Topic 8 Discussion 1

Research the SANS Institute security life cycle and in your own words, provide a brief summary of the purpose, the scope of the ideology, and how you will apply this to your future career as a cybersecurity professional. Be sure to include the four steps within the process.

Hello Class,

The SANS Institute security lifecycle is a best practice methodology indented to ensure ongoing security from threats. The scope includes any IT network as security needs to exist at all levels. The four steps as identified in the SANS lifecycle 592 document are as follows:

Prevention – The implementation of security devices such as firewalls, anti-virus, phishing/malware detectors, etc.

Assessment – An asset management database identifying what the organization has and how it’s being securely protected.

Detection – Having systems in place such as Intrusion Detection System to identify when an intrusion occurs.

Response – A plan is necessary to understand the response approach if and when a security threat is identified.

The above steps are an on-going process as technology is ever evolving and infrastructure architecture is continually updating. As new hardware/software is introduced, the process needs to be completed again to ensure new vulnerabilities are identified and remediated as soon as possible.

The SANS life cycle can be applied to any security program. The purpose of the cycle is to be a guide for the continues improvement of security, and it needs continuous attention. The ideology of the SANS life cycle is to provide a model of the four basic steps: Identify, Assess, Protect and Monitor. The scope of the lifecycle includes phases of systems investigation, analysis, logical and physical design, implementation, maintenance, and testing. With the completion of the implementation phase, the maintenance and testing phases cycle for the remainder of the project. As a cyber security professional, I will apply the four steps of the SANS life cycle to identify, assess, protect and monitor the systems that I am working with continuously.

Reference:

*Security Lifecycle - Managing the Threat | SANS Institute*. (n.d.). Www.sans.org. https://www.sans.org/white-papers/592/