CYBER SECURITY

PROBLEM STATEMENTS

1. Self-Healing Cybersecurity Systems

Problem Statement

Traditional cybersecurity systems rely heavily on manual intervention, making them slow to respond to emerging threats. A self-healing system is needed to automatically detect vulnerabilities and mitigate attacks in real time.

Core Challenge

- Detect vulnerabilities and threats autonomously
- Predict potential attacks using AI/ML
- Apply real-time mitigation without human intervention
- Continuously adapt to new attack techniques
- Maintain system stability and trust

2. AI-Driven Security Operations Center (SOC) Enhancement

Problem Statement

Modern SOC teams are overwhelmed by massive volumes of security data, leading to delayed responses and missed threats. AI-driven tools are required to enhance SOC efficiency and accuracy.

Core Challenge

- Automate threat detection and incident response
- Reduce false positives and alert fatigue
- Prioritize high-risk security incidents
- Integrate with existing SOC tools and workflows

- Maintain transparency and analyst control

3. Enhanced Security for Cloud-Native Applications

Problem Statement

Cloud-native applications built using microservices, containers, and serverless architectures introduce new security challenges. Traditional security models fail to provide adequate protection.

Core Challenge

- Secure microservices and containerized workloads
- Protect dynamically changing runtime environments
- Maintain visibility across distributed components
- Enforce consistent security policies
- Preserve scalability and performance

4. Dynamic Access Control Systems

Problem Statement

Static access control systems cannot adapt to changing user behavior and risk levels. A dynamic, intelligent access control system is required to improve security without affecting usability.

Core Challenge

- Analyze user behavior and context in real time
- Dynamically adjust access permissions
- Detect anomalous or risky access patterns
- Enforce least-privilege access

- Balance security and user experience

5. Cybersecurity for Remote Work Environments

Problem Statement

The rise of remote work has expanded the attack surface, exposing organizations to new security risks. A dedicated security solution is required to protect remote users and systems.

Core Challenge

- Secure remote endpoints and personal devices
- Protect data and communication channels
- Enforce consistent security policies remotely
- Detect and prevent unauthorized access
- Maintain productivity and usability

6. Risk-Based Vulnerability Management

Problem Statement

Organizations face thousands of vulnerabilities but lack the ability to prioritize them effectively. A risk-based vulnerability management system is needed to focus on the most critical threats.

Core Challenge

- Assess vulnerability risk based on context and impact
- Prioritize vulnerabilities intelligently
- Optimize remediation under limited resources
- Integrate with existing vulnerability tools

- Support informed security decision-making

7. Integration of Security in DevSecOps Pipelines

Problem Statement

Fast-paced DevOps workflows often overlook security checks. Security must be seamlessly integrated into CI/CD pipelines without slowing development.

Core Challenge

- Embed automated security checks in CI/CD
- Provide early feedback during development
- Detect vulnerabilities in code and dependencies
- Minimize impact on deployment speed
- Support continuous security enforcement

8. AI-Enhanced Cloud Threat Detection & Mitigation System

Problem Statement

Cloud environments generate complex activity patterns that traditional security tools fail to analyze effectively. An AI-powered system is needed to detect and mitigate advanced cloud threats.

Core Challenge

- Analyze large-scale cloud activity data
- Detect sophisticated and evolving threats
- Trigger automated mitigation actions
- Minimize false positives

- Ensure service availability and resilience

9. AI-Based Cloud Access Control with Behavioral Analytics

Problem Statement

Credential-based access control is insufficient to protect cloud services from misuse and account compromise. An AI-driven behavioral access control system is required.

Core Challenge

- Monitor user behavior continuously
- Detect abnormal or malicious access patterns
- Dynamically adjust cloud permissions
- Prevent account misuse and compromise
- Avoid disruption to legitimate users

10. AI-Driven Ransomware Detection and Automated Response

Problem Statement

Ransomware attacks are becoming faster and more sophisticated, often encrypting critical systems before human intervention is possible. Traditional signature-based defenses fail to detect novel ransomware behaviors. An AI-driven system is required to detect ransomware activity early and trigger automated containment actions.

Core Challenge

- Monitor system or file behavior in real time
- Detect ransomware patterns such as rapid encryption or abnormal file access
- Identify both known and unknown ransomware variants
- Automatically isolate infected systems or processes
- Minimize false positives while ensuring rapid response