**Evaluation Only. Created with Aspose.Words. Copyright 2003-2024 Aspose Pty Ltd.**

Dear Mr. / Ms.

I am submitting herewith my resume for your perusal consideration for the post in Information Security Trainer in your organization.

A systematic, organized, hardworking and dedicated team player with keen interest in security and enthusiasm to learn I have experience of 15+ years across Vulnerability Analysis, Web Server security, Unified Threat Management, Information security Governance Risk & Management.I have knowledge of Penetration Testing Methodologies, legal agreements, report &documentation. I have innate sense of task prioritization, managerial aptitude and result oriented attitude towards accelerating organizational growth and that too in a high pressured, time bound and competitive environment.

I am a dedicated and focused individual, determined to add value to the organization I work for, through my exceptional knowledge and learning ability. I possess well developed communication skills with reputation of unwavering accuracy, credibility and integrity.

At this stage I find myself to be groomed enough to look outward and explore the possibility of placement at a suitable professional position with higher responsibilities. A tour through my enclosed resume shall familiarize you with the details and I am confident, in my credentials, you would find a perfect fit for the said job. Thanks in advance for sparing your time.

The above credentials along with my enclosed resume make me ideally suitable for a position in your organization. I would appreciate an opportunity for interview.

Thanking you.

Yours Sincerely

Mohammed Zeeshan Farooq

**MOHAMMED ZEESHAN FAROOQ**

**IT / COMPUTER INSTRUCTOR - MCT**

**Contact information:**

**10-3-274/11 HUMAYUN NAGAR HYDERABAD**

**Mobile: +9581902611/9553995551**

**E-mail: Zeeshm215@gmail.com,zeeshanfarooqceh@gmail.com**

**Objective:**

**To contribute exceptionally strong technical aptitude and education to an organization that can use a skilled manager, trainer, and hands-on information systems/communications professional.**

**Summary of Qualifications**

**Computer Technology Instructor with extensive experience in Network Administration, Project Management and Quality Management. Consistently recognized and awarded for performance. Key areas of expertise include**

**Instruction:**

***􀁸*** Technical Instruction 􀁸 Research and Evaluation 􀁸 Student Assessment

􀁸 Curriculum Development 􀁸 Lecture Techniques 􀁸 Lesson Plans

**Computers:**

􀁸 Microsoft Operating System 􀁸 Mac Operating System 􀁸 Cyber Security

􀁸 Network Administration 􀁸 Data Forensics 􀁸 Software Configuration

􀁸 Malware Analysis 􀁸 Cissp 􀁸 Web Development

􀁸 Internet Technology 􀁸 Python programming 􀁸 MS Office Professional

Skills worked on

   Application Security

•         Access Control - MAC, DAC, UNIX

•         Malware Analysis - Memory Forensics

•         Intrusion Detection - HIDS, NIDS

•         Honeypots

•         Reverse Engineering

•         Web Security

•         Data Security - Cryptography

•         Network Security + VPN

•         Secure Development - Secure Coding + DevSecOp

•         Android Security

•         Hands-on Security - Network traffic analysis + CTF + VAPT

**Professional Experience and Assignments**

Overall Work Experience – ***11 years 4 months***

Teaching/Training Experience ***– 11 years 4 months (5 years 5 months at Corporate and college level)***

Senior Cyber Security Instructor at Grey Campus/e hack academy /gps infotech/IHT/SFG for WIPRO CLIENT Feb 2015- Present

Cyber Security And Network Trainer, have provided 400+ Technical hands-on training to various clients & institutions practices with Lab Assistance covering over 40,000 participants from across the globe.

PROVIDED TRAIING FOR CIS BATCH IN WIPRO

WINDOWS BASIC AND ADVANCED

LINUX BASIC AND ADVANCED

ADVANCED NETWORKING   
● Trained on **Threat and Incident Management Team(SOC)**

 Analyze and research on network based issues and addresses them effectively and independently using the SIEM

tool (Qradar).

 Deal with system vulnerabilities, security exploits, system compromises and other threat issues.

 Reporting of any unusual attacks on the network to business while monitoring IDS, IPS.

 Proactive identification of critical alerts or security breach incidents and resolve the issues within the timelines.

 Proactively identifying malicious websites from IDS events generated in a given day and also blocking the

malicious website on proxies to prevent further download of virus if any user accessed.

 Perform detailed protocol analysis of firewall events, routers, and system and application logs.

 Daily IDS and Brute force attacks monitoring is performed at QRadar level.

 Daily DOS and DDOS attacks results are verified through IDS traffic monitoring.

 Daily SQL Injection vulnerabilities are verified through Guardium log capturing tool.

 All the privileged activities are validated through the Incident and Change order tickets from GSDE tool.

 Authenticating the network security of various systems, platforms, databases and applications and governance of

VMware and Citrix

**Experience in providing monitoring and response to security events in Security Operations Center**

Working on vulnerability Management Life-cycle : Reporting  
● Reviewing the Configurations of the Network: Incident Response  
● Designed content of Cyber Security E learning for many companies including one of Big4  
● Designed content of CCNA and CCNP E Learning for multiple clients.

**Senior Cyber Security Trainer at value c Consulting/workopolis as Freelancer Feb 2019- Present**

within 10 Months of Joining.  
  
Projects :  
a. Network Security Audit ( Govt. Client)  
● Compliance readiness, Audit preparation & Third-party audits in partnership with other security teams in the organization  
● Firewall Audit  
● Information Security Policy Gap Assessment according to ISO 27001:2013  
● Defined Network Processes for the organization  
● Perform security assessments such as VA/PT, Web Application, Source Code Review & configuration  
● Developed & Implement MBSS (Minimum Baseline Security Standard) for Core/IT infrastructures  
● Security Assesment of SDWAN including of ACI and APIC  
b. OS Configuration Review (US Client)  
● Operating system and network configuration review according industry practice.  
c. Cyber Security Assessment of Scada/ ICS system of a leading government client  
● Network Architecture Review of SCADA and IT network  
● Vulnerability analysis and security design of SCADA/ICS Control systems  
● Configuration Review of SCADA networkFirewalls

Roles and Responsibilities ( ArcSight)

 Experience in Security Operations

 Develop and maintain documentation for security systems and procedures for better security

outcomes. Respond to, where appropriate, resolve or escalate reported security incidents,

raising alerts through proper methodologies and ticketing tools.

 Creation of reports, queries and filter for the events that are generated in ArcSight console

on the basis of severity and priority of the events. Ensure application availability and SLA

adherence.

 **Real time monitoring and analysing system logs, SIEM tools** and network traffic for unusual or

suspicious activity, interpret such activities and make recommendations for resolutions.

Recognize cyber attacks with their signatures. Differentiate the false positive from true intrusion

attempts and prevent.

 Regular interaction with associated customers to update regarding security issues being noted in

their infrastructure.

 Configuring and managing use cases including standard, correlation and anomaly based rules.

Configuring, managing and fine tuning of event, flow and common rules.

 Creating complex correlation rule for identifying attacks and mapping each rule with cyber kill

chain phase.

 Creation of custom Reports, Dashboards, Searches as per SOC requirements.Publishing of

Security Incident reports to CISO.

 Creation of Security operation documents, run book, knowledge base and SOPs.

 Creation of Incident Response and Closure document for each use case created and fine tuned.

 Evaluating and processing client Adhoc Queries.

 Real time identification, analysis and resolution of Security events using Dashboard , Active

Chanel and Active List.

 Creating Daily, Weekly and Monthly Trend Analysis Reports and sharing with client with proper  
● Security Solutions and Policy Review of IT and SCADA System as per NIST 800-82  
● Web Application security assessment of applications used by IT and SCADA users  
● Penetration testing of critical infrastructure of SCADA and IT network  
● Assessment of Historian Services and Yokogawa system.  
d. BCP/DR  
● Worked on Business Impact Analysis  
● Recovery strategies  
● Backup Strategies  
● DR Plan

Cyber Security Trainer at freelancer with various institution like Aon Soft//gps infotech May 2013- Jan 2015

* Responsible for day to day operations of the department.
* Scheduling classes on a quarterly basis on **Labs** and allocation accordingly.
* Handling special batches with **Lab work** and corporates within the area of expertise.
* Allocation of resources and Utilization.
* Technically competent professional with experience across Vulnerability Analysis, Web Server Security, UTM, IT Risk Management and Technical support.
* Expertise in handling diverse range of information security domains, including policy design and development, risk assessment & treatment, intrusion detection & prevention as well as Malware amongst others.
* Responsible for proactive **threat hunting activities** across the network leveraging intelligence from multiple internal and
* external sources.
*  Conduct threat hunt operations using known adversary tactics, techniques and procedures (TTP’s) as well as Indicators
* of Attack (IoA) in order to detect adversaries with persistent access to the enterprise.
*  Collect and Provide actionable intelligence inputs from various internal & external sources.
*  **Perform Malware Analysis** [Basic Static and Dynamic Analysis].
*  Conduct RCA and help team to fine-tune security incidents.
*  Perform forensic analysis of network packet captures, DNS, proxy, Netflow, malware, host-based security and
* application logs, as well as logs from various types of security sensors.
*  Designing **Threat Model based on IoC’s and IoA’s.**
*  Incident Response -triage Incidents in Internal and customers.
*  Active Threat Hunting.
*  Helping team in investigating threats identified using models.
*  Provide ideas for new Threat Hunting models using Big Data Analytics and Machine Learning algorithms.
*  Fine tuning existing models.
*  Working SOC/SIEM and other teams to resolve the issues with respect to log flow and mitigation of threats.
*  Vulnerability & Threat Assessment by creating category of threats level using business / process impact, network traffic.
*  Helping customers to mitigate Cyber Security related issues.
* Professional expertise in detecting threats to information security from unauthorized entrants and applying the countermeasures to mitigate them.
* Focused and hardworking professional equipped with thorough knowledge and technical understanding coupled with an analytic bent of mind and confident to take challenging assignments.
* Conducting and reporting vulnerability assessments against the Infrastructure and Software
* Assisted in Internal Network Testing
* Network & Log Monitoring for security incidents
* Install, update, operate and maintain Malware protection software in accordance with the Security Policy .
* Identify unpatched, unauthorized and unprotected systems and remediate in accordance with the Security Policy
* Provided security awareness training to the users
* Monitoring of various Security devices and submitting monthly report on security health systems
* Coordinated with outside vendors & suppliers regarding implementation of new software when needed
* Maintaining records of course preparation (lesson plans, etc.) and evaluation tools (examinations, quizzes, project/portfolio assignments, etc.), and submits as required.
* Additionally had been training Security(Security+, Security Awareness, Data Science and Machine Leaning ,CEH, CASP etc.), Networking (A+,N+CCNA etc, Programming(Java,Asp.net etc) & Database(Oracle, MS SQL etc.) courses.

**Cyber Security Trainer at Technosoft May 2013- Jan 2015**

I have worked for OTSI as Senior Analyst within the Risk Advisory Services - Cyber Security OTSI.  
  
Network : Configuration of all series of routers, switches, access points, firewalls, wireless controllers.  
  
Tools Used - Nessus Agents/Plugin Scripting, Nmap, Ettercap, Wireshark; Hardware - Firewalls (Stateful and Stateless), IDS (Network & Host based), IPS (Network & Host based), Packet Shaper, VPN (Checkpoint and Cisco); Capability - Active & Passive Information Gathering, Reconnaissance, Banner Grabbing, Port Scanning, Services Enumeration, OS Fingerprinting  
  
Server : Installation of all type of servers (HP, IBM, Dell, CISCO), VMsphere  
System: Software - Linux (Kali, Backtrack, Ubuntu), MAC OS X, Microsoft Windows (95, 98, 2000,  
NT, 2003 Server, XP, 2008 Server, 7, 2012 Server); Capability - Kernel modification, Inter Process Communication, CPU Scheduling manipulation, Device driver signature modification, Registry manipulation  
  
  
  
I was responsible for:  
  
1. Conducting Configuration review/audit of Network Devices and Operating Systems.  
2. Conducting Web Application Security Assessments.  
3. Conducting Vulnerability Assessments & Penetration Testing of Networks and Web Applications.  
4. Performing GAP Analysis and Risk Assessment on implemented ISO 27001 controls.  
5. Preparation of Cyber Security program and ISMS - polices, process and procedures  
6. Actively supporting internal business development initiative

Nleague information security Analyst

Configuration and Management of Network components. (Routers, Switches and firewalls)  
• Configuration and Management of Servers. ( MS 2003,2008 R2, 2012R2, Red hat)  
• Conduct security audits and manage remediation plans.  
• Perform VA on Network Infra.  
• Create, manage and maintain user security awareness.  
• Monitor and advice on information security issues related to the systems and workflow to ensure the internal security controls for the campus are appropriate and operating as intended.  
• Conduct Training Sessions for internal Employees.  
• Develop and publish Information Security policies, procedures, standards and guidelines based on knowledge of best practices and compliance requirements.see less

HP (Hewlett-Packard) Staff Management (L2 Security Analyst) June 2007- Dec 2012(Team Lead of 2 Years’ experience)

Rack Servers of

Face book,Google Microsoft (Handling all Security isuues

**Security Incident Handling & Management**, analyzing events and raw logs for possible Incidents and finding RCA for the same.  
-Collecting, analyzing and preserving the evidence related to incidents.  
-Log analysis utilizing Enterprise Products

-Security Incident Handling & Management, analyzing events, and raw logs for possible Incidents and finding RCA for the same.  
-Preparing Reports and Presentations based on Incidents Reported.  
-Endpoint Compliance which includes device control compliance, AV Compliance check, insecure shares and admin account privileges review, Desktop and Laptop USB Compliance check etc.  
-Develop indicators and analyze network logs, in conjunction with operation teams to identify emerging threats.  
-Administration of ARCOS (Privilege Identity Management), Seclore (Data Rights Management) and McAfee DLP, tools.  
-Review and respond to internal security issues.  
-Present monthly security review to the management on monthly and quarterly basis.  
-Investigating and streamlining Security Incidents based on root cause analysis.

**Projects Handled**

**Project 1:** Trained 935 Military Technical College Students

With an Overall staff strength of 8, effectively trained 935 Military College students on IC3 course within a short period of 3 months

**Project 2:** Trained 110 candidates on Cyber Security within a span of 3 months

Omantel sponsored candidates been trained on Cyber Security within a short duration of 3 months.

**Project 3:** GITTC project of Oman

GITTC (Phase 3) is a government funded project to train 7000 candidates in IC3in Labs . With 4 vendors selected all over Oman, Polyglot Institute is one of them with me managing the project as a Project head.

Tools used

IT Trainer at Tekskills , Houston TX USA’ 08 to April’ 12

* Conducted computer training needs assessment by collecting information pertaining to work procedures, work flow, and reports; understanding job-specific functions and tasks.
* Determined system utilization requirements by researching and testing systems.
* Designed computer training manuals by identifying and describing information needs; used desktop publishing; submitted initial versions for review; revised and edited final copy.
* Maintained safe and healthy training environment by following organization standards and legal regulations.
* Projects: random album generator, predict housing prices, best classifier model,
* Conducted training classes by presenting job-specific, company-specific, and generic software applications and personal computer classes.
* Ensured operations of equipment by completing preventive maintenance requirements; followed manufacturer's instructions; troubleshooting malfunctions; called and maintained equipment inventories; evaluating new equipment and techniques.
* Maintained quality service by establishing and enforcing organization standards.
* Evaluated the training by assessing regularly the effectiveness of training to specific job applications.

**Education/Professional Qualifications:**

B.Tech (CSIT) Completed in 2005

**Certification:**

**This document was truncated here because it was created in the Evaluation Mode.**

**This document was truncated here because it was created in the Evaluation Mode.**

**This document was truncated here because it was created in the Evaluation Mode.**