Career paper

Audrey Gyane

Old Dominion University

Cybersecurity and Social Science 201s

Professor Matthew Umphlet

Apr 3, 2024

Senior security engineers are in charge of securing networking, information, and computer systems are created and carried out by them. They are in charge of developing security protocols, evaluating potential risks, and conducting tests to identify vulnerabilities. They also conduct extensive inspections into incidents, supervise the handling of security breaches and advise the safety group. They have to keep up with the newest advancements in security and the trends that go on. Additionally, they must be able to communicate difficult subject matters to groups that vary in levels of technical expertise.

Over the course of the project's phase, the duties comprise detecting and reducing risks and hazards related to network protection. This matches up with determinism because it maintains that events, such as attacks on security systems, exist for established reasons and might be partly predicted and managed by intentional behavior. The role's fairness is demonstrated by its emphasis on verifying, examining, and reviewing system security installations and requirements in comparison to many legal standards. Stressing objectivity analysis and complying to proven rules shows how important objectivity is to guaranteeing the efficiency and dependability of security protocols. Equal treatment and balance while making choices are essential components of ethical neutrality, especially when it comes to ethical issues. Improved network safety and reducing risks are the main focuses of the work, but it must also entail upholding moral standards like honesty, privacy, as well as protection information that is given. Further, advising program directors, technical specialists and staff members on matters of ethics and encouraging moral fairness in risk related choices and actions are all part of the job description of someone who has had experience in the area in security frameworks. Relativism shows us that opinions and meanings can change depending on others viewpoints or situations. In order to take into consideration relativism within the way decisions are made, this position

requires taking into account the opinions of many different parties, including program leaders, the client association, and in-house technical professionals, in addition to suggesting and carrying out technical improvements according to up to date system safety designs. In summary, this position's duties show how the concepts of social sciences relate to the area of securing systems, highlighting the significance of cautious method, accurate evaluation, taking into account a variety of viewpoints, and following moral values in protecting systems and data.

The first challenge is the growing number and complications of cyberattacks highlight the pressing requirement for the strong defenses. The speed at which hackers are taking advantage of the weaknesses in cyber systems is causing a sense of worry and this is creating a lack of awareness of senior executives and a regular person who is not aware of all types of cyberattacks. Next, is the need for technical knowledge and skill and skill increases along with the advancement of the internet, like quantum computing, artificial intelligence (AI) and driverless cars. Lastly, when it comes to cyber security, the growing significance of ensuring the safety of supply chains raises serious questions about company survival. Because of the increasing availability of open source intelligence (OSINT) and the increasing influence of false information, roaming the internet requires greater caution and judgment from the stuff that happened in the past.

Psychology is used a lot when it comes to senior information system security engineers, they use it to make their tactics better. By understanding the way people act, it could help create training programs for security that are more successful by taking personality traits and new patterns into account. Because of the threat concept they must always be evaluating and reacting to numerous cyberattacks that their company might be exposed to. To find possible threats, examine attack routes and set priorities for managing them, they use threat data. They protect

crucial information and systems from bad criminals by being alert and aggressive in spotting and stopping new attacks. In the context of the natural experiment concept , they might run into unwanted predicaments or network breakdowns inside their area, offering chances to study how cybersecurity affects the real world. These experiences are like quick attacks or unknown risks that provide important new ways to look at the value of the current procedures and policies. They are met with limitations when they attempt to lessen cyberattacks, resulting from things like limited resources, constantly shifting ways of the internet and mistakes made by humans. Even with strong measures put in place to protect the security, companies might not be able to identify and stop advanced incidents that take advantage of newly discovered weaknesses.

Information systems security requirement views are shaped by senior management through normative procedures that are influenced by peer groups and training. Through imitation of effective methods, mimicking processes affect top management views and involvement in ISS projects. Before collecting data, researchers must determine whether to deal with combined formal and reflection variables. These kinds of models, components based SEM, particularly partial least squares (PLS). In this work, creative measures for model mass and mirror variables for putting what were evaluated as part of the model testing process using repetition analysis inside PLS.

Citation

How to become a senior security engineer: What it is and Career Path. Zippia. (2024, March 14). https://www.zippia.com/senior-security-engineer-jobs/#

IEEE.pdf. (n.d.). https://www.iitrpr.ac.in/library/pdf/IEEE.pdf

On the benefits of Senior Executives' Information Security Awareness. AIS Electronic Library (AISeL) - ICIS 2019 Proceedings: On the Benefits of Senior Executives' Information Security Awareness. (n.d.). https://aisel.aisnet.org/icis2019/cyber_security_privacy_ethics_IS/cyber_security_privacy/25/

Senior information system security engineer (ISSE) in Annapolis Junction, Maryland, United States: Engineering & Technology at BAE Systems. BAE Systems. (2023, September 13). https://jobs.baesystems.com/global/en/job/98641BR/Senior-Information-System-Security-Engineer-ISSE