Group № 05

Jakh, Dmitriy, Alex, Asad

University Of Roehampton

Course: Cyber Security

SECURE SOFTWARE DEVELOPMENT

Portfolio № 1

**Use Case №1**

Company Name: LuminaX

Company Specialisation: Start-up based on AI solutions

Cyber risk appetite: Very Low (LuminaX prioritizes minimizing potential risks over potential rewards)

**Use Case №2**

Company Name: Pitrix

Company Specialisation: Advanced vehicle tracking and navigation systems for professional motor racing teams.

Cyber risk appetite: High Risk

“This risk treatment plan is designed to protect Pitrix NavTrack’s critical assets and data while allowing flexibility for innovation in line with the company’s high cyber risk appetite. By implementing these targeted measures, Pitrix can better manage risks and improve resilience against cyber threats” – **Jakh’s speech.**

This comprehensive risk treatment plan addresses the key vulnerabilities identified in the threat model while considering Pitrix's **high cyber risk appetite** and current security posture. The plan focuses on both technical controls and human factors, with special attention to the areas highlighted in red in this threat model diagram.

**Risk Treatment Plan for Pitrix (NavTrack) Project**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № | Risk | Description | Impact | Likelyhood | Risk Owner | Timeline | Treatment Plan |
| 1 | Data Breach | Unauthorized access to  sensitive user data. | High | Medium | IT Security Team | Continuous | Multi-factor authentication, end-to-encryption,  access controls. |
| 2 | Low Employee Awareness | Low awareness leading  to increased vulnerability to cyber threats. | High | High | HR Manager & IT Security Manager | Start   Immediately / On a regular basis | Develop and implement comprehensive cyber  security training programs, engage employees in  policy development. |
| 3 | Model Inaccuracy | Inaccurate real-time navigation and  telemetry data. | High | Medium | Data Science Team | Monthly | Regularly update and retrain models with new data, implement validation processes, conduct thorough testing. |
| 4 | Incoming Unfiltered Traffic | from Vehicle Devices (Malware/Ransomware) | High | High | IT Security Team | Regularly | Intrusion detection, antivirus, employee cybersecurity training. |
| 5 | Network   Issues | Interruptions in data  transmission due to  network failures. | Medium | Medium | Network Security Team | Ongoing | Utilize reliable cellular networks (4G/5G) or satellite communication, implement redundancy and  failover mechanisms. |
| 6 | Compliance | Non-compliance   with data protection  regulations. | High | Low | Legal & Compliance Team | Quarterly | Ensure adherence to GDPR, CCPA, and other relevant regulations through regular audits and updates to privacy policies. |
| 7 | Trust Boundary Compromise | Violation of trust  boundary leading to  security breaches. | High | Medium | IT Security Team | Continuous | Implement strong input validation, authentication,  authorization, and encryption measures. |
| 8 | Mobile  Application  Insecurity | Vulnerabilities in mobile applications leading to  potential data breaches and attacks. | High | Medium | Software Development  Team & IT Security Team | Regularly | Follow secure coding practices, conduct regular security audits, use mobile security testing tools, keep the app and its components updated. |