**TOUFIK ZAOUI**

**Cyber Security Professional**

Ottawa, ON

 **Mobile**: 343-987-1444 | **E-mail**: zaoui.toufik@gmail.com | https://www.linkedin.com/in/toufik-zaoui

**Summary Of Qualifications**

A dynamic and innovative IT expert, proficient in both English and French, boasting over 8 years of hands-on experience in the IT field, complemented by a master’s degree in engineering and a Cyber Security diploma. Demonstrated proficiency in deploying, administering, monitoring, and resolving issues related to computer networks (routing and switching), Windows servers, Linux Ubuntu/OpenSUSE, and virtualization. A proactive and team-oriented professional, excelling in high-pressure environments to meet tight deadlines. Exceptional communication skills, dedicated to delivering top-quality results, ensuring client satisfaction, and fostering organizational growth with unwavering passion.

**Technical Skills**

Kali Linux l Splunk l Snort IDS l Active Directory l OpenVPN l Windows Firewall l Linux iptables l Volatility Framework l FTK Imager l Autopsy l NetworkMiner l OpenStego l ShellBags Explorer l winmd5free l Magnet RAM Capture l Redline l HxD l HashCalc l Exeinfo PE l PDF Stream Dumper l FileAlyzer l Yaazhini Vulnerability Scanner l APKTool l Ghidra l HashCompare l UPX Easy GUI l Metasploit l SQLMap l Elasticsearch l Kibana l Webhise data l Web Scraping l Tor Brows | TCP/IP | DNS | DHCP |Cisco routing & switching | Windows and Linux administration | Virtualization | Dell EMC NAS storage |SMB and NFS | Superna Eyeglass & ECA | Telus EMR | Microsoft Office Suite | Ticketing software: Request tracker, Zendesk, Salesforce.

**Education And Certifications**

* **Comptia Security + (In progress) 2023**
* **Cybersecurity Connections Program – IBM SkillsBuild 2023**
* **NSE 1,2,3 2023**
* **Cyber Security Diploma** – Lighthouse Labs  **2023**
* **Master’s degree in Electrotechnical engineering (Canadian equivalency with WES Ref # 4283181) 2009**

 Institute of technology, University of Medea, Algeria

**Projects**

* **Cybersecurity Diploma Final Project - Root Cause Analysis Report (2023**)

**Description**: Conducted a comprehensive Root Cause Analysis report on a cybersecurity incident where an unauthorized individual gained access to the company's webserver. Analyzed the attack, identified vulnerabilities, and proposed security enhancements.

**Key Achievements:**

* Investigated the attack, including the use of a reverse shell and lateral movement within the network.
* Analyzed the potential impact on the business, emphasizing the importance of data security and reputation management.
* Recommended security measures to prevent future attacks, including stronger server and network security, password management, and multi-factor authentication.
* **Vulnerability Assessment Project - Practera Platform (2023)**

**Description**: Conducted a real industry vulnerability assessment of a website using tools such as nmap, Owasp ZAP, and OpenVAS. Produced a comprehensive report detailing vulnerabilities, their severity, scores, and recommended remediation measures. Presented findings to the client.

**Key Achievements:**

* Performed a thorough vulnerability assessment using industry-standard tools, ensuring the identification of potential security risks.
* Produced a detailed report that categorized vulnerabilities by severity and provided clear recommendations for mitigation.
* Effectively communicated assessment results to the client, facilitating informed decision-making for enhancing website security.
* **Network Expansion Project (2016)**

**Description**: Led a team of 15 engineers to seamlessly connect the main site with 64 remote locations, resulting in a 25% reduction in network downtime, 30% faster data transfer, and improved data privacy and operational efficiency. Accomplished this within budget and met a challenging 6-month deadline.

**Key Achievements:**

* Successfully orchestrated the expansion of the network infrastructure, connecting multiple remote sites to the main network hub.
* Achieved a significant reduction in network downtime, enhancing operational efficiency and data transfer speed.
* Implemented robust security measures to improve data privacy and protect against potential threats.
* Managed the project within budget constraints and met the tight 6-month deadline, ensuring minimal disruption to operations.

**Work Experience**

**Technical Support**

Telus health | Ottawa, Canada **Jun 2021-Dec 2021**

* Provided technical support to 1000+ company’s clients including electronic medical record system, operating systems, network, VPN and database
* Followed documented procedures to resolve incidents and requests, achieving more than 90% resolution rate.
* Recorded and analyzed service calls and follow-ups until problems are resolved using the incident management tool
* Ensured security processing for access to servers and client OS
* Performed debugging and validated the solution found
* Adjusted and executed Oracle scripts
* Documented and maintained support operation procedures

**Accomplishment**

* Consistently achieved a high-resolution rate of 90% and streamlined support operations through efficient documentation, benefiting over 1000 clients. Expertly handled over 20 service calls per day, ensuring proactive issue resolution and maintaining robust system security.

**Technical Support**

Superna | Kanata, Canada **Feb 2020- May 2021**

* Installed and configured Superna products (Eyeglass, ECA) in over a 100 customers vCenters (vSphere and Hyper V)
* Walked customers through to configure AD delegation, DNS delegation and service principal name in ADSI Edit tool
* Assisted more than 100 customers with Failover/failback using Eyeglass DR solution and troubleshooted any issues during the event
* Troubleshot and supported customers issues daily with a resolution rate of more than 90% through Zendesk ticketing system or on zoom/Webex meeting
* Documented customer installations. Raised product bugs, worked with design on the fix and documented the fix

in quality center bug tools, delivered the fix to customers via Webex meeting

* Installed patches/updates and walked customers through the solution
* Setup debug and recreated customers networking and cluster environments (virtual machines, PowerScale clusters, networking, shares, exports, quotas)
* Delivered advanced DR assessment service by processing cluster configuration and building report for review by engineering senior team
* Assisted with delivery of DR information gathering and updating Design documents for customer networks and clusters
* Created or updated test plans and test cases based on customer requirements or identified problems
* Ran a series of tests against new features of software and analyzes the results
* Triaged cases, monitored support processes, acted as an escalation point

**Accomplishment**

* Deployed and supported Superna products for 100+ customers, achieving a 90%+ resolution rate and expertly troubleshooting complex issues. Acted as an escalation point, ensuring efficient support processes and delivering advanced DR assessment services.

**Bilingual Helpdesk Analyst**

National Capital FreeNet | Ottawa , Canada **Aug** **2019-Feb 2020**

* Assisted members in resolution of internet , Email and related technical issues
* Configured ADSL & VDSL modem and troubleshooted connectivity issues.
* Recorded issues through Help-desk ticketing system using request tracker
* Teached members how to set up and use internet services
* Provided detailed assistance and training to non-technical members
* Helped prepare documentation and training materials

**Network Engineer Dec 2013-May 2019**

Directorate of National Transmissions | Medea, Algeria

* Designed and implemented scalable and secure network infrastructures.
* Configured and managed routers, switches, firewalls, and other network devices.
* Troubleshot and resolved network-related issues and outages promptly.
* Implemented and managed network security protocols, including firewalls, VPNs, and intrusion detection systems.
* Conducted network assessments and recommended improvements to enhance efficiency and reliability.
* Participated in the planning and execution of disaster recovery and business continuity strategies for network infrastructure.
* Collaborated with cross-functional teams to plan and execute network upgrades and expansions.
* Administered biometric platforms, ensuring continuity of service by providing permanent support and maintenance.
* Updated internal documentation and validated KB articles.

**Accomplishment**

* Led a team of 15 engineers to seamlessly connect the main site with 64 remote locations, resulting in a 25% reduction in network downtime, 30% faster data transfer, and improved data privacy and operational efficiency, all within budget and within a 6 months deadline.