Group №5

Pitrix

Software development plan

Use Case №1

1. **Introduction and Scope**

Pitrix is a company which is going to be the manufacturer of advanced vehicle tracking and navigation systems for professional motor racing teams. The company aims to optimize vehicle performance, reduce lap times, and enhance overall racing experience through the creation of a mobile application which will provide real-time navigation data, vehicle telemetry and analytics. The end goal is to allow professional motor racing teams to gain a competitive edge to increase their chances of winning.

2. **Objective**

To develop a secure software solution that provides accurate navigation and telemetry data for vehicle tracking, while minimizing cyber risks.

3. **Roles and Responsibilities**

**IT Security Team**: Responsible for implementing cybersecurity controls, including multi-factor authentication, encryption, intrusion detection, and security training.

**HR Manager**: Hiring new employees, managing employee relations, handling training and development, and ensuring workplace policies are followed.

**Data Science Team**: a group of professionals who use data analysis, machine learning, and statistical methods to extract insights and make data-driven decisions.

**Network Security Team**: Manages network infrastructure and its security, redundancy, and failover mechanisms.

**Legal & Compliance Team**: Ensures the software adheres to relevant data protection regulations (e.g., GDPR, CCPA).

**Software Development Team**: Develops secure code, updates mobile applications, and collaborates with the IT Security Team on vulnerability management.

4. **Requirements and Specifications**

Functional Requirements:

* + Implement secure user authentication (multi-factor).
  + Enable real-time tracking with high data accuracy.
  + Provide mobile access with secure communication protocols.

Non-Functional Requirements:

* + Ensure high availability and reliability of network connections.
  + Comply with privacy regulations and policies.

Technical Requirements:

* + Use end-to-end encryption for data transmission.
  + Enable secure coding practices for mobile applications.

5. **Development Methodology**

Agile Methodology:

* Due to the project’s need for continuous updates and frequent security enhancements, Agile is chosen as the development methodology. Sprint reviews will be conducted to ensure timely responses to security requirements and risk management actions.

6. **Quality Assurance (QA) and Testing**

Testing Approach:

* + Security testing to detect vulnerabilities in mobile apps and data transmission.
  + Model validation tests to ensure data accuracy.
  + Regular penetration testing and security audits.

KPIs:

* + Number of security incidents detected and mitigated.
  + Compliance rate with data protection regulations.
  + Model accuracy rate for real-time navigation data.

7. **Deployment and Release Plan**

* Deployment Strategy: Cloud deployment with high availability and redundancy.
* Release Management: Version control for phased releases, ensuring each version is tested for security and compliance.
* Rollback Plan: Establish a rollback strategy to revert to a previous stable version if issues arise.

8. **Maintenance and Support Plan**

* Ongoing Security Updates: Regular patches for security vulnerabilities, especially for mobile applications.
* Employee Training: Periodic refresher training on cybersecurity for relevant team members.
* Compliance Checks: Quarterly audits and regular updates to privacy policies as laws evolve.

9. **Tools for securing software development**

* **OWASP ZAP** and **Burp Suite** - Essential for penetration testing of the mobile app and web interfaces, identifying vulnerabilities that could impact real-time data accessibility.
* **Snyk** - Scans open-source dependencies for known vulnerabilities, ensuring secure third-party libraries in the application.
* **SonarQube** - Analyses code quality and detects security vulnerabilities in the mobile app and backend.
* **ELK Stack (Elasticsearch, Logstash, Kibana)** - Manages logs and helps identify suspicious activity in telemetry data, navigation data, and personal information access.
* **Prometheus** and **Grafana** - Monitors system health, performance metrics, and real-time data transmission to ensure uninterrupted service during races.
* **Tenable Nessus** - Vulnerability scanner for network and system security, particularly useful for securing the data center and communication networks.
* **Cloudflare** or **Akamai** WAF - Protects against DDoS attacks and malicious traffic that could disrupt data transmission and telemetry analysis.
* **Aqua Security** and **Docker Bench for Security** - Ensures security of any containerized components, such as the Data Center’s data processing units.