NARAYANAN K

Cybersecurity

Edappal,Kerala | narayanank468@gmail.com | +91 7034599845 | Linkedin

Professional Summary

SOC Analyst fresher with foundational knowledge in Security Operations, network defense, and incident handling. Skilled in monitoring security events using SIEM tools, analyzing alerts, and identifying potential threats. Hands-on experience with lab simulations of threat detection, log analysis, and security incident triage. Familiar with security frameworks, intrusion detection systems (IDS/IPS), and common attack vectors. Strong foundation in networking concepts such as TCP/IP, DNS, HTTP/HTTPS, and firewalls. Continuously learning malware analysis, digital forensics, and vulnerability management to enhance SOC operations expertise.

Skills

Cybersecurity Tools: Splunk, Sumologic, Cybereason EDR, Sophos XDR , Cymulate, Wazuh, ELK Stack, Wireshark, Suricata/Snort, Nmap, Nessus, OpenVAS, Burp Suite, MISP, Zeek.
Security Operations: SIEM Monitoring, Log Analysis, Incident Response, Threat Hunting, Packet Analysis, MITRE ATT&CK, Alert Triage, Network Monitoring.
Networking & Security Fundamentals: Firewalls, VLAN, VPN, IDS/IPS, OSI & TCP/IP Models, DNS, HTTP/HTTPS, ICMP, ARP, Network Devices, Access Control.
Operating Systems: Windows (Client & Server), Linux (Ubuntu, Kali).

Projects

Automated Incident Response System for SOC: Built a Python-based system integrated with SIEM tools (Splunk, ELK Stack) to automate malware, phishing, and brute-force incident responses. Used Threat Intelligence APIs (VirusTotal, AlienVault OTX) for real-time analysis, reducing manual response time by 30%.
SIEM Data Analysis for Threat Detection: Analyzed security logs with Splunk and ELK Stack, creating correlation rules for detecting brute-force, malware, and privilege escalations. Automated incident reporting and enhanced detection accuracy through threat intelligence integration.

Certificates

Introduction to cybersecurity – CISCO
Cybersecurity – Blearn

Education

B.E Computer Science Engineering – Hindusthan College Of Engineering And Technology,Coimbatore
Diploma In Computer Engineering – Hindusthan Polytechnic College,Coimbatore

Soft Skills

- Incident report writing & documentation
- Analytical thinking & problem-solving
- Time management in high-pressure environments
- Team collaboration & cross-functional communication
- Adaptability & quick learning
- Attention to detail in threat analysis

Launguages

Python (automation, log parsing, incident scripts), **Bash scripting** (Linux automation), **SQL** (security log queries, database analysis)

Soc Specific Skills

Incident triage & prioritization, Security event correlation & log analysis, SIEM dashboard creation & alert tuning, Threat intelligence integration & enrichment, Documentation of incidents & playbooks, Use of MITRE ATT&CK for threat classification, Writing post-incident reports & lessons learned.

Declaration

I hearby declare that the information furnished above is true to the best of my knowledge and belief

Narayanan k