SHANMUKH PISINI

Senior Consultant - Cyber Security

CONTACT

+91 9542670762

shanmukhpisini.96@gmail.com

Hyderabad

https://www.linkedin.com/in/Shanmukhpisini

EDUCATION

2014 - 2018

GVP COLLEGE OF ENGINEERING

B TECH EEE

SKILLS

- Security Tools: Splunk, Microsoft Sentinel,
- Threat Intelligence & Hunting: MITRE ATT&CK, YARA rules
- Endpoint Security: EDR/XDR solutions, Windows/Linux/MacOS forensics
- Network Security: IDS/IPS, Wireshark, NetFlow analysis
- Cloud Security: AWS Security Hub, Azure Defender, Google Chronicle
- Incident Response: SOAR automation, forensic analysis, log correlation, malware reverse engineering
- Compliance & Standards: NIST, ISO 27001, CIS Controls, GDPR, SOC 2

PROFILE SUMMARY

Results-driven Security Analyst with 5 years of experience in security operations, threat detection, incident response, and vulnerability management. Proficient in SIEM solutions, EDR, IDS/IPS, malware analysis, and cloud security. Adept at investigating security incidents, responding to threats, and improving security postures. Holds multiple security certifications and skilled in scripting and automation to enhance SOC efficiency.

WORK EXPERIENCE

Sr. Security Consultant -LTI Mindtree

Microsoft Project — DEC 2021 - PRESENT

- Monitored, analyzed, and triaged security alerts from SIEM, IDS/IPS, and EDR to detect threats.
- Investigated and responded to cyber incidents, malware infections, and phishing attacks.
- Conducted threat hunting activities to proactively identify potential security breaches.
- Developed custom detection rules in Splunk to improve threat visibility.
- Collaborated with incident response teams to mitigate security breaches effectively.
- Participate in the development and execution of Proof of Concepts (POCs) for new security tools and technologies, ensuring alignment with business needs.
- Analyze and interpret security alerts, utilizing the MITREATT&CK framework to assess adversarial tactics and techniques.
- Collaborate with the team to maintain and enhance incident response procedures and improve detection capabilities in the 24/7 Security Operations Center (SOC).
- Respond promptly to cyber security incidents, providing detailed reports and recommendations for remediation.
- Assisted in compliance audits (SOC 2, ISO 27001) and implemented security best practices.

ACHIEVEMENTS & CERTIFICATIONS

- Received A- Team award for performing well in the team and played important role in implementing security measures for cloud environments.
- Security analyst associate (SC-200) From Microsoft) 2022
- Azure Security Engineer (AZ-500)
- AWS Security Speciality.
- ComptIA security +

Tata Consultancy Services

Security analyst Jun 2018-Mar 2020

- Managed security alerts and performed deep-dive log analysis to identify attack patterns.
- Responded to DDoS attacks, insider threats, and privilege escalation incidents.
- Implemented SOAR playbooks to automate incident response workflows.
- Analyzed malware behavior using sandboxing and forensic techniques.
- Provided security awareness training to employees on phishing and social engineering threats.