# DOMAIN 2: Cyber Security & Blockchain

### PS-2.1: Advanced AI-Based Phishing and Social Engineering Detection Platform

### Problem Description

Phishing and social-engineering attacks have evolved into highly targeted, context-aware threats such as BEC and impersonation scams. Traditional filters fail to detect these sophisticated attacks in real time.

### Objectives

- Detect phishing, BEC, and impersonation attacks
- Analyze email content, URLs, metadata, and user behavior
- Provide explainable alerts to end users

### Constraints

- High false-positive sensitivity
- Evolving attack patterns
- Real-time detection requirements

### Expected Deliverables

- AI-based phishing detection system
- Risk scoring and attack classification module
- Explainable alert interface

## PS-2.2: Intelligent Web Application Firewall with Adaptive Learning

### Problem Description

Traditional WAFs rely on static rules and fail against zero-day and evolving web attacks.

### Objectives

- Detect known and unknown web attacks
- Reduce false positives using adaptive learning
- Visualize real-time attacks

### Constraints

- High traffic throughput
- Low latency enforcement
- Encrypted traffic handling

### Expected Deliverables

- Adaptive WAF prototype
- Attack detection dashboard
- Security logs and reports

---

## PS-2.3: Autonomous Network Reconnaissance and Risk Scoring System

### Problem Description

Organizations lack real-time visibility into assets, vulnerabilities, and attack paths.

### Objectives

- Automatically discover network assets
- Identify vulnerabilities and attack paths
- Generate risk scores

### Constraints

- Partial network visibility
- Dynamic IP and asset changes
- Accuracy of CVE mapping

### Expected Deliverables

- Network reconnaissance engine
- Risk heatmaps and reports
- Visualization dashboard

---

## PS-2.4: Adaptive Password Security and Breach-Aware Policy Engine

### Problem Description

Static password policies do not account for breach data or user risk profiles.

### Objectives

- Adapt password policies dynamically
- Detect reused or breached credentials
- Improve authentication security

### Constraints

- User experience vs. security trade-off
- Privacy concerns
- Real-time breach intelligence integration

### Expected Deliverables

- Adaptive password policy engine
- Admin management dashboard
- Evaluation report

---

## PS-2.5: Automated Malware Behavior Analysis and Detection Framework

### Problem Description

Signature-based malware detection fails against polymorphic and zero-day malware.

### Objectives

- Analyze malware behavior dynamically
- Classify malware types
- Generate indicators of compromise

### Constraints

- Safe sandbox isolation
- Resource-intensive analysis
- Evasion techniques

### Expected Deliverables

- Malware sandbox system
- Behavior visualization dashboard
- Malware analysis reports

---

# PS-2.6: Zero-Trust Security Framework for IoT Environments

### Problem Description

IoT devices lack strong authentication and secure communication mechanisms.

### Objectives

- Implement zero-trust communication
- Secure device identity lifecycle
- Detect compromised devices

### Constraints

- Resource-constrained devices
- Lightweight cryptography requirements
- Scalability challenges

### Expected Deliverables

- Zero-trust IoT prototype
- Device trust scoring system
- Attack simulation results

---

# PS-2.7: Blockchain-Based Self-Sovereign Digital Identity System

### Problem Description

Centralized identity systems expose users to privacy and identity theft risks.

### Objectives

- Enable user-controlled digital identities
- Support verifiable credentials
- Ensure privacy-preserving authentication

### Constraints

- Blockchain scalability
- Key recovery challenges
- Regulatory compliance

### Expected Deliverables

- SSI wallet and verifier portal
- Smart contract-based identity system
- Use-case demonstrations

---

## PS-2.8: Dark Web Threat Intelligence and Early Warning System

### Problem Description

Cyber threats often emerge on dark web forums and marketplaces before attacks occur.

### Objectives

- Monitor dark web sources (simulated/legal)
- Detect emerging threats
- Generate early warnings

### Constraints

- Ethical and legal limitations
- Noisy and multilingual data
- False threat signals

### Expected Deliverables

- Threat intelligence dashboard
- Alerting and reporting system
- Trend analysis reports

# PS-2.9: Real-Time Credit Card Fraud Detection with Explainable AI

### Problem Description

Financial fraud detection requires real-time processing with regulatory transparency.

### Objectives

- Detect fraudulent transactions in real time
- Provide explainable decisions
- Handle concept drift

### Constraints

- Low-latency requirements
- Imbalanced datasets
- Privacy regulations

### Expected Deliverables

- Fraud detection engine
- Explainability dashboard
- Performance evaluation report

# PS-2.10: AI-Driven Automated Incident Response and SOAR Platform

### Problem Description

Manual incident response is slow and inconsistent across security teams.

### Objectives

- Automate incident detection and response
- Generate adaptive response playbooks
- Improve response time and consistency

## Constraints

- Tool integration complexity
- False-positive incident alerts
- Compliance reporting requirements

## Expected Deliverables

- SOAR platform prototype
- Incident simulation results
- Executive and technical reports