ARUN J

Security Analyst

☎ +91 9952217572
✉ arunit8484@gmail.com
Coimbatore

Professional Summary

A highly motivated Cyber Security Analyst with extensive experience in identifying and mitigating security threats, as well as monitoring security alerts and network traffic. I am seeking a dynamic role to advance my skills and contribute to enhancing organizational security through effective risk mitigation strategies.

Technical Skills

Security Tools

- CrowdStrike Falcon (EDR)
- McAfee MVISION Cloud (CASB)
- IBM QRadar (SIEM)
- Zscaler Internet Access (SWG)

Vulnerability Assessment

- Insight VM Tool

OS Administration

- Active Directory

Networking

- Switch
- Router
- Firewall

Certification

Zscaler Internet Access (ZIA)
Administrator Certification

Education

Bachelor of Science in Information Technology

Dr.N.G.P Arts and Science College,
Coimbatore.
Graduated with 7.3 CGPA
2018 - 2021

Work Experience

Tata Consultancy Services
08/2021 - 12/2024
Chennai, India

- Having over 3.4 years of experience as a Security Analyst, skilled in utilizing CASB, EDR, SIEM, and Proxy solutions to enhance threat detection, incident response, and data security.
- Actively monitored and analyzed network traffic, security alerts, and logs using SIEM solutions to detect and respond to security incidents promptly.
- Proficient in monitoring and managing CrowdStrike for real-time threat detection, forensic analysis, and incident response.
- Conducted regular vulnerability assessments, analyzed results, and collaborated with IT teams to remediate identified vulnerabilities.
- Created custom correlation rules in SIEM solutions, improving detection of unauthorized access attempts.
- Implemented advanced web filtering rules to block phishing sites, malware downloads using Zscaler Internet Access.
- Have provided support for Zscaler-related incidents, resolving issues within defined SLAs.
- Specialized in analyzing Zscaler logs and reporting.
- Evaluating user data exfiltration practices from the CASB tool.
- Investigated high-risk user activities such as accessing malicious websites, data exfiltration, and anomalous file downloads.
- Monitored firewall logs to detect and report suspicious outbound connections.
- Investigated network-level vulnerabilities, analyzing open ports, weak encryption, and insecure protocols.
- Utilized risk assessment tools and methodologies to evaluate potential threats and formulate action plans.
- Worked closely with incident response teams to evaluate risks from security breaches and improve future defenses.
- Maintained accurate records of security incidents, vulnerabilities, and mitigation efforts for auditing and compliance purposes.
- Provided regular updates to management on the status of security initiatives and ongoing risks.
- Have strong analytical and problem-solving skills and open to innovation in order to enhance performance.
- Have outstanding abilities in communication and building interpersonal relationships.