VAMSI KRISHNA TURANGI

CONTACT

E-mail: turangi.vamsi2605@gmail.com

Phone: 9398636069

Address: Hyderabad, India 500072

PROFESSIONAL SUMMARY

Actively seeking an opportunity in the field of cyber security where Ican put my knowledge and skills to work for the organization and improve my experience through continuous learning.

EXPERIENCE

SOC - ANALYST, 07/2023 – Till Date

Virinchi Technologies - Hyderabad**,** Telangana.

- Endpoint & Network analysis, to include analysis of relevant logs and data, and background using a variety of analysis tools like EDR, SIEM, Firewall (WAF -Imperva, cisco), Proxy etc.
- Hands on experience on tools , Trellix (Email Threat Protection-ETP), Trellix (Host Security -HX), Trellix (Network Security - NX), Forcepoint (DLP -Data Loss Prevention), SIEM & XDR(Rapid 7).
- Follow-up with incident response team for remediation.
- Working level knowledge on security solutions like Antivirus, Firewall, IPS, Email Gateway, Proxy, IAM, TI, VA Scanners, WAF etc.
- Exposure to using frameworks and compliances like MITRE ATT&CK. CIS Critical Controls, OWASP.
- Documentation of alerts & Drafting shift hand-overs.
- Acknowledging and closing false positives and raising tickets for validated incidents.

Intern Trainee, 02/2023 - 06/2023

Secops 24 - Hyderabad**,** Telangana

- Monitoring Security alerts generated by SIEM.
- Deep dive analysis of triggered alerts using SIEM and other analysis tools.
- Knowledge on the creation of dashboards and alerts using Splunk.
- Assist IRT/SME teams in incident remediation by providingsupporting data and recommendations.

EDUCATION

Bachelor of science (B.sc , computer science), 2017- 2021

G.C.S.R Degree College.

GPA: 7.2

CERTIFICATIONS

- Certified Ethical Hacker (CEH) SPLUNK Certification Fortinet NSE1 andNSE2.
- Certified Training from SOC Experts.

CORE QUALIFICATIONS

- Web Technologies like HTML and CSS.
- knowledge on Python and SQL.
- Good knowledge on cyber attack
- Good knowledge of network concepts: OSI model, NAT, PAT, ports & protocols/IP model , DNS, DCP.
- Good knowledge of firewall concepts, antivirus software, intrusion detection/prevention systems and endpoint security solutions
- A basic understanding of security concepts such as CIA Thread, Risk Management, threat intelligence and incident response
- Good understanding of various SOC processes like monitoring, analysis, playbooks, escalation, incident documentation, SLAs, client meetings, report walk throughs, bridge calls, RFPs, etc.
- Good Knowledge in Microsoft Office (Word, Power Point, Excel).

INTERESTS

Travelling, surfing internet, listening music, playing badminton.