POOJITHA MERNEEDI

Email: poojithapoojitha408@gmail.com

SOC Analyst

Mobile: 9390075239

PROFILE

Aspiring SOC Analyst | Skilled in Identifying and Mitigating Phishing Attacks | Passionate About Cyber Threat Detection and Incident Response

Work Experience

Capital Technologies PVT.LTD | Bangalore, India SOC Analyst — Intern

• Supported 24/7 SOC by utilizing Security tools to assess threats, validate and escalate Alerts based on established escalation procedures on a strict SLA within a fast-paced 100+ client environment.

• Researched on latest cyber-attacks, Attack Vectors, and IOC's- created Use cases and lists of malicious Hashes.

• Performed Rule Tuning and Triage and checked for abnormal activities based on event correlation.

• Onboarded clients by installing and deploying security agents in their environments to enable 24/7 security monitoring and threat detection

TECHNICALEXPOSURE

- Solid understanding on common network services and protocols
- Good knowledge on SIEM Log monitoring, Log Analysis and Phishing Email Analysis.
- Working knowledge on security solutions like Anti-virus, Firewall, IPS, Email-gateway, Proxy and EDR.
- Basic knowledge on malware analysis.
- Having good exposure towards cyber frameworks like cyber kill chain, MITRE Attack.
- Good knowledge on SOC monitoring, analysis, playbooks, run books, escalation,
- Having good knowledge on Phishing email analysis and categorizing them as spam, legitimate and phishing.
- I have been trained as SOC analyst and have knowledge on different tools like Microsoft defender, DLP alerts, MCAS alerts, IBM QRadar.
- Trained in performing log analysis from different log sources.
- Good understanding on open-source threat intel sites and also on sandboxes on how to analyze different files and Ips or URLs.
- Trained in email communication with users and resolving different incidents.
- Good knowledge on Networking Concepts (TCP/IP,DNS,VPN's).

TOOLS

- SIEM tools: IBM Qradar, Microsoft Azure Sentinel and Rapid7
- EDR: Sentinel one and CrowdStrike
- Phishing tools: Microsoft O365 Defender, Proofpoint
- Phishing and Spam email analysis
- Ticketing tools: Service Now and Jira
- Sandbox Analysis
- Basic knowledge in C-language and Core Java
- Office Tools: Microsoft word, Microsoft Excel, Microsoft PowerPoint.
- HTML software • Python • MS-Office • Basics in Networking • Basics in C language

EDUCATION HISTORY

B. Tech (ECE): Adarsh College of Engineering, Gollaprolu in 2024 with 7 CGPA
Diploma (ECE): VSM College of Engineering In 2019 with 68.65%
S.S.C: Z P HIGH SCHOOL Vakada, in 2016 with 8.0 CGPA.

INTERNSHIP

Internship in IOT Domain
Completed internship of IOT at SkillDzire in Collaboration of Andhra Pradesh Council of Higher Education.

Project in IOT domain
Project on power meter billing system using IOT.For IOT, Used Arduino and ESP32 as our controlling elements.

Result: Obtained a smart energy meter which can set the billing budget and accurately measure power consumption

INTERESTS

- Collaborative team member and Quick learner.
- Analytical Skills
- Comprehensive problem-solving skills.
- Active and well-prepared

LANGUAGES KNOWN

- English
- Telugu

DECLARATION

I hereby declare that the information provided above is true and accurate to the best of my knowledge

(POOJITHA.M)