CONTACT

☎ 8341050990
✉ ramyahnk03@gmail.com
📍 Warangal, Telangana, India.

EDUCATION

MSC Computer Science
Kakatiya University
2020-2022

CERTIFICATIONS

- Sophos Engineer
- Sophos Technician
- Sophos Firewall Engineer
- Fortinet – NSE1 & NSE2
- EC-Council – SQL Injection Attacks
- EC-Council – Network Defence Essentials(NDE)
- EC-Council – Digital Forensic Essentials(DFE)
- EC-Council – Ethical Hacking Essentials(EHE)

SKILLS

- Security Information and Event Management (SIEM) tools : Seceon
- Incident response and handling
- Vulnerability Assessment using Openvas
- Threat intelligence analysis
- Web Application Testing using ZAP and Burpsuite.
- Security policies and procedures
- Communication and collaboration
- Email Header Analysis using MxToolbox, mailheader.org .
- Static and basic dynamic malware analysis using PE – Studio, Bintext, Hash – Calc, Exeinfo – PE.

RAMYA HANUMAKONDA

SOC Analyst L1

PROFILE

I am working as a SOC Analyst, focusing on monitoring and analyzing security alerts. And Looking for an exciting Information Security career where I can grow and be creative. I want to enhance my skills through hard work, contribute to the field, and help organizations succeed by providing value to customers.

WORK EXPERIENCE

SOC ANALYST - L1 Oct 2022 to Present

- Monitor and manage Sophos XDR alarms on behalf of Wydur customers and conduct deep investigations to provide risk assessments and take actionable actions as required.
- Malware Analysis and Threat Hunting.
- Analyzing Phishing E-mails with MxToolbox and cross-referencing the IP address and attachments with threat intelligence (IP void, virus total, urlscan.io, URL checker)
- Monitor and manage endpoint system agents to ensure that log collection is active and that there are no heartbeats missing, resolve and escalate as needed.
- Monitor the security board for priority tickets and take actions on all tickets in a timely and prompt manner.
- Block Malicious IP Addresses on blacklisted IP's that are deemed to be threats or security impacts and notify the customer and internal management as required.
- Using GVM to perform a network vulnerability assessment scan.
- Making generated reports available to stakeholders/customers.
- Assist senior leads in managing and maintaining SOC tools and services.
- Responsible in on-call rotations to provide 24/7 coverage for incident detection and response.