Mozhar Alhosni

✉ **Email address:** mozharalhosni@gmail.com

🌐 **Website:** https://mozhars.garden

ABOUT ME

Cybersecurity Engineer with expertise in both Offensive and Defensive Security.
I bring hands-on technical proficiency alongside strong leadership and strategic insight.

SKILLS

Infrastructure Security – Network Segmentation, Firewalls, Zero Trust Principles / Linux System Administration / Offensive Security – Penetration Testing, Red Teaming, Exploitation Techniques / Microsoft 365 Security – Offensive & Defensive Techniques, Hardening, Threat Detection / C# Web Development – ASP.NET, MVC and Minimal APIs, Blazor / Web Application Security – Vulnerability Assessment, Secure Coding and Design, Secure DevOps

WORK EXPERIENCE

🏢 *MDD Plus for Debt-based Crowdfunding* – Riyadh, Saudi Arabia

City: Riyadh | **Country:** Saudi Arabia | **Name of unit or department:** Cybersecurity - **Business or sector:** Financial and insurance activities

Cybersecurity Engineer

[25/06/2024 – 25/11/2025]

Cloud Infrastructure & DevOps:
- Designed and implemented a **cloud-native infrastructure** on **Huawei Cloud SA (Linux)** from the ground up.
- Built and deployed a **DevOps architecture** using **GitHub Actions (CI/CD)** to enable rapid delivery.
- **Implemented on-prem tools** like **MDM and secure file-sharing** to meet **SAMA compliance requirements**.

Cybersecurity Leadership:
- Acted as the **primary Cybersecurity contact**, overseeing all security initiatives.
- Adapted the **Saudi NCA Cybersecurity Policies, Standards, and Procedures** across the organization.
- Conducted compliance assessments for **SAMA's MVC**, **CRFR**, and **CSF frameworks**, implementing required controls and addressing third-party audit feedback.
- Architected and implemented a **cybersecurity architecture** using open-source tools supported by policies and procedures.
- Applied **CIS benchmarks** and **CIS Critical Security Controls** across core technologies to strengthen security posture.
- Performed **penetration tests and secure coding reviews** on the core application to identify and remediate vulnerabilities.
- Developed and deployed **third-party integrations in C#**, including: **Nafith integration** and **SingleView** integration for IBAN verification.

🏢 *MDD Supply Chainer* – Riyadh, Saudi Arabia

City: Riyadh | **Country:** Saudi Arabia

Cybersecurity Officer

[25/06/2024 – 25/11/2025]

Cloud Transformation & Infrastructure:
- Transformed the company into a **cloud-native environment** on **Alibaba Cloud SA** (Linux-based).
- Reduced infrastructure costs by 60%+ through optimization and migration, applying **FinOps** best practices.
- Automated **90% of infrastructure and application management tasks**.
- Implemented **backup & disaster recovery strategies** ensuring **99.9% system availability**.

- Modernized applications by migrating from **.NET Framework → .NET Core** and **Exchange.Online → Microsoft Graph API**.
- Built a **DevOps architecture** with **GitHub Actions** (CI/CD).

Cybersecurity Leadership:
- Led the company's **cybersecurity function**, acting as the primary authority for both strategy and execution.
- Architected and implemented a **comprehensive cybersecurity architecture** using tools (**OpnSense**, **Wazuh**, **ClamAV**, **Suricata)** supported by **policies** and **procedures**.
- Secured and managed the **Microsoft 365 suite**, strengthening identity, access, and data protection.
- Performed risk assessments.
- Adapted the **Saudi NCA Cybersecurity Policies, Standards, and Procedures** across the organization.
- Applied **CIS benchmarks** and **CIS Critical Security Controls** across core technologies to strengthen security posture.

🏢 *Hack The BOX Ltd* – Folkstone, Kent (Remote), United Kingdom

City: Folkstone, Kent (Remote) | **Country:** United Kingdom | **Business or sector:** Information and communication

Training Developer

[08/02/2022 – 28/06/2024]

- *Created*, *maintained* (via version control), and *continuously improved* the **Academy Walkthroughs** project. Authored over 60 walkthroughs and collaborated with other Training Coordinators on the project.
- *Reviewed*, *quality-controlled*, *improved*, and *proofread* HTB Academy modules, with a primary focus on all modules for the **Certified Web Exploitation Expert** (**CWEE**) certification and **Certified Active Directory Pentesting Expert** (**CAPE**).
- Developed an **autopwn** script with over 3,000 lines of code for the entire **CWEE** exam environment and authored the exam's official walkthrough.
- Created the "**Blazorized**" HTB Machine.
- Authored the "**API Attacks**" module for HTB Academy.
- Co-authored the "**DACL Attacks I**" and "**NTLM Relay Attacks**" modules and contributed the "**Logon Scripts**" section (including the exercise VMs) to the "**DACL Attacks II**" module.
- Collaborated with HTB Academy module authors to enhance the quality and effectiveness of their work.

EDUCATION AND TRAINING

Bachelor of Science in Computer Science (Cyber Security) with First Class Honours
Asia Pacific University of Technology and Innovation (APU / APIIT) [01/09/2019 – 10/03/2023]

City: Kuala Lumpur | **Country:** Malaysia

Bachelor of Science in Computer Science (Cyber Security) with First Class Honours
De Montfort University [01/09/2019 – 10/03/2023]

City: Kuala Lumpur | **Country:** Malaysia

HOBBIES AND INTERESTS

Technical Hobbies & Projects
- **.NET Development**: Highly proficient in C#, focusing on MVC APIs, Minimal APIs, and Blazor, with an emphasis on secure coding practices.
- **Personal Projects**: Built a **Digital Garden website** with standalone Blazor WebAssembly, inspired by Material for MkDocs.
- **Hack The Box Machines**: Developed two custom machines: **Blazorized** and **TargetedOps**.
- **Open-Source Contributions**: Actively contributed to **C#** projects including **CrucibleC2**.
- **Book Reviews**: Participate in reviewing books from **Manning Publications**, including: *Secure APIs; Acing the ISC2 Cybersecurity Certification; and Learn Docker in a Month of Lunches, 2E*
- **Emerging Tech & Security**: Passionate about WebAssembly (WASM) and staying current with web security trends and research.