# UTSAV BHEDA

Information Security Engineer | SOC Analyst | Cybersecurity Specialist
+91-7977036526 ⋄ Mumbai, India ⋄ utsavbheda93@gmail.com
www.linkedin.com/in/utsav-bheda-cybersecurity

## OBJECTIVE

Information Security Engineer with hands-on experience with 2+ years of enterprise-grade DLP (TrendMicro, Forcepoint), email security, and WAF solutions (Akamai). Proven ability to deploy and fine-tune enterprise security solutions (TrendMicro, Forcepoint, Akamai WAF, Microsoft Defender) to reduce incidents, enhance threat detection, and strengthen organizational security posture.

## EXPERIENCE

**Information Security Engineer** June 2023 - Present
Aujas CyberSecurity, Full-Time *Mumbai, India*

- **WAF & Symantec Proxy - UK Client**
  1. Microsoft has deployed and configured Microsoft Defender for Office 365 and MessageLabs to block phishing, malware, and spam, improving the email security posture.
  2. Deployed and managed Symantec Proxy SWG was deployed and managed for enterprise-scale environments, including high-availability setups, SSL interception, and custom policy layers to enforce secure internet access.
  3. Monitored traffic via Akamai Security Center and integrated SIEM for real-time threat detection and mitigation of L7 DDoS, SQLi, and XSS.
  4. Managed IP and URL whitelisting policies, improving accessibility without compromising security.
- **Data Loss Prevention (DLP) - Indian Client**
  1. Reduced DLP alerts by 30% through user training, policy refinement, and real-time data flow monitoring.
  2. Investigated and resolved data loss incidents by performing root cause analysis and implementing rule fine-tuning, reducing incident reoccurrence by 60%.
  3. Implemented DLP policies for PII and financial data on TrendMicro, Seqrite, and Forcepoint DLP platforms.
  4. Led agent deployments and DLP server configurations aligned with enterprise compliance and security standards.

**Cybersecurity Intern – Digital Forensics & VAPT** December 2022 - June 2023
Maharashtra Cyber, Internship *Mumbai, India*

- Created forensic images for over 5+ devices daily, including HDDs, SSDs, and mobile phones, for criminal investigations.
- Conducted analysis using tools like EnCase, FTK Imager, Autopsy, Magnet Axiom, and UFED.
- Drafted legal notices under IT Act (Sec. 91 & 79) and analyzed logs (CDR, IPDR, TDR, firewall) to aid law enforcement.

## EDUCATION

**Bachelor of Computer Science**, Universal College Of Engineering August 2016 - June 2020
GPA - 6.64/10 Mumbai, India
Skills gained: Networking, Kali-Linux, Teamwork, Problem solving, Critical analysis.

## SKILLS

**Technical Skills:** Python, SQL, HTML/CSS, JavaScript, PHP, Networking, Kali-Linux, Penetration Testing

**Security Tools:** Akamai WAF, TrendMicro, Forcepoint DLP, Microsoft Defender for Endpoint & Office 365, MessageLabs, SIEM (Splunk/ELK), EnCase, Autopsy, UFED, FTK, Wireshark, Nessus, Burp Suite, Acunetix, Nmap, Maltego, Symantec Proxy, F5.

**Soft Skills:** Incident Response, Root Cause Analysis, Threat Hunting, Communication, Problem-Solving, Critical Thinking, Team Collaboration

## ACHIEVEMENT

- Ncourage Emerging Champion (FY 23-24).
- Best Customer Champion Award.

## PROJECTS

**Automated System Defense Using Machine Learning**

- Created a research-based project on a local network analysis tool for a real-time platform.
- Researched and prepared a large dataset for machine learning applications to enhance program learning.
- Collaborated in developing a deeper understanding of network packets through Wireshark, focusing on extracting important information for users, and assisting with coding Matplotlib and socket libraries.

## CERTIFICATION

- API & APP Protector Basic Services & Support Certification for Partners
- Symantec Web Protection - Basic Cloud SWG Administration R2
- Ethical Hacking and I.T. Security (MSTB Certification).
- Managed security configurations and protocols in Google Cloud Platform (GCP).
- Web Application Security Testing with Burp Suite.