CURRICULAM VITAE

GEETA PRAVEENA BADIGANTI
Phone: 9502630240
E-mail: geethabadiganti7728@gmail.com

SUMMARY

- ❖ Currently Working in WIPRO Hyderabad since March– 2022.
- ❖ 2.9 Years of work experience in Security Operation Center.
- ❖ Capable of independently learning new technology by utilizing available documentation and vendor support resources.
- ❖ Strong hands-on experience in security management tools like IBM Q radar, Azure Sentinel, Alien Vault, and experienced in Global Delivery operations support model.
- ❖ Good experience in working with cross-functional IT infrastructure teams like network, system, database, application, security to build and manage effective security operations.

PROFESSIONAL EXPERIENCE

In General

- ➢ Working with vendors and skill groups to ensure successful delivery of security operations center capabilities.
- ➢ Documentation customer support and collaboration with other team members.
- ➢ Provides support on all issues relative to engineering activities for SOC capabilities.
- ➢ Coordinate with multiple stakeholders to ensure timely and satisfactory resolution to technical issues and completion of projects.
- ➢ Working experience in the Information Security domain, trained in Incident Response, SIEM and SOC having working experience in Internal Security and multi-customer SOC environment.
- ➢ Perform Security Operational task- Analysis, Filters, Reports Suggestion on fine tuning on existing rules

WIPRO

Wipro is one of the leading professional Information technology services and consulting company which has a culture focused on client needs.
Period- 2nd March 2022 - 24th December 2024.
Skills Used: IBM-Q radar, Alien Vault, Azure Sentinel, Service Now, Anomaly
Current designation- Associate
Delivery Project- Multiple Finance Sector and other Clients (Confidential)

ROLES & RESPONSIBILITIES

- Proactive monitoring, analysis, responding, and reporting for IT Security Incident response 24*7.
- Exhibited knowledge and ability to collaborate on SIEM functional requirements: logging, event collection, normalization, correlation.
- Handling multiple clients to support the Information Security infrastructure.
- Working on Email Security/Phishing Incident Response by analyzing spam, phishing, and malicious emails
- Acknowledging User reported Phishing emails, escalating to Client L2 team for validating of our notes and owning the Incidents till closure.
- Publishing security advisory, threat and ask the respective team to block the IOC's.
- Analyzing SIEM and SOAR alerts by following runbooks and using various tools.
- Working knowledge on endpoint devices such as Microsoft Defender, CrowdStrike
- Use case, Reports and Dashboards creation. Identifying, investigating, and responding to potential security incidents in a way that minimizes impact and remediation steps to recover from the attack.
- Providing support for internal audit for the techs regarding threat analysis.
- Contributing to preparing SOC documents including SOP, Internal Playbook, Reports, and other process related documents.

Skills Used

- SIEM   : IBM Q Radar, Azure Sentinel, Alien Vault.
- EDR   : Microsoft Defender, CrowdStrike
- Analysis Tools : IP Void, Virus Total, Anomaly, Palo alto.
- Ticketing Tool : Service Now.

ACADEMIC DETAILS

- Bachelor of Civil engineering - 2017.

PERSONAL DETAILS

- Date of Birth   : 18-02-1996
- Gender   : Female.
- Marital Status   : Married.
- Nationality   : Indian.
- Languages Known   : English, Hindi and Telugu.

Declaration

I hereby declare that the information given herewith is correct to my knowledge and I will be responsible for any discrepancy.

Geeta Praveena B