Personal Data

✉ akshatahujare@gmail.com

📱 9370540329

📅 25/08/1998

📍 Pune, Maharashtra India

Education:

» **B.Tech (Computer)** Dr. Babasaheb Ambekar University, Lonere, Maharashtra, India

» **HSC (Science)** Maharashtra State board, India

» **SSC** Maharashtra State board, India

Languages:

» English

» Hindi

» Marathi

AKSHATA MARUTI HUJARE

Professional Summary:

A detail-oriented Security Operations Centre (SOC) Analyst with a solid foundation in cybersecurity principles and proven experience in monitoring, analyzing, and responding to security incidents. A dept at conducting in-depth log analysis, contributing to incident response efforts, documenting security incidents, and collaborating effectively with cross-functional teams. With a commitment to continuous improvement, actively participating in enhancing SOC processes and maintaining a vigilant security posture.

Work Experience & Responsibilities:

DXC Technology.
Professional II Information Security *(February 2022 to November 2024)*

- A Cyber Security Analyst with 2.10 years of experience.
- Monitoring and actioning the security alerts from different SIEM tools such as Azure Sentinel, Defender and ArcSight, CrowdStrike for multiple customers.
- Identifying and responding to threats.
- Documenting incident details, findings, and remediation responses.
- Investigate malicious phishing emails, domains and Ips using open-source tools and recommend proper based on analysis.
- Identify suspicious/malicious activities.
- Maintaining the SLA, following SOPs and runbooks for the alert escalation and triage process.
- Following up with clients and Security Leads on the necessary incidents.
- Analyzing incidents and alerts by collecting, detecting, and investigating from the data collected through the logs. Checking for IOC's and potentially malicious entities by analyzing the logs.
- Making the initial analysis and investigation and escalating it to the next Tier whenever necessary. Determining the True Positive and False Positive events.
- Working in a SOC team which operates 24/7.
- Sending the Handover and alerts reports to the team, attending the daily Cyber Defense call to know the daily trends and updates.

Skills:

- Microsoft Azure Sentinel
- Microsoft Defender for endpoint and O365
- Microsoft Defender for cloud apps security and Identity
- Information and Event Management (SIEM),
- Security Monitoring
- Log Analysis
- SOC Operations
- CrowdStrike
- Splunk
- PDGS/ Falcon
- ServiceNow
- ArcSight

Certifications:

- Microsoft Azure - AZ-900 and Microsoft Security (SC-900)
- FALCON 101- Falcon Platform Technical Fundamentals
- Qualys Certified Specialist - Vulnerability Management Detection & Response
- ESM200D-76 - ArcSight ESM 7.6 Administrator and Analyst
- CQL 101 - CrowdStrike Query Language Fundamentals 1
- Certified Cyber security SOC Phishing analysis from Scratch
- Certified Sumo Logic
- Certified SC-200-2023-Microsoft Security Operations Analyst
- Certified Phishing email investigation
- FALCON 104 - Getting Started with the Endpoint Security Module
- FALCON 120 - Investigation Fundamentals
- Qradar-Modern IBM 7.5 SIEM Administration (Udemy)

Declaration:

I hereby declare that the above written particulars are true and correct to the best of my knowledge and belief.

Date:

Place:

(Akshata M. Hujare)