NAVEENKUMAR

Security Analyst

+91 6380178584 • Chennai • https://nacn-25.github.io • naveennk055@gmail.com

ABOUT ME

Cybersecurity professional with nearly five years of dedicated experience in Security Operations, Incident Detection and Response. I possess deep expertise in designing, testing, and fine-tuning detection rules across SIEM, WAF, EDR, and NIPS platforms to minimize false positives and expedite the identification of genuine threats. I have successfully automated numerous workflows to eliminate manual effort and enhance operational efficiency. Strong communicator, skilled in crafting concise technical reports.

EDUCATION

KARPAGAM ACADEMY OF HIGHER EDUCATION
BCA - Bachelor of Computer Application 2017 - 2020

PALANI GOUNDER HIGHER SECONDARY SCHOOL
HSC 2015 - 2017

CERTIFICATION

- **EC COUNCIL CERTIFIED SECURITY ANALYST (CSA)**
- **ISC^2 CERTIFIED SECURITY OPERATIONS ANALYST ASSOCIATE**
- **MICROSOFT : SECURITY OPERATIONS ANALYST ASSOCIATE (SC-200), CERTIFICATE ID 1687-8656**

SKILL

- Securitytools : SIEM, EDR(Crowdstrike, NIPS(Cisco ftd and fmc), WAF and NGFW (Fortigate)
- Python, Basic : Java, Bash, JavaScript and C
- Operating System: Linux and Windows
- Application, Network, Endpoint, Email Security
- Wireshark, NMAP, Burp suite, Email header analysis
- Written and verbal communication

WORK EXPERIENCE

ZOHO Corporation

SEP 2023-NOW

Security Analyst

- Developed detection rules tailored to trends and the specific environment, refining them to minimize false positives. This includes implementing Regex-based parsers and enrichment pipelines.
- Triage and investigation of security alerts generated by SIEM, WAF, IPS, and EDR platforms, including those escalated by junior analysts.
- Coordinate and escalate confirmed incidents to the Incident Response team, providing detailed findings and analysis and remediation.
- Implement automated SOC workflows and reporting to reduce manual efforts.
- Provide training and raise awareness about security practices for junior staff and users.

Tata Consultancy Services (TCS)

OCT 2020 - SEP 2023

SOC Analyst (L1 &L2)

- Functioned within a 24/7 Security Operations Center, analyzing and escalating security alerts to incident response teams.
- Collaborating with the team to perform security assessments and risk analyses.
- Developing and sustaining reports, playbooks, and standard operating procedures (SOPs).
- Adjusting or developing a log parser utilizing regex (Regular Expression).
- Learned new skills and applied to daily tasks to improve efficiency and productivity.