S.No	Problem Statement ID	Problem Statement Name	Domain
17	CT-CS - 04	Endpoint Security Management	Corporate Sec

Description:

Endpoint Security Management is a system designed to protect all devices (called endpoints) that connect to a corporate network, such as laptops, desktops, mobile phones, and servers. These devices can be entry points for cyber threats like malware, phishing, or unauthorized access.

The system monitors, protects, and responds to potential threats on these devices, ensuring the corporate network and sensitive data remain secure. It plays a critical role in safeguarding remote workers, preventing data breaches, and complying with corporate security standards.

Objectives:

1. **Protect Endpoints from Cyber Threats:**
   - Shield devices from malware, ransomware, phishing attacks, and unauthorized access.
2. **Monitor Endpoint Activity:**
   - Track activity on all devices in real-time to detect unusual or suspicious behavior.
3. **Centralized Management:**
   - Allow IT administrators to manage security for all devices from a single platform.
4. **Enable Remote Threat Response:**
   - Quickly isolate and secure compromised devices, even in remote locations.
5. **Ensure Compliance:**
   - Meet corporate and regulatory security standards to avoid penalties and ensure data protection.

Expectations:

1. **Comprehensive Security:**
   - A robust system that protects all endpoints, including corporate and employee-owned devices (BYOD).
2. **Proactive Threat Detection:**
   - Detect and mitigate threats before they can cause harm.
3. **Seamless Integration:**
   - Work seamlessly with other corporate security systems like firewalls, antivirus, and intrusion detection systems.
4. **User-Friendly Management:**
   - Provide IT teams with easy-to-use tools for monitoring and managing endpoint security.

Expected Results:

1. **Enhanced Corporate Security:**
   - Strong protection for devices ensures the corporate network remains safe.
2. **Reduced Data Breach Risks:**
   - Quick detection and response prevent unauthorized access and data theft.
3. **Increased Employee Productivity:**
   - Secure endpoints allow employees to work safely without fear of cyber threats.
4. **Cost Savings:**
   - Preventing cyber incidents saves the organization from potential financial losses and reputational damage.