BHARGAVI BODDULA

~MOBILE: 7013063870 ~ E-MAIL: BHARGAVIBODDULA08@GMAIL.COM ~ LOCATION: HYDERABAD

PROFESSIONAL SUMMARY

- Experienced and detail-oriented Cybersecurity Analyst with 3 years of hands-on experience in security environments. Proficient in leveraging SIEM tools such as McAfee ESM and QRadar for real-time threat detection, analysis, and incident response.
- Seeking a challenging SOC Analyst position to further develop expertise in Cybersecurity tools and systems while contributing to an organization's security and operational efficiency.

WORK EXPERIENCE

Security Analyst – Augur Cyberx [March 2024 to Till Date] Hyderabad, India.

Security Intern – Unirac [Jun 2022 to Feb 2024] Hyderabad, India.

CERTIFICATIONS

- Certified Ethical Hacker - CEH
- Cybersecurity Certification – NSDC
- Cybersecurity Analyst Professional – Itronix Solutions
- Security Operation Center Analyst - Udemy

ROLES AND RESPONSIBILITIES

- Perform 24/7 real-time monitoring, security incident handling, investigation, analysis, report, optimize, manage, and escalate security events from multiple log sources to customer.
- Working on incidents and reviewing the alerts and doing detailed analysis on alerts.
- Detect Incidents by monitoring the SIEM console, Rules, Reports and Dashboards.
- Creating an incident ticketing, Analyzing, Managing, and Tracking security incidents to closure by coordinating with different teams.
- Monitor the SIEM console resources to identify any anomalies.
- Recognize potential, successful, and unsuccessful intrusion attempts/compromises thorough review and analysis of relevant event detail and summary information.
- Investigating and Monitoring Endpoint Alerts and blocking malicious hashes/URLs/files, creating watchlist/rules for malicious processes, files, and hashes.
- Monitoring and analyzing network traffic during incident triage using various security solutions namely IDS/IPS alerts, AV alerts, Mail GW logs etc.
- Monitoring inbound and outbound traffic for the firewall and investigating the events.
- Monitoring various logs, Dashboard and Alert creations using QRadar , McAfee ESM.
- Report the confirmed incidents to customer and escalate them further to the concerned L2 team.
- Track incident status to closure as per Standard Operating Procedures (SOP) defined.
- First level Triage of events as provided in Standard Operating Procedures and automate analysis if possible.
- Proactively identify vulnerabilities in customer infrastructure environments and suggest updating of SIEM use cases to generate alerts.
- Suspicious Email Analysis (phish/spam) and analyzing in a sandbox environment.
- Performing investigations requested by customer and submitting the report.

- Proficient in endpoint security solutions, with hands-on experience in Crowd Strike for threat detection, incident response, and endpoint protection.
- Creating and submitting the weekly report which includes all details regarding the escalated incidents, devices , investigations and so on.
- Ensure confidentiality and protection of sensitive customer data.
- Proficient in Cyber Kill Chain methodology, MITRE ATT&CK Framework, and OWASP Top 10, with a strong understanding of threat detection, attack techniques, and vulnerability mitigation.
- Strong foundation in networking concepts, including OSI layers, TCP/IP protocols, port communication, and WAN/LAN architectures, with the ability to analyze network traffic and identify potential security risks.

SKILLS

- **SIEM Tools**: McAfee ESM, QRadar
- Crowd strike, Proof Point, Zimbra Mail, Forcepoint, Audit plus, Azure AD, Symantec Endpoint, Palo Alto, Cisco Secure IPS, FortiClient, Beyond insight, Trellix epo, Spam & Phishing Analysis, Microsoft Office Tools.

STRENGTHS AND ACCOMPLISHMENTS

- A team player who can also take the initiative to work individually.
- Flexible to take new responsibilities/challenges irrespective of any changes within the company environment.
- A team player with excellent communication, analytical, problem-solving and relationship management skills.

EDUCATION

- B. Tech (Civil) (Pass out 2021) from (OU), Hyderabad.

PERSONAL DETAILS

- Fathers Name: Sambaiah.
- Date of Birth: 11 Aug 1998.
- Gender: Female.
- Marital Status: Unmarried.
- Nationality: INDIAN.
- LinkedIn: www.linkedin.com/in/bhargavi-boddula-0b2a5018b

Declaration: The information provided above is accurate to the best of my knowledge.

Kind Regards,
BODDULA BHARGAVI.