Linkedin Profile QR Code

HASEEB ULLAH SHAH

Cyber Security Analyst

ihaseebshahh@gmail.com

www.linkedin.com/in/ihaseebshahh

+92 316 6369242

CAREER OBJECTIVE:

A Cyber Security Analyst protects company hardware, software, and networks from cyber criminals. The analyst's primary role is to understand company IT infrastructure in detail, to monitor it at all times, and to evaluate threats that could potentially breach the network. Often, cyber security analysts work to prevent security breaches and respond to breaches quickly. Many cyber security analysts have skills in programming and cryptography. I am looking for an opportunity which can further fuel my curiosity and assist me in expanding my expertise within Physical Security, Cyber Security, GRC and technical tidbits in solving business problems.

PROFESSIONAL SUMMARY:

Cybersecurity, Linux SysAdmin, and IT GRC/ISO 27001 Professional, collectively having 7.9 years of experience in Cybersecurity/IT/GRC Domain.

PROFESSIONAL TRAININGS & CERTIFICATIONS:

- CISSP (Updated)
- ISO Lead Implementer & Auditor 27001, 27002 – Hands-on Approach
- ISO 27001 and 9001 Certified from SkillFront
- CIS Top 20 Controls Hands-on Implementation
- SIEM a Hands-On Approach In Line with Various Frameworks and Standards
- Vulnerability Assessment In Line with Various Frameworks and Standards – Hands-on Approach
- Web Application Penetration Testing In Line With Various Frameworks and Standards – Hands-on Approach
- Network Penetration Testing In Line With Various Frameworks and Standards – Hands-on Approach
- WSTG (Web Security Testing Guide) – Hands-on Approach
- Linux RHEL Intensive Boot Camp (CentOS/Ubuntu/RedHat/Kali) – Hands-on Approach
- Red Hat Certified Specialist in Linux Diagnostics and Troubleshooting – Hands-on Approach
- Red Hat Certified Specialist in Linux Security and Virtualization – Hands-on Approach
- LPIC-1: 101 & 102 (v5) Linux System Administrator – Hands-on Approach
- LPIC-2: 201 & 202 (4.5) Linux Engineer – Hands-on Approach
- RedHat Certified System Administrator (RHCSA) – Hands-on Approach
- IT GRC (NIST CSF & RMF, ISO 27001, 27002, ISO 9001) – Hands-on Approach
- Practical Ethical Hacking – Hands-on Approach, from TCM Security
- Canva
- MySQL (Fundamentals) – Hands-on Approach

ACADEMIC QUALIFICATION:

- **BS in English Literature and Linguistics** from National University of Modern Language, Hyderabad

PROFESSIONAL WORK EXPERIENCE

Ghanimah, Canada.

Cyber Security Analyst | Al Nafi **Jan 2022 – Till Date**

Responsibilities:

- Settings and implementing user access controls and identify and access management systems.
- Monitoring network and application performance to identify irregular activity.
- Performing regular audits to ensure security practices are compliant.
- Deploying endpoint detection and prevention tools to thwart malicious hacks.
- Setting patch management systems to update applications automatically.
- Implementing comprehensive vulnerability management systems across all assets on premises and in the cloud.
- Working with IT operations to set up a shared disaster recovery business continuity plan.
- Working with HR and the team leads to educating employees on how to identify suspicious activity.
- Technical lead for the Behavior Analytics platform for the entire company and accountable for the availability, reliability and performance of the platform.
- Collaborate with IT infrastructure, Application teams and business security leaders to define and gather Analytics requirements.
- Understand the company's IT Infrastructure, Applications, Business model, processes, Security controls and develop Threat Detection Models within the Behavior Analytics platform.
- Coordinate and perform security testing activities (penetration testing, vulnerability scanning, application security testing), report on results, track metrics & trends, and drive remediation.
- Coordinate and perform proactive security monitoring, event analysis, incident response, and trending.
- Managing and performing on teams that conduct analyses related to forensic investigations, cybercrimes, or cyberattacks and supporting various and dynamic security analysis needs of the team.
- Analyzing security logs, monitoring logs, firewall logs, intrusion prevention system logs, and network- and core-related logs.
- Analyzing and developing baselines for all related risks from Security Analytics and other log management tools, emphasizing security analysis of critical system logs and network protocols.
- Managing analyses of logs, traffic flows etc. to identify malicious activity, design rules that trigger response to malicious activity, analyzing the findings on malicious activity and preparing reports; developing response procedures for addressing potential security threats and driving the on-boarding of new logs into Security Analytics.
- Conducting analyses of evidence of network penetrations and data theft using firewalls, active directory, Windows operating systems, intrusion detection/prevention systems, proxy servers, breach indicators, and log aggregation technology.
- Conduct vulnerability and risk assessment on Information Systems to ensure they are in compliance with security standards and measures utilizing Assured Compliance Assessment Solution (ACAS) and Nessus Scanner.
- Hands-on troubleshooting, analysis, and technical expertise to resolve incidents and service requests previous experience in troubleshooting day-to-day operational processes such as security monitoring, data correlation, security operations.
- 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.
- Building and developing long term relationships with all stakeholders internally and with clients.
- 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.

SKILLS AND EXPERTISE:

- OWASP, SANS, CIS, CSET
- Wireshark, Nmap, Snort, Metasploit, Nessus, Recon, JTR, Hydra, Hashcat, Burp Suite, Sherlock, ZAP, Masscan, BloodHound, Mimikatz, Empire Framework, Netcat
- Windows / Linux OS / RHEL Enterprise
- Python / Bash Scripting
- MS Office - Excel/PowerPoint/Outlook

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.