Aman Singh
SOC Analyst, Vertisystem Global Private Limited, Indore
Mobile: 8882418162
E-Mail- caaman.singh123@gmail.com

Career Objective

To associate with an innovative and vibrant organization, allowing me to put my competencies to the best use, to add value to the organization and contribute to my overall growth as an individual.

Professional Summary

- **Tools Used:** Crowdstrike Falcon, MS Defender/Azure/Entra admin, Carbon Black, Botsink, Forcepoint DLP, Duo Admin, Stealth Defend, Stealth Audit, Secret Server
- **SIEM Tools:** Exabeam, Optiv (Devo), ArcSight
- **Vulnerability Management:** Qualys, Nessus
- **Incident Analysis Tools:** Anyrun Sandboxing , CISCO Talos, Mx Toolbox, Virus Total etc.
- **Certifications:** SIEM SOC Analyst Foundation, SIEM certified SOC Expert, Qualys Vulnerability Management, Fortinet NSE1,NSE2

- A competent professional with 3.2 **Years** of experience, Presently working in **VertiSystems Global Private Limited as Security Analyst.**
- Cyber Security Analyst with proficient and thorough experience and a good understanding of information technology.
- Specialized in proactive network monitoring of SIEM
- Good understanding of security solutions like Anti-virus, Firewall, IPS/IDS, Email Gateway, Proxy etc.
- Hands on experience with Optive (Devo), ArcSight SIEM tool for logs monitoring and analysis.
- Hands on over Jira, Sharepoint, Security onion, Service Now ticketing tool for incident management.
- Good knowledge on networking concepts including OSI layers, subnet, TCP/IP, ports, DNS, DHCP etc.

Organizational Experience

Security Analyst – January 2024- Till date in VertiSystems Global Pvt Ltd.

Job Responsibilities:

- **Phising Emails: (I)** Doing **Header analysis** to Check DMARC,SPF,DKIM, Return path Via open source tools like MS Azure Header Analyzer, CISCO Talos,WHOIS.

  (ii) Checking Various Urls or attachments using sandboxing tool Anyrun.

- **Botsink Alerts:** Investigating and Mitigating alerts like, ARP Flood, Duplicate IP address detected, Multiple hosts resolve to single IP.
- **MS Defender Alerts:** Using Defender to Mitigate alerts like Impossible travel activity, Malicious links Clicked by user.
- **Crowdstrike Incidents:** Investigating alerts like Privilege escalation via process injection, Execution via command and scripting interpreter, Execution via malicious file
- **Carbon Black Approval Requests:** Manually approving/blocking the execution of specific files on end point devices.
- **Optive Incidents:** Mitigating Alerts like Network mapping, Brute force attack, Netskope alerts on DLP.

VULNERABILITY MANAGEMENT DETECTION & RESPONSE (VMDR)

- Managed vulnerability and security tasks using Jira, prioritizing and tracking progress through project workflows.

IDENTITY & ACCESS MANAGEMENT (IAM)

- Hands on in Privileged Access Management Utilizing PowerShell scripting for Identity and Access Management (IAM) tasks, including Creation and management of privileged accounts, Assigning role groups and permissions.
- Experience configuring role-based access control (RBAC), attribute-based access control (ABAC), and policy-based access control.

Previous Experience

Security Analyst – November 2021- December 2023 at Geniebee Systems Pvt Ltd.
Job Responsibilities:

- Working in a 24x7 Security Operations Center
- Monitoring the customer network using SIEM
- Analyzing real time security incidents and checking whether its true positive or false positive
- Escalating the security incidents based on the client's SLA and providing meaningful information related to security incidents by doing in-depth analysis of event payload, providing recommendations regarding security incidents mitigation which in turn makes the customer business safe and secure.

Education

- **B.Com, DHSGU Central University in 2013**
- **CA Finalist May 2021**

(Aman Singh)