OUARDI MOHAMED HAMDI
Cybersecurity operations Engineer

Email: medhamdiouardi@gmail.com LinkedIn : in/ Mohamed Hamdi Ouardi
Mobile : + (216) 52 817 808 Medium: medium.com/@mohamedhamdiouardi

SUMMARY

Mohamed Hamdi Ouardi is a cybersecurity expert and Security information system administrator, his role involves a broad spectrum of responsibilities, including information system administration, security architecture implementation, penetration tests, and vulnerability analysis , and actively provides IT and cybersecurity training.

Mohamed's impact extends beyond his current position, as he's delivered cybersecurity training for international organizations, contributing to global cybersecurity awareness and expertise. Additionally, he served as an IT and Cybersecurity instructor at ESPRIT University, offering lectures on a wide array of topics like Certified Ethical Hacker Certification (CEH) , Mohamed's instructional expertise encompasses Linux system administration, cloud computing security, virtualization, and more. Furthermore, he's a verified instructor in the American Cybersecurity education platform securzy.io, enriching cybersecurity knowledge in the United States.

PROFESSIONAL EXPERIENCE

Arab Tunisian Bank - ATB **August 2024 – currently**

Cybersecurity infrastructure and operations Engineer (onsite -full time)

- Participate in network/security engineering projects
- Identify and troubleshoot WAN, LAN, and Internet infrastructure
- Deploy network/security solutions
- Network/Security administration and configuration
- Participate in the design and implementation of network/security solutions for business applications
- Determine needs, propose and guide the implementation of solutions; Manage network and security incidents
- Provide technical user support and offer necessary security advisory services as well as security recommendations for new IT solutions and services
- Document network/security designs and standards; Manage security devices (Firewall, IPS, IDS, WAF, HIPS, DLP .)
- Participate in the development of IT policies and procedures (IT P & P)
- Contribute to projects for implementing complex systems across multiple sites and study and implement the Disaster Recovery/Business Continuity Plan (PRA/PRI)

SFM GROUP **December 2021 – July 2024**

Cybersecurity Engineer and Information Security System Administrator (onsite -full time)

- Security Monitoring and Incident Response: Set up security monitoring tools and establish incident response procedures to detect and respond to security incidents in a timely manner.
- Regular Security Audits and Assessments: Conduct regular security audits and assessments to evaluate the effectiveness of the security infrastructure, identify areas for improvement, and ensure compliance with security standards and regulations.
- Monitoring and analyzing security events and alerts to identify potential threats and vulnerabilities
- Conducting investigations into security incidents, including analyzing logs and network traffic
- Utilizing SIEM tools to correlate and analyze security data.
- Providing support for incident response activities, including containment, eradication, and recovery
- Employee Training and Awareness: Provide ongoing training and awareness programs to educate employees about security best practices, phishing attacks, and other cybersecurity threats to minimize human error risks.

- Implement vendor risk management processes to assess the security postureof third-party vendors and ensure that they adhere to the organization's security standards and requirements.
- Implementing Robust Security Measures: Spearheading the implementationof comprehensive security protocols and measures to fortify the integrity and confidentiality of the Information System for the clients
- Skill Transference to IT Team: Facilitating knowledge transfer sessions and workshops to empower the IT team with the latest skills and best practices in information system management.
- Contributing to Strategic Digital Development: Actively engaging in the formulation and refinement of SFM's strategic plan for digital advancement, ensuring alignment with organizational objectives.
- Migration to DevOps/DevSecOps: Steering the migration towards DevOps/DevSecOps methodologies to enhance collaboration, efficiency, and security across development and operations teams.
- Innovative Backup Solutions Design and Management: Leading the design and management of cutting-edge backup solutions to safeguard critical data and ensure business continuity in the face of potential disruptions.
- Infrastructure Security Oversight: Taking charge of ensuring the robustness and resilience of infrastructure security measures, proactively identifying and mitigating vulnerabilities.
- Tailored Training Delivery: Delivering tailored training programs and workshops to equip staff with the necessary skills and knowledge tailored to SFM's specific requirements.
- Internal Information System Auditing: Conducting thorough internal audits of SFM's Information System to assess compliance, identify areas for improvement, and ensure adherence to industry standards and regulations

- Risk Assessment: Conduct a comprehensive risk assessment to identify potential threats and vulnerabilities to the organization's infrastructure.
- Security Policy Development: Develop and implement robust security policies and procedures that align with industry standards and regulatory requirements.
- Access Control Measures: Implement access control measures such as role-based access control (RBAC), multi-factor authentication (MFA), and least privilege principles to limit unauthorized access to sensitive data and systems.
- Network Security: Deploy firewalls, intrusion detection and prevention systems (IDPS), and virtual private networks (VPNs) to protect the organization's network from external threats.
- Data Encryption: Implement encryption mechanisms to protect data both at rest and in transit, ensuring that sensitive information remains confidential even if compromised.

ESPRIT UNIVERSITY **January 2023 -June 2024**

IT and Cybersecurity University Instructor (onsite - part time)

- Leading the mentorship program for comprehensive projects while overseeing educational achievements.
- Spearheading the implementation of a centralized real-time log and event management system.
- Establishing a Security Operation Center (SOC) utilizing a suite of Open-Source tools.
- Pioneering the deployment of a Security Orchestration, Automation, and Response (SOAR) solution to enhance SOC capabilities.
- Delivers specialized NIDS (Network Infrastructure and Data Security) courses for engineering students. Topics include virtualization and security, identity control, access management, DevSecOps, and Certified Ethical Hacker Certification."

EXPERTISE FRANCE

Cybersecurity Trainer (Tripoli – part time – onsite) **April 2024- May 2024**

- Provided A specialized IT security training program in Tripoli targets information technology (IT) teams from key government institutions: the Tax Authority, Ministry of Finance, General Information Authority, National Information Security and Safety Authority, and Ministry of Interior of Libya

  The training forms part of the E-nable project, funded by the European Union and implemented by Expertise France. The E-nable project supports the digitization and diversification of the Libyan economy.

SECURZY.IO

Cybersecurity mentor (United States - part time - full remote) **July 2022- Present**

- Verified Instructor at securzy.io, a prestigious American Cybersecurity education platform.
- Dedicated to empowering the next generation of cybersecurity professionals.
- Conduct dynamic bootcamps and comprehensive training programs.
- Equip individuals with essential skills and knowledge in cybersecurity.
- Passionate about fostering deep understanding of cybersecurity principles.
- Elevate expertise of individuals and companies.
- Ensure proficiency in the intricacies of the cybersecurity field.

FORMA PRO

Cybersecurity instructor (onsite- part time) **June 2021- October 2022**

- Designing and facilitating courses for BTS and BTP computer science classes, I take pride in delivering expansive training programs that encompass a wide array of essential skills and knowledge:
- Immerse students in the intricacies of computer security, Ethical Hacking, and Pentesting, guiding them through hands-on exercises and real-world scenarios to fortify their understanding and proficiency in safeguarding digital systems.
- Foster a comprehensive grasp of coding languages such as web languages, PHP, MySQL, Python, Java, and C++, providing students with a robust foundation in software development and programming principles essential for modern technological landscapes.
- Lead comprehensive preparation courses meticulously crafted to prepare students for the rigors of CCNA exams. Through in-depth curriculum coverage and practical exam simulations, students are empowered to confidently navigate networking concepts and emerge ready to excel in their certification endeavors.

INTERNSHIPS

HLI Tunisia Consulting **TUNIS, TN**

Cybersecurity Intern |Master degree final project (onsite) ***02/*2021 - 08/2021**

- In spearheading the development of sophisticated shell hardening scripts, my primary focus was on automation the security posture of both Active Directory (AD) and Microsoft SQL servers. This intricate undertaking involved conducting an exhaustive analysis of potential cyber threats, ranging from advanced persistent threats to emerging attack vectors.
- My overarching goal was to create a multi-layered defense mechanism, ensuring that these critical servers remained resilient in the face of ever-evolving cyber risks. The script development process included the meticulous implementation of security best practices, encryption protocols, and access controls, with an emphasis on preemptive measures to thwart potential exploits.
- Simultaneously, I orchestrated the creation of automation scripts tailored to expedite the remediation of vulnerabilities on Windows servers. This involved a proactive approach to identifying and rectifying misconfigurations promptly, minimizing the window of exposure to potential threats. The automation aspect
- not only streamlined the correction process but also ensured consistency across server environments, thereby establishing a robust baseline security standard.

Key Achievements:

- Development of Shell Hardening Scripts based on PowerShell
- Emphasis on automating security for Active Directory (AD) and Microsoft SQL servers.
- Comprehensive analysis of cyber threats, from persistent to emerging vectors.
- Establish a resilient defense mechanism for critical servers.
- Implementation of security best practices, encryption, and access controls.

SFM GROUP

Cybersecurity intern Final bachelor degree project supervised by Mr. Nizar Ben Neji **TUNIS, TN**
(The current Tunisian minister of telecommunications) ***01/*****2019 - 06/2019**

- involved leading a thorough penetration test on the organization's information system, utilizing a finely tuned analytical approach to meticulously identify and scrutinize potential vulnerabilities.
- During the subsequent correction phase, I showcased a robust work ethic, collaborating seamlessly with a dedicated team to implement precise solutions. This phase not only required technical proficiency but also underscored my commitment to excellence and thoroughness in addressing security concerns.
- expanded my responsibilities to include fortifying the information system against a wide array of threats. This entailed strategic planning and the implementation of robust measures, demonstrating my ability to navigate the intricacies of cybersecurity with precision and dedication.
- Under the insightful guidance of Mr. Nizar Ben Neji, who serves as the Minister of Telecommunications, this experience not only deepened my understanding of cybersecurity intricacies but also highlighted my resilience in navigating challenging projects. My role at SFM Technologies stands as a testament to my unwavering commitment to making meaningful contributions to the cybersecurity landscape.

Key Achievements:

- Conducted an exhaustive penetration test on the organization's information system, showcasing a keen analytical approach to identify and scrutinize potential vulnerabilities.
- Demonstrated a strong work ethic during the subsequent correction phase, collaborating seamlessly with a dedicated team to implement precise solutions.

STB BANK **Bizerte, TN**
Cybersecurity Analyst Intern (onsite) ***06/*****2018 - 08/2018**

- My responsibilities included vigilant monitoring of the system's security to proactively identify and mitigate potential threats.
- took charge of ensuring the secure execution of online transactions and electronic signatures, contributing to a robust and protected digital environment.
- A key aspect of my work involved synthesizing insights and experiences into comprehensive recommendations reports, aimed at elevating the bank's overall security posture.

Key Achievements:

- Monitored the information system's security to safeguard against potential threats.
- Ensuredthe secure execution of online transactions and electronic signatures.
- Developed and presented detailed recommendations reports to enhance the overall security level of the bank

TUNISIE TELECOM **Bizerte, TN**
Network Intern (onsite) ***06/*2017 - 07/2017**

- In this internship I have a robust background in the telecommunications industry, where I was dedicated to the supervision and maintenance of GSM networks. My responsibilities included a deep dive into understanding the intricate architecture of the network and its functions, ensuring seamless operations. Moreover, in comprehending the organizational intricacies of the Line Construction Center (CCL).

EDUCATION

University of Carthage (Faculty of Sciences Bizerte) **Bizerte, TN**
Professional Master's degree specializing in Network Expertise and Information Security **2019-2021**

University of Carthage (Faculty of Sciences Bizerte) **Bizerte, TN**
Bachelor of Information Network Technologies and Telecommunications ***2016-2019***

SPEAKER AT THOSE EVENTS

- **SPEAKER AT TEDx UNIVERSITY ENSTAB (Link to the talk on the international official TEDx channel :** **https://www.youtube.com/watch?v=tfVvvkdJ_as&t=740s**
- **Infragard speaker (Infra G ard is a partnership between the Federal Bureau of Investigation (FBI) and membersof the private sector for the protection of United states) :**
  https://drive.google.com/file/d/1XCdqNrq7KFe2BR1laOOokLJxavJTDK-m/view?usp=drive_link
  https://drive.google.com/file/d/1f81GhWNYHItfyxgI2jZuCW2gM6_jIUz1/view?usp=drive_link
- **MCCE (Maghreb Cybersecurity & Cloud Expo 2023) Speaker**
  https://drive.google.com/file/d/1bsy7YaRpTEf4Fxx4NiNW4UoY0njRtdJp/view?usp=drive_link

- **You can check all the events where I've been invited as a speaker by following this link**
https://drive.google.com/drive/folders/1_qOF4jpiMTec7jaW8E6R8dlj7R50XtrG

Tools & Technologies

- Shell Scripting (bash/sh/powershell)
- Penetration tests OS (Kali ,parrot ...)
- Offensive tools (Metasploit , OwaspZap , Acunetix , burpsuite ...)
- Fortigate 60F , PFSENSE , Palo Alto , CISCO Catalyst
- SIEM (wazuh , OSSIEM , ELK)
- Snort
- Suricata
- Security Onion
- Nessus
- WAF (Mod security ..)
- Network security implementation and policy management (Active Directory)
- Monitoring (Prometheus/Gafana,Nagios)
- DevOps and DevSecOps (jenkins , SonarQube , Docker , Gitlab...)
- APEX one
- APEX central
- Deep Discovery Email Inspector Trend micro
- Deep Discovery Analyzer
- Cisco Identity Services Engine (ISE)
- Walix
- Firemon

CERTIFICATES

- Certified Ethical Hacker (Tunsian cloud)
- Penetration Testing and Ethical Hacking (cybrary)
- Systems Security Certified Practitioner (cybrary)
- Cloud Native Security Conference – DevSecOps (IBM)
- IBM Blockchain Foundation Developer V2 (IBM)
- Website Hacking Techniques (EC-Council)
- Network Desfense Essentials :NDE (EC-Council)
- FCA - FortiGate 7.4 Operator Self-Paced (Fortinet)
- NSE 1-2-3 Network SecurityAssociate
- XM Cyber- Exposure Management Expert
- Foundations of OperationalizingMITRE ATT&CK – (AttackIQ)
- Secure Digital Transformation (AttackIQ)
- CCNA Routingand Switching: (Cisco)
- NDG Linux Unhatched (Cisco)
- Scrum Fundamentals Certified (SCRUMstudy - Accreditation Bodyfor Scrum and Agile)
- Scrum Fondation Professional certificate SFPC™ (certiprof)
- STEM MOOC (U.S. Department of State)
- Attestation premiers secours APS (CRT)

You can Check all my digital badges in Credly
https://www.credly.com/users/mohamed-hamdi-ouardi

Reference as trainer:

https://drive.google.com/drive/folders/1FQyUOn
a8dYOzdfFZqI7N_6hjJntkmDj?usp=sharing

ADDITIONAL INFORMATION

- As the host of the Cyber Corner podcast, where I engage in enlightening conversations with field experts, I am deeply committed to empowering individuals in the realm of cybersecurity. Drawing from my extensive background as an IT professional, I specialize in crafting compelling and instructive content spanning Cybersecurity, IT, Cloud, DevOps, and Hacker Attacks.
- My podcast serves as a platform to facilitate learning and growth, offering invaluable insights from industry leaders to both novices and seasoned professionals. Through these discussions, I aim to demystify complex technical concepts, rendering them accessible through tutorials, guides, and resources.
- Driven by a passion for education, I take pride in simplifying intricate subjects and fostering a culture of security consciousness. With a proven track record of excellence, I am dedicated to aiding individuals and organizations in staying abreast of the ever-evolving landscape of technology.
- The Cyber corner podcast on youtube : https://youtube.com/@the_cyber_corner?si=_7lEX_AQcRA5M5TD

- EP4 with The IBM distingusged engineer, technical sale , and CTO : Dr.jeff Crume
  https://youtu.be/sRfK4lX4oFQ?si=FeBi_pOtMtki2oPv

- My radio intervention on Express FM talking about using AI in offensive way and cybersecurity attacks and how we can protect businesses and individuals against that , you can watch full intervention from here :
  https://drive.google.com/file/d/1F8t5SAqzvBoqLkq9hLhQFhctqcu1awqP/view?usp=sharing