Inter IIT

PROBLEM STATEMENT 1

Approach for improving Cyber Security Audit processes and outcomes of Audit

KEY FEATURES

- Blockchain backed dashboard
- AI driven continuous monitoring
- Natural language processing (NLP) for automation in documentation review
- End-to-end Encryption in data transfer
- Database-driven response plan
- AI powered learning

AUDITING PROCESS STEPS :

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

IDENTIFY:

- Understanding the organization’s assets (e.g., data, hardware, software, systems, facilities, services, people), suppliers, and related cybersecurity risks enables an organization to prioritize its efforts consistent with its risk management strategy and the mission needs

- **Blockchain-Backed Dashboard**: Establish a central dashboard for real-time communication, document exchange, and tracking audit progress, enhancing transparency and efficiency for all stakeholders.

PROTECT:

- Once assets and risks are identified and prioritized, the ***PROTECT*** function secures assets to reduce the likelihood and impact of cybersecurity incidents while enhancing opportunities. Key outcomes include identity management, access control, data and platform security, and ensuring the resilience of technology infrastructure.

- **Secure Data Handling & Encryption**: Implement end-to-end encryption (E2EE) to ensure all data exchanged during the audit process is secure and confidential.

PROTECT:

- **Continuous Monitoring for Compliance**: Leverage AI-driven continuous monitoring tools to ensure that ongoing compliance is maintained. This keeps the organization protected from evolving risks throughout the audit lifecycle.

- **Automated Document Review:** Deploy Natural Language Processing (NLP) tools to securely review policies, past audit reports, and other documents to identify potential compliance gaps or risks early on.

DETECT:

- Timely detection and analysis of anomalies, indicators of compromise, and other potential threats, helping identify cybersecurity attacks and incidents. This supports effective incident response and recovery efforts.

- As the audit progresses, **AI-driven monitoring systems** provide real-time insights, ensuring that auditors and stakeholders are constantly updated.

- **Behavioral Analytics & AI-Enhanced Detection:** Use AI and behavioral analytics to detect patterns or anomalies in the data, identifying potential risks such as insider threats, compliance violations, or fraud.

RECOVER:

- Assets and operations affected by a cybersecurity incident are restored. RECOVER supports the timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable appropriate communication during recovery efforts.

POST RECOVERY:

- **AI-Powered Learning**: The system continuously learns from completed audits, updating risk models and audit workflows based on historical data, regulatory changes, and stakeholder feedback.

By focusing on enhancing the audit experience for all stakeholders, this application aims to improve audit outcomes, increase compliance, and strengthen the overall security posture of organizations. The multifaceted approach ensures that auditors, auditees, and regulators can collaborate effectively while addressing the challenges faced in modern auditing

THANK YOU