

Professional Profile

Dedicated Cyber Security expert with a proven track record in designing, implementing, and maintaining security architectures that comply with ISO 27001 and NIST standards. Successfully led and completed 15+ complex projects, resulting in an average of 20% cost savings and 30% improvement in efficiency.

With over 7 years of experience as a Project Leader, I have consistently delivered projects on time and within budget, while effectively managing and mentoring global team members.

As a resourceful Cyber Defender, I have responded to a wide range of technical and cyber security challenges with a focused and creative approach, resulting in a 25% decrease in security incidents.

Core Skills

- ✓ Technical Skills: Solution architecture, Threat analysis, Risk analysis, Project management, Soc Engineering, Soc Analyst, Threat Hunting, Incident Response, Digital Forensic, Malware Analysis, Penetration Testing, Purple Teaming.
- ✓ Soft Skills: Organization, Creativity, Flexibility, Autonomy, Active listening, Adaptability, strong analytical skills
- ✓ Management Skills: Team leadership, Crisis management, Planning.

Professional Experience

- **Chief Information Security Officer, Tunisian Air Force (Jun 2016 – Mar 2024)**
 - ✓ Led a technology team of 15, overseeing all cyber security activities for the Air Force IT Center, resulting in a 30% improvement in overall system security.
 - ✓ Designed and implemented comprehensive incident response protocols using tools like SIEM, XDR, CTI, and SOAR. This initiative successfully reduced incident resolution time by 60% and minimized potential risk by 40%.
 - ✓ Initiated crisis intervention strategies by streamlining communication protocols. This resulted in a 40% decrease in response time and ensured swift resolution of critical incidents.
- **Web Technology Manager, Kartajen International (Feb 2012 - Aug 2015)**
 - ✓ Collaborated with cross-functional teams on web development projects using agile methodologies such as Scrum and Kanban. These projects led to a 20% increase in product delivery efficiency.
 - ✓ Presented design ideas to clients, ensuring their satisfaction and meeting their expectations. This led to a 25% increase in client retention rate.

Education

- **Master of Cyber Security and Smart Industry at FSS - Faculty of Sciences of Sfax (Sep 2021 - Nov 2022)**
 - ✓ Specialized in Information Security Management Systems (ISMS), DevSecOps, Cloud Security, Smart Tools for Industry 4.0, Cyber-Physical Systems and Communication Protocols for the Industry 4.0.
 - ✓ Completed courses such as Ethical Hacking (CEH v11 Certification Training), Fundamentals of Cybersecurity & SOC, Cloud Security (AZ500 Certification Training) and Cyber-Physical System.
 - ✓ Worked on projects such as:
 - Information Security Management Systems (ISMS): Implemented an ISMS based on ISO 27001 standard for a hypothetical organization using tools such as Microsoft Visio, Microsoft Excel and Microsoft Word.
 - Cloud Security (AZ500 Certification Training): Deployed and secured a web application on Azure cloud platform using services such as Azure App Service, Azure SQL Database, Azure Key Vault, Azure Active Directory and Azure Security Center.

- **Master of Computer and Information Systems Security at ISIM Gabes Tunisia (Sep 2010 - Jun 2012)**
 - ✓ Specialized in Information Systems Security, Information Systems Security Risk Analysis, Digital Forensics, Systems Security and Secure Enterprise Computing.
 - ✓ Completed courses such as Cryptography, Information Systems Security, Information Systems Security Risk Analysis, Digital Forensics, Systems Security and Secure Enterprise Computing.
 - ✓ Worked on projects such as:
 - Information Systems Security Risk Analysis: Conducted a risk assessment and mitigation plan for a hypothetical organization using tools such as Microsoft Excel, Microsoft Word and Microsoft Visio.
 - Digital Forensics: Performed forensic analysis on various digital devices and media using tools such as FTK Imager, Autopsy and EnCase.

- **Bachelor of Science in Multimedia & Web Technology at ISI Med Tunisia (Sep 2007 - Jun 2010)**
 - ✓ Learned the fundamentals of graphics, multimedia, web development, system software, operating system, digital fundamentals and computer architecture.
 - ✓ Completed courses such as Graphics & Multimedia, System Software and Operating System, Web Development, Digital Fundamentals and Computer Architecture.

▪ **Cyber Security :**

- ✓ Cyber Security Expert by Saudi Digital Academy: Completed a comprehensive course on cyber security covering topics such as cyber security governance, cyber security risk management, cyber security incident response.
- ✓ IBM Cybersecurity Fundamentals
- ✓ edX Honor Code Certificate for LINUXFOUNDATIONX - LFS101x.2

▪ **Cloud Security:**

- ✓ Certified Cloud Security Professional (CCSP) training: Prepared for the CCSP certification exam by learning the core concepts and best practices of cloud security such as cloud architecture, cloud data security, cloud platform and infrastructure security, cloud application security, cloud operations security and cloud legal and compliance issues.
- ✓ Cloud Security (AZ500 Certification Training): Learned how to secure Azure cloud platform using services such as Azure App Service, Azure SQL Database, Azure Key Vault, Azure Active Directory and Azure Security Center.

▪ **Cyber Defense:**

- ✓ M6-108 Network Security by NATO SCHOOL OBERAMMERGAU: Learned how to protect network infrastructure and data from cyber attacks using tools and techniques such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), virtual private networks (VPN), encryption protocols and network monitoring.
- ✓ Log analysis and SIEM NATO cyber security course: Learned how to analyze network logs and use SIEM (Security Information and Event Management) tools such as Splunk, ELK and Wazuh to detect and respond to network anomalies and incidents.

▪ **Digital Forensics And Malware Analysis:**

- ✓ TREND MICRO CYBERTALENT DFIR and Malware Analysis: Learned how to perform digital forensics and malware analysis using tools such as FTK Imager, Autopsy, EnCase, Volatility Framework, IDA Pro and OllyDbg.
- ✓ Digital Forensics: Performed forensic analysis on various digital devices and media using tools such as FTK Imager, Autopsy and EnCase.

▪ **Purple Teaming And MITRE ATT&CK Framework:**

- ✓ Foundations of Operationalizing MITRE ATT&CK: Learned how to use the MITRE ATT&CK framework to understand the tactics, techniques and procedures (TTPs) of cyber adversaries and to improve cyber defense capabilities.
- ✓ Intermediate Purple Teaming: This course delves deeper into concepts from Foundations of Purple Teaming, providing background and instruction on the key processes enabling sound threat intelligence integration and organizational threat alignment in support of Purple team

exercises. Students will create emulation plans based on the business requirements and IT architecture of a fictional organization and, in doing so, derive the skills required to understand their own threat environment and prepare actionable plans.

Additional

Languages

Arabic, English, French

Awards

- Tunisian Armed Forces CTF 2023(1st)
- Cybersecurity & smart factory hackathon s2t 2022(2nd)
- Tunisian Armed Forces CTF 2021(1st)
- Tunisia National Cybersecurity CTF by trend micro-2021(2nd)
- Arab and Africa Regional CTF by trend micro-2021(10th)
- Tunisian Armed Forces CTF 2019(1st)