|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **E-mai:** [**jamal-397104@gulfjobseeker.com**](mailto:jamal-397104@gulfjobseeker.com)  Jamal |  |  | Canadian-PassportsizePic-02-06-2014 |  |

**CAREER OBJECTIVE:** In quest of challenging assignments in Information Security.

**PROFESSIONAL CERTIFICATIONS**

|  |  |  |
| --- | --- | --- |
| * **ISACA:**Certified Information Security Manager (**CISM**) * **IBM** Certified Associate Analyst - Security **QRadar SIEM** * **IBM** Security**QRadar SIEM** V7.2.7 Deployment * **Cisco** CCNA Cyber Ops (SOC) * **Trend Micro™** Certified Security Expert (**TCSE**) * **Kaspersky** Lab Certified Consultant (**KLCC**) | * **Mile2:** Certified Penetration Testing Engineer (**CPTE**) * **EC-Council:**Certified Ethical Hacker (**CEH**) * **EC-Council:**Certified Security Analyst (**ECSA**) * **Barracuda Networks** Certified Support Engineer (**BCSE**) * **Microsoft** Certified IT Professional: Server Admin**(MCITP)** * **Microsoft** Certified Solutions Associate(**MCSA**) |  |
|  |  |

**CORE TECHNICAL KNOWLEDGE AND SKILLS**

15+ years of experience in supporting large-scale, distributed client/server, multi-platform environment and working on Windows Servers/Workstations and several different variants of Linux/Unix, strong understanding of Security technologies such as:

|  |  |
| --- | --- |
| * **OS** | Windows 8/Server 2008/2012, Linux (Red Hat, Kali), Cisco IOS (various versions) |
| * **Security Applications** | IBM QRadar,IBM Guardium, Gemalto, Barracuda Spam Firewall for SMTP, Trend Micro Office Scan (Anti-Virus Server), Kaspersky Security Center 10 (Anti-Virus Server),Arbor (PeakFlow-X| SP), WSUS |
| * **Pentest Tools** | IBM Appscan, Acunetix Web Vulnerability Scanner, Netsparker Web Security Scanner, Burp Suite, OpenVAS, Nessus, Rapid7 NeXpose Vulnerability Scanner, Nmap, Nikto, Metasploit, SEToolkit, Sparta, Sqlmap, Fimap, hash-identifier, Hashcat, Hydra, W3af, Uniscan, Arachni, Wpscan, joomscan. |
| * **Virtualization** | Vmware ESXi 4.1, VSphere, Vmware WorkStation, MicroSoft Virtual PC, Hyper-V |
| * **Reporting tool** | Dradis Framework, KeepNote |

**WORK EXPERIENCE**

|  |  |
| --- | --- |
|  | Sep 2017 ~ Till Date |

**Senior Information Security Consultant**(Reporting to CEO)

* Simulate Phishing attack on the entire network in financial institutions.
* Investigated ownership of account taken via Social engineering drill, ransomware, and online scams.
* Recovered Hacked Card (Credit / Debit) and remove those cards details from the Deep / Dark Web via Secure Coat flagship Card Recovery tool "**Threat Ninja**" (For detail:http://www.securecoat.net/dark-web-monitoring.html)
* Deployed, fine-tuned, integration, administrated QRadar SIEM project at Meezan Bank (deployed QFlow separately), Silk Bank, Getz Pharma, Summit Bank (QRadar at SAN), HMB and with QVM (QRadar Vulnerability Manager), QRM (QRadar Risk Manager) at CDC and with High Availability at Faisal Bank.
* Deployed, fine-tuned, integration, administrated IBM Resilient project at Algeria Gulf Bank and implemented DOS, Malware and phishing workflows.
* Manage Bank Alfalah’s SOC (Security operations Center) via IBM QRadar, create use cases in heterogeneous network environment for intrusion detection including handle SOC’s tickets.Monitor, triage, and prioritize events, alerts and tips for further investigation. Wrote parser of un-supported devices and applications for integration.
* Investigate network traffic for potential security incidents at QRadar. Preparing Reports based on Incidents Reported.

|  |  |
| --- | --- |
| **Udemy** | July 2018 ~ Till Date |

**Cyber Security Instructor**

* Learn about deep web, dark web & how Credit / Debit Card does hack & recover cards practically via Card Recovery tool
  + This is the first course in the whole market with a practical approach that you can recover your Credit / Debit cards details (Card number, Expiry date, PIN, CVV, Track 1&2, etc.) and save you from the Fraud. This course is focused on the handy side of Deep and Dark Web Monitoring without disregarding the hypothesis behind each attack.
* No Theory Only Demonstration - Find critical vulnerabilities which full your pocket by doing the Manual bug bounty
  + This course is totally in light of real-life security vulnerabilities. This is where individuals make a huge number of dollars by simply reporting one major bug to the big organizations like Google, Facebook, Microsoft, Apple, etc.

|  |  |
| --- | --- |
| **Trillium Information Security Systems** | July 2016 ~ Aug 2017 |

**Information Security Lead Consultant**(Reporting toCEO)

* Leading IBM QRadar SIEM project at JS bank and Soneri Bank and conducted QRadar SIEM PoC at Parco to perform event/flow correlation across all critical systems.Collecting, analyzing and preserving the evidence related to incidents.
* Manage Bank Alfalah’s SOC (Security operations Center) via IBM QRadar, create use cases in heterogeneous network environment for intrusion detection including handle SOC’s tickets.Monitor, triage, and prioritize events, alerts and tips for further investigation. Wrote parser of un-supported devices and applications for integration.
* Investigate network traffic for potential security incidents at QRadar. Preparing Reports based on Incidents Reported.
* Investigated Hacker Methodology using Cyber Kill Chain model in both CyberFraud and Cybersecurity.
* Directed NeXpose Vulnerability (Risk)Assessment Solution projectwith audited offline configuration file of network devices at Bank Alfalah, Soneri Bank & project at NIB bank.Deployed Web Application Firewall at TISS
* Conducted Gemalto access control 2FA and IBM Guardium Database (DB) Activity Monitoring (DAM) PoC at Bank Alfalah.
* Complianceof PCI DSS, CIS, HIPAA, FISMA, FDCC, DISASTIGS and USGCB and Assist clients with architecting and implementing security solutions.
* Execution of security projects including pentesting, vulnerability assessment, reporting, reviewing, configuration audit etc.
* Managing Pre-Sales activities including solution design, technical Demo and Technical RFP Response in the Region for QRadar, Rapid7 Nexpose, Metasploit Pro, McAfee Total Protection for Data Loss Prevention (DLP), Imperva WAF.
* Configured Endpoint Security, encryption, patch management, Virus Outbreaks and application Whitelisting via Kaspersky at Soneri Bank, PSX and Parco. Integrated Mobile device management solution via IBM Maas360 at K-Electric.
* Deployed Metasploit project at Affiniti and conducted PCI DSS Gap Analysis at UBL.
* Conducted File integrity Monitor solution (NNT) at HMB Bank to track any unauthorized modification.

|  |  |
| --- | --- |
| **[Secure](https://www.linkedin.com/vsearch/p?company=Self+Employed+Freelance+Work&trk=prof-exp-company-name" \o "Find others who have worked at this company) Coat** | Nov 2014 ~ June 2016 |

**Senior Web Penetration Tester**(Reporting to CEO)

* Scan and exploit for a range of data center groundwork and application weaknesses, subsequent defined rules of commitment and attack scenarios (Ethical Hacking). Provide risk mitigation recommendations for vulnerabilities.
* Manually test OWASP 10 vulnerabilities for Web and Mobile such as Cross Site Scripting,CSRF, SQL Injection, etc.
* Training for improvement - OWASP top 10, hands-on hacking workshop and threat modeling.
* Social Engineering Pentesting. Personnel’s assessment and exercise for the prevention of Social Engineering attacks.
* Conducted how pentesters can be under attack in their pentest activities of web application & network via Snagterpreter.
* Generated PoC of the attacks mostly from Burpsuite and reports with solution of the attacks.
* Detected bugs & classifying based on severity and experience in defect tracking and analysis as documented in SDL bug bar
* Conducted info security risk assessments based on a defined risk framework. Identify and evaluate mitigating controls.
* Investigated the strengths and weaknesses of applications, security architectures, and network devices.
* Conducted pentest (black box / white box testing) and code analyses (manual and automated) for vulnerabilities analysis.

|  |  |
| --- | --- |
| **LERCO (Dubai, UAE / Ras Lanuf, Libya)** | Oct 2012 ~ Oct 2014 |

**Penetration Tester / Network Expert**(Reporting to ICT Division Head, CFO)

* Supervising design and execution of vulnerability assessments, penetration tests and security audits and review security patches for all affected systems. Conducted Web Application Vulnerability Assessment & Threat Modelling, Gap Analysis, and secure code review on the applications w.r.t guidelines provided.Web Application Vulnerability Assessment document creation.
* Managed and administrated GUI based console of Cisco ASA 5510 firewall i.e. Cisco ASDM (Adaptive Security Device Manager) 7.11.
* Deployment and Configuration of Cisco Routers and Switches and Access Points and Wireless Routers.Responsible for Project documentations, Product technical comparisons & analysis and Disaster Recovery/BR Planning, designing & deployment.
* Deployment, administration and Monitoring of traffic (Internal/External interfaces) of Arbor Peakflow SP appliance for internal threat specially DoS/DDoS attack.
* Active Directory administration and management including Group policy management and Setting up user accounts, permissions, passwords.Managing Email, Anti-Spam, Monitoring network usage via PRTG, WSUS, Virus Outbreaks via Kaspersky Anti-Virus Server and ISA Proxy Server.
* Responsible for developing and managing ICT, ICT help desk, ICT Security and telephonic policies and act as a single point of contact for all Security technology issues.
* Involved with the administrative tasks pertaining to Security related activities and system management.

|  |  |
| --- | --- |
| **HURCCON (Karachi, Pakistan)** | April 2009 ~ June 2012 |

**System Security Officer** (Reporting to Manager Systems)

* Managed compliance of internal controls and programs against information security related regulations, policies and standards.
* Developed secure LAN with controlled internet/intranet access and configured centralized Antivirus system (TrendMicro).
* Responsible for developing an IT Security Standard Operating Procedure (SoP) for handling security incidents.
* Installation / Maintenance of Win2k3 Server, ISA 2004, WSUS, Anti-Virus Server on Compac servers, GFI Web monitor and Barracuda Spam Firewall appliance (This included all the configurations i.e. mirroring, networking, tweaking and tuning ).
* Provided consultancy to troubleshoot for performance hike and bug removal for different System and Security Products.
* Responsible for designing Support Level Agreements (SLAs) contracts with service providers.

|  |  |
| --- | --- |
| **Net Access (Karachi, Pakistan)** | Aug 2006 ~ March 2009 |

**Senior System Engineer** (Reporting to Manager Systems)Jan 2008 ~ March 2009

* Pentesting and Vulnerability Assessment implementation in different Sectors of Pakistan’s Banking and Financial institutions.
* Implementation of Port based security with Cisco 2950-2960T switches.
* Planning and management of IT NOS (Network Operations Center) by integrating views and reports from various monitoring systems including PRTG, Cisco network assistant, Firewall and Intrusion Prevention system.
* Managed projects & PoC’s of Security & Systems Infrastructure solutions involving solutions from multiple vendors i.e. Arbor Networks, IPSwitch, Plixer, Barracuda Networks, GFI, Foundry, Virus Outbreaksvia Kaspersky, Virus Outbreaksvia Trendmicro, Microsoft, Captaris, Citrix, GFI, etc.

**System Engineer** (Reporting to Lead Engineer) Aug 2006 ~ Dec 2007

* Provided onsite pre-sales technical support to prospective clients with minimal supervision.
* Identify organization's IT strengths and weaknesses and suggest areas of improvement.
* Involve in planning and deployment of Enterprise data infrastructure security measures.
* Prepare technical training material and deliver training towards customers. Tested of new features and functionality required by the customer in a R&D lab and verify that they are operating correctly in the live production environment.

|  |  |
| --- | --- |
| **Cyber Bridge, Karachi, Pakistan** | Feb 2005 ~ July 2006 |

**System/Network Administrator** (Reporting to CEO)

* Design, deployment, administration, monitoring and troubleshooting of LAN/WAN, wireless networkand Active Directory administration, resolution of software issues for common applications.
* Setting up VPN Connection to outside users, configured the appropriate security options in domain-level (GPO).

**EDUCATION**

## **2004 | B.S. Computer Engineering (**SSUET**) 1st Division (A Grade)**

Registered as a **Professional Engineer**from **P.E.C.** (Reg. # COMP-3027)

|  |
| --- |
| **INTERNATIONAL TRAININGS** |
| **2007**Got Corporate Advanced technical training in Dubai, UAE of **Barracuda** (Spam Firewall, Other products)  **2019** Conducted Corporate Instructor-led training in Algeria of **IBM** QRadar and Resilient  **PUBLICATION**   * Bank Islami Debit Card Attack Analysis * Wordpress is easy to use but not SECURE * Why IBM QRadar is best SIEM?   **HONORS & AWARDS** Microsoft Security Researcher (January2019) -[Reported DOM based XSS vulnerability.](https://portal.msrc.microsoft.com/en-us/security-guidance/researcher-acknowledgments-online-services) Top of Form  Bottom of Form Cisco Global CyberSecuirty Scholarship (Dec 2016) -CCNA CyberSecurity (Cyber Ops) will assist me to work with cybersecurity analysts within Security Operations Centers (SOC’s). **NASA (October 2016)** - [Found SQL injection vulnerability at NASA website.](https://www.youtube.com/watch?v=lFUBzEU4D0Q) BarracudaLabs Hall of Fame (July 2014)–[Listed as a Security Researcher (Clickjacking Vulnerability).](https://barracudalabs.com/research-resources/bug-bounty-program/bug-bounty-hall-of-fame-2/)Microsoft Security Researcher (July 2014) -[Reported XSS vulnerability.](http://technet.microsoft.com/en-us/security/cc308575.aspx#0714) |