SATYABRATA BEHERA

+91 7008004557 | Noida, India
satyabratabehera645@gmail.com | LinkedIn |

EDUCATION

Jain University **Bangalore, India**
Master of Computer Application in ISMS, CGPA: 7.45 August 2021 – Jun 2023

EXPERIENCE

Cyber Security Engineer **Noida, India**
Alyssum Global Services September 2024 – Present

- Designed and implemented the architecture of an MDR platform, integrating SIEM, log management, SOAR, and threat intelligence tools for centralized detection and incident response.
- Implemented log ingestion using Fluent Bit and Graylog, and integrated TheHive and Cortex for alert triage, enrichment, and response.
- Integrated MISP threat intelligence, mapped detections to MITRE ATT&CK, and built automation scripts to improve SOC efficiency.
- Deployed and configured Wazuh SIEM across multiple endpoints for centralised log collection, analysis, and threat detection.
- Conducted real-time log monitoring and correlation of over 1,000 system logs weekly, reducing average incident response time by 30 minutes.
- Customized Wazuh rules, decoders, and active response scripts to detect brute-force, malware, and privilege escalation attempts.
- Performed penetration testing using tools like Burp Suite and Nessus; discovered and documented 15 vulnerabilities (2 critical, 3 high), with remediation strategies.
- Created structured incident response reports with actionable mitigation steps, contributing to improved overall SOC efficiency.

VAPT Training **Bangalore, India**
Forensic. Academy May 2024 – June 2024

- Conducted vulnerability assessments using industry-standard frameworks; improved detection capabilities by integrating findings into security protocols, which enhanced overall response time to threats by 40%.
- Achieved a 95% accuracy rate in identifying critical vulnerabilities and provided actionable insights for enhancing security posture.

Cyber Security Intern **Bangalore, India**
Rubixe June 2023 – December 2023

- Conducted comprehensive vulnerability assessments and penetration tests, identifying 15 critical security vulnerabilities; implemented fixes that fortified system defenses and reduced potential security risks by 45%.
- Assisted in the preparation of detailed reports and documentation for management and regulatory bodies, outlining security incidents, mitigation strategies, and overall security improvements. Analysed over **100+** security documentation and reports to ensure compliance with industry standards and regulations.

SKILLS

- **Technical Skills:** SIEM, MDR, EDR, Log Management, IAM, Scripting & Automation (Bash, Python – basic), Network & Application Security
- **Cyber Security Frameworks:** ISO 27001, NIST, MITRE ATT&CK, OWASP Top 10
- **Soft skills:** Problem analysis, Incident Handling, Communication, Teamwork, Management, Resiliency
- **Tools:** Wazuh, Fluent Bit, Graylog, TheHive, Cortex, MISP, Wireshark, Keycloak, Zitadel, Nessus, Qualys, Kali Linux, Maltego, VirusTotal, Zap Proxy, Metasploit

PROJECTS

Wazuh SIEM Implementation

- Deployed Wazuh in an enterprise setup for centralized log collection and security monitoring.
- Tuned detection rules for custom alerts on brute-force, malware, and system anomalies.
- Improved threat detection efficiency by 35% through log correlation and automated responses.

MDR Platform Development

- Designed the end-to-end MDR platform architecture, defining log ingestion, correlation, enrichment, and response workflows.
- Implemented integrations using Fluent Bit, Graylog, Wazuh, TheHive, Cortex, and MISP.
- Built automation and ATT&CK-aligned detections to improve SOC visibility and response efficiency.

Implemented IAM Solution

- Deployed and configured Identity and Access Management (IAM) solutions for internal office infrastructure.
- Implemented Zitadel and Keycloak for centralized authentication, authorization, and role-based access control (RBAC).
- Integrated IAM services with internal applications to enforce secure access policies and reduce unauthorized access risks.

API Security Testing

- Performed security testing of REST APIs using Postman, Burp Suite, and OWASP ZAP.

- Detected and reported vulnerabilities including IDOR, Broken Authentication, and Sensitive Data Exposure.
- Validated JWT and OAuth 2.0 implementations; ensured compliance with OWASP API Security Top 10.
- Documented findings with PoC, CVSS scores, and mitigation recommendations.

VAPT Project (Web & Network)

- Conducted vulnerability assessments and penetration testing using Nmap, Nessus, Burp Suite, and Metasploit.
- Identified and exploited critical issues including SQL Injection, XSS, and misconfigurations.
- Aligned findings with OWASP Top 10 and CVE standards; delivered detailed reports with CVSS scoring.
- Validated remediation through re-testing and supported secure system hardening.

CERTIFICATES

- **Certifications:**
  EC-Council: CEHv12
  Internshala: Ethical Hacking
  NASSCOM: Ethical Hacking
  LinkedIn Skill Assessment: Passed Cyber Security test.

ACHIEVEMENTS

- **PortSwigger:** Solved **60+** hands-on labs on PortSwigger Web Security Academy (focused on XSS, SQLi, IDOR).
- **Research Paper:** Published a peer-reviewed paper in JETIR journal titled ‘KYC Verification in Banking System Based on Blockchain’; provided a framework for secure, efficient KYC processes, reducing verification time by 40%.