Ben Bouali Dhia

Cybersecurity Engineer

Tunisia, Manouba • +216 20655774 • boualidhia76@gmail.com

Github • LinkedIn

Arabic: Native • English: B2 • French: B2

Professional Experience

Security Implementer Intern, SEGULA Technologies **Feb 2025 - Jul 2025**

- Conducted a gap analysis between the company's existing security practices and TISAX requirements
- Proposed an enhanced, redundant network architecture to improve system availability
- Designed and implemented a network infrastructure labeling system for the data center
- Prepared a cyber risk assessment, identifying threats and formulated a mitigation action plan

Web Security Intern, HORIZOP ENERGY **Jul 2024 - Sep 2024**

- Performed structured threat modeling using Microsoft Threat Modeling
- Enhanced website security by implementing OWASP ASVS and security checklist best practices
- Performed Static and dynamic Application Security Testing, discovering and resolving vulnerabilities
- Established a company password policy focused on best practices

Academic Project

Identity and Access Management Infrastructure with Active Directory **Apr 2025 - May 2025**

- Deployed and configured Active Directory within a virtualized environment
- Created and applied Group Policies (GPOs) to manage users, permissions
- Integrated Active Directory with Keycloak to enable Single Sign-On (SSO) capabilities.
- Conducted vulnerability assessment of the AD environment using PingCastle

AI-Powered Threat Intelligence Platform **Feb 2025 - Mar2025**

- Developed and deployed an AI-driven Threat Intelligence Platform using Flask
- Built and trained two machine learning models
- Used labeled datasets combining normal and malicious traffic/emails for model training
- Integrated the platform with Snort IDS and a configured email server
- Simulated real attacks, including DDoS attacks and phishing emails, to test model effectiveness.

Threat Hunting and Intelligence Ecosystem for Banking Organizations **Oct 2024 - Feb 2025**

- Setting up firewall rules and segmenting the network
- Deploying Wazuh SIEM for log aggregation, including the development of custom detection rules.
- Implementing automated incident response playbooks with Shuffle.
- Integrating Cortex and MISP to enrich logs with threat intelligence data

Education

Engineering Degree in Network Infrastructure and Data Security **Tunis - Sep 2023 - Present**
Esprit

Master in Information Systems and Infrastructure Security **Tunis - Sep 2023 - Sep 2025**
Higher Institute of Computer Science (ISI)

Bachelor of Computer Engineering Embedded system and IOT **Tunis - Sep 2020 - Aug 2023**
Faculty of Sciences of Tunis (FST)

Technical Skills

Malware Analysis, Identity and Access Management, Threat Modeling Network Analysis, Python Scripting, Threat Assessment, Firewall, MISP, SOAR, SIEM, IDS/IPS, Ubuntu, Kali Linux, Debian, Windows Server