SAMMED VIDYASAGAR BUKSHETE

📍 Pune. | ✉️Sammedb0@gmail.com| 📞+91 9834444959|
🔗 linkedin.com/in/sammed-bukshete-a9b326343
🔗 Google Scholar: https://scholar.google.com/citations?user=xV0AJLcAAAAJ

PROFESSIONAL SUMMARY

Cyber Security professional with 3+ years of experience in Security Operations Center (SOC) operations, SIEM monitoring, and Vulnerability Assessment & Penetration Testing (VAPT). Holder of internationally recognized EC-Council certifications including Certified Ethical Hacker (CEH) and Certified SOC Analyst (CSA). Demonstrated expertise in log analysis, alert correlation, and threat detection using tools such as Splunk, Wireshark, and Burp Suite.

Successfully designed and delivered 50+ hands-on cybersecurity training sessions and 30+ practical labs, enhancing real-world security skills for 500+ learners, and supervised 15+ postgraduate students across two institutions in SOC operations and applied cybersecurity research.

Actively engaged in cybersecurity research with multiple publications in peer-reviewed journals, focusing on areas such as network security, QR code-based attacks, and cybersecurity ethics, with contributions recognized through indexed publications and citations.

Research interests include AI-driven cybersecurity, SIEM optimization, and false positive reduction in SOC environments, with a strong focus on developing intelligent and adaptive threat detection systems for real-world applications. Currently applying for PhD research in Australia, focusing on adaptive and explainable AI-based SIEM alert correlation for false positive reduction in SOC environments.

CORE COMPETENCIES

- **Security Tools:** Nmap, Metasploit, Burp Suite, OWASP ZAP, Wireshark, Nessus, OpenVAS, SQLMap
- **SOC & SIEM:** Splunk, Log Correlation, Incident Detection, IOC Analysis
- **Web Security:** OWASP Top 10, SQLi, XSS, CSRF
- **Threat Monitoring:** IDS/IPS (Snort), Packet Capture, Threat Hunting
- **Scripting:** Python, Bash, PowerShell
- **Frameworks:** MITRE ATT&CK, NIST, ISO 27001
- **Penetration Testing:** Web App Testing, Network Scanning, Exploitation
- **Platforms:** Linux, Kali Linux, Windows Security
- **OSINT Tools**: VirusTotal, Threat Intelligence Platforms

PROFESSIONAL EXPERIENCE

Assistant Professor – Cyber Security

MIT ACSC, Pune | Aug 2025 – Present

- Delivered 50+ hands-on training sessions in ethical hacking and SOC operations, enhancing practical cybersecurity skills among 500+ students in network defense and incident response.
- Conducted 30+ practical labs on scanning, exploitation, and threat detection, improving student understanding of real-world attack scenarios.

- Designed cybersecurity practical labs aligned with MITRE ATT&CK and OWASP methodologies.
- Guided students in CTFs, bug bounty basics, and research activities.
- Supervised 10 postgraduate students in SOC and WAPT projects, mentoring them in threat detection, vulnerability assessment, and applied cybersecurity research.

Assistant Professor – Cyber & Digital Science

Dr. D.Y. Patil ACS College, Pune | Jan 2023 – July 2025

- Taught cybersecurity, Linux security, digital forensics, and penetration testing.
- Designed and implemented SIEM-based labs using Splunk, enabling real-time log monitoring and alert analysis for simulated SOC environments
- Mentored students in vulnerability scanning using Nmap, Nessus, and OpenVAS.
- Developed academic projects aligned with SOC workflows and security standards.
- Supervised 5 postgraduate students in cybersecurity research projects, guiding them in problem formulation, experimentation, and technical report writing.
- Awarded formal recognition certificate by Dr. D.Y. Patil ACS College for cybersecurity syllabus development and laboratory workbook preparation for the Cyber & Digital Science programme

Coordinator – Cyber Doot Initiative

- Led cybersecurity awareness initiatives, delivering training sessions to **non-technical communities**, improving awareness of cyber hygiene and fraud prevention
- Delivered simplified training on cyber hygiene, online fraud prevention, and safe internet usage.
- Conducted field sessions and interactive demonstrations for public awareness.

Research Interest

- AI-driven Cybersecurity and Threat Detection
- SIEM Optimization and Alert Correlation
- Security Operations Center (SOC) Automation
- False Positive Reduction using Machine Learning
- Threat Intelligence and Log Analytics
- Network Security and Intrusion Detection Systems

Publications

- **Kulkarni, R. P., Bukshete, S. V., & Toke, P. P. (2026)**
  A Hop Count–Based Distance Vector Routing Model for Dynamic Networks.
  International Journal of Latest Technology in Engineering Management & Applied Science (IJLTEMAS).
  DOI- 10.51583/IJLTEMAS **|** ISSN: 2278-2540 | Indexed: ISSN Portal

- **Bukshete, S. V., & Chaudhari, L. (2025)**
  Ethical Hacking Against QR Code-Based Attacks: Simulating Real-World Scenarios of QR Code Exploitation in Public Spaces.
  DOI- 10.51583/IJLTEMAS **|**ISSN: 2278-2540 | Indexed: ISSN Portal

- **Dhondwad, G., Sakhare, A., & Bukshete, S. (2024)**
  The Study on Legal and Ethical Issues in Cyber Security in India.
  International Journal of Research and Analytical Reviews (IJRAR), 11(2).
  DOI- 10.2139/ssrn.4876076
  Indexed: Google Scholar | Citations: 1

RESEARCH SKILLS

- Research Methodology and Problem Formulation
- Experimental Design and Performance Evaluation (Accuracy, Precision, Recall)
- Literature Review and Gap Identification
- Academic Writing and Technical Documentation

CERTIFICATIONS

- **Certified Ethical Hacker (CEH)** – EC-Council | ECC2709615483
- **Certified SOC Analyst (CSA)** – EC-Council | ECC7836240591
- **Ethical Hacker Expert** – Star Certification | STR21EHE00169679
- **Cyber Secure User** – Star Certification | STR19SCU00092112

Projects

- **SOC Log Analysis Using Splunk**
  - Developed dashboards and correlation rules for security monitoring.
  - Detected brute-force login attempts and anomalous user behavior using Splunk dashboards and correlation rules, improving threat visibility in simulated SOC environment
  - Implemented alert systems for threat detection.

- **Malware Traffic Analysis**
  - Analyzed malicious network traffic (PCAP) using Wireshark and identified command-and-control communication patterns, improving understanding of real-world malware behavior
  - Utilized OSINT tools such as VirusTotal for verification and threat intelligence analysis

- **Web Application Penetration Testing**
  - Performed vulnerability assessment and exploited OWASP Top 10 vulnerabilities, identifying security weaknesses and recommending mitigation strategies.

- **Linux System Security Hardening**
  - Implemented SSH security configurations and auditing controls.
  - Configured system monitoring and access control policies.

EDUCATION

- **Master of Computer Applications (MCA)** – Savitribai Phule Pune University | CGPA: 7.98|2024
- **Bachelor of Computer Applications (BCA)** – Shivaji University, Kolhapur | 80%|2022