# Comprehensive Threat Model Evaluation Report (Combined)

## Executive Summary & Comparative Analysis

### 1. Threats & Mitigations Maturity Ranking (Across Models)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Rank** | **Model Name** | **Threats & Mitigations Score** | **Maturity** | **Reasoning** |
| 1 | payments-processing-platform-anthropic-claude-sonnet-4-5-20250929 | 93 | 🏆 Excellent | Broad, balanced STRIDE coverage across actors, processes, and boundary-crossing flows; precise, actionable mitigations (e.g., PKCE, mTLS, token binding, signed webhooks) and strong contextual accuracy. |
| 2 | payments-processing-platform-openai-gpt-5 | 87 | 🌟 Good | Strong coverage and realism; high-fidelity flow-level threats and merchant/Stripe alignment; minor overemphasis in places but consistently practical mitigations. |
| 3 | payments-processing-platform-anthropic-claude-opus-4-1-20250805 | 85 | 🌟 Good | Solid, balanced threats across key flows and components with sound mitigations; a few gaps in completeness and proportionality compared to the top two. |
| 4 | payments-processing-platform-xai-grok-4-latest | 67 | ✅ Adequate | Extensive enumeration across categories; mitigations are often generic and occasionally misapplied, but overall coverage enables useful risk discussions. |
| 5 | payments-processing-platform-novita-deepseek-deepseek-v3.1-terminus | 62 | ✅ Adequate | Reasonable breadth with mostly plausible threats; mitigations are concise but often high-level; some categories underdeveloped. |
| 6 | payments-processing-platform-xai-grok-4-fast-reasoning-latest | 54 | ⚙️ Fair | Many threats listed, but inconsistencies and misprioritization; mitigations tend to be generic; realism varies. |
| 7 | payments-processing-platform-novita-qwenqwen3-coder-480b-a35b-instruct | 51 | ⚙️ Fair | Heavy skew toward “unencrypted flow” findings; coverage is broad but contextual accuracy and mitigations are frequently off-target. |
| 8 | payments-processing-platform-gemini-gemini-2.5-pro, | 35 | ⚠️ Poor | Sparse threat set; multiple key flows lack threats; mitigations are minimal and not comprehensive for an internet-exposed payment system. |
| 9 | payments-processing-platform-ollama-qwen330b | 15 | ❌ Inadequate | Threat coverage is largely absent across critical flows and components; not decision-useful for risk treatment. |

### 2. Overall Model Maturity

#### 2.1 Evaluation Summary

All models share a materially common DFD: Customer actor; Customer Client in a “Customer/Internet” zone; a Merchant Web Server; Stripe API and Stripe Payment Service within “Stripe/Web”; and labeled cross-boundary flows (steps 1–11). Trust boundaries and process roles are consistently clear and intuitive. Missing data stores and limited decomposition constrain completeness, yet the sequence of flows is logical. As a shared foundation for security analysis, the DFD is readable and sufficient, though adding data stores, authentication/identity components, and explicit data classifications would improve depth.

#### 2.2 Scoring Table

|  |  |  |  |
| --- | --- | --- | --- |
| **Dimension** | **Weight** | **Score** | **Reasoning** |
| Clarity and Readability | 25% | 80 | Clear trust zones and labeled steps (1–11); processes are named consistently; visual mental model is straightforward. |
| Completeness and Coverage | 30% | 75 | Core components and flows are present, but persistent data stores and identity/secret stores are not modeled; limited decomposition. |
| Accuracy and Logical Consistency | 25% | 78 | Flow sequence and trust crossings are coherent; the overall lifecycle reflects realistic PaymentIntent orchestration. |
| Usability for Security Analysis | 20% | 76 | Adequate for attack-surface reasoning; would benefit from explicit data classifications, protocol/encryption correctness, and datastore inclusion. |

**Overall Model Maturity Total Score (0–100):** 77 **Overall Model Maturity:** 🌟 Good

### 3. Individual Model Evaluations (Threats & Mitigations Only)

### ##################################################################################

### payments-processing-platform-anthropic-claude-opus-4-1-20250805

### This section provides the dedicated Threats & Mitigations analysis for this specific model.

### ##################################################################################

#### Threat Landscape Snapshot "(Per Model)"

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STRIDE Category** | **High** | **Medium** | **Low** | **Observations** |
| Spoofing | 3 | 1 | 0 | Customer identity, OAuth flows, Stripe API impersonation covered. |
| Tampering | 5 | 1 | 0 | Strong focus on PaymentIntent manipulation, response forgery, and internal service tampering. |
| Repudiation | 0 | 2 | 0 | Transaction logs and auditability gaps identified. |
| Information Disclosure | 4 | 2 | 0 | Card data, PaymentIntent status leakage, API key exposure addressed. |
| Denial of Service | 1 | 2 | 0 | Client resource exhaustion and API rate limit bypass considered. |
| Elevation of Privilege | 2 | 0 | 0 | Merchant server compromise and payment service authorization bypass noted. |

Methodology balance is solid, with emphasis on tampering and disclosure relevant to payments; repudiation is present but limited.

#### Mitigation Quality & Alignment "(Per Model)"

#### payments-processing-platform-anthropic-claude-opus-4-1-20250805

|  |  |  |
| --- | --- | --- |
| **Control Area** | **Adequacy** | **Observations** |
| Relevance & Specificity | ✅ | PKCE, HSTS, CSP, mTLS, HMAC signing, idempotency keys well targeted to flow threats. |
| Practicality | ✅ | Feasible within modern payment stacks; aligns with Stripe and PCI practices. |
| Completeness & Coverage | ✅ | Most critical flows/components addressed; minor opportunities around datastore/secret handling. |
| Effectiveness | ✅ | Controls map to root causes (token theft, in-transit tampering, spoofing). |
| Standards Alignment | ✅ | Good alignment with industry practices for web payments; PCI implications recognized. |
| Traceability & Justification | ✅ | Threat-to-control mapping is explicit across flows. |

**Summary Rating:** ✅ Adequate

#### Gaps, Blind Spots & Prioritized Fixes "(Per Model)"

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Finding** | **Impact** | **Effort** | **Recommendation** |
| 1 | Limited non-repudiation depth | Medium | Low | Add digital signature receipts and immutable logs with correlation IDs for all payment lifecycle events. |
| 2 | Secrets lifecycle not modeled | High | Medium | Add threats/controls for API key storage/rotation, CI/CD scanning, and secret managers. |
| 3 | Missing datastore-centric threats | Medium | Low | If any persistence exists (orders/logs), add encryption-at-rest, access control, and tamper-evident logging threats. |

#### Threats & Mitigations Maturity Assessment "(Per Model)"

|  |  |  |  |
| --- | --- | --- | --- |
| **Dimension** | **Weight** | **Score** | **Reasoning** |
| DFD Element Coverage | 30% | 85 | Actors, processes, and key flows are covered; persistent stores not considered. |
| Methodology Coverage & Balance | 30% | 86 | STRIDE categories well represented, with expected emphasis on Tampering/Disclosure. |
| Contextual Accuracy | 20% | 84 | Threats align to payment semantics and trust crossings. |
| Mitigation Validity | 10% | 82 | Controls are largely effective and implementable. |
| Proportionality & Realism | 10% | 84 | Severities and focus areas are broadly appropriate for a card payment flow. |

**Threats & Mitigations Total Score (0–100):** 85 **Threats & Mitigations Maturity:** 🌟 Good

#### Strategic Recommendations "(Per Model)"

#### payments-processing-platform-anthropic-claude-opus-4-1-20250805

* Add explicit threats/controls for merchant secret storage (server-side keys, rotation, detection of leakage).
* Enrich non-repudiation: digitally signed receipts, webhook signature verification, immutable audit stores.
* Model fraud/risk checks (e.g., 3DS/SCA) as mitigations tied to spoofing/tampering of cardholder actions.
* Include datastore threats (order history, logs) with encryption-at-rest and access control.
* Add threat coverage for certificate transparency monitoring and DNSSEC validation in endpoint trust.
* Clarify client vs server responsibilities for validation (never trust client-supplied amounts).
* Extend internal service integrity controls with service identity (SPIFFE/SVID) where applicable.

### ##################################################################################

### payments-processing-platform-anthropic-claude-sonnet-4-5-20250929

### This section provides the dedicated Threats & Mitigations analysis for this specific model.

### ##################################################################################

#### Threat Landscape Snapshot "(Per Model)"

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STRIDE Category** | **High** | **Medium** | **Low** | **Observations** |
| Spoofing | 5 | 1 | 0 | Robust coverage: auth endpoints, merchant/Stripe spoofing, endpoint pinning. |
| Tampering | 7 | 1 | 0 | Deep on PaymentIntent integrity, confirmCardPayment, internal service responses. |
| Repudiation | 0 | 3 | 0 | Receipts, signed logs, and webhook reconciliation recommended. |
| Information Disclosure | 6 | 2 | 0 | Card data, PaymentIntent/token leakage, response minimization addressed. |
| Denial of Service | 2 | 2 | 0 | API saturation, customer client resilience, and service-layer throttling. |
| Elevation of Privilege | 2 | 1 | 0 | Merchant API exploitation, Stripe API keys, client manipulation scenarios. |

Methodology balance is strong, with precise and layered mitigations grounded in realistic payment operations.

#### Mitigation Quality & Alignment "(Per Model)"

#### payments-processing-platform-anthropic-claude-sonnet-4-5-20250929

|  |  |  |
| --- | --- | --- |
| **Control Area** | **Adequacy** | **Observations** |
| Relevance & Specificity | ✅ | Controls are precise (PKCE, token binding, webhook signatures, mTLS, SRI, CSP). |
| Practicality | ✅ | Consistent with payment processor patterns and Stripe best practices. |
| Completeness & Coverage | ✅ | Comprehensive across boundary crossings and critical processes. |
| Effectiveness | ✅ | Addresses root causes (replay, manipulation, spoofing, exposure) with layered defenses. |
| Standards Alignment | ✅ | Aligns with modern web/payments security; PCI-conscious. |
| Traceability & Justification | ✅ | Clear mapping to targeted threats and risk drivers. |

**Summary Rating:** ✅ Adequate

#### Gaps, Blind Spots & Prioritized Fixes "(Per Model)"

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Finding** | **Impact** | **Effort** | **Recommendation** |
| 1 | Persistent stores not modeled | Medium | Low | Add threats/mitigations for any DB/logs (cryptographic integrity, access control). |
| 2 | Fraud/SCA not explicit | Medium | Low | Tie spoofing/payment repudiation to 3DS/SCA and fraud telemetry. |
| 3 | Key management lifecycle not explicit | Medium | Medium | Add rotation, vaulting, and leakage detection to maintain API key hygiene. |

#### Threats & Mitigations Maturity Assessment "(Per Model)"

|  |  |  |  |
| --- | --- | --- | --- |
| **Dimension** | **Weight** | **Score** | **Reasoning** |
| DFD Element Coverage | 30% | 94 | Extensive coverage across actors, processes, and flows; minor datastore gap. |
| Methodology Coverage & Balance | 30% | 94 | STRIDE categories are consistently represented and balanced. |
| Contextual Accuracy | 20% | 92 | Threats tightly match payment context and trust zones. |
| Mitigation Validity | 10% | 90 | Highly actionable and effective mitigations. |
| Proportionality & Realism | 10% | 92 | Prioritization and severity reflect payment industry realities. |

**Threats & Mitigations Total Score (0–100):** 93 **Threats & Mitigations Maturity:** 🏆 Excellent

#### Strategic Recommendations "(Per Model)"

#### payments-processing-platform-anthropic-claude-sonnet-4-5-20250929

* Add datastore threats (orders, logs) and controls (encryption-at-rest, row-level ACLs, tamper-evident logs).
* Include explicit fraud management and SCA steps linked to spoofing/repudiation scenarios.
* Expand secret management coverage (key rotation frequency, detection of leaked keys, CI/CD secret scanning).
* Model response minimization and redaction in logs as persistent controls across components.
* Consider service identity (SPIFFE/SVID) for internal requests to strengthen integrity beyond mTLS.

### ##################################################################################

### payments-processing-platform-gemini-gemini-2.5-pro,

### This section provides the dedicated Threats & Mitigations analysis for this specific model.

### ##################################################################################

#### Threat Landscape Snapshot "(Per Model)"

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STRIDE Category** | **High** | **Medium** | **Low** | **Observations** |
| Spoofing | 0 | 0 | 0 | Not meaningfully covered. |
| Tampering | 1 | 0 | 0 | Limited (PaymentIntent flow); many critical flows lack threats. |
| Repudiation | 0 | 0 | 0 | Absent. |
| Information Disclosure | 1 | 0 | 0 | Minimal coverage versus real exposure. |
| Denial of Service | 1 | 0 | 0 | Single DoS concern; lacks breadth. |
| Elevation of Privilege | 1 | 0 | 0 | One logic-abuse threat; others missing. |

Coverage is sparse; major underrepresentation of realistic boundary-crossing risks.

#### Mitigation Quality & Alignment "(Per Model)"

#### payments-processing-platform-gemini-gemini-2.5-pro,

|  |  |  |
| --- | --- | --- |
| **Control Area** | **Adequacy** | **Observations** |
| Relevance & Specificity | ⚠️ | Some correct ideas (HSTS, TLS), but too few and not tied to all key flows. |
| Practicality | ✅ | Suggested controls are feasible. |
| Completeness & Coverage | ❌ | Significant omissions across most flows and categories. |
| Effectiveness | ⚠️ | Where present, mitigations are reasonable but partial. |
| Standards Alignment | ✅ | General web security alignment; not comprehensive for payments. |
| Traceability & Justification | ⚠️ | Weak mapping; many flows have no threats or controls. |

**Summary Rating:** ⚠️ Partially adequate

#### Gaps, Blind Spots & Prioritized Fixes "(Per Model)"

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Finding** | **Impact** | **Effort** | **Recommendation** |
| 1 | Missing threats on cross-boundary flows | High | Medium | Add STRIDE threats on login, confirmCardPayment, PaymentIntent return/status. |
| 2 | No coverage of spoofing/repudiation | High | Low | Include endpoint spoofing, session fixation, signed receipts/webhooks. |
| 3 | Secrets and key management not addressed | High | Low | Add API key storage/rotation, detection of credential leakage. |

#### Threats & Mitigations Maturity Assessment "(Per Model)"

|  |  |  |  |
| --- | --- | --- | --- |
| **Dimension** | **Weight** | **Score** | **Reasoning** |
| DFD Element Coverage | 30% | 35 | Majority of flows/components lack threats. |
| Methodology Coverage & Balance | 30% | 34 | STRIDE categories underrepresented. |
| Contextual Accuracy | 20% | 40 | Limited items are plausible but too few. |
| Mitigation Validity | 10% | 30 | Minimal and generic. |
| Proportionality & Realism | 10% | 35 | Not scaled to an internet-exposed payment platform. |

**Threats & Mitigations Total Score (0–100):** 35 **Threats & Mitigations Maturity:** ⚠️ Poor

#### Strategic Recommendations "(Per Model)"

#### payments-processing-platform-gemini-gemini-2.5-pro,

* Populate threats for each boundary-crossing flow: OAuth login, order intent, confirmCardPayment, internal attempt/response, and status return.
* Add spoofing controls (certificate pinning, DNSSEC, mTLS, webhook signatures).
* Cover non-repudiation: immutable logs, digital receipts, correlation IDs.
* Include secret management threats/controls; prevent client-side leakage of keys.
* Layer request integrity: HMAC/signatures for PaymentIntent and internal calls.
* Add client-side protections: CSP/SRI, tokenization, hosted payment fields.

### ##################################################################################

### payments-processing-platform-novita-deepseek-deepseek-v3.1-terminus

### This section provides the dedicated Threats & Mitigations analysis for this specific model.

### ##################################################################################

#### Threat Landscape Snapshot "(Per Model)"

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STRIDE Category** | **High** | **Medium** | **Low** | **Observations** |
| Spoofing | 0 | 1 | 0 | Minimal (customer identity). |
| Tampering | 2 | 0 | 0 | Order intent and PaymentIntent tampering present. |
| Repudiation | 0 | 1 | 0 | Basic coverage for PaymentIntent repudiation. |
| Information Disclosure | 2 | 0 | 0 | Card data and order data risks acknowledged. |
| Denial of Service | 0 | 2 | 0 | Internal payment attempt and merchant server DoS addressed. |
| Elevation of Privilege | 1 | 0 | 0 | Merchant/Stripe privilege escalation captured. |

Balanced but shallow; mitigations are high-level.

#### Mitigation Quality & Alignment "(Per Model)"

#### payments-processing-platform-novita-deepseek-deepseek-v3.1-terminus

|  |  |  |
| --- | --- | --- |
| **Control Area** | **Adequacy** | **Observations** |
| Relevance & Specificity | ⚠️ | Controls are directionally correct but generic. |
| Practicality | ✅ | Suggested controls are feasible to deploy. |
| Completeness & Coverage | ⚠️ | Multiple flows and categories are not fully covered. |
| Effectiveness | ⚠️ | Lacks depth (e.g., signatures, idempotency, webhook verification). |
| Standards Alignment | ✅ | Aligns broadly with web security; payment specifics could be stronger. |
| Traceability & Justification | ⚠️ | Partial mapping; limited per-flow control rationale. |

**Summary Rating:** ⚠️ Partially adequate

#### Gaps, Blind Spots & Prioritized Fixes "(Per Model)"

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Finding** | **Impact** | **Effort** | **Recommendation** |
| 1 | Generic mitigations | Medium | Low | Specify PKCE, webhook signatures, idempotency keys, CSP/SRI. |
| 2 | Sparse spoofing/repudiation | High | Medium | Add endpoint pinning/DNSSEC and signed receipts with immutable audit logs. |
| 3 | Internal service integrity | Medium | Medium | Add mTLS, service identity, and message signing for internal flows. |

#### Threats & Mitigations Maturity Assessment "(Per Model)"

|  |  |  |  |
| --- | --- | --- | --- |
| **Dimension** | **Weight** | **Score** | **Reasoning** |
| DFD Element Coverage | 30% | 64 | Covers key processes/flows; gaps persist. |
| Methodology Coverage & Balance | 30% | 62 | All categories present but shallow. |
| Contextual Accuracy | 20% | 62 | Generally plausible, limited depth. |
| Mitigation Validity | 10% | 60 | High-level; not always addressing root causes. |
| Proportionality & Realism | 10% | 62 | Severity mostly reasonable; more prioritization needed. |

**Threats & Mitigations Total Score (0–100):** 62 **Threats & Mitigations Maturity:** ✅ Adequate

#### Strategic Recommendations "(Per Model)"

#### payments-processing-platform-novita-deepseek-deepseek-v3.1-terminus

* Specify transport integrity (TLS 1.3, mTLS, certificate pinning) on all boundary-crossing flows.
* Introduce message integrity (HMAC/signatures) on PaymentIntent flows; enforce idempotency keys.
* Add signed webhook verification and reconciliation logic for final state confirmation.
* Include client-side hardening (CSP, SRI, hosted payment fields/tokenization).
* Expand non-repudiation via immutable logs and signed receipts.

### ##################################################################################

### payments-processing-platform-novita-qwenqwen3-coder-480b-a35b-instruct

### This section provides the dedicated Threats & Mitigations analysis for this specific model.

### ##################################################################################

#### Threat Landscape Snapshot "(Per Model)"

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STRIDE Category** | **High** | **Medium** | **Low** | **Observations** |
| Spoofing | 1 | 0 | 0 | Limited handling beyond “unencrypted” narratives. |
| Tampering | 1 | 0 | 0 | Minimal coverage; generic controls. |
| Repudiation | 0 | 2 | 0 | Logging suggested; lacks signed proofs. |
| Information Disclosure | 8 | 0 | 0 | Overemphasis on “unencrypted flow” even for internal/API paths. |
| Denial of Service | 0 | 3 | 0 | Several DoS items; not prioritized. |
| Elevation of Privilege | 0 | 1 | 0 | Minimal coverage of authZ threats. |

Heavily skewed to disclosure; accuracy is uneven (e.g., asserting widespread lack of encryption).

#### Mitigation Quality & Alignment "(Per Model)"

#### payments-processing-platform-novita-qwenqwen3-coder-480b-a35b-instruct

|  |  |  |
| --- | --- | --- |
| **Control Area** | **Adequacy** | **Observations** |
| Relevance & Specificity | ⚠️ | Many mitigations assume unencrypted defaults; limited specificity to flow context. |
| Practicality | ✅ | Controls like TLS, logging are practical. |
| Completeness & Coverage | ⚠️ | STRIDE categories unbalanced; key spoofing/tampering areas omitted. |
| Effectiveness | ⚠️ | Controls focus on symptoms (encryption only) rather than root causes (authn/z, integrity). |
| Standards Alignment | ✅ | General web standards referenced; payments-specific practices underused. |
| Traceability & Justification | ⚠️ | Weak linkage of threats to controls; repeated generic statements. |

**Summary Rating:** ⚙️ Partially adequate

#### Gaps, Blind Spots & Prioritized Fixes "(Per Model)"

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Finding** | **Impact** | **Effort** | **Recommendation** |
| 1 | Overfocus on “unencrypted flow” | Medium | Low | Add integrity (signatures), spoofing (pinning/mTLS), and non-repudiation controls. |
| 2 | Missing spoofing threats | High | Medium | Include endpoint spoofing, token theft, key misuse, and webhook forgery risks. |
| 3 | Weak client-side coverage | High | Low | Add CSP/SRI, hosted payment fields, tokenization, anti-XSS for card data entry. |

#### Threats & Mitigations Maturity Assessment "(Per Model)"

|  |  |  |  |
| --- | --- | --- | --- |
| **Dimension** | **Weight** | **Score** | **Reasoning** |
| DFD Element Coverage | 30% | 62 | Many flows addressed, but shallow and uneven. |
| Methodology Coverage & Balance | 30% | 50 | Overweighted to disclosure; spoofing/tampering/repudiation thin. |
| Contextual Accuracy | 20% | 44 | Several assertions about encryption are questionable; missing integrity/spoofing focus. |
| Mitigation Validity | 10% | 42 | Controls under-address root causes. |
| Proportionality & Realism | 10% | 46 | Prioritization misaligned with real payment risks. |

**Threats & Mitigations Total Score (0–100):** 51 **Threats & Mitigations Maturity:** ⚙️ Fair

#### Strategic Recommendations "(Per Model)"

#### payments-processing-platform-novita-qwenqwen3-coder-480b-a35b-instruct

* Add spoofing-focused controls (pinning, DNSSEC, mTLS) and threats on Stripe/merchant endpoints.
* Introduce message signing/HMAC and idempotency for PaymentIntent and internal flows.
* Expand non-repudiation beyond logging (signed receipts, immutable audit trails).
* Strengthen client-side protections and tokenization to keep PAN out of merchant origin.
* Calibrate severities and coverage to payment fraud vectors (replay, confirmation spoofing).

### ##################################################################################

### payments-processing-platform-ollama-qwen330b

### This section provides the dedicated Threats & Mitigations analysis for this specific model.

### ##################################################################################

#### Threat Landscape Snapshot "(Per Model)"

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STRIDE Category** | **High** | **Medium** | **Low** | **Observations** |
| Spoofing | 0 | 0 | 0 | No coverage. |
| Tampering | 0 | 0 | 0 | No coverage. |
| Repudiation | 0 | 0 | 0 | No coverage. |
| Information Disclosure | 1 | 0 | 0 | Single item on internal exposure; insufficient. |
| Denial of Service | 0 | 0 | 0 | No coverage. |
| Elevation of Privilege | 0 | 0 | 0 | No coverage. |

Threat coverage is effectively absent.

#### Mitigation Quality & Alignment "(Per Model)"

#### payments-processing-platform-ollama-qwen330b

|  |  |  |
| --- | --- | --- |
| **Control Area** | **Adequacy** | **Observations** |
| Relevance & Specificity | ❌ | Almost no mitigations provided. |
| Practicality | ⚠️ | N/A in most areas due to absence. |
| Completeness & Coverage | ❌ | Critical flows lack threats/controls entirely. |
| Effectiveness | ❌ | Insufficient basis for evaluation. |
| Standards Alignment | ⚠️ | Not demonstrable from current content. |
| Traceability & Justification | ❌ | Lacks structured threat-to-mitigation mapping. |

**Summary Rating:** ❌ Inadequate

#### Gaps, Blind Spots & Prioritized Fixes "(Per Model)"

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Finding** | **Impact** | **Effort** | **Recommendation** |
| 1 | Near-total absence of threats | High | Medium | Populate threats on all flows and processes using STRIDE. |
| 2 | No mitigations for boundary crossings | High | Medium | Add TLS/mTLS, signatures, PKCE, webhook verification, tokenization, CSP/SRI. |
| 3 | No non-repudiation or secrets coverage | High | Low | Add immutable logs, signed receipts, and secret management controls. |

#### Threats & Mitigations Maturity Assessment "(Per Model)"

|  |  |  |  |
| --- | --- | --- | --- |
| **Dimension** | **Weight** | **Score** | **Reasoning** |
| DFD Element Coverage | 30% | 15 | Almost all elements unaddressed. |
| Methodology Coverage & Balance | 30% | 14 | STRIDE categories largely absent. |
| Contextual Accuracy | 20% | 20 | Single internal disclosure item plausible but insufficient. |
| Mitigation Validity | 10% | 10 | Lacks substantive mitigations. |
| Proportionality & Realism | 10% | 15 | Not commensurate with internet-exposed payments. |

**Threats & Mitigations Total Score (0–100):** 15 **Threats & Mitigations Maturity:** ❌ Inadequate

#### Strategic Recommendations "(Per Model)"

#### payments-processing-platform-ollama-qwen330b

* Build a baseline threat set for each flow (login, order intent, confirmCardPayment, internal attempt/response, status return).
* Add realistic mitigations (PKCE, TLS 1.3/mTLS, CSP/SRI, tokenization, signed webhooks, idempotency keys).
* Include spoofing and tampering scenarios with endpoint pinning and message integrity.
* Address non-repudiation with signed receipts and immutable audit trails.
* Incorporate secret management: vaulting, rotation, and leak detection.

### ##################################################################################

### payments-processing-platform-openai-gpt-5

### This section provides the dedicated Threats & Mitigations analysis for this specific model.

### ##################################################################################

#### Threat Landscape Snapshot "(Per Model)"

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STRIDE Category** | **High** | **Medium** | **Low** | **Observations** |
| Spoofing | 4 | 0 | 0 | Merchant impersonation, client/Stripe endpoint spoofing captured. |
| Tampering | 6 | 2 | 0 | PaymentIntent and internal service tampering well developed. |
| Repudiation | 0 | 2 | 0 | Logging and correlation emphasized. |
| Information Disclosure | 5 | 1 | 0 | Response minimization and token leakage considered. |
| Denial of Service | 0 | 3 | 0 | API saturation and availability controls addressed. |
| Elevation of Privilege | 0 | 1 | 0 | Merchant server/client manipulation threats included. |

Balanced, realistic, and focused on boundary crossings.

#### Mitigation Quality & Alignment "(Per Model)"

#### payments-processing-platform-openai-gpt-5

|  |  |  |
| --- | --- | --- |
| **Control Area** | **Adequacy** | **Observations** |
| Relevance & Specificity | ✅ | Threat-to-control mapping is strong and practical. |
| Practicality | ✅ | Controls mirror industry practices (mTLS, idempotency, webhook signatures). |
| Completeness & Coverage | ✅ | Most critical flows are covered. |
| Effectiveness | ✅ | Layered defenses target root causes effectively. |
| Standards Alignment | ✅ | Well aligned with contemporary payment security measures. |
| Traceability & Justification | ✅ | Clear rationale and mapping throughout. |

**Summary Rating:** ✅ Adequate

#### Gaps, Blind Spots & Prioritized Fixes "(Per Model)"

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Finding** | **Impact** | **Effort** | **Recommendation** |
| 1 | Data stores absent | Medium | Low | Add threats/controls for logs/order persistence (integrity, encryption-at-rest, access control). |
| 2 | Fraud/SCA tie-in | Medium | Low | Incorporate 3DS/SCA linkage to spoofing/repudiation threats. |
| 3 | Key lifecycle management | Medium | Medium | Add secret rotation, leak detection, and environment scoping explicitly. |

#### Threats & Mitigations Maturity Assessment "(Per Model)"

|  |  |  |  |
| --- | --- | --- | --- |
| **Dimension** | **Weight** | **Score** | **Reasoning** |
| DFD Element Coverage | 30% | 88 | Strong flow/process coverage; no persistent stores. |
| Methodology Coverage & Balance | 30% | 88 | Categories well represented without skew. |
| Contextual Accuracy | 20% | 86 | High contextual fidelity to payment operations. |
| Mitigation Validity | 10% | 84 | Practical, high-value controls. |
| Proportionality & Realism | 10% | 86 | Appropriate severity/prioritization. |

**Threats & Mitigations Total Score (0–100):** 87 **Threats & Mitigations Maturity:** 🌟 Good

#### Strategic Recommendations "(Per Model)"

#### payments-processing-platform-openai-gpt-5

* Add datastore-centric threats/controls (tamper-evident logs, encryption-at-rest).
* Include explicit fraud/SCA steps to mitigate spoofing and repudiation.
* Extend secret management: rotation cadence, scoping, detection, and key hygiene in CI/CD.
* Clarify response minimization and redaction guidance for error handling and logs.
* Consider service identity for internal invocation hardening beyond mTLS.

### ##################################################################################

### payments-processing-platform-xai-grok-4-fast-reasoning-latest

### This section provides the dedicated Threats & Mitigations analysis for this specific model.

### ##################################################################################

#### Threat Landscape Snapshot "(Per Model)"

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STRIDE Category** | **High** | **Medium** | **Low** | **Observations** |
| Spoofing | 2 | 0 | 0 | Some login/payment endpoint spoofing; needs expansion. |
| Tampering | 3 | 0 | 0 | Covers PaymentIntent and status tampering. |
| Repudiation | 0 | 1 | 0 | Basic logging noted. |
| Information Disclosure | 2 | 0 | 0 | Limited and generic. |
| Denial of Service | 0 | 2 | 0 | Internal and API DoS included. |
| Elevation of Privilege | 0 | 1 | 0 | Limited handling. |

Coverage is moderate but mitigations are often generic, with some questionable prescriptions.

#### Mitigation Quality & Alignment "(Per Model)"

#### payments-processing-platform-xai-grok-4-fast-reasoning-latest

|  |  |  |
| --- | --- | --- |
| **Control Area** | **Adequacy** | **Observations** |
| Relevance & Specificity | ⚠️ | Sometimes misapplied (e.g., HMAC for login flows); lacks detail. |
| Practicality | ✅ | Generally deployable but underspecified. |
| Completeness & Coverage | ⚠️ | Key spoofing, integrity, and non-repudiation items are thin. |
| Effectiveness | ⚠️ | Controls do not consistently address root causes. |
| Standards Alignment | ⚠️ | Broad alignment, but payments-specific best practices underused. |
| Traceability & Justification | ⚠️ | Threat-to-control linkage is uneven. |

**Summary Rating:** ⚙️ Partially adequate

#### Gaps, Blind Spots & Prioritized Fixes "(Per Model)"

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Finding** | **Impact** | **Effort** | **Recommendation** |
| 1 | Inconsistent control prescriptions | Medium | Low | Replace generic HMAC guidance with PKCE, webhook signatures, and mTLS where appropriate. |
| 2 | Sparse spoofing defenses | High | Medium | Add DNSSEC, pinning, certificate transparency, and strict endpoint allowlisting. |
| 3 | Weak non-repudiation | Medium | Low | Incorporate signed receipts and immutable logs with correlation IDs. |

#### Threats & Mitigations Maturity Assessment "(Per Model)"

|  |  |  |  |
| --- | --- | --- | --- |
| **Dimension** | **Weight** | **Score** | **Reasoning** |
| DFD Element Coverage | 30% | 58 | Moderate; some critical flows underdeveloped. |
| Methodology Coverage & Balance | 30% | 56 | STRIDE categories uneven; spoofing/repudiation light. |
| Contextual Accuracy | 20% | 50 | Mixed accuracy; some control misapplications. |
| Mitigation Validity | 10% | 48 | Generic mitigations; limited root-cause focus. |
| Proportionality & Realism | 10% | 52 | Prioritization needs alignment to payment risks. |

**Threats & Mitigations Total Score (0–100):** 54 **Threats & Mitigations Maturity:** ⚙️ Fair

#### Strategic Recommendations "(Per Model)"

#### payments-processing-platform-xai-grok-4-fast-reasoning-latest

* Replace generic or misapplied mitigations with targeted ones (PKCE, webhook signatures, token binding).
* Extend spoofing defenses: pinning, DNSSEC, certificate transparency monitoring.
* Add message signing and idempotency for PaymentIntent and internal service flows.
* Strengthen non-repudiation with signed receipts and immutable audit trails.
* Add client-side protections: CSP/SRI, hosted fields/tokenization.

### ##################################################################################

### payments-processing-platform-xai-grok-4-latest

### This section provides the dedicated Threats & Mitigations analysis for this specific model.

### ##################################################################################

#### Threat Landscape Snapshot "(Per Model)"

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STRIDE Category** | **High** | **Medium** | **Low** | **Observations** |
| Spoofing | 6 | 0 | 0 | Broadly covered across flows; needs stronger control precision. |
| Tampering | 6 | 0 | 0 | Comprehensive but often generic integrity guidance. |
| Repudiation | 0 | 3 | 0 | Logging acknowledged; signatures not consistently specified. |
| Information Disclosure | 5 | 0 | 0 | Good breadth; limited response minimization guidance. |
| Denial of Service | 0 | 4 | 0 | Internal and API DoS present; prioritization unclear. |
| Elevation of Privilege | 3 | 0 | 0 | Addresses EoP scenarios in client and services. |

Wide coverage but mitigations frequently generic; some inaccuracies (e.g., AES payload suggestions vs. TLS).

#### Mitigation Quality & Alignment "(Per Model)"

#### payments-processing-platform-xai-grok-4-latest

|  |  |  |
| --- | --- | --- |
| **Control Area** | **Adequacy** | **Observations** |
| Relevance & Specificity | ⚠️ | Often generic and sometimes misdirected (payload AES vs TLS). |
| Practicality | ✅ | Deployable but would benefit from precision (mTLS, signatures, idempotency). |
| Completeness & Coverage | ✅ | Good breadth across flows and categories. |
| Effectiveness | ⚠️ | Would be improved by root-cause targeting and signed webhook reconciliation. |
| Standards Alignment | ⚠️ | General web security alignment; payment-specific best practices inconsistently applied. |
| Traceability & Justification | ⚠️ | Mapping exists but lacks depth on several flows. |

**Summary Rating:** ✅ Adequate

#### Gaps, Blind Spots & Prioritized Fixes "(Per Model)"

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Finding** | **Impact** | **Effort** | **Recommendation** |
| 1 | Generic mitigations | Medium | Low | Specify PKCE, certificate pinning, mTLS, HMAC/signatures, idempotency keys explicitly. |
| 2 | Non-repudiation under-specified | Medium | Low | Adopt signed receipts, immutable audit logs, and webhook signature verification. |
| 3 | Client-side controls sparse | High | Low | Add CSP/SRI, hosted payment fields, tokenization, and response minimization. |

#### Threats & Mitigations Maturity Assessment "(Per Model)"

|  |  |  |  |
| --- | --- | --- | --- |
| **Dimension** | **Weight** | **Score** | **Reasoning** |
| DFD Element Coverage | 30% | 70 | Broad coverage across flows/components. |
| Methodology Coverage & Balance | 30% | 68 | Categories present, balance acceptable but not deep in all. |
| Contextual Accuracy | 20% | 64 | Some mitigation suggestions are imprecise for payments. |
| Mitigation Validity | 10% | 62 | Lacks targeted root-cause controls in places. |
| Proportionality & Realism | 10% | 66 | Reasonable but could prioritize spoofing/integrity more. |

**Threats & Mitigations Total Score (0–100):** 67 **Threats & Mitigations Maturity:** ✅ Adequate

#### Strategic Recommendations "(Per Model)"

#### payments-processing-platform-xai-grok-4-latest

* Replace generic advice (e.g., “encrypt payload with AES”) with correct transport and message integrity controls (TLS 1.3/mTLS, HMAC/signatures).
* Add explicit webhook signature verification and reconciliation against server-side state.
* Specify client-side controls (CSP/SRI, tokenization) to limit exposure of card data.
* Document response minimization practices and masking in logs.
* Incorporate service identity (SPIFFE/SVID) for internal flows to strengthen integrity.

## 4. Conclusion

* Comparative strengths/weaknesses (threats & mitigations):
* Best-in-class models (Anthropic Claude Sonnet; OpenAI GPT-5) provide broad, balanced STRIDE coverage with highly actionable mitigations and strong contextual accuracy.
* Solid performers (Anthropic Claude Opus) are near the top but can strengthen non-repudiation and secret lifecycle coverage.
* Adequate models (XAI Grok 4 Latest; Novita Deepseek) cover many areas but rely on generic controls; adding targeted payment-grade mitigations (PKCE, webhook signatures, idempotency, tokenization) would notably increase maturity.
* Fair to Poor models (XAI Grok 4 Fast Reasoning; Novita Qwen) show breadth but lack realism, balance, and root-cause alignment; the “unencrypted flow” overemphasis should be replaced with integrity/spoofing/non-repudiation fundamentals.
* The weakest model (Ollama Qwen) lacks substantive threats and mitigations, making it unsuitable for guiding risk reduction.
* Common DFD-Only maturity: 🌟 Good (77/100).

The shared architecture is clear and logically consistent across files, with labeled steps and trust boundaries. To elevate DFD utility, add persistent data stores, identity/secret services, and data classification details to improve completeness and enable deeper security reasoning.

* Next steps to elevate shared architecture and per-model threat quality:
* Extend the DFD with data stores (orders, logs, tokens), secret management components, and explicit data classifications.
* Ensure every boundary-crossing flow includes STRIDE-aligned threats and precise mitigations: TLS 1.3/mTLS, PKCE, token binding, message signing/HMAC, webhook signatures with reconciliation, idempotency keys, CSP/SRI, hosted payment fields/tokenization.
* Strengthen non-repudiation across all models with digitally signed receipts and immutable, correlated audit logs.
* Calibrate severities and prioritization to realistic payment fraud routes (spoofing, replay, tampering, key leakage).
* Institutionalize secret lifecycle management: vaulting, rotation, leak detection, and CI/CD hygiene.

---