SSD Project threat modeling

Current Risk Summary report

Wed Apr 23 2025 09:20:52 GMT+0000 (Coordinated Universal Time)

Project description: *No description*

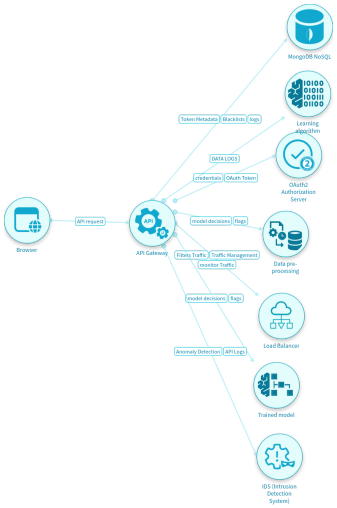
Filtered by: *No filters*

Unique ID: ssd-project-threat-modeling-1745397657250

Owner: Ahmed Amjad

Workflow state: Draft

Tags: *No tags*



Content menu

Current risk summary

Components

Accepted Risks

Current Risks

- API Gateway
- Browser
- Data pre-processing
- IDS (Intrusion Detection System)
- Learning algorithm
- Load Balancer
- MongoDB NoSQL
- OAuth2 Authorization Server
- Trained model

Current Risk summary

Inherent risk description: The Inherent Risk before countermeasures were applied.
- **Risk Rating:** 69% High

The Current Risk description (the risk we are at now): The Current Risk is based on the current implementation status of the countermeasures and test results.
- **Risk Rating:** 8% Low

Projected Risk description: The Projected Risk is the level of risk that would be reached should the required countermeasures be implemented.
- **Risk Rating:** 8% Low

Components

- API Gateway

  Model questionnaire information:
  - **Credit Card Data: How is it handled by this component?** Stored
  - **Customer Data: How is it handled by this component?** Stored
  - **Does this component handle personally identifiable information from citizens of the European Union?** No
  - **Does this component have to be CCPA-compliant?** Yes
  - **Does this component have to be CCPA-compliant?** No
  - **Is API traffic continuously monitored and analyzed?** Yes, it is implemented
  - **Is a token translation service implemented between distributed gateways?** Yes, it is implemented
  - **Is access token generation enabled for client requests?** Yes, it is implemented
  - **Is the API gateway integrated with an identity management application?** Yes, it is implemented
  - **Is the system integrated with an identity provider (IdP)?** Yes, it is implemented
  - **Personally Identifiable Information: How is it handled by this component?** Stored
  - **Protected Health Information: How is it handled by this component?** Stored
  - **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Know
  - **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Correct
  - **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Limit
  - **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Delete

- Browser

  Model questionnaire information:
  - **Credit Card Data: How is it handled by this component?** Stored
  - **Customer Data: How is it handled by this component?** Stored
  - **Does this component handle personally identifiable information from citizens of the European Union?** No
  - **Does this component have to be CCPA-compliant?** Yes
  - **Is encrypted communication currently in place and regularly updated on all client machines?** Yes, it is implemented
  - **Is strict certificate validation currently active and updated on all client machines?** Yes, it is implemented
  - **Is the URL filtering mechanism currently active and updated on all client machines?** Yes, it is implemented
  - **Is the activation and regular update of built-in browser security filters currently in place?** Yes, it is implemented
  - **Is the anti-phishing protection system currently active and continuously updated?** Not sure
  - **Is the automatic browser update configuration currently in place?** Yes, it is implemented
  - **Is the client-side script blocker currently implemented and updated regularly on all client machines?** Yes, it is implemented
  - **Is the extension whitelisting policy in place and regularly updated?** Yes, it is implemented
  - **Is the secure management of browser extensions currently active and updated on client machines?** Yes, it is implemented
  - **Is the security hardening measures update and configuration applied on all client machines?** Yes, it is implemented
  - **Personally Identifiable Information: How is it handled by this component?** Stored
  - **Protected Health Information: How is it handled by this component?** Stored
  - **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Know
  - **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Correct
  - **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Delete

- Data pre-processing

  Model questionnaire information:
  - **Are measures to maintain data quality, integrity, and representativeness during data pre-processing currently implemented?** Yes, it is implemented
  - **Are the identification and mitigating measures for bias in data currently implemented?** Yes, it is implemented
  - **Credit Card Data: How is it handled by this component?** Stored
  - **Customer Data: How is it handled by this component?** Stored
  - **Does the system monitor the data pipeline for drift?** Yes, it is implemented
  - **Does this component handle personally identifiable information from citizens of the European Union?** No
  - **Does this component have to be CCPA-compliant?** Yes
  - **Personally Identifiable Information: How is it handled by this component?** Stored
  - **Protected Health Information: How is it handled by this component?** Stored
  - **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Know
  - **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Correct
  - **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Delete

- IDS (Intrusion Detection System)

  Model questionnaire information:
  - **Credit Card Data: How is it handled by this component?** Stored
  - **Customer Data: How is it handled by this component?** Stored
  - **Does this component handle personally identifiable information from citizens of the European Union?** No

- **Does this component have to be CCPA-compliant?** Yes
- **Is the IDS configured to send alerts to a central location?** Yes, it is implemented
- **Is the Intrusion Detection System regularly updated?** Yes, it is implemented
- **Is there an out-of-band management channel for IDS in place?** Yes, it is implemented
- **Personally Identifiable Information: How is it handled by this component?** Stored
- **Protected Health Information: How is it handled by this component?** Stored
- **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Know
- **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Correct
- **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Delete

- Learning algorithm

  Model questionnaire information:
  - **Credit Card Data: How is it handled by this component?** Stored
  - **Customer Data: How is it handled by this component?** Stored
  - **Does the system properly protect/restrict the model's parameters and hyperparameters?** Yes, it is implemented
  - **Does this component handle personally identifiable information from citizens of the European Union?** No
  - **Does this component have to be CCPA-compliant?** Yes
  - **Have you carefully considered the model choice in your system?** Yes, it is implemented
  - **Have you considered robust learning and defenses against poisoning attacks in your ML/AI system?** Yes, it is implemented
  - **Have you reviewed the representational robustness of your modeling?** Yes, it is implemented
  - **Personally Identifiable Information: How is it handled by this component?** Stored
  - **Protected Health Information: How is it handled by this component?** Stored
  - **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Know
  - **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Correct
  - **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Delete

- Load Balancer

  Model questionnaire information:
  - **Are regular audits of Load Balancer configurations conducted to adhere to security best practices?** Yes, it is implemented
  - **Credit Card Data: How is it handled by this component?** Stored
  - **Customer Data: How is it handled by this component?** Stored
  - **Does this component handle personally identifiable information from citizens of the European Union?** No
  - **Does this component have to be CCPA-compliant?** Yes
  - **Is DDoS protection service already integrated with your load balancer?** Yes, it is implemented
  - **Is secure session handling through the load balancer currently implemented in your system?** Yes, it is implemented
  - **Is the TLS encryption enforced for all traffic through the Load Balancer?** Yes, it is implemented
  - **Is the monitoring system for tracking Load Balancer resource usage currently in place?** Yes, it is implemented
  - **Personally Identifiable Information: How is it handled by this component?** Stored
  - **Protected Health Information: How is it handled by this component?** Stored
  - **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Know
  - **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Correct
  - **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Delete

- MongoDB NoSQL

  Model questionnaire information:
  - **Credit Card Data: How is it handled by this component?** Stored
  - **Customer Data: How is it handled by this component?** Stored
  - **Does this component handle personally identifiable information from citizens of the European Union?** No
  - **Does this component have to be CCPA-compliant?** Yes
  - **Does this component have to be CCPA-compliant?** No
  - **Is MongoDB protected by strong authentication and role-based access control implemented?** Yes, it is implemented
  - **Is strict role management with audit logs in place for MongoDB?** Yes, it is implemented
  - **Is the MongoDB configuration hardened and unnecessary features like HTTP interface or MongoDB shell disabled?** Yes, it is implemented
  - **Is the MongoDB data encrypted both during transit and when stored?** Yes, it is implemented
  - **Is the encryption and access limitation for MongoDB backups currently in place?** Not sure
  - **Is the encryption and access limitation for MongoDB backups currently in place?** Yes, it is implemented
  - **Is the input sanitization and use of parameterized queries for MongoDB implemented in your current project?** Yes, it is implemented
  - **Is the rate limiting and connection pooling strategy for MongoDB currently in place?** Yes, it is implemented
  - **Is the restrictive access and regular auditing process for MongoDB currently in place?** Not sure
  - **Personally Identifiable Information: How is it handled by this component?** Stored
  - **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Know
  - **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Correct
  - **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Delete

- OAuth2 Authorization Server

  Model questionnaire information:
  - **Credit Card Data: How is it handled by this component?** Stored
  - **Customer Data: How is it handled by this component?** Stored
  - **Does this component handle personally identifiable information from citizens of the European Union?** No
  - **Does this component have to be CCPA-compliant?** Yes
  - **Is HTTPS and modern TLS enforced for secure communication in your system?** Yes, it is implemented
  - **Is monitoring and logging of critical events currently set up in your OAuth2 Authorization Server?** Yes, it is implemented
  - **Is the PKCE enforcement for public clients currently implemented in the security of OAuth2 Authorization Code Flow?** Yes, it is implemented
  - **Is the high-entropy client secret protection and brute-force attack safeguard implemented in the OAuth2 Authorization Server?** Yes, it is implemented
  - **Is the principle of least privilege enforced in scope management for OAuth2 Authorization Server configurations?** Yes, it is implemented
  - **Is the process of using short-lived access tokens with refresh token rotation and token binding currently implemented?** Yes, it is implemented

- **Is the token validation as per OAuth2 Authorization Server regulations currently in place?** Yes, it is implemented
- **Is the validation of redirect URIs against a strict whitelist currently set up in the OAuth2 authorization process?** Yes, it is implemented
- **Personally Identifiable Information: How is it handled by this component?** Stored
- **Protected Health Information: How is it handled by this component?** Stored
- **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Know
- **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Correct
- **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Delete

- Trained model

  Model questionnaire information:
  - **Credit Card Data: How is it handled by this component?** Stored
  - **Customer Data: How is it handled by this component?** Stored
  - **Do you keep detailed documentation about the content used for training/fine-tuning models?** Yes, it is implemented
  - **Does the modeling/application use privacy-preserving techniques and strategies?** Not sure
  - **Does the modeling/application use privacy-preserving techniques and strategies?** Yes, it is implemented
  - **Does this component handle personally identifiable information from citizens of the European Union?** No
  - **Does this component have to be CCPA-compliant?** Yes
  - **Is there a logging mechanism that records and securely manages all interactions with the model?** Yes, it is implemented
  - **Is there a process in place for choosing the most appropriate algorithm for your use case/application?** Yes, it is implemented
  - **Is there a process in place for maintaining detailed technical documentation about the model building and its usage?** Yes, it is implemented
  - **Is there measures in place for protecting data and IP (Intellectual Property) when sharing or shipping models?** Yes, it is implemented
  - **Is there measures in place to identify and avoid potentially trojanized models?** Yes, it is implemented
  - **Personally Identifiable Information: How is it handled by this component?** Stored
  - **Protected Health Information: How is it handled by this component?** Stored
  - **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Know
  - **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Correct
  - **Which of the following CCPA rights do you want this software component to be compliant with?** Right to Delete

Accepted Risks

No data

Current Risks

Component: API Gateway

Use case: Elevation of Privilege

CRT1. Threat name: Authentication bypass

- **Inherent risk:** High
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR1. Countermeasure name:** The API gateway should have a connector to an artifact that can generate an access token for the client request
  - **Status:** IMPLEMENTED
- **CR2. Countermeasure name:** Connectors should be provided for integrating with identity providers (IdPs)
  - **Status:** IMPLEMENTED
- **CR3. Countermeasure name:** Integrate the API gateway with an identity management application
  - **Status:** IMPLEMENTED
- **CR4. Countermeasure name:** Distributed gateway deployments should have a token translation (exchange) service between gateways
  - **Status:** IMPLEMENTED

Use case: Repudiation

CRT2. Threat name: Exploitation of insufficient logging and monitoring

- **Inherent risk:** High
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR5. Countermeasure name:** Securely channel all traffic information to a monitoring and/or analytics application
  - **Status:** IMPLEMENTED

Component: Browser

Use case: Spoofing

CRT3. Threat name: Attackers conduct phishing attacks through deceptive websites

- **Inherent risk:** Critical
- **Current risk:** Medium
- **Projected risk:** Medium
- **State:** Partly-Mitigated
- **CR6. Countermeasure name:** Deploy anti-phishing protection
  - **Status:** RECOMMENDED
- **CR7. Countermeasure name:** Activate URL filtering mechanisms
  - **Status:** IMPLEMENTED

CRT4. Threat name: Attackers intercept browser communications through man-in-the-middle (MitM) attacks

- **Inherent risk:** Critical
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR8. Countermeasure name:** Utilize encrypted communication tools
  - **Status:** IMPLEMENTED
- **CR9. Countermeasure name:** Enforce strict certificate validation
  - **Status:** IMPLEMENTED

Use case: Tampering

CRT5. Threat name: Attackers distribute malware through compromised browser extensions

- **Inherent risk:** Critical
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR10. Countermeasure name:** Implement extension whitelisting policies
  - **Status:** IMPLEMENTED
- **CR11. Countermeasure name:** Manage browser extensions securely
  - **Status:** IMPLEMENTED

Use case: Elevation of Privilege

CRT6. Threat name: Attackers exploit browser vulnerabilities to execute malicious code

- **Inherent risk:** Critical
- **Current risk:** Very Low

- **Projected risk:** Very Low
- **State:** Mitigate
- **CR12. Countermeasure name:** Apply security hardening measures
  - **Status:** IMPLEMENTED
- **CR13. Countermeasure name:** Configure automatic browser updates
  - **Status:** IMPLEMENTED

Use case: Information Disclosure

CRT7. Threat name: Attackers inject malicious scripts via cross-site scripting (XSS)
- **Inherent risk:** High
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR14. Countermeasure name:** Activate built-in browser security filters
  - **Status:** IMPLEMENTED
- **CR15. Countermeasure name:** Implement client-side script blockers
  - **Status:** IMPLEMENTED

Use case: CCPA Requirements

CRT8. Threat name: Client application does not offer any mechanism to let the user exercise their Right to Correct
- **Inherent risk:** Medium
- **Current risk:** Medium
- **Projected risk:** Medium
- **State:** Expose
- **CR16. Countermeasure name:** Develop an online form that users can fill out to submit their request
  - **Status:** RECOMMENDED

CRT9. Threat name: Client application does not offer any mechanism to let the user exercise their Right to Delete
- **Inherent risk:** Medium
- **Current risk:** Medium
- **Projected risk:** Medium
- **State:** Expose
- **CR17. Countermeasure name:** Develop an online form that users can fill out to submit their request
  - **Status:** RECOMMENDED

CRT10. Threat name: Client application does not offer any mechanism to let the user exercise their Right to Know
- **Inherent risk:** Medium
- **Current risk:** Medium
- **Projected risk:** Medium
- **State:** Expose
- **CR18. Countermeasure name:** Inform the user about which data will be collected
  - **Status:** RECOMMENDED
- **CR19. Countermeasure name:** Develop an online form that users can fill out to submit their request
  - **Status:** RECOMMENDED

Component: Data pre-processing

Use case: Tampering

CRT11. Threat name: Changing data distribution and properties will affect the performance of the future model
- **Inherent risk:** High
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR20. Countermeasure name:** Monitor for data drift, especially for new data and future online models
  - **Status:** IMPLEMENTED

CRT12. Threat name: Data encoding, normalization, filtering, feature selection, and annotation, may all introduce biases or affect the predictive and generalization qualities of the model
- **Inherent risk:** Critical
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR21. Countermeasure name:** Maintain data quality and integrity during data pre-processing
  - **Status:** IMPLEMENTED
- **CR22. Countermeasure name:** Identify potential bias in the data
  - **Status:** IMPLEMENTED

Component: IDS (Intrusion Detection System)

Use case: Elevation of Privilege

CRT13. Threat name: Accessing functionality not properly constrained by ACLs
- **Inherent risk:** High
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR23. Countermeasure name:** Use an out-of-band management connection for IDS
  - **Status:** IMPLEMENTED

Use case: Information Disclosure

CRT14. Threat name: Attackers gain access to the system and are not detected
- **Inherent risk:** High
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR24. Countermeasure name:** Configure the IDS to send alerts to a central location
  - **Status:** IMPLEMENTED

CRT15. Threat name: Attackers gain access to unauthorised data by exploiting vulnerabilities in the service
- **Inherent risk:** High
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR25. Countermeasure name:** Update IDS regularly
  - **Status:** IMPLEMENTED

Component: Learning algorithm

Use case: Information Disclosure

CRT16. Threat name: Adversaries may exploit algorithmic leakage or data representation issues to extract data or attack the model
- **Inherent risk:** Critical
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR26. Countermeasure name:** Carefully consider the model choice
  - **Status:** IMPLEMENTED
- **CR27. Countermeasure name:** Review the representation robustness
  - **Status:** IMPLEMENTED

Use case: Tampering

CRT17. Threat name: An adversary may be able to manipulate an online learning system
- **Inherent risk:** Critical
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR28. Countermeasure name:** Consider robust learning and defenses against poisoning attacks for online models
  - **Status:** IMPLEMENTED

CRT18. Threat name: An adversary may be able to manipulate model parameters or hyperparameters
- **Inherent risk:** Critical
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR29. Countermeasure name:** Perform sensitivity analyses and secure/restrict the set of model parameters and hyperparameters
  - **Status:** IMPLEMENTED

Component: Load Balancer

Use case: Spoofing

CRT19. Threat name: Attackers can hijack sessions by gaining unauthorized access to a user's active session
- **Inherent risk:** Critical
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR30. Countermeasure name:** Implement secure session handling to prevent session hijacking through the Load Balancer
  - **Status:** IMPLEMENTED

Use case: Information Disclosure

CRT20. Threat name: Attackers can intercept traffic through Load Balancer vulnerabilities
- **Inherent risk:** High
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR31. Countermeasure name:** Enforce TLS encryption for all traffic through the Load Balancer to prevent interception
  - **Status:** IMPLEMENTED

CRT21. Threat name: Attackers exploit security misconfigurations
- **Inherent risk:** Critical
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR32. Countermeasure name:** Conduct regular audits of Load Balancer configurations to ensure adherence to security best practices
  - **Status:** IMPLEMENTED

Use case: Denial of Service

CRT22. Threat name: Attackers use DDoS attacks to overwhelm the Load Balancer
- **Inherent risk:** High
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR33. Countermeasure name:** Implement DDoS protection services to safeguard Load Balancers against attacks
  - **Status:** IMPLEMENTED

CRT23. Threat name: Attackers use resource exhaustion tactics to overwhelm the Load Balancer
- **Inherent risk:** High
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR34. Countermeasure name:** Implement monitoring tools to track Load Balancer resource usage and prevent exhaustion
  - **Status:** IMPLEMENTED

Component: MongoDB NoSQL

Use case: Information Disclosure

CRT24. Threat name: Attackers can access unsecured backups
- **Inherent risk:** High
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR35. Countermeasure name:** Encrypt backups and limit backup access
  - **Status:** IMPLEMENTED

CRT25. Threat name: Attackers can intercept unencrypted data
- **Inherent risk:** Critical
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR36. Countermeasure name:** Enable encryption for data in transit and at rest
  - **Status:** IMPLEMENTED

Use case: Elevation of Privilege

CRT26. Threat name: Attackers can exploit default configurations
- **Inherent risk:** Critical
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR37. Countermeasure name:** Harden configuration and disable unused features
  - **Status:** IMPLEMENTED

CRT27. Threat name: Attackers can gain unauthorized access
- **Inherent risk:** High
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR38. Countermeasure name:** Implement strong authentication and RBAC
  - **Status:** IMPLEMENTED

CRT28. Threat name: Malicious users can escalate privileges
- **Inherent risk:** Medium

- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR39. Countermeasure name:** Enforce strict role management and audit logs
  - **Status:** IMPLEMENTED

Use case: Denial of Service

CRT29. Threat name: Attackers can overload the database with DoS attacks
- **Inherent risk:** High
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR40. Countermeasure name:** Use rate limiting and connection pooling
  - **Status:** IMPLEMENTED

Use case: Tampering

CRT30. Threat name: Attackers take advantage of injection vulnerabilities
- **Inherent risk:** High
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR41. Countermeasure name:** Sanitize inputs and use parameterized queries
  - **Status:** IMPLEMENTED

CRT31. Threat name: Insider threats can compromise data integrity
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR42. Countermeasure name:** Restrict access and conduct regular audits
  - **Status:** RECOMMENDED

Component: OAuth2 Authorization Server

Use case: Repudiation

CRT32. Threat name: Attackers bypass detection due to lack of logging and monitoring
- **Inherent risk:** Medium
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR43. Countermeasure name:** Log key actions and monitor for unusual activity
  - **Status:** IMPLEMENTED

Use case: Tampering

CRT33. Threat name: Attackers exploit insufficient token validation
- **Inherent risk:** High
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR44. Countermeasure name:** Validate tokens by verifying signature, claims, and expiration
  - **Status:** IMPLEMENTED

Use case: Information Disclosure

CRT34. Threat name: Attackers exploit open redirects
- **Inherent risk:** Medium
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR45. Countermeasure name:** Validate redirect URIs against a strict whitelist
  - **Status:** IMPLEMENTED

CRT35. Threat name: Attackers intercept tokens over unencrypted communication channels
- **Inherent risk:** High
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR46. Countermeasure name:** Enforce HTTPS and modern TLS for secure communication

- **Status:** IMPLEMENTED

Use case: Elevation of Privilege

CRT36. Threat name: Attackers exploit weak access policies
- **Inherent risk:** Critical
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR47. Countermeasure name:** Enforce principle of least privilege in scope management
  - **Status:** IMPLEMENTED

Use case: Spoofing

CRT37. Threat name: Attackers inject malicious authorization codes
- **Inherent risk:** High
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR48. Countermeasure name:** Bind authorization codes to specific clients and enforce PKCE for public clients
  - **Status:** IMPLEMENTED

CRT38. Threat name: Attackers perform brute force on client credentials
- **Inherent risk:** Critical
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR49. Countermeasure name:** Mandate high-entropy client secrets and protect against brute-force attacks
  - **Status:** IMPLEMENTED

CRT39. Threat name: Attackers perform token replay attacks
- **Inherent risk:** High
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR50. Countermeasure name:** Use short-lived access tokens with refresh token rotation and validate token binding
  - **Status:** IMPLEMENTED

Use case: CCPA Requirements

CRT40. Threat name: Server application does not offer any mechanism to let the user exercise their Right to Correct
- **Inherent risk:** Medium
- **Current risk:** Medium
- **Projected risk:** Medium
- **State:** Expose
- **CR51. Countermeasure name:** Develop a dashboard or reporting tool to track and monitor requests
  - **Status:** RECOMMENDED

CRT41. Threat name: Server application does not offer any mechanism to let the user exercise their Right to Delete
- **Inherent risk:** Medium
- **Current risk:** Medium
- **Projected risk:** Medium
- **State:** Expose
- **CR52. Countermeasure name:** Develop a dashboard or reporting tool to track and monitor requests
  - **Status:** RECOMMENDED

CRT42. Threat name: Server application does not offer any mechanism to let the user exercise their Right to Know
- **Inherent risk:** Medium
- **Current risk:** Medium
- **Projected risk:** Medium
- **State:** Expose
- **CR53. Countermeasure name:** Develop a dashboard or reporting tool to track and monitor requests
  - **Status:** RECOMMENDED

Component: Trained model

Use case: Information Disclosure

CRT43. Threat name: An adversary may be able to reveal sensitive information available in the model or the data used to build it
- **Inherent risk:** Critical
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate

- **CR54. Countermeasure name:** Carefully consider the model choice
  - **Status:** IMPLEMENTED
- **CR55. Countermeasure name:** Keep a history of queries to the model
  - **Status:** IMPLEMENTED
- **CR56. Countermeasure name:** Consider privacy-preserving techniques and strategies
  - **Status:** IMPLEMENTED

Use case: Tampering

CRT44. Threat name: An adversary may take advantage of model sharing and/or transfer

- **Inherent risk:** Critical
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR57. Countermeasure name:** Consider possible trojanized versions when acquiring shared models
  - **Status:** IMPLEMENTED
- **CR58. Countermeasure name:** Protect data and IP (Intellectual Property) when sharing or shipping models
  - **Status:** IMPLEMENTED

Use case: Repudiation

CRT45. Threat name: Lack of sufficient details about the model (algorithm), its architecture, or its data

- **Inherent risk:** High
- **Current risk:** Very Low
- **Projected risk:** Very Low
- **State:** Mitigate
- **CR59. Countermeasure name:** Keep sufficient details and documentation about the content used for training/fine-tuning models
  - **Status:** IMPLEMENTED
- **CR60. Countermeasure name:** Maintain sufficient technical documentation about the model building and usage
  - **Status:** IMPLEMENTED

End of Current Risk Report