
Education: B.E in Computer Engineering from Mumbai University, PG Diploma in IT Systems and Security from CDAC Juhu

CORE COMPETENCIES

SIEM-QRadar: Monitoring, Detect and Reporting, Rule Creation

Vectra AI: Monitoring LAN network, Integration, Rule creation for whitelisting alerts

Qualys Guard: Immediate Scan, Schedule Scan, Authentication Scan, Create Option profile, Generate report, PCAP Scan, Debug Scan

TECHNICAL SKILLS

SIEM Tools	IBM QRadar, Vectra
Vulnerability Assessment	Qualys Guard, Nessus
Penetration Testing	Burp Suite
Threat Detection	McAfee, Malwarebytes
EDR Tool	Carbon Black
Ticketing Tools	Service Now and IBM Resilient
Other Tools	Zenmap, Wireshark

PROFESSIONAL DETAILS

Work Experience:

Date	Organization	Role
01 March 2018 – Present	Saint Gobain India Pvt Ltd , Mumbai	Associate Security Engineer

Key Responsibilities:

QRadar (SIEM tools):

Worked on SIEM tools like QRadar and Vectra. Have majorly worked on QRadar.

Job responsibilities includes performing active monitoring as initial level analysis for alerts, to investigate proactively and suggest recommendations for any suspicious activity. Further, managed day to day Incident response and provided mitigation steps based on incidents.

Worked as, assisted in evaluating new / emerging security threats and L2 Incident

Identified and removed multiple false positives and fine-tuned the multiple use cases in SIEM

Worked on Monitoring live data from the devices integrated from the client workstation.

Working on the QRadar with the event monitoring, analysis and fixing the solution to the vulnerability.

Preparing daily handover checklist as well as pulling monthly quality checklist report on quality analysis of Incidents.

Carbon Black (EDR):

Detect the behavior and traffic activity of any System or IP. Able to see the behavior against every user and their activity.

Quarantine, Bypass and other related activity to take action against the system. Reputation check, change reputation against the application or hash value.

Root cause and to investigate the total flow any application.

Resilient:

Working in GSOC (Global security Operation center) with multiple clients.

Creating Reports alerts and investigate issues identified during monitoring the live traffic. Preparing Daily/weekly/Monthly Reports.

Support security incident response processes in the event of a security breach by providing incident reporting.

Maintain and keep track of KPI data and SLA of every incident.

McAfee:

Logs check in detail for infected file.

Check threat events and its related information for better investigation.

Qualys Guard:

Scheduling scans for multiple clients' server.

Technical report generation for the scans completed.
Preparing management report for specific clients.

Work on with basic troubleshooting techniques for the IP's failed to scan.

Coordinate with the implementation team for security-related changes to the equipment, software and related services in accordance with the Security Policy and Change Management Policy

Coordinate with technology towers for the issue remediation and suggesting control measure to avoid the same in future.

Soft Skills

- Flexible approach towards work and ability to work in a team
- Ability to learn quickly and work efficiently by training the peer group and junior level associates
- Learn and share attitude

Achievements & Strengths

- ✔ Bug Bounty on bugcrowd.com − Hall of fame from programs by Pinterest, Caviar, TripAdvisor, etc.
- ✔ Have received certificate of appreciation, thank you card from cyber security head and Shift lead position within 8 months of joining
- ✔ Action Oriented: Optimistic, Speaking, Smart working, Problem-Solving skills and Team-Oriented
- ✔ Adventurous: Open-Minded, Spontaneous, Good Communication and Thoughtful
- ✔ Analytical: Organized, strong analytical & logical thinking, Responsible, Social, friendly and Trustworthy

Additional Responsibilities:

- ✔ Team management (Managing team working 24x7, Roster / Shift management, Resource Planning)

Extra Activities:

WAPT – Searching for websites by using Google dorks, finding vulnerabilities and exploiting them by using Burp Suite, Reporting the vulnerability with appropriate remediation on the platform of Bug crowd

VAPT – Creating a VPN session with the extension pack, taking access of the

machine, performing scanning with nmap scripts, Finding the vulnerabilities, exploiting with the help of exploitable tools from Kali Linux like Mimicatz and MSF venom, Get the root access and find the flag to complete the challenge in Hack the Box

Have experience on Nessus for scanning the Machines

Have knowledge about Mobile Application Testing

Personal Information

- Date of Birth : 09/12/1994
- Gender : Male
- Nationality : Indian
- Language known : English, Hindi, Marathi
- Address : KL- 5/36, Room No: 12, Sector-3E, Kalamboli, Navi Mumbai - 410218

Declaration

I hereby declare that all the information provided by me in this application is factual and correct to the best of my knowledge and belief.

Place: Navi Mumbai (Sarang Ambotkar)