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. |

**Risk Treatment Plan for LuminaX 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 | Implement multi-factor authentication (MFA),  AES-256-GCM encryption, and strict access controls for sensitive data. |
| 2 | Low Employee Awareness | Low awareness among employees, increasing vulnerability to phishing and data mishandling. | High | High | HR Manager & IT Security Team | Start Immediately/Regular | Conduct regular training on secure data handling, phishing awareness, and enforce strong passwords with MFA. |
| 3 | Tampering with Data in Transit | Potential compromise of data integrity through unauthorized alterations between components. | High | Medium | IT Security Team | Ongoing | Use HTTPS/TLS for all data in transit, AES-256-GCM for encryption, and validate message integrity using cryptographic signatures. |
| 4 | DoS Attack on API Gateway | Attackers may overwhelm the API Gateway, causing service disruption and unavailability. | High | Medium | IT Security Team | Regular Monitoring | Apply rate limiting, IP-based throttling, automated request filtering, and deploy a Web Application Firewall (WAF) for malicious traffic patterns. |
| 5 | Insider Threat | Unauthorized data access or modifications by employees with elevated access privileges. | High | Medium | IT & HR Security Managers | Continuous | Implement role-based access control (RBAC), enforce logging, and regularly audit user actions for unusual access patterns. |
| 6 | Privilege Escalation | Unauthorized users could exploit vulnerabilities to access sensitive backend services. | High | Medium | Software Development Team & IT Team | Ongoing | Enforce RBAC, validate permissions on each request, and ensure consistent application of security policies across backend services. |
| 7 | Data Leakage via Monitoring Logs | Sensitive information in logs could be exposed if not properly secured or sanitized. | High | Medium | IT Security & Monitoring | Ongoing | Restrict log access, encrypt sensitive information in logs, sanitize logs to remove PII, and limit access to authorized personnel. |
| 8 | Unencrypted Data in Database | Sensitive data stored in the database could be accessed if encryption isn’t enforced. | High | Medium | Database Administrator | Continuous | Encrypt all sensitive data at rest using AES-256, enforce access controls, and conduct regular reviews of database encryption and access logs. |
| 9 | Model Tampering | Attackers may alter AI models to produce biased or inaccurate results. | High | Medium | AI Development Team | Regular Audits | Apply checksums or cryptographic hashes to AI model files and restrict write access to model files. Perform regular integrity checks. |
| 10 | User Identity Spoofing | Attackers might impersonate users by exploiting authentication mechanisms. | High | Medium | IT Security Team | Continuous | Implement MFA and OAuth 2.0 with JWT tokens for identity validation. Regularly audit authentication logs for suspicious activity. |
| 11 | Repudiation of User Actions | Users may deny actions if proper logging and accountability mechanisms are absent. | Medium | Medium | IT Security & Compliance | Continuous | Implement detailed logging with unique session identifiers and secure logs within Monitoring & Logging Services. |
| 12 | Phishing and Accidental Data Breaches | Employees may fall for phishing or mishandle sensitive information. | High | High | HR & IT Security Team | Quarterly Training | Conduct regular cybersecurity awareness training, enforce secure password practices, and utilize anti-phishing tools. |
| 13 | Resource Exhaustion via Model Processing | Excessive requests to AI Engine could cause resource exhaustion, impacting system performance. | Medium | Medium | IT Operations | Ongoing | Apply request throttling and quotas on model processing, utilize load balancing, and monitor resource usage to prevent overload. |
| 14 | Tampering with Data in Database | An attacker could modify or corrupt data in the database, compromising data integrity. | High | Medium | Database Administrator | Continuous | Implement strict access controls, use data integrity checks (e.g., hashing), and regularly monitor the database for unauthorized changes. |
| 15 | Cloud Misconfigura-tion | Misconfigured cloud settings could expose sensitive services and data to the internet. | High | Medium | Cloud Security Team | Regular Audits | Conduct regular cloud configuration reviews, enforce access controls, and use automated tools to detect and remediate misconfigurations. |
| 16 | Token Expiry and Revocation Issues | Expired or unrevoked tokens could allow unauthorized access beyond intended sessions. | Medium | Medium | IT Security & Development | Ongoing | Implement strict token expiration policies, enforce token revocation on logout, and regularly audit session management mechanisms. |
| 17 | Vulnerable APIs | Public-facing APIs may have vulnerabilities that can be exploited by attackers. | High | Medium | IT Security Team | Regular Security Scans | Conduct regular security testing on APIs, implement input validation, and use API gateways with rate limiting and WAF protections. |
| 18 | Unrestricted Database Access | Insufficient access controls on database lead to unauthorized access or data breaches. | High | Medium | Database Administrator | Ongoing | Enforce least privilege access, implement RBAC, and perform periodic access reviews and audits to detect unusual access patterns. |

**Security Requirements (Pitrix)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | Title: | Asset | Threat | Narrative | Work required | Verification criteria: |
| 1 | Cybersecurity Awareness and Training for All Team Members | Employee Knowledge and Cybersecurity Practices | Users may fall for phishing or social engineering attacks due to low awareness. | Employees with low cybersecurity awareness are more susceptible to social engineering attacks, potentially giving attackers unauthorized access to systems or sensitive data. This includes falling for phishing emails, mishandling sensitive data, or not recognizing malicious actions. | 1) Develop and implement a mandatory cybersecurity training program covering phishing, secure data handling, and secure access practices.  2) Conduct quarterly phishing simulations and analyze results to identify improvement areas.  3) Set up regular refreshers and knowledge checks to reinforce key concepts. | 1) Track completion rates and post-training test scores to gauge awareness levels.  2) Evaluate phishing simulation outcomes (e.g., success rates of identifying phishing emails).  3) Assess incident reports related to phishing to determine if awareness has improved. |
| 2 | Accurate Real-Time Navigation and Telemetry Data | AI Model for Real-Time Navigation and Telemetry | Manipulation of the AI model or input data affecting accuracy. | Inaccurate telemetry or navigation data could mislead drivers or team members, leading to poor decision-making during races. This can occur if data is manipulated during transmission or if the model fails to process real-time inputs accurately. | 1) Integrate input validation processes for telemetry data to ensure it is consistent and unaltered.  2) Implement periodic model retraining with validated data to reduce inaccuracies and model drift.  3) Apply cryptographic checksums on model files to detect and prevent tampering. | 1) Perform end-to-end tests simulating real-time data to confirm the model provides accurate telemetry information.  2) Conduct regression testing after model updates to ensure accuracy across typical data scenarios.  3) Regularly validate checksum values for model files to detect unauthorized modifications. |
| 3 | Unauthorized Access to Sensitive User Data | Sensitive User Data | Unauthorized access to or disclosure of sensitive data. | Unauthorized access could expose sensitive information like driver details, telemetry, and navigation data, which should only be accessible to authorized team members. This may result from weak authentication, insufficient access controls, or compromised credentials. | 1) Implement multi-factor authentication (MFA) for all users with access to sensitive data.  2) Use role-based access control (RBAC) to ensure that only authorized users can access specific data.  3) Regularly audit user access logs to detect and respond to suspicious access patterns. | 1) Conduct penetration testing focusing on access control to ensure only authorized users can reach sensitive data.  2) Perform regular audits of access logs to check for unauthorized access attempts.  3) Test MFA implementation by simulating unauthorized access attempts with and without MFA to confirm its effectiveness. |

**Security Requirements (LuminaX)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | Title: | Asset | Threat | Narrative | Work required | Verification criteria: |
| 1 | Secure APIs for Safe Data Exchange | API Endpoints for LumiMind’s Data Access and Processing | APIs can be targeted to gain unauthorized access, manipulate data, or disrupt services. | Vulnerable APIs could expose LumiMind’s data to unauthorized users, allow manipulation of requests, or enable denial-of-service attacks that degrade system performance. This risk is heightened when APIs are accessible over public networks. | 1) Implement input validation and output encoding on all API endpoints to prevent injection and manipulation attacks.  2) Use API gateway features like rate limiting, IP filtering, and a Web Application Firewall (WAF) to prevent DoS attacks and mitigate traffic spikes.  3) Enforce strong authentication (OAuth 2.0) and authorization (RBAC) for API access, especially for sensitive functions. | 1) Conduct regular API security testing (using tools like OWASP ZAP, Burp Suite) to check for vulnerabilities.  2) Perform penetration testing on API endpoints to simulate real-world attacks and confirm defences.  3) Monitor API access logs for unusual activity, such as repeated failed access attempts or traffic spikes. |
| 2 | Cybersecurity Training and Awareness Program | Employee Knowledge on Cybersecurity Best Practices | Employees may unintentionally compromise security by falling for phishing or social engineering attacks due to low awareness. | Employees lacking cybersecurity awareness are more prone to social engineering attacks, which could result in unauthorized access to LuminaX’s systems and data. Such attacks could lead to compromised credentials, data leakage, and even financial or reputational loss. | 1) Develop a cybersecurity training program covering key topics such as phishing awareness, data handling, password management, and reporting suspicious activity.  2) Conduct monthly refresher courses and quarterly phishing simulations to reinforce training.  3) Include knowledge checks and assessments to measure training effectiveness and adjust content as needed. | 1) Track completion rates and performance on post-training assessments.  2) Measure the success rate in identifying phishing simulations and conduct follow-up training as necessary.  3) Review security incident reports for any social engineering-related incidents to assess training impact. |
| 3 | Prevent Unauthorized Data Access and Modification by Internal Users | Sensitive Internal Data and Systems | Insiders with privileged access may misuse their rights to view, modify, or exfiltrate sensitive data. | Insider threats involve employees or contractors with privileged access who may intentionally or unintentionally misuse their access to perform unauthorized actions, risking data privacy and system integrity. This can lead to data leaks, data manipulation, or reputational damage. | 1) Implement role-based access control (RBAC) to restrict access to sensitive data based on job requirements.  2) Use monitoring tools (e.g., ELK Stack, Splunk) to log and analyze access and activity for anomalous patterns.  3) Enforce periodic reviews of access permissions and remove access for users who no longer require it. | 1) Conduct regular audits of access logs to detect suspicious behaviour, such as unauthorized data access or out-of-hours activity.  2) Review RBAC implementations to ensure that access levels align with job functions and that sensitive data is appropriately restricted.  3) Simulate insider threat scenarios and verify that monitoring and logging tools detect and respond to suspicious activities effectively. |