Information Security Analyst Job Description

Duties and Responsibilities:

- Responsible for defining access privileges, control structures, and resources to protect systems
- Operate software to protect systems and information infrastructure, including firewalls and data encryption programs; and install security measures
- Handle cyber-threats by applying reactive and proactive measures
- Undertake research, simulate and run penetration tests using publicly available and proprietary tools
- Provide leadership for security projects along with other security and R&D groups
- Responsible for developing and maintaining lab environments to evaluate new security threats
- Continuously undertake research on new attack vectors and techniques
- Participate in product security reviews with R&D and product management teams
- Identify abnormalities, recognize problems, and report violations
- Assess current situation, evaluating trends and anticipating requirements to implement security improvements and processes
- Provide support for executive reporting through analysis of information security trends, metrics, and statistics
- Provide support for user access administration processes and user entitlement reviews
- Conduct periodic audits to determine security violations and inefficiencies
- Implement and maintain security controls to upgrade systems
- Prepare performance reports and communicate system status to keep users informed

- Implement and oversee security training awareness program within the organization
- Maintain industry compliance certifications for the organization
- Review Third Party information and Vendor software/hardware security controls/risks and document gaps and issues for action
- Support customer security reviews for new and existing customers
- Conduct security research in keeping abreast of latest security issues and Maintain technical knowledge by attending educational workshops; reviewing publications.

Information Security Analyst Requirements – Skills, Knowledge, and Abilities

- Education: To work as an information security analyst requires a post-secondary education, preferably a Bachelor's degree in Business, Information Technology, or Cyber Security, or in other technology related discipline
- Certification: It is also a plus to be certified or working towards certification from accredited bodies, including Certified Information Systems Security Professional (CISSP), Certified Information Security Auditor (CISA), or Certified Information Security Management (CISM)
- Experience: Depending on the needs of the recruiter, they may require 2-5+ years of experience in security analysis or related field; with experience in leading security analysis project/team independently for the full project lifecycle; scripting/coding experience (Python, Perl, Ruby, Bash, PowerShell, .NET, HTML5, PHP, etc.) for developing, extending, or modifying exploits, shellcode or exploit tools; and hands-on experience in static and dynamic malware analysis
- Knowledge: Information security analysts are required to have strong understanding of security principles, policies, and industry best practices. They must also possess networking knowledge – an understanding of networking essentials, data flows, architecture, ports, and protocols, wireless, etc.
- It is also important that they possess general operating system knowledge – a solid understanding and practical experience in various

flavors of Windows and Linux, OS configuration, file system structures, OS components, mobile operating systems, etc.

- It is also vital that they possess knowledge of TCP/IP, computer networking, routing and switching; cloud computing, including AWS and Azure security and best practices to protect cloud infrastructure; and Penetration testing of cloud and on-premise applications and infrastructure
- Communication skills: Information security analysts require great oral and written communication skills for technical writing, including assessment reports, presentations, and operating procedures
- Interpersonal skills: They require interpersonal skills to work collaboratively and effectively with others
- Troubleshooting skills: They require the ability or skill to recognize the cause of a problem and get to a root cause, as well as conduct forensic investigation and analysis of how and why a crack or some other compromise occurred
- Problem-solving and analytical skills: It is essential that information security analysts are natural problem solvers committed to utilizing their technical and collaborative skills in deriving solutions to identified problems
- Organizational skills: they require this skill to effectively prioritize tasks and work simultaneously on several projects.