Akash Reddy

SOC Analyst

7386183536 | akashreddy4271@gmail.com | Bangalore

Summary

Adept SOC Analyst with 2 years of proven track record at ITC, mastering Cyber Security SIEM tools like Splunk and excelling in critical thinking. Skilled in identifying and mitigating vulnerabilities using Nessus, and enhancing email security. Demonstrates exceptional analytical skills and a solidunderstanding of Incident response life cycle, ensuring robust security postures.

EXPERIENCE

SOC Analyst **April2023 - Present**

ITC Infotech, Bangalore

- Actively investigated the latest in security vulnerabilities.
- Performing security incident detection, detailed investigation of incidents and managing servicelevel agreements.
- Troubleshooting non-reporting devices.
- Worked in 24x7 Security Operational support.
- Conduct details analytics queries and investigations, identifies area that require specific attention,Identity Indicator of Compromise (IOC) and Indicator of attacker (IOA).
- Detect security issues, create customer tickets and manage problems until closed.
- Hands on Experience on Incident response activities like Malware Analysis, Brute force Analysis,Phishing Email Analysis.
- Antivirus, Data Leak/Loss Prevention (DLP) deployment to all end point machines through SCCM.

Education

B.SC. Forensic Science **2020 - 2023**

Garden City University, Bangalore

Skills

- Cyber Security SIEM : Splunk Enterprise Security and sentinel
- Endpoint Security : Micrososft365 Defender and Crowdstrike
- Vulnerability Assessment : Nessus
- Email Security and Protection : Proofpoint
- Security skills : Cyber Kill Chain, Incident response life cycle
- Ticketing Tools :ServiceNow
- Operating Systems : Windows Server and Linux

Professional Knowledge

- Having an Knowledge of in “Security Operations Center Analyst”
- Raise of incident for true positive cases and assigning it to L2 team with own recommendation.
- Knowledge in Monitoring and reporting of SIEM” Tool
- Knowledge in “Vulnerability” assessment tools like Nessus
- Knowledge in “Service Now” Ticketing Tool
- Knowledge on EDR tools like Microsoft 365 Defender and cloud apps for ATP
- Analysing Spam, Phishing and other Suspicious and spoofed Emails
- Good exposure to different security vulnerabilities with OWASP Top 10

Certificates

- Cybersecurity
- SOC
- Fortinet NSE1 and NSE2
- ABCS of Malware Analysis
- Splunk