Dhikshitha Konda

+918790457006 ◇ dhikshithakonda@gmail.com ◇ Nizamabad, Telangana, India ◇ LinkedIn

SUMMARY

A keen and passionate Security Professional with 2+ years of experience who is always enthusiastic about learning new trends in the cyber security field and intensively collects information on how to mitigate them.I am open to face new challenges and possibilities.

EXPERIENCE

Senior Security Associate Nov '23 — Jul '24
Trisun Hyderabad, India

- Incident Response Leadership: Spearhead incident response efforts by leveraging Crowd Strike Falcon,coordinating with relevant teams, and ensuring swift resolution of security incidents.
- Endpoint Security Management: Administer and optimize Crowd Strike Falcon to protect endpoints, ensuring effective threat detection, response, and containment.
- Penetration Testing Proficiency: Conduct comprehensive penetration testing using tools such as Nmap, BeEF, OWASP ZAP, and Burp Suite to identify and exploit vulnerabilities in the environment.
- Perform thorough assessments of network infrastructure, web applications, and other critical assets to uncover potential weaknesses and provide actionable recommendations.
- Vulnerability Management with Qualys: Conduct thorough vulnerability assessments using Qualys, Prioritize remediation efforts, and ensure compliance with security standards, especially PCI DSS/ISO
- Alert Logic Log Analysis: Utilize Alert Logic for log analysis, correlating security events to identify potential threats,and taking proactive measures to enhance the overall security posture.

Security Analyst Jul '22 — Nov '23
Kinfotech.pvt.ltd

- Conducted in-depth analysis of cyber security incidents and provided recommendations to clients for improving their security posture using Falcon Crowd Strike EDR.
- Developed specific method, increasing specific aspect by Collaborated with internal teams to develop custom security solutions for clients based on their needs.
- Provided technical expertise and support to clients during security incidents and breaches, including conducting forensic investigations and incident response.
- Responsible for monitoring of Security Alarms using LogRhythm SIEM tool and Initiating Information Security incident ticket.
- Use mutual database to log customer information and reduce database clutter by consolidating information
- Examined security logs to identify security incidents and malicious activities and categorize them as false positive or true positive.
- Determining indicators of compromise (IOC) or Indicators of Attack (IOA) that need further investigatio

EDUCATION

Bachelor Of Technology in Electronics Communication, Kakatiya Institute of Technology Science (GPA: (63/100) Nizamabad, India

Highschool diploma in Class XII, Kakatiya Ravi Junior College (GPA: 54.7/100) Nizamabad, India

Highschool diploma in Secondary Education, Kakatiya High School (GPA: 6.7/100) Nizamabad, India

SKILLS

- **Security Operations (SOC) & Incident Response**
- **SIEM Tools**: IBM QRadar, Splunk, ArcSight, Microsoft Sentinel, LogRhythm
- **Penetration Testing**: Kali Linux, Burp Suite, Metasploit, OWASP ZAP
- **Application & Web Security**: Email security, phishing email analysis
- **Threat Intelligence & Digital Forensics**: CrowdStrike, Forcepoint, AlertLogic
- **Vulnerability Assessment & Management**: Qualys Guard, PCI DSS Complianc
- **Network Security**: Firewalls (**Palo Alto, Cisco ASA**), VPN, IDS/IPS (**Cisco Firepower**)
- **Compliance & Regulations**: ISO 27001, ITIL, PCI DSS
- **Networking Protocols**: TCP/IP, proxies, and security best practices