Sahil Dipak Shriwas *Cybersecurity Analyst*

Sahilshriwas02@gamil.com

9322953009

Pune, Maharashtra

linkedin.com/in/sahil-shriwas-470a57235

tryhackme.com/p/Sahilshriwas

Profile

Cybersecurity Analyst with hands-on experience in SOC environments, penetration testing, and incident response. Proficient in SIEM (SeconIT), Cortex XDR, and multiple cybersecurity frameworks and standards (NIST, GDPR, PCI-DSS, HIPAA, ISO-27001). Strong skills in monitoring, detecting, and responding to threats, with practical knowledge in compliance, vulnerability assessment, and threat mitigation.

Professional Experience

SOC Analyst
Altisec Technologies Pvt Ltd | 06/2024 - Present

- Monitor and respond to real-time security incidents using SeconIT SIEM and Cortex XDR.
- Conduct in-depth analysis of events, alerts, and anomalies, identifying potential threats.
- Contribute to the SOC team on incident response and threat mitigation.
- Maintain SOC documentation and process enhancements to optimize security posture.

Penetration Testing Intern
CFSS | 11/2023 - 12/2023 | Remote, India

- Executed penetration tests utilizing Nessus, Burp Suite, and Metasploit.
- Created comprehensive reports with remediation recommendations for vulnerabilities discovered.

Hackostric Pentesting Intern
Data Insider | 05/2023 - 07/2023 | Amravati, India

- Conducted vulnerability assessments focusing on OWASP Top 10 risks.
- Collaborated with cybersecurity teams for remediation and process improvements.

Cyber Security Engagement Intern
Data Insider | 09/2022 | Amravati, India

- Assisted in developing and implementing security policies for organizational security.
- Enhanced practical skills in risk management and threat identification

Projects

1. Web Application Security Assessment Project

- Conducted a full-scale security assessment of a web application, focusing on OWASP Top 10 vulnerabilities.
- Utilized tools such as Burp Suite and Nessus for vulnerability scanning and manual penetration testing.
- Presented detailed findings with recommendations, resulting in a 50% reduction in identified security risks.

2. Network Security Monitoring Using SIEM

- Set up and configured Seceon SIEM for a simulated network environment to monitor and log security events.
- Created custom dashboards and alerts for various threat vectors, including brute force attacks, malware detection, and unauthorized access.
- This project provided a comprehensive view of network security status, demonstrating proficiency in SIEM configuration and analysis.

3. Endpoint Security Implementation with Cortex XDR

- Led a project to deploy Cortex XDR on virtual endpoints to detect and respond to threats in real time.
- Developed response playbooks and incident workflows, enhancing the speed and accuracy of threat responses.
- Documented the setup process and trained peers on using XDR tools for future endpoint security needs.

Key Skills

Cybersecurity | Information Security | Network Security | Application Security | Data Security | OS Security | Malware Analysis | Frameworks | SIEM (Wazuh, SentinelOne, Splunk, Seceon) | Identity Access Management | Encryption | Vulnerability Assessment and Penetration Testing (VAPT) | Incident Response | NIST | GDPR | PCI-DSS | HIPAA | ISO-27001 | SOC Cortex XDR | SOAR | Burp Suite | Nmap | Metasploit | Nessus | Wireshark | Python

Achievements

- Identified and reported multiple vulnerabilities in top MNCs, demonstrating strong skills in vulnerability assessment and threat mitigation.

Cyber Security Intern

Skolar | 11/2023 - 01/2024 | Remote, India

Participated in compliance audits and security assessments using tools like Nmap and Wireshark.

Education

B.Voc Cyber Security

H.V.P.M College of Engineering and Technology

2021/07 – 2024/05 | Amravati, India

HSC

Manibai Gujrati High School And Junior College

2019/07 – 2021/04 | Amravati, India

Courses

Cyber Security

Skolar | Remote, India

2023/11 – 2024/01

Ethical Hacking for Beginners

Simplilearn

2022/12 | Remote, India

Ethical Hacking Essential (EHE)

EC-Council

2022/12 | Remote, USA

- Developed a foundational understanding of cybersecurity fundamentals, including threat detection and risk management.

Certificates

- ISO Information Security Associate Certificate
- Ministry of Electronics & IT - Password Security Certificate
- 50-day Cybersecurity Training, Data Insider

SOFT SKILL

Communication skills

Teamwork

Problem-Solving