

SHAHIL KHAN

SOC Engineer L1

+91 73563 73946 | shahilkhansh@outlook.com | Kerala, India

CAREER SUMMARY

Cybersecurity professional with 2+ years of experience in security monitoring, incident response, and vulnerability management. Skilled in SIEM tools (Wazuh, Splunk, AlienVault), threat intelligence, penetration testing, and cloud security (AWS, Azure). Strong understanding of network protocols, log analysis, and risk mitigation. Passionate about securing digital infrastructures with proactive threat detection and response strategies.

WORK EXPERIENCE

Worksent

SOC Engineer L1 | 2023 - Present

- Improved threat detection and response efficiency by deploying and configuring Wazuh SIEM, reducing incident resolution times.
- Monitored security alerts from SIEM tools, firewalls, and IDS/IPS to identify and mitigate cyber threats.
- Conducted vulnerability assessments using Nessus and BurpSuite, reducing security risks.
- Triaged security events, performed intrusion detection, and escalated critical incidents to the appropriate teams, ensuring swift remediation.
- Performed operating system updates, upgrades, and patches, bolstering system security and minimizing vulnerabilities.
- Performed malware and phishing analysis, investigating suspicious emails and mitigating attacks.
- Delivered actionable insights to management via detailed incident reports and weekly/monthly security summaries.
- Collaborated with security teams to improve SOC operations in a 24x7 environment

PROJECTS

1. VAPT

- Conducted automated vulnerability assessments using Nessus and BurpSuite to identify critical flaws in target Web Application.
- Exploited privilege escalation vulnerabilities to demonstrate real-world exploitability and potential impact.
- Delivered comprehensive documentation detailing identified vulnerabilities, severity levels, and actionable remediation strategies.

2. Logical Design of Network Infrastructure

- Designed and implemented a secure network architecture tailored to organizational requirements, ensuring operational efficiency and data protection.
- Deployed Port Address Translation (PAT) to enhance privacy and secure external communication.
- Configured a DHCP system to automate IP address assignments, streamlining network management.

3. Security Information and Event Management (SIEM) Deployment

- Deployed and optimized Wazuh SIEM for real-time threat monitoring.
- Configured log sources and fine-tuned detection rules to reduce false positives.

SKILLS & TOOLS

Security & Threat Detection:

✔ Security Monitoring | ✔ Incident Response | ✔ Threat Intelligence | ✔ Malware Analysis

Technical Expertise:

✔ SIEM (Wazuh, Splunk, AlienVault) | ✔ IDS/IPS | ✔ Firewalls | ✔ AWS Security

Networking & Protocols:

✔ TCP/IP | ✔ DNS | ✔ HTTP/S | ✔ VPN | ✔ FTP

Penetration Testing & Compliance:

✔ Nessus | ✔ BurpSuite | ✔ Security Auditing | ✔ Cloud Security

CERTIFICATIONS

- Fortinet NSE 1, 2, 3 – Network Security Associate
- Splunk Infrastructure Overview
- CISCO Cybersecurity Essentials
- Palo Alto Fundamentals of SOC

EDUCATION

- **Bachelor of Computer Application - BCA** 2019 - 2022
University Of Calicut
- **Higher Secondary School** 2017 - 2019
PHSS - Computer Science

LANGUAGES

- English
- Hindi
- Arabic
- Malayalam

