**Hanzla Nawaz**

**Email:** [hanzlanawaz151@gmail.com](mailto:hanzlanawaz151@gmail.com)

**LinkedIn:** [www.linkedin.com/in/hanzlanawaz](http://www.linkedin.com/in/hanzlanawaz)

**Contact No:** +92 343 4023151

**CAREER OBJECTIVE:**

To secure a position offering responsibility challenges and personal growth. A position where my talents can be effectively utilized to improve operations and contribute to the company's goals.

**PROFESSIONAL EDUCATION & TRAININGS:**

* CISSP (Prep Completed Exam Schedule December 2022)
* ISO Lead Implementer & Auditor 27001,27002,27017,27018
* CIS Top 20 Controls Implementation
* SIEM a Hands-On Approach In Line With Various Frameworks and Standards
* Ethical Hacking & Incident Response Management
* SCADA / ICS Security & Prevention & Detection
* Vulnerability Assessment In Line With Various Frameworks and Standards
* Machine Learning-Supervised & Unsupervised
* Linux RHEL Intensive Boot Camp
* Programing in Python
* Programing in R
* Data Collection & Data Wrangling
* Exploratory Data Analysis

**ACADEMIC QUALIFICATION:**

* Bachelor of Artificial Intelligence
* FSC Pre Medical

**WORK EXPERIENCE**

Ghanimah Labs, Canada

**CYBER SECURITY: Jan 2021 aug 2022**

* Initiated and led a project to improve the existing Information Security Management System (ISMS) as per the guidelines outlined in cybersecurity standards such as ISO 27001 and 27002 and IEC 62443
* Building secure and compliant networks in line with CIS v8, ISO 27001, SOC 1 type II, IEC 62443, and other key standards.
* Configuring the GCP and AWS cloud architecture in line with ISO 27001, ISO 27017 and ISO 27018 requirements.
* Effectively perform different cyber security assessments including elaborative Risk Assessments based on IEC62443, NIST or equivalent, dedicated towards Operational Technology (OT) engagements.
* Comfortable in performing Technical Vulnerability Assessment and Penetration Testing on OT environment with tool based and manual methods.
* Conducting ICS/OT site assessments to identify business critical systems and develop effective risk mitigation measures.
* Develop cybersecurity architectures for IT/OT integrated environments detailing out component level information.
* Develop IT/OT Operating model, Governance frameworks including Development of Policies, guidelines, and procedures apt for the specific business environment of clients
* Large scale design and implementation of OT Visibility and Threat management solutions covering all OT systems and devices across plants considering network performance and security requirements.
* Design IT/OT Security Operation center (SOC) strategies, implement technical integration solutions, develop SOC use cases.
* Developing OT cyber security strategies, developing and implementing transformation programs.
* Drafting and presenting impactful reports as part of delivery activities suitable for Plant Operation, Maintenance stakeholder as well as management & cybersecurity stakeholders including and up to C-level executives.
* Support business development by preparing responses to RFI & RFPs by clients including effort estimation.
* Support innovation by identifying and developing potential accelerators to bring in efficiency in terms of offering and delivering.
* Building and developing long term relationships with all stakeholders internally and with clients.
* Extensive knowledge and experience (designing, commissioning, or maintaining) ICS systems e.g., SCADA, SIS, EMS, DCS or PLC. Experience in supporting or troubleshooting industrial protocols such as Ethernet/IP, OPC, Modbus, Profinet, HART, FF etc.
* Strong experience in designing and configuring network security devices like next generation/OT firewalls of popular vendors, IDS, IPS etc. and endpoint security solutions apt for OT environments
* Developed and evaluated technology policies, technical engineering standards and operational procedures in line with ISO 27001, 27017, 27018, and IEC 62443
* Hands-on skills with Wazuh (SIEM and FIM), Nessus (Vulnerability management), Open Audit (Asset management), NGINX (Web application Firewall), Metasploit, security onion and OSSEC tools.

**TECHNICAL SKILLS:**

* **Configuration:** VLANs, Access List, Router and Switches Configuration and Troubleshooting, Basic Configuration of Switch, VLAN setup.
* **Monitoring Tools:** Task Manager, Nagios, Zabbix
* **Operating Systems:** RHEL Enterprise, Parrot, CentOS, Ubuntu, Kali Linux, Windows XP, Windows 7/8/8.1/10/11
* **Security:** Advanced user of intrusion-detection, IDS/IPS, DLP, SIEM, vulnerability-scanning, Web gateway, proxy appliances and antivirus tools.

**ALNAFI CONSULTANCY & SERVICES**

**TRAINEE SYSTEM ADMINISTRATOR: Jan 2020 till Jan 2021**

* Worked as Trainee System Administrator, responsible for installation, upgrading and maintenance of operating systems. I have installed software, upgraded hardware components as per requirement.
* Maintenance and Troubleshooting of Computers and Network.
* Implementation and configuration of network printers.
* Provides support to site-managed technical staff regarding system administration and usage.
* Work as a junior member of the team, providing technical and administrative support to Organization IT systems and networks.
* Troubleshooting any kind of Hardware problems and all the Networks and Systems problem.
* Create Users, Group as per user Creation policy
* Change ownership of file and set permissions on file system for owner, group and others
* Installation and configuration of Linux OS as per client’s requirement
* Installation of software and packages by using YUM server and RPM
* Managing of partitions and File System using Logical Volume Manager and fdisk command
* Add new partitions and Logical Volume, Swap to a system
* File System Operations (Create, Mount, Unmount and Remove)
* Linking File using Hardlink and Softlink
* Creating & and Managing Notes Groups, Renaming Groups, Deleting Groups
* Solving Password Related problems of the users
* Troubleshooting Network and System Issues
* Handling & Proper Guidance to Customer
* Check process that are consuming more resources then expected using (Tools: top, sar, free -m)
* Monitoring CPU utilization for critical process like “httpd”, “Apache” using (Tools: top, sar, free -m)
* Taking system backup to the remote server using “Rsync” tools compression backup with (tar, gzip, bzip)
* Installing patch for the system using YUM and periodically check for update
* Monitoring network traffic which are accessing server using tools like TcpDump and Wireshark
* Configuring firewall/iptables adding rules for incoming traffic
* Writing shell script [bash] to automate task such as transfer logs, taking backup
* Ensure network connectivity throughout company’s LAN and also WAN using tools such as Ping, Traceroute , ip, netstat arp
* Administrators, servers, laptops, printers, desktops and other devices troubleshoot the problems
* Changing as assign custom permissions using setfacl, chmod, chown, etc
* Configuring IP address to the interface using ifconfig and sometime static IP by editing ifcfg-eth0 file
* Clearing cache and buffer after approaching application team using echo 3 > /proc/sys/vm/drop\_cache
* Stop unwanted services on a server using kill command [protecting server]
* Creating a user/deleting/set permission using useradd, userder, setfacl, creating group and adding members using chgrp, usermod, groupdel etc.

**PERSONAL SKILLS:**

* Self-confidence, perception and determination are my assets in order to defy critical situations.
* Being an optimist I can eradicate problems without pressure.
* High team spirit and capabilities to take individual care.
* Quest to learn new things and hard work.
* Zeal to accept new challenges.

**PERSONAL INFORMATION:**

* **Date of Birth:** April 23, 2002
* **Gender:** Male
* **Languages Known:** Urdu, English
* **Hobbies:** Reading, Computer Programming, Gardening, Playing Football

**DECLARATION:**

I hereby declare that the information furnished above is true to the best of my knowledge.