# SUMBAL ILYAS
**CYBERSECURITY SPECIALIST**

+923063548328
SUMBALILYAS77@GMAIL.COM

(Sumbal Ilyas | LinkedIn)
ISLAMABAD, PAKISTAN

## OBJECTIVE

Experienced Cybersecurity Consultant with expertise in SOC operations, cybersecurity consulting, and business development. Skilled in risk assessments, compliance with ISO 27001, NIST, and PCI DSS, and managing cloud security. Adept at delivering security solutions, developing policies, and driving cybersecurity sales growth.

## SKILLS & ABILITIES

- **SOC Operations & Incident Management**: Skilled in Security Operations Center (SOC) processes, incident detection, and response, including SIEM implementation and threat intelligence.

- **Risk Assessment & Compliance**: Proficient in conducting risk assessments and ensuring compliance with ISO 27001, NIST, PCI DSS, and other industry standards.

- **Cloud Security**: Hands-on experience in cloud security architecture, data protection, and service security management.

- **Cybersecurity Advisory Services**: Expertise in providing tailored cybersecurity solutions and strategic advisory to enhance organizational security.

- **Cybersecurity Sales & Business Development**: Engaged in pre-sales activities, RFP/RFI responses, and technical client consultations to grow cybersecurity sales.

- **Vulnerability Assessment & Penetration Testing (VAPT)**: Experienced with tools like Burp Suite, Nmap, Metasploit, and Nessus for identifying and mitigating vulnerabilities.

- **Security Policy Development**: Adept at developing and enforcing security policies and procedures to enhance IT security posture.

## EXPERIENCE

### 2023-2024 — Cybersecurity Consultant and Business Development Specialist
IPCS-Saudi Arabia-

- Provided expert cybersecurity solutions to USA, Saudi Arabia, and Pakistan organizations.

- Assessed security risks, designed architectures, and ensured compliance with ISO 27001, NIST, PCI DSS, and other U.S. and Saudi standards.

- Conducted vulnerability assessments, incident response, and staff training on cybersecurity best practices.

- Led business development efforts, engaging clients and generating cybersecurity leads.

- Organized webinars and workshops to raise cybersecurity awareness and promote best practices.

### 2022-2024 — Presales Cybersecurity Engineer
Logic Finder – US-based Company

- Worked on U.S. government proposals, including RFPs, RFIs, and white papers for DoD and other federal agencies.

- Implemented cybersecurity measures across multiple platforms, ensuring compliance with U.S. government standards.

- Demonstrated products, highlighting features and benefits to potential clients.

- Specialized in U.S. Government contracting (DoD, DAF, and federal agencies), identifying opportunities, managing RFP/RFI submissions, and navigating the procurement process.

- Led business development efforts, built partnerships, and developed tailored cybersecurity services compliant with FAR/DFARS.

- Drove cybersecurity sales and maintained relationships with key stakeholders in federal agencies.

- Experienced in using GovWin and SAM.gov for federal procurement.

- Delivered cybersecurity services and supported R&D projects, including SOC Tier 1 operations and cybersecurity implementations.

# INTERNSHIP

*2022-2023*          **Cloud Security Engineer**
MicrotechX

- Skilled in cloud data protection and securing cloud services across multiple platforms.

- Developed and implemented digital and social media strategies to enhance company presence.

- Provided operational support and contributed to strategic planning for cloud infrastructure.

- Ensured compliance with industry standards and best practices for cloud security.

*Feb-July 2022*          **SOC Intern**

National Cyber Security Auditing and Evaluation Lab (NCSAEL), MCS NUST

- Implemented a SIEM solution using Elastic Search for log management and threat detection.

- Configured data sources, parsers, and correlation rules to improve incident detection and response.

- Developed custom dashboards and reports to visualize security events and streamline analysis.

- Conducted testing and fine-tuning to reduce false positives and improve accuracy.

- Applied expertise in SIEM, incident handling, threat intelligence, network security, and log analysis to enhance overall SOC operations

# PROJECTS

*2024*          **Engagement with Fintrek Management Consultancies LLC - Dubai**

*Subcontractor (Freelance Basis)*

**Project Description:** Delivered advisory services remotely from Pakistan to clients in the UK and the Middle East.

**Responsibilities:**

- Facilitated workshops with clients and SOC vendors to formalize incident management processes.

- Developed documentation templates and conducted workshops on SOC and security incident management, focusing on evidence collection.

**Relevant Skills:**

- Proficient in remote work practices since 2018, ensuring effective communication and collaboration.

- Demonstrated ability to deliver high-quality advisory services.

- Strong commitment to professionalism and adherence to contractual agreements.

*Jan - April 2023*          **IT Audit Project – HLB-**

**Pakistan Poverty Alleviation Fund (PPAF)**

- Conducted comprehensive end-to-end reviews of IT infrastructure and performed risk assessments.

- Developed and executed audit plans to evaluate IT controls and compliance.

- Conducted stakeholder interviews to gather information, analyze data, and identify trends and patterns.

- Successfully identified and addressed vulnerabilities within the IT environment.

- Recommended action plans for risk mitigation and vulnerability patching.

- Improved IT security awareness and understanding of risk management among stakeholders.

## EDUCATION

*2018-2020*  **Master in Information Technology**
Virtual University of Pakistan

- **Merit Scholarship Recipient**

- **Project:** Developed an Online Ticket Reservation System using HTML and PHP.

*2022-2024*  **MS in Cybersecurity**
Air University Islamabad

**Thesis:** Focused on malware detection

## CERTIFICATION

- SOC Essentials
- Introduction to Web Services Development
- IT E-Commerce
- Fundamentals of Front-End Development
- (ISC)² Systems Security Certified Practitioner (SSCP) Specialization
- (ISC)² Certified in Cybersecurity

## WEBINARS & SPEAKING ENGAGEMENTS

- **Co-Host, CISSP Webinar – "Talk to Experts" - IPCS**
  **Date:** 24 August 2024

  - Co-hosted a live webinar with Shakeel Server (Director of Business Development & Senior Consultant IPCS) on YouTube and LinkedIn, focused on CISSP certification and engaging with the cybersecurity community.

  - Received a Certificate of Appreciation from IPCS (Ideal Proposition Cybersecurity) for contributions to the event.

  - Collaborated with esteemed speakers Ebrima N. Ceesay, PhD, Muhammad Razzaq Chishty, and Salman Aslam to deliver an insightful and impactful session.

  - **Link:** CISSP Webinar - Talk to Expert (youtube.com)

## SKILLS

- Security Trends, Threats, and Vulnerabilities

- Risk Assessment

- Zero Trust Architecture

- VAPT Tools: Burp Suite, Nmap, Metasploit, Tenable Nessus

- Penetration Testing: Web, Mobile, Network, API Security

- Security Standards: OWASP Top 10, SANS Top 25

- Compliance & Standards: ISO 27001, NIST, HIPAA, PCI DSS

- Common Attack Vectors: SQL Injection, CSRF, XSS, Session Fixation

- Incident Management: SOC Operations, Threat Intelligence

- Proposal Writing Skills

## COMMUNICATION

Strong written and verbal communication skills, including the ability to provide constructive feedback and collaborate effectively with a team.

## LEADERSHIP

Ability to manage multiple projects simultaneously and meet tight deadlines, while maintaining the highest standards of quality.

## REFERENCE

Available upon request.