# ABUTHALIB FATHIMA ZEENATH ~ Dependent Visa

## CYBER THREAT INTELLIGENCE ANALYST

**Mobile**: +971 582791867 || **Email**: zeenathabuthalib44@gmail.com || **Location:** Dubai, UAE || https://www.linkedin.com/in/zeenat h-abuthalib/

- Cybersecurity Analyst **with 6+ years of experience** in threat intelligence, network security, incident response, and digital forensics, ensuring proactive defense against cyber threats.
- Expert in penetration testing & SOC operations, conducting security assessments, ethical hacking, and ensuring compliance with GDPR, ISO 27001, and NIST standards.
- Proficient in security tools like Splunk (SIEM analysis), Wireshark (network monitoring), CrowdStrike (endpoint security), Nessus (vulnerability scanning), and Burp Suite (web security testing) to detect and mitigate cyber risks.
- Skilled in cryptographic solutions (AES, RSA, ECC, PKI), implementing encryption, secure communication protocols, and key management systems to safeguard sensitive data.
- Strong analytical & problem-solving skills, adept at investigating, neutralizing cyber threats, conducting root cause analysis, and enhancing cybersecurity strategies.

## EMPLOYMENT OUTLINE

**Present**: **Cyber Security Analyst**
Zenect Technology | Sri Lanka

Key Deliverables:

- **Threat Monitoring & Incident Response:** Proactively monitoring threats using advance tools & conducting rapid incident response to mitigate risks
- **Risk Assessment & Penetration Testing:** Performing through risk assessment to identify security gaps and conducting penetration test to strengthen defences.
- **Security Tools & Technologies:** Expertise in SIEM platforms (Splunk, QRadar) for threat detection and end-point security using CrowdStrike
- **Regulatory Compliance:** Ensured alignment with industry standards (ISO 27001, NIST) for cybersecurity governance.

**Jul. 2024 – Nov. 2024**: **Threat Hunter (Contract)**
White2net | Belgium

Key Deliverables:

- **Threat Intelligence:** Proactively detected and mitigated cyber threats, including malware and advanced persistent threats (APT).
- **Incident Response:** Leveraged Splunk, CrowdStrike, and Snort for security event analysis and response.
- **Forensic Analysis:** Conducted in-depth network traffic analysis to identify and neutralize malicious activities.
- **Endpoint Security** – Monitored and secured endpoints using EDR solutions to prevent unauthorized access and malware infections.

**Apr. 2024 – Aug. 2024**: **Network Design Specialist (Freelance)**
Warsaw | Poland

Key Deliverables:

- **Infrastructure Optimization:** Designed and deployed secure, scalable network architectures using GNS3.
- **Security Assessments:** Conducted IT security assessments and implemented firewall rules for enhanced protection.
- **Data Transmission:** Integrated VPNs and wireless security solutions to prevent unauthorized access.

## SKILL SET

Threat Intelligence & Response

Problem Solving & Decision Making

Risk Assessment & Mitigation

Firewall Configuration & Management

Malware Analysis

Vulnerability Management

Identity Management

Cryptography Implementation & Encryption

Forensic Investigation & Analysis

Collaboration & Teamwork

Endpoint Security & Hardening

Phishing Detection & Prevention

Cloud Security

## EDUCATION CREDENTIALS

- **BSc (Hons) Cyber Security & Digital Forensics |** Kingston University - London | 2025
- **Qualifi Level 5 Extended Diploma in Networking and Cyber Security |** Qualifi | 2024

**Feb. 2024 – Jun. 2024**: **Digital Forensics Consultant (Contract)**
Wintan Health | Kenya

Key Deliverables:

- **Forensic Investigations:** Analyzed compromised websites, logs, and databases to trace unauthorized access.
- **Evidence Preservation:** Utilized EnCase and Wireshark to collect and preserve digital evidence with integrity.
- **Incident Reporting:** Documented findings and recommended security enhancements to prevent future breaches.
- **Security Collaboration:** Worked closely with IT and security teams to implement stronger defense mechanisms and improve incident response readiness.
- **Data Recovery:** Recovered and validated critical data from compromised systems to ensure minimal disruption and data integrity.

**Jan. 2024 – Dec. 2024**: **Security Architect**
Veed.io | United Kingdom

Key Deliverables:

- **Risk Mitigation:** Conducted security risk assessments and developed incident response plans.
- **Security Deployment:** Implemented security tools, including SIEM systems, IDS, and endpoint security solutions.
- **Audit Compliance:** Ensured adherence to GDPR and ISO 27001 through regular audits and policy enforcement.

**Jan. 2023 – Dec. 2023**: **Website Developer (Freelance)**
Beautiful India | United States

Key Deliverables:

- **Web Security:** Designed and developed secure, responsive websites integrated with CMS platforms.
- **SEO Optimization:** Enhanced website ranking through SEO best practices and security updates.
- **Custom Development:** Developed tailored website features, including booking systems, interactive maps, and dynamic content management.

## PROJECTS & RESEARCH

- **AIQUSEC - AI-based Quantum Safe Cyber Security Automation:** Developed AI-driven automation and quantum-safe cryptography for enhanced cybersecurity.
- **ISO 27001 Implementation Report:** Led ISMS implementation, ensuring compliance with cybersecurity frameworks.
- **Bug Bounty Pentesting Reports:** Conducted penetration testing and reported vulnerabilities to strengthen security measures.
- **Review Paper on Healthcare Cybersecurity:** Researched IoMT security threats and implemented Software Defined Networking (SDN) for enhanced protection.

## COMMUNITY INVOLVEMENT

- Contributed to OWASP Mobile Application Security Testing Guide.
- Secured platforms like Writco and Mirakee through vulnerability assessments.
- Provided pro-bono cybersecurity consulting to small businesses, advising on firewalls, SSL certificates, and MFA.

## CERTIFICATIONS

- **Cisco Certified Network Associate (CCNA)** – Cisco
- **Cisco Certified Network Professional Enterprise (CCNP)** - Cisco
- **Cybersecurity Attack and Defense Fundamentals -** EC-Council
- **Google Cybersecurity -** Google
- **Microsoft Cybersecurity Analyst -** Microsoft
- **Certified Cloud Security Professional -** Infosec
- **CEH (Certified Ethical Hacker) –** EC- Council **(**Reading)
- **CISSP (Certified Information Systems Security Professional) –** Reading

## EXTRACURRICULAR ACTIVITIES

- **Member – Internet Society (Sri Lanka):** Promoting digital literacy and cybersecurity awareness.
- **Content Writer - Medium:** Published articles on cybersecurity, data protection, and internet security.

## TECHNICAL SKILLS

- **Programming Languages:** C, C++, JavaScript, PHP, Python, SQL, HTML
- **Security Tools:** Burp Suite, Nmap, Nessus, VirusTotal, Wireshark, Netsparker, NSLookup, MobSF, Wfuzz
- **Networking:** Linux Distros, VPNs, Firewall Configuration, IDS/IPS
- **Cybersecurity Domains:** SOC Operations, Malware Analysis, Vulnerability Management, OWASP Top 10

## REFERENCES

- **Sharonath Purusothemen**
  Director - Pioneer International Campus
  Email: sharon@idm.edu | Mobile: +94778822799
- **Bevan Kanishka Liyanage**
  Program Coordinator/ Lecturer – IT, ESOFT Metro Campus Kandy
  Email: beven.liyanage@esoft.lk | Mobile: +94710432847

## PERSONAL DOSSIER

- **Languages:** English, Tamil, Sinhala