Network Penetration Ethics Paper

The profession of a Security Engineer is an interesting one. Security Engineers develop and supervise data and technology security systems to prevent breaches, taps and leaks associated with cybercrime. There are other titles that are associated with Security Engineer and they include information assurance engineer, information systems security engineer, and information security engineer. Cybersecurity dates back all the way to the early 1970s, when Ray Tomlinson invented and implemented the first email program on the ARPANET system, precursor to the Internet. As the need for more advanced cybersecurity defenses grew in the late 1970s and the early 1980s, there were many institutions, like U.S. Air Force, Stanford University, and University of California Los Angeles, that went through extensive research and development of new cybersecurity software. In the 1980s, TCSEC (Trusted Computer System Evaluation Criteria) was created by the United States government. This team was tasked with establishing new cybersecurity protocols that would have a great influence on the next generation of security developments. The work of the TCSEC team led to the United States and Europe working together to create the Common Criteria, which was a new standard of internationally focused security practices. Some of the protocols of the Common Criteria are still in practice today, but organizations and businesses today rely on security engineers for defense. Security engineers help tailor cybersecurity defenses to meet their clients' needs in nuanced, effective ways.

There are many roles and responsibilities that a security engineer has, like developing a set of security standards and practices and creating new ways to solve security production issues, but security engineer is mainly responsible for testing and screening security software and for monitoring networks and systems for security breaches and intrusions. Security engineers are the first line of defense, for a company, against unauthorized access from outside sources and potential security threats. Security engineers should know how to pin-point any potential threats, as well as know how to plan and prepare before any security threats take place. They resemble and all-in-one security team by implementing and testing strategies, reporting on any incidents for future preparation, keeping track of the status of network security, and educating other employees to raise security awareness.

To become a security engineer, employers look for people who have a bachelor’s degree or higher in a field like, computer science, computer programming, software engineering, systems engineering or information systems. Some positions also require certification and five to ten years of experience. Security engineers should also consider getting a master’s degree and also a variety of other certifications as well. Certifications that people nay wish to consider include, CEH: Certified Ethical Hacker, CCNP Security: Cisco Certified Network Professional Security, GSEC/GCIH/GCIA: GIAC Security Certifications, and CISSP: Certified Information Systems Security Professional. These are just a few of the highly recommended ways to becoming a security engineer.