KORADA PURNA SAI

7780411816| siddhukorda756@gmail.com| LinkedIn

PROFESSIONAL SUMMARY

Detail-oriented SOC Analyst with hands-on experience in monitoring, investigating, and responding to security incidents using Microsoft Sentinel and Microsoft Defender. Strong experience in DLP policy design and tuning, vulnerability management, analytical rule creation, and incident root cause analysis. Actively involved in strengthening organizational security posture through policy improvements, SOP development, and proactive threat detection.

PROFESSIONAL EXPERIENCE

AUXILIUM IT SERVICES PVT LTD | SOC Analyst - *Current Role*

Security Operations

- Monitored, triaged, and investigated alerts using Microsoft Sentinel and Microsoft Defender.
- Performed phishing email and malicious link analysis with remediation actions.
- Conducted RCA for incidents including unusual sign-in attempts and account misuse.
- Investigated Intune non-compliant devices and documented mitigation steps.

Detection Engineering & SOPs

- Tuned analytical rules to improve alert quality and reduce false positives.
- Identified and corrected port scan detection logic.
- Created analytical rules for:
  -Global Administrator password reset activity
  -Abuse of forgot-password method using audit logs
- Authored SOPs for port scan detection and email analysis.

KEY PROJECTS

Microsoft Purview DLP Tuning Project

- Tuned DLP policy logic, rule conditions, severity, and confidence levels.
- Identified policy gaps such as incorrect catch rules, low confidence false positives, and missing exclusions.
- Performed testing, validation, and documentation.
- Delivered final report approved by Security Architect and deployed to production.

Vulnerability Management Program

- Conducted software discovery and maintained device and application inventory.
- Identified endpoint vulnerabilities and configuration weaknesses.
- Documented findings and remediation status in vulnerability reports.

ePHI DLP Implementation (New Acquisition)

- Designed and implemented DLP policies for ePHI data.
- Created custom Sensitive Information Types (SITs).
- Applied sensitivity labels, detection logic, and enforcement actions.
- Completed compliance-ready documentation and reporting.

TECHNICAL SKILLS

- **Cybersecurity Expertise:** Endpoint Security & Compliance, Email & Phishing Analysis , Incident Response & RCA , SIEM Monitoring & Rule Tuning .
- **Cloud Skills:** Microsoft Sentinel , Microsoft Defender for Endpoint ,Microsoft Defender for Office 365 , Microsoft Purview (DLP, SITs, Labels) , Microsoft Intune
- **Tools:** SIEM,IDS/IPS, Firewalls **,**Kali Linux, Nmap, Metasploit, Wireshark, Burp Suite, Nessus.
- **Programming Languages:** Python, HTML, CSS.
- **Web Security:** SQL injection, cross-site scripting (XSS), web application security analysis ,OSWAP Top 10 Attacks.
- **Operating Systems:** Linux (expert), Windows (expert).
- **Other Tools:** Git, Microsoft Office Suite (Excel, Word, PowerPoint).

EDUCATION

MCA (Masters of Computer Applications) (2024-2026)
Andhra University
Percentage: 70.0%

BCA (Bachelor of Computer Applications) (2021-2024)
Gayatri Vidya Parishad College for Degree and P.G Courses (A)
Percentage: 70.0%

Intermediate MPC (2019-2021)
Sri Chaitanya Junior College
Percentage: 73.3%

CERTIFICATIONS

- Microsoft SC -200
- AWS Academy Graduate – Machine Learning Foundations
- Cyberthreya Elite Mastery
- NIKIST Hacker Mentorship Club Internship
- Palo Alto Cybersecurity Internship
- IIDT Cybersecurity Internship

ADDITIONAL ACTIVITIES

- Participated in Capture The Flag (CTF) challenges focused on real-world security scenarios.
- Hands-on exposure to penetration testing and internal network assessments.