Md Waish Siddiqui

Address : Okhla , Jasola vihar
Delhi

E-mail: mdwaish2801@gmail.com
Phone: +91-8738844922

SUMMARY

- A technology-oriented professional with 1 years of expertise in specializing in security monitoring, threat detection, and incident response. With hands-on
- experience in managing SIEM tools, performing initial triage, and responding to security incidents, he plays a critical role in safeguarding organizational
- infrastructure. Hands-on exp on SIEM (Splunk), Hold Certifications || Splunk Fundamentals || CEH v13 ||

WORK EXPERIENCE

CyberON Technologies Pvt Ltd — NOV 2023 — Present

Designation : SOC Analyst

- Monitor and analyze network traffic, system logs, and security alerts using SIEM tools such as Splunk to identify potential security threats and incidents.
- Investigate, triage, and respond to security incidents, ensuring prompt detection, response, and mitigation of risks.
- Conduct regular vulnerability assessments and collaborate with teams to address weaknesses in network and system infrastructure.
- Utilize Splunk and other security tools to correlate events, create dashboards, and escalate incidents based on severity.
- Support the development and execution of incident response procedures, reducing recovery time and minimizing damage.
- Generate comprehensive reports on security incidents, system health, and compliance metrics for internal stakeholders.
- Stay updated on emerging security trends, threats, and best practices to enhance overall security posture.

Reload digital India Pvt Ltd — Sep 2022 — Nov- 2022

Designation : Intern Cybersecurity Analyst

- Managing SOC (Security Operations Center) operations, also involve optimizing resource allocation, meeting customer and senior management requirements.
- Security event investigation, qualified potential security breaches, raise security incident alerts and perform technical & management escalation
- Established the advisory process for handling all threat intelligence feeds received by the organization.
- Formation of Threat Hunting services for multiple projects and execution of process in daily operations
- Crafting SOPs (Standard Operating Procedures) for incidents generated by SIEM.
- Use-case, Dashboard, & SIEM Report Modification/creation based on customer requirement
- Performed internal audit for SIEM technology on other projects to improve the entity's operation

CERTIFICATIONS

- Cybersecurity Threat Hunting for SOC Analysts -Udemy Online course
- Certified Threat Intelligence Analyst (CTIA) - EC Council Certified
- Certified Ethical Hacker (CEH v13) - EC Council Certified
- Fundamentals Certified Splunk Fundamentals Certified Online course

EDUCATION QUALIFICATIONS

BCA

Aug 2021 — Jun 2024

IIMT GROUP OF COLLEGES, Greater Noida Cleared 1st Division in

FROM CHAUDHARY CHARAN SINGH UNIVERSITY

Intermediate

April 2018 — March 2020

SETH M.R JAIPURIA SCHOOL BABATPUR Passed 1st Division in Physics, Chemistry, Math's, English and Hindi (CBSE Board).

High school

April 2016 — March 2018

SETH M.R JAIPURIA SCHOOL BABATPUR

Passed 1st Division in all Subjects (CBSE Board).

HANDS ON EXPERIENCE

- Security Tools: Splunk, VMware, kiwi- Syslog, Proxy, Smokescreen
- Ticketing Tools: Demisto, Threat Center, Service Now
- Network Device: Cisco Router 3800 Series, Cisco Switch 3750G, 3560
- NETWORKING CABLES: UTP Ethernet Cable, Coaxial (RG6 & RG11) Cable, Optical Fiber (12 /24 core)

EXTRA CURRICULAR ACTIVITY

- National-Level Air Pistol Shooter
  Competed at the national level in air pistol shooting.
  Won 2nd prize in a state-level competition, showcasing precision, focus, and dedication.

- Cultural Fest Organizer – College
  Managed and organized all cultural fest activities, including event planning, budgeting, and coordination.
  Developed strong leadership, organizational, and communication skills through successful execution of large-scale events.

HOBBIES

- Playing computer games
- Playing Sports