Mohamed Jamaldeen

Sivagangai, TN, India
+91 7824951548
mohamedjamaldeen214@gmail.com

Objective

Cybersecurity enthusiast with proficient and thorough 2.5 years of experience as a Security Operations Analyst and works on various security tools and technologies. I am dedicated to continuous learning and passionate about expanding my cybersecurity knowledge by work and external platforms.

Tools & Technologies

- SIEM-Splunk Enterprise Security
- EDR-CrowdStrike Falcon & Fireeye
- NDR - Darktrace
- SOAR - Cortex XSOAR
- Email gateway-Microsoft
- Analysis tools: Virus-total, Cisco talos, ANY.RUN, IP void, MxToolBox, AbuseIP, Browserling, URLScan, etc

Experience

GAVS Technologies, Chennai

Feb 2024 - Present

Information Security Analyst

- Monitor, analyze and validate alerts triggered in SIEM, EDR, NDR.
- Acknowledge and close false positives alerts and validate true positive incidents
- Works on Investigation of IP, File, URL, Command, Process and Application alerts
- Analyse Phishing emails and worked on remediation process
- Investigate incidents, tracked and followed-up on incident closures with relevant teams and stakeholders.
- Remediation action on validated incidents
- Identify and perform Root Cause Analysis of the incidents with Team Lead.
- Built weekly and monthly Reports as per SOC Manager requirements.
- Educate affected users on mitigating threats.

Infosys, Chennai
Jun 2022 - Jan 2024
Security Operation Center Analyst
• Monitor and investigate alerts from SIEM(Logrhythm) ,EDR (Fireye) which triggered in SOAR (Cortex xsoar)
• Analyse and validate true positive incidents and close false positive alerts
• Perform Phishing email analysis and log analysis
• Escalate TP incidents to L2 analysts
• Educate threat affected users to refrain from future attacks

Technical Knowledge

• Endpoint and Network security.
• Security solutions like SIEM, EDR, NDR,SOAR, Firewall, IPS, IDS, Proxy, Email Gateway, Antivirus
• Cyber Kill Chain and MITRE Attack Frame work
• Phishing email, Malware analysis & Log analysis
• Different types of Cyber Attacks
• OSI and TCP/IP model, DHCP, DNS, CIA Traid

Skills

SIEM, EDR, NDR alerts

Phishing email analysis

Log analysis

OSINT analysis

Education

Dhaanish Ahmed College of Engineering
2017-2021
B.E Computer Science Engineering
7.2 GPA

Maharishi Vidya Manddir Higher Secondary School
2017
12th HSC
75%

Christhuraja Higher Secondary School, Tiruppathur
2015
10th SSLC
90%

Certifications

• SOC Experts certified security operations analyst
• Cisco Certified Network Associate- CCNA
• Splunk Certifications