Learning Outcome 5: Monitor security system

Learning Activities

The following are the performance criteria:

- Performance of the security systems is evaluated
- Reports on security system are generated
- Security systems are updated or overhauled based on the security system report

Trainees to demonstrate knowledge in relation to:

- Define monitoring criteria
- Evaluation of system security performance based on defined criteria
- Updating and overhauling of security systems
- Generate monitoring report

Content

Given the ubiquitous, unavoidable nature of security risks, quick response time is essential to maintaining system security and automated, continuous security monitoring is the key to quick threat detection and response. **Monitoring criteria** should be for hackers and malware, to disgruntled or careless employees, to outdated or otherwise vulnerable devices and operating systems, to mobile and public cloud computing, to third-party service providers.

The evaluation criteria developed include the following objectives:

- **Measurement:** Provides a metric for assessing comparative levels of trust between different computer systems.
- **Guidance:** Identifies standard security requirements that vendors must build into systems to achieve a given trust level.
- **Acquisition:** Provides customers a standard for specifying acquisition requirements and identifying systems that meet those requirements.
- **Security policy:** The rules and procedures by which a trusted system operates.
- **Discretionary access control (DAC):** Owners of objects are able to assign permissions to other subjects.
- **Mandatory access control (MAC):** Permissions to objects are managed centrally by an administrator.
- **Object reuse:** Protects confidentiality of objects that are reassigned after initial use. For example, a deleted file still exists on storage media; only the file allocation table (FAT) and first character of the file have been modified. Thus, residual data may be restored, which describes the problem of data remanence. Object-reuse requirements define procedures for actually erasing the data.
- **Labels:** Sensitivity labels are required in MAC-based systems.
- **Assurance:** Guarantees that a security policy is correctly implemented.
- **System integrity:** Hardware and firmware operate properly and are tested to verify proper operation.
- **Updating and overhauling of Security systems:** When a company needs new data security practices, an external viewpoint can prove invaluable. Remember, a data security auditor has experience helping many different kinds of companies find what

they need to change, and that experience can prove invaluable in creating the *right* kind of overhaul plan. Third party intervention provided broader view of the problem at hand for an organization.

Read: Planning security overhauling: https://www.infiniwiz.com/planning-a-securityoverhaul-here-are-key-tips-on-how-to-start/

Self-Assessment

i. Define monitoring criteria?

ii. Explain evaluation of system security?

iii. What is overhauling of security?

iv. ________ identifies standard security requirements that vendors must build into systems to achieve a given trust level.

   a) System integrity
   b) Assurance
   c) Guidance
   d) Acquisition

v. ______Hardware and firmware operate properly and are tested to verify proper operation.

   a) System integrity
   b) System architecture
   c) Covert channel analysis

vi. _______ provides a metric for assessing comparative levels of trust between different computer systems.

   a) Guidance
   b) Measurement
   c) Security policy
   d) Monitoring criteria

vii. You are a Network security administrator and your company. Your company has been attacked by hackers, how will you identify what sort of information have been hacked?

viii. You are an ICT manager of a hotel. The General Manager of your hotel called you this afternoon, since he is having difficulty in accessing past customer details. The files are randomly opening and there is gibberish. What are the possibilities that customer data have been hack? What are your suggestion actions?

Tools, Equipment, Supplies and Materials

Network Performance Monitor, Nmap, Computer

References

- https://www.dummies.com/programming/certification/evaluation-criteria-systemssecurity-controls/
- https://www.infiniwiz.com/planning-a-security-overhaul-here-are-key-tips-on-how-tostart/
- https://pdfs.semanticscholar.org/45a2/775770d870b8675fb1301919224c9bcb7361.pdf
- Cyber Security, authored by John G. Voeller published by Wiley 2014