Naveenkumar

nacn-25.github.io | linkedin.com/in/naveennk055
Location: Chennai, India
Email: naveennk055@gmail.com | Mobile: 91+ 6380178584

Security Engineer

Cybersecurity Professional with **5 years of Security Operations Center (SOC), Incident Detection and Response** experience. Proven track record of designing and fine-tuning **SIEM/EDR/IPS** detection rules to **reduce false positives by 70%**. Proficient in automating security workflows using scripting languages.

Technical Skills

SecurityPlatforms SIEM (DNIF, Splunk), EDR/XDR (Crowdstrike, SentinelOne), NIPS (Cisco FTD and FMC), WAF and NGFW (Fortigate), SOAR (Cortex XSOAR)

Threat Detection : SIEM rule development, Snort/Sigma rules, YARA signature creation, MITRE ATT&CK framework, regex tuning

Security Tools : Wireshark, Nmap, tcpdump, Burp Suite, Volatility

Languages : Python, Bash, JavaScript, Java, HTML, CSS

OperatingSystems Linux, Windows

Experience

Security Analyst SEP 2023 – Present
ZOHO Corporation *Chennai, India*

- Developed and fine-tuned detection rules to cut **false positives by 50–70%.**
- Handled alerts from **SIEM, WAF, IPS, and EDR**, escalating and coordinating actions throughout the incident lifecycle.
- Collaborated with Security teams to identify and detect emerging threats
- **Automated** SOC workflows and reporting, reducing manual overhead
- Mentored junior analysts, raising SOC awareness and skill levels.

SOC Analyst (L1 & L2) Oct 2020 – Sep 2023
Tata Consultancy Services (TCS) *Chennai, India*

- Functioned within **247 SOC**, handling real-time threat detection, triage, and escalation.
- Conducted **log analysis and parser tuning (regex)** to enhance detection accuracy.
- Supported risk assessments, vulnerability reviews, and security controls testing.
- **Documented incidents and alerts handling** processes and maintained knowledge base articles.

Projects

Feed Ingestion : Developed scripts to fetch and parse multiple threat intelligence feeds and ingest indicators into the SIEM, automating enrichment of alerts; reduced analyst triage time by 50%.

AlertManagement Developed a script to detect and merge duplicate alerts, improving efficiency.

Certifications

- EC COUNCIL : Certified SOC Analyst (CSA)
- ISC2 : Certified in Cybersecurity (CC)
- MICROSOFT: SECURITY OPERATIONS ANALYST ASSOCIATE (SC-200)

Education

KARPAGAM ACADEMY OF HIGHER EDUCATION Coimbatore, India
BCA-Bachelor of Computer Application *2017 – 2020*