**Technical Competencies – Security Engineer – System & Infrastructure**

**Applicant Name:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **N** | **Technology** | **Years of experience** | **Competence (rating : 1=basic  5=excellent)** | **Detailed description of how this specific professional experience was gained.** | **Companies where you applied these skills / knowledge, according to your professional experience, e.g. 1-the most recent position, etc.** |
|  | Advanced university degree in Computer Engineering, Computer Science; |  |  |  | 1,2,3,4,5,6,7,8 |
|  | Certified Ethical Hacker certification or equivalent; |  |  |  | 1,2,3,4,5,6,7,8 |
|  | SANS, EC-COUNCIL CISSP, CCNA and CISA certifications would be an advantage; |  |  |  | 1,2,3,4,5,6,7,8 |
|  | Depending on the expertise required, specific Windows, Unix, Network, Database or Storage certifications would be an advantage; |  |  |  | 1,2,3,4,5,6,7,8 |
|  | Excellent knowledge of IT security processes, features, issues and solutions associates with operating systems, applications infrastructure and networking devices security such as but not limited to Windows, UNIX, Database, Storage, Firewalls, Routers, etc; |  |  |  | 1,2,3,4,5,6,7,8 |
|  | Excellent knowledge of Linux command line, debug and monitoring tools and kernel calls; |  |  |  | 1,2,3,4,5,6,7,8 |
|  | Excellent knowledge of Windows Active Directory and MS Exchange; |  |  |  | 1,2,3,4,5,6,7,8 |
|  | Experience in performing security testing on infrastructure platforms (such as Windows and UNIX-based OS, firewalls, routers, etc.) and infrastructure applications (such as Oracle and SQL databases, J2EE, .NET, Apache, IIS, etc); |  |  |  | 1,2,3,4,5,6,7,8 |
|  | Experience in testing practices on authentication, authorisation and session management, HTML injection, input validation, information leakage and denial-of-service; |  |  |  | 1,2,3,4,5,6,7,8 |
|  | Experience in performing operational acceptance processes under time and resource constraints; |  |  |  | 1,2,3,4,5,6,7,8 |
|  | Good knowledge in ethical penetration test methodologies (OSSTMM, OWASP) and best practices; |  |  |  | 1,2,3,4,5,6,7,8 |
|  | Good knowledge in data recovery techniques, encryption, service protocols and computer privacy; |  |  |  | 1,2,3,4,5,6,7,8 |
|  | Knowledge and experience with commercial testing tools (Nessus, Core Impact, WebInspect, etc) as well as open source tools such as Metasploit, Nmap, Nikto, Paros, Burp, etc.; |  |  |  | 1,2,3,4,5,6,7,8 |
|  | Knowledge and experience with software development and scripting languages such as Perl and Python, C/C++, Java programming experience would be an advantage; |  |  |  | 1,2,3,4,5,6,7,8 |
|  | Ability to linking IT security with business processes; |  |  |  | 1,2,3,4,5,6,7,8 |
|  | Experience in process analysis including definition of Standard Operating Procedures; |  |  |  | 1,2,3,4,5,6,7,8 |
|  | Ability to research security topics and produce briefing notes (technical and non-technical); |  |  |  | 1,2,3,4,5,6,7,8 |
|  | Strong interpersonal skills and result-oriented approach; |  |  |  | 1,2,3,4,5,6,7,8 |
|  | Good writing skill and ability to explain complex ideas clearly and concisely; |  |  |  | 1,2,3,4,5,6,7,8 |
|  | Teaching and technical training experience is an advantage; |  |  |  | 1,2,3,4,5,6,7,8 |