SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING-IOT Including CS&BCT

COURSE NAME : 19SB402 NETWORKING AND CYBERSECURITY

II YEAR / IV SEMESTER

Unit V- **CYBER ANALYSIS**

Topic :Critical security components

- When conducting cyber analysis, several critical security components need to be considered to ensure effective analysis and protection against cyber threats.

- Here are some key security components:

Threat Intelligence

- Stay up-to-date with the latest threat intelligence, including information on known vulnerabilities, attack techniques, and emerging threats.

- This helps in understanding the current threat landscape and anticipating potential risks.

Incident Response

- Have a well-defined incident response plan in place to handle security incidents promptly and effectively.

- This includes procedures for detection, containment, eradication, and recovery from security breaches or cyber attacks.

Network Security

- Implement robust network security measures, including firewalls, intrusion detection and prevention systems (IDPS), network segmentation, and secure configuration of network devices.

- Regularly monitor network traffic and analyze logs to identify any suspicious activities.

Endpoint Protection

- Employ comprehensive endpoint protection solutions, such as antivirus software, host-based intrusion detection systems (HIDS), and endpoint detection and response (EDR) tools.

- Continuously update and patch endpoints to protect against known vulnerabilities.

Threat Hunting

- Conduct proactive threat hunting activities to actively search for signs of compromise or suspicious activities within the network.

- This involves analyzing logs, network traffic, and endpoint data to identify potential threats that may have evaded traditional security measures.

Security Information and Event Management (SIEM)

- Utilize SIEM solutions to collect, correlate, and analyze security events and logs from various sources within the network.
- This helps in detecting and responding to security incidents more effectively.

Vulnerability Management

- Implement a robust vulnerability management program to regularly scan systems and applications for known vulnerabilities.
- Prioritize and remediate identified vulnerabilities to reduce the attack surface.

Data Protection

- Implement strong data protection measures, including encryption, access controls, and data loss prevention (DLP) solutions.
- Regularly backup critical data and test data restoration processes to ensure data integrity and availability.

User Awareness and Training

- Conduct regular security awareness training programs for employees to educate them about common cyber threats, phishing attacks, social engineering techniques, and best practices for secure computing.

Continuous Monitoring and Auditing

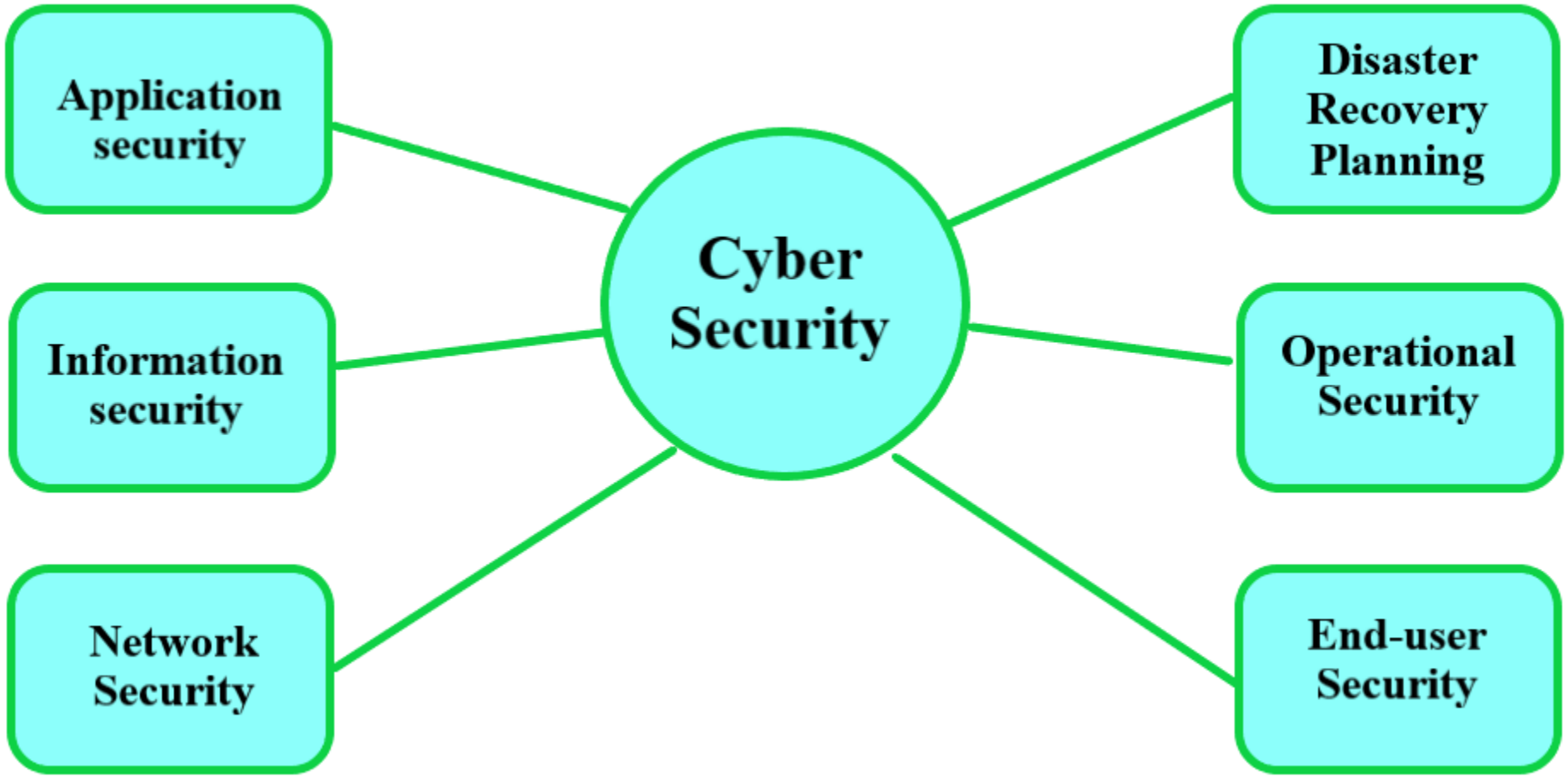
- Implement continuous monitoring and auditing processes to detect any deviations from the expected security posture.
- Monitor systems, logs, and user activities to identify potential security incidents or policy violations.

Regular Patching and Updates

- Maintain a robust patch management process to promptly apply security patches and updates to operating systems, applications, and firmware.
- This helps address known vulnerabilities and protect against attacks.

Collaboration and Information Sharing

- Foster collaboration and information sharing with other organizations, industry groups, and security communities.
- Sharing threat intelligence and best practices helps in staying ahead of evolving cyber threats.


Application security
Information security
Network Security
Cyber Security
Disaster Recovery Planning
Operational Security
End-user Security

Any Query????

Thank you……