

Ashok Kumar MT

7204220458 . BTM Layout, Bengaluru, 560076 . ashokmantha45@gmail.com .

<https://www.linkedin.com/in/ashokmantha/>

Professional Summary

Experienced Security Analyst with 2.4 years in real-time monitoring, analyzing security logs, responding to incidents. Collaborative team player skilled in threat mitigation and investigations. Aspires to enhance skills, contribute to cutting-edge projects and stay at the forefront of emerging threats.

WORK EXPERIENCE

ZeroFox –Bengaluru, Karnataka

July-2022 - PRESENT

Security Analyst / Platform Operation Specialist – SOC East

Roles and responsibilities:

- Worked in a 24x7 Security Operations Center (SOC) Environment to monitor and Analyze an organization's network traffic for unusual and potential threats.
- Event and Log Correlation: Analyze security event data from Domain Tools and correlate it with an in-house SIEM. Conduct log analysis using an AI-Based Disruption Tool integrated with the SIEM. Perform event and log correlation to detect patterns or anomalies that could indicate malicious activities. Correlate to uncover hidden threats, reduce false positives and prioritise incidents that need immediate attention.
- Incident Management: Follow standard operating procedures (SOPs) to analyze, escalate, and assist in the remediation of critical information security incidents. Investigate and take down compromised credentials, Phishing/spoofed domains, and phishing emails. Raise incidents with concerned teams, respond to incidents and service requests, and gather additional information to either resolve or escalate issues.
- Monitoring and Analysis: Monitor and analyze security events to determine intrusion and malicious activities. Detect suspicious events, analyze intension of the attacker and create reports that are easily understandable by clients. Conduct monitoring of fraudulent domains and vulnerable websites to ensure the integrity and protection of the organization's brand reputation.
- Malware Analysis: Perform static malware analysis. Analyze suspicious files and activities. collect and document relevant data, create initial reports and escalate complex cases to L2 analysts for the remediation process.
- Customer Interaction: Promptly respond to customer inquiries via phone, email, mail, or social media. Take follow-ups and close tickets based on client responses, providing communications related to security events. Contributed to a 30% increase in the customer base during 2023 due to the delivery of quick service.
- Open-Source Tool Utilization: Use open-source tools to identify and investigate malicious phishing emails, domains, and IPs, and recommend appropriate blocking measures based on analysis and using Vulnerability scanning tool to discover loopholes.
- Escalation: Gather all the information and evidences with clear documentation of the incident, including detailed logs and initial findings and escalate issues to Level 2.

EDUCATION

Bengaluru North University - Krupanidhi Group of Institutions- Bengaluru

Master of Computer Application (MCA)

2020-2022

PROFESSIONAL SKILLS

- Experience in analyzing email headers and blocking domains on MX server/Email server.
- Comprehensive grasp of Information Security Principles, Technologies, and Best Practices.
- Specialised knowledge in Firewall, TCP/IP, Network Security,IDS, IPS and Encryption Standards.
- Understanding of cyber kill chain, software development lifecycle and Knowledge on different types of malware, attack vectors, and mitigation techniques.
- Experience in creating Playbooks, monitor dashboards and investigating workflows
- Demonstrates excellent written and verbal communication skills.
- Raising incident with concerns teams, respond to the incidents and service requests and bring together additional information to either resolve or escalate the issue to the appropriate teams.
- Take follow-ups and closing of the tickets based on the client response. Provide communications relating to security events.
- Detecting suspicious event, analyzing graphs and creating reports for easy understandable by client .
- Excellent communication skills with a focus on team-building and customer relations.
- Blocking malicious Url's , sender id and domains to prevent from future attack.

TOOLS AND TECHNOLOGIES

- **OS:** Windows, Mac
- **Vulnerability Scanning:** Nessus
- **Email Gateway:** Barracuda
- **OSINT Tools:** Virus Total, MX Toolbox, URLScan.io, CentralOps, WhoIs Lookup, Cisco Talos
- **SIEM Tools:** In-house SIEM with Sentinel

CERTIFICATIONS

- Cyber Security Virtual Experience Program by MasterCard
- Cisco Verified End Point Security

LANGUAGE COMPETENCIES

- English: Full Professional Proficiency (speaking, reading, writing)
- Kannada: fluent (speaking, reading, writing)
- Hindi: intermediate (speaking, reading, writing)
- Telugu: fluent (speaking, reading , writing)