LOWPREP

LOWPREP

Handling Computer Security Incidents

CYBER SECURITY CHALLENGE

INTER IIT TECH MEET MADRAS

Introduction

A cybersecurity audit is a comprehensive and systematic evaluation of an organization's information systems, policies, and practices to proactively identify vulnerabilities, threats and associated mitigation options to address potential security risks before malicious actors can exploit them. Regular assessments allow organizations to adapt to changing threats, technologies, and business processes.

Problem Statement - 1

Approach to improving cyber security audit processes and outcomes of audits.

Deliverables

- Design (not develop) an application/ tool to enhance the quality of Audits.
- The solution should have a multifaceted approach focusing on enriching the process of Audit for all the stakeholders i.e. Auditor, Auditee, Regulator etc.

Problem Statement - 2

Approach for reducing vulnerabilities in products, software and Applications.

Deliverables

- Developing a security baseline to safeguard different dimensions of application.
- Focus should be on a proactive approach to building applications with a focus on preventing security vulnerabilities and minimizing the risk of exploitation.

Problem Statement - 3

Approach for application development that leads to applications having features to detect, report and respond to attempts of attacks.

Deliverables

- Suggest the elements/techniques that can be incorporated into the development process that can detect, report, and respond effectively to various forms of cyber threats.
- The suggested elements/techniques should be provided along with the action plan to implement the same.

Evaluation Criteria

Submission Deadline - **12th December**

- Relevance - 5
- Clarity of presentation - 20
- Implementability - 20
- The extent of the objective being fulfilled - 20
- Depth of work and research - 20
- Clarity of illustrations - 5
- Originality - 10