Comprehensive Threat Model Evaluation Report (Combined)

Executive Summary & Comparative Analysis

This report evaluates nine Threat Dragon models for the Husky AI system, a machine learning platform for classifying husky vs. non-husky images using Azure services and a CNN model. All models share a common architecture with two trust zones (Experimental and Production), key actors (Engineer, Infra Admin, Azure Cognitive Services, User), processes (Gather Images Application, Jupyter Notebook, Deployment, Simple Python Web Server, API Gateway, Bastion), and data stores (Training and Validation Images, API Key, Machine Learning Model, Source Code and Configuration, Authorized Keys). The models differ primarily in the depth and coverage of threats and mitigations, with some providing detailed, context-specific threats while others are sparse or generic. Overall, the shared DFD architecture is solid but exhibits gaps in encryption for internal flows and stores, leading to risks in data transit and at rest. The threat models vary in maturity, with advanced LLMs (e.g., Claude variants) offering comprehensive coverage and practical mitigations, while others are underdeveloped. Recommendations focus on enhancing encryption, authentication, and cross-zone controls to address common vulnerabilities.

1. Threats & Mitigations Maturity Ranking (Across Models)

Rank	Model Name	Threats & Mitigations Score	Maturity	Reasoning
1	husky-ai-model-anthropic-claude-sonnet-4-5-20250929	95	🏆 Excellent	Extensive threats across all STRIDE categories with highly specific, zone-aware descriptions and actionable mitigations; covers supply chain, poisoning, and escalation risks comprehensively.
2	husky-ai-model-anthropic-claude-opus-4-1-20250805	90	🏆 Excellent	Detailed threats focusing on credential compromise, data poisoning, and privilege escalation; mitigations emphasize MFA, encryption, and auditing, with strong balance across categories.
3	husky-ai-model-openai-gpt-5	85	🌟 Good	Balanced coverage of spoofing, tampering, and DoS; mitigations are practical but slightly less granular than top models, with good focus on cross-zone risks.
4	husky-ai-model-novita-qwen-qwen3-coder-480b-a35b-instruct	70	✅ Adequate	Solid threats on tampering and disclosure, but fewer instances; mitigations are relevant but lack depth in areas like supply chain and insider threats.
5	husky-ai-model-novita-deepseek-	65	✅ Adequate	Covers key areas like spoofing and tampering, but mitigations are basic and uneven; misses some DoS and repudiation threats.

	deepseek-v3.1-terminus			
6	husky-ai-model-gemini-gemini-2.5-pro	60	⚙ Fair	Limited threats, mostly on tampering and disclosure; mitigations are generic and do not fully address methodology balance.
7	husky-ai-model-xai-grok-4-fast-reasoning-latest	55	⚙ Fair	Sparse threats focused on basic risks; mitigations are underdeveloped, with gaps in coverage for elevation and repudiation.
8	husky-ai-model-xai-grok-4-latest	50	⚠ Poor	Few threats, primarily spoofing and tampering; mitigations are simplistic and do not cover all categories adequately.
9	husky-ai-model-ollama-gemma327b	40	⚠ Poor	Minimal threats, unbalanced toward tampering; mitigations are vague and lack specificity for the system's ML-specific risks.

2. Overall Model Maturity

The shared DFD architecture across all models depicts a clear separation of experimental (development/training) and production zones, with actors interacting via SSH or HTTPS flows. Strengths include well-defined boundaries and flows for data ingestion, model training, deployment, and inference. However, gaps exist in labeling some internal flows as unencrypted and inconsistent encryption on stores, reducing visibility into confidentiality risks. The layout logically flows from external inputs to production serving, but lacks detail on auxiliary components like logging or monitoring.

2.1 Evaluation Summary

The DFD provides a solid foundation for understanding the Husky AI system's data flows, with clear trust zones distinguishing development from production environments. Strengths lie in mapping key processes and stores, facilitating identification of boundary crossings. Key gaps include incomplete encryption annotations on internal flows and stores, which could obscure transit risks, and limited decomposition of auxiliary security controls.

2.2 Scoring Table

Dimension	Weight	Score	Reasoning
Clarity and Readability	25%	85	Elements are consistently labeled with descriptive names; trust zones are visually distinct, and flows use standard symbols, making the diagram easy to follow despite minor overlaps in positioning.
Completeness and Coverage	30%	75	Covers core actors, processes, stores, and flows; includes key interactions like SSH for admin access and HTTPS for external inputs, but omits details on auxiliary elements like monitoring or backup systems.
Accuracy and	25%	80	Flows align with system logic (e.g., external to experimental for

Logical Consistency			training, then to production); no major redundancies, though some unencrypted internal flows contradict stated security practices like TLS emphasis.
Usability for Security Analysis	20%	70	Enables quick identification of boundary risks (e.g., SSH cross-zone), but inconsistent encryption flags and lack of data classification on flows hinder deeper risk assessment and extensibility.

Overall Model Maturity Total Score (0–100): 78 **Overall Model Maturity:** 🌟 Good

3. Individual Model Evaluations (Threats & Mitigations Only)

##

husky-ai-model-anthropic-claude-opus-4-1-20250805

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

##

Threat Landscape Snapshot (husky-ai-model-anthropic-claude-opus-4-1-20250805)

STRIDE Category	High	Medium	Low	Observations
Spoofing	5	2	1	Strong focus on credential compromise and impersonation across actors and flows.
Tampering	6	3	0	Comprehensive coverage of data/model poisoning and tampering in training/deploy.
Repudiation	1	1	0	Limited but relevant to logging gaps in SSH/admin actions.
Information Disclosure	4	4	2	Balanced on encryption failures and key exposure.
Denial of Service	3	2	1	Covers resource exhaustion in notebooks and APIs.
Elevation of Privilege	5	2	0	Emphasizes cross-zone SSH risks and bastion compromise.

Balanced across STRIDE with emphasis on tampering and elevation, plausible for an ML pipeline with external dependencies.

Mitigation Quality & Alignment (husky-ai-model-anthropic-claude-opus-4-1-20250805)

Control Area	Adequacy	Observations
Relevance & Specificity	✅	Mitigations directly target threats like MFA for SSH and encryption for flows.
Practicality	✅	Feasible steps such as key rotation and anomaly detection.
Completeness & Coverage	✅	Covers most threats but could expand on repudiation.
Effectiveness	✅	Addresses root causes, e.g., sandboxing for notebooks.
Standards Alignment	✅	Aligns with NIST/OWASP (e.g., least privilege, auditing).
Traceability &	✅	Clear links between threats and mitigations.

Justification		

Summary Rating: ✅ Adequate

Gaps, Blind Spots & Prioritized Fixes (husky-ai-model-anthropic-claude-opus-4-1-20250805)

#	Finding	Impact	Effort	Recommendation
1	Limited repudiation threats	Medium	Low	Add threats for audit log tampering and mitigations like immutable logging.
2	Underemphasis on supply chain in libraries	High	Medium	Include threats for dependency confusion attacks with SCA tool integration.
3	No threats for model inversion attacks	High	High	Add inference-time threats and differential privacy mitigations.

Threats & Mitigations Maturity Assessment (husky-ai-model-anthropic-claude-opus-4-1-20250805)

This section evaluates the completeness, contextual quality, and methodological balance of threats and mitigations within the model. It focuses on whether the threat model demonstrates a credible and comprehensive application of the selected methodology (e.g., STRIDE) across all relevant elements of the DFD.

Dimension	Weight	Score	Reasoning
DFD Element Coverage	30%	90	All major actors, processes, stores, and flows have associated threats; critical paths like SSH and data ingestion are well-covered.
Methodology Coverage & Balance	30%	85	Strong balance across STRIDE, with good representation of tampering and elevation; minor undercoverage in repudiation.
Contextual Accuracy	20%	90	Threats are plausible and tied to ML-specific risks like poisoning; aligns with zone exposures.
Mitigation Validity	10%	85	Mitigations are effective and root-cause focused, though some could specify tools (e.g., Sigstore).
Proportionality & Realism	10%	90	Severities match system risks; realistic for a cloud-based ML app with external integrations.

Threats & Mitigations Total Score (0–100): 90 **Threats & Mitigations Maturity:** 🏆 Excellent

Strategic Recommendations (husky-ai-model-anthropic-claude-opus-4-1-20250805)

1. Add threats for repudiation in admin flows to cover audit gaps, justifying with logging best practices.
2. Enhance supply chain threats by including vendor risk assessments, as external libraries are a key vector.
3. Incorporate model-specific threats like adversarial examples during inference, with mitigations like robust training.
4. Remove redundant threats on basic encryption to streamline focus on unique ML risks.

5. Expand mitigations with quantifiable metrics, e.g., key rotation frequency, to improve traceability.

##

husky-ai-model-anthropic-claude-sonnet-4-5-20250929

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

##

Threat Landscape Snapshot (husky-ai-model-anthropic-claude-sonnet-4-5-20250929)

STRIDE Category	High	Medium	Low	Observations
Spoofing	7	3	1	Extensive on credentials and actors.
Tampering	8	4	1	Deep coverage of poisoning and flows.
Repudiation	2	2	0	Improved logging threats.
Information Disclosure	6	5	2	Detailed on encryption and exfiltration.
Denial of Service	4	3	1	Resource and API focus.
Elevation of Privilege	6	3	0	Cross-zone and bastion emphasis.

Highly balanced, with advanced ML-specific threats like inversion attacks.

Mitigation Quality & Alignment (husky-ai-model-anthropic-claude-sonnet-4-5-20250929)

Control Area	Adequacy	Observations
Relevance & Specificity	✅	Highly targeted, e.g., differential privacy for models.
Practicality	✅	Actionable with tools like Sigstore.
Completeness & Coverage	✅	Comprehensive, covering all categories.
Effectiveness	✅	Root-cause oriented, e.g., zero-trust networking.
Standards Alignment	✅	Strong NIST/OWASP ties.
Traceability & Justification	✅	Explicit links and justifications.

Summary Rating: ✅ Adequate

Gaps, Blind Spots & Prioritized Fixes (husky-ai-model-anthropic-claude-sonnet-4-5-20250929)

#	Finding	Impact	Effort	Recommendation
1	Minor gaps in low-severity DoS	Low	Low	Add mitigations for low-impact floods.
2	Overlap	Medium	Low	Consolidate duplicate escalation threats.

	in similar threats			
3	Limited focus on physical access	Medium	Medium	Include threats for data center access.

Threats & Mitigations Maturity Assessment (husky-ai-model-anthropic-claude-sonnet-4-5-20250929)

Dimension	Weight	Score	Reasoning
DFD Element Coverage	30%	95	Near-complete coverage of all elements with threats.
Methodology Coverage & Balance	30%	95	Excellent STRIDE balance, including advanced categories.
Contextual Accuracy	20%	95	Highly plausible for ML systems.
Mitigation Validity	10%	95	Effective and innovative mitigations.
Proportionality & Realism	10%	95	Well-prioritized risks.

Threats & Mitigations Total Score (0–100): 95 **Threats & Mitigations Maturity:** 🏆 Excellent

Strategic Recommendations (husky-ai-model-anthropic-claude-sonnet-4-5-20250929)

6. Consolidate overlapping threats to avoid redundancy while maintaining coverage.
7. Add low-severity threats for completeness, justifying with minor risk scenarios.
8. Incorporate physical security threats, as cloud models often overlook on-prem risks.
9. Enhance mitigations with cost-benefit analysis for implementation.
10. Integrate emerging threats like AI supply chain attacks from recent advisories.

##

husky-ai-model-gemini-gemini-2.5-pro

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

##

Threat Landscape Snapshot (husky-ai-model-gemini-gemini-2.5-pro)

STRIDE Category	High	Medium	Low	Observations
Spoofing	2	1	0	Basic credential risks.
Tampering	3	2	1	Focus on data poisoning.
Repudiation	0	0	0	Absent.
Information Disclosure	2	1	1	Encryption gaps.
Denial of	1	1	0	Resource exhaustion.

Service				
Elevation of Privilege	2	1	0	Bastion focus.

Unbalanced, heavy on tampering; misses repudiation.

Mitigation Quality & Alignment (husky-ai-model-gemini-gemini-2.5-pro)

Control Area	Adequacy	Observations
Relevance & Specificity	⚠️	Generic, not always tied to threats.
Practicality	⚠️	Basic suggestions like encryption.
Completeness & Coverage	⚠️	Incomplete for missing categories.
Effectiveness	⚠️	Addresses symptoms more than roots.
Standards Alignment	⚠️	Loose ties to standards.
Traceability & Justification	⚠️	Limited justification.

Summary Rating: ⚠️ Partially adequate

Gaps, Blind Spots & Prioritized Fixes (husky-ai-model-gemini-gemini-2.5-pro)

#	Finding	Impact	Effort	Recommendation
1	No repudiation threats	High	Medium	Add logging threats and immutable audit mitigations.
2	Sparse coverage overall	High	Low	Expand to cover all STRIDE categories.
3	Ignores supply chain	Medium	Medium	Add library tampering threats.

Threats & Mitigations Maturity Assessment (husky-ai-model-gemini-gemini-2.5-pro)

Dimension	Weight	Score	Reasoning
DFD Element Coverage	30%	70	Covers main processes but misses some flows.
Methodology Coverage & Balance	30%	60	Uneven; repudiation absent.
Contextual Accuracy	20%	70	Plausible but shallow.
Mitigation Validity	10%	65	Basic effectiveness.
Proportionality & Realism	10%	70	Somewhat realistic.

Threats & Mitigations Total Score (0–100): 60 **Threats & Mitigations Maturity:** ⚙️ Fair

Strategic Recommendations (husky-ai-model-gemini-gemini-2.5-pro)

11. Add repudiation threats to balance methodology.
12. Expand tampering coverage with ML-specific examples.
13. Include supply chain risks for libraries.
14. Improve mitigation specificity with tools.
15. Add threats for all actors and flows.

##

husky-ai-model-novita-deepseek-deepseek-v3.1-terminus

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

##

Threat Landscape Snapshot (husky-ai-model-novita-deepseek-deepseek-v3.1-terminus)

STRIDE Category	High	Medium	Low	Observations
Spoofing	3	2	1	Credential and flow spoofing.
Tampering	4	2	1	Data and model focus.
Repudiation	1	0	0	Basic logging.
Information Disclosure	3	2	1	Key and data leaks.
Denial of Service	2	1	0	Resource risks.
Elevation of Privilege	2	1	0	Bastion emphasis.

Fair balance, but shallow depth.

Mitigation Quality & Alignment (husky-ai-model-novita-deepseek-deepseek-v3.1-terminus)

Control Area	Adequacy	Observations
Relevance & Specificity	✅	Relevant to threats.
Practicality	⚠️	Feasible but generic.
Completeness & Coverage	⚠️	Gaps in repudiation.
Effectiveness	⚠️	Addresses basics.
Standards Alignment	✅	Aligns with common practices.
Traceability & Justification	⚠️	Some justification.

Summary Rating: ⚠️ Partially adequate

Gaps, Blind Spots & Prioritized Fixes (husky-ai-model-novita-deepseek-deepseek-v3.1-terminus)

#	Finding	Impact	Effort	Recommendation
1	Weak repudiation coverage	Medium	Low	Add audit threats.
2	Limited DoS details	Medium	Medium	Expand resource threats.
3	No advanced ML risks	High	High	Include poisoning variants.

Threats & Mitigations Maturity Assessment (husky-ai-model-novita-deepseek-deepseek-v3.1-terminus)

Dimension	Weight	Score	Reasoning
DFD Element Coverage	30%	75	Good on main elements.
Methodology Coverage & Balance	30%	65	Fair balance, repudiation weak.
Contextual Accuracy	20%	70	Plausible.
Mitigation Validity	10%	70	Adequate.
Proportionality & Realism	10%	65	Realistic but basic.

Threats & Mitigations Total Score (0–100): 65 **Threats & Mitigations Maturity:** ✅ Adequate

Strategic Recommendations (husky-ai-model-novita-deepseek-deepseek-v3.1-terminus)

16. Bolster repudiation with logging mitigations.
17. Add DoS threats for completeness.
18. Incorporate ML-specific risks like inversion.
19. Refine mitigations for specificity.
20. Balance categories evenly.

##

husky-ai-model-novita-qwen-qwen3-coder-480b-a35b-instruct

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

##

Threat Landscape Snapshot (husky-ai-model-novita-qwen-qwen3-coder-480b-a35b-instruct)

STRIDE Category	High	Medium	Low	Observations
Spoofing	3	1	1	User and key spoofing.
Tampering	4	2	1	Data and config focus.

Repudiation	1	1	0	Logging gaps.
Information Disclosure	3	2	1	Encryption issues.
Denial of Service	2	1	0	Basic.
Elevation of Privilege	3	1	0	Privilege abuse.

Adequate balance, focused on core risks.

Mitigation Quality & Alignment (husky-ai-model-novita-qwen-qwen3-coder-480b-a35b-instruct)

Control Area	Adequacy	Observations
Relevance & Specificity	✅	Tied to threats.
Practicality	✅	Practical steps.
Completeness & Coverage	✅	Good coverage.
Effectiveness	✅	Effective basics.
Standards Alignment	✅	OWASP-aligned.
Traceability & Justification	✅	Clear.

Summary Rating: ✅ Adequate

Gaps, Blind Spots & Prioritized Fixes (husky-ai-model-novita-qwen-qwen3-coder-480b-a35b-instruct)

#	Finding	Impact	Effort	Recommendation
1	Sparse repudiation	Medium	Low	Add audit threats.
2	Limited supply chain	Medium	Medium	Include library risks.
3	No model inversion	High	High	Add inference threats.

Threats & Mitigations Maturity Assessment (husky-ai-model-novita-qwen-qwen3-coder-480b-a35b-instruct)

Dimension	Weight	Score	Reasoning
DFD Element Coverage	30%	80	Covers essentials.
Methodology Coverage & Balance	30%	70	Adequate, repudiation weak.
Contextual Accuracy	20%	75	Plausible.
Mitigation	10%	75	Solid.

Validity			
Proportionality & Realism	10%	75	Balanced.

Threats & Mitigations Total Score (0–100): 70 **Threats & Mitigations Maturity:** ✅ Adequate

Strategic Recommendations (husky-ai-model-novita-qwen-qwen3-coder-480b-a35b-instruct)

21. Enhance repudiation coverage.
22. Add supply chain threats.
23. Include advanced ML risks.
24. Specify tools in mitigations.
25. Ensure even category distribution.

##

husky-ai-model-ollama-gemma327b

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

##

Threat Landscape Snapshot (husky-ai-model-ollama-gemma327b)

STRIDE Category	High	Medium	Low	Observations
Spoofing	1	0	0	Minimal.
Tampering	2	1	0	Data focus.
Repudiation	0	0	0	Absent.
Information Disclosure	1	1	0	Basic.
Denial of Service	1	0	0	Limited.
Elevation of Privilege	1	0	0	Sparse.

Heavily skewed toward tampering; incomplete.

Mitigation Quality & Alignment (husky-ai-model-ollama-gemma327b)

Control Area	Adequacy	Observations
Relevance & Specificity	⚠️	Vague and generic.
Practicality	⚠️	Basic advice.
Completeness & Coverage	❌	Major gaps.
Effectiveness	⚠️	Low impact.
Standards Alignment	⚠️	Minimal.
Traceability & Justification	⚠️	Poor.

Summary Rating: ❌ Inadequate

Gaps, Blind Spots & Prioritized Fixes (husky-ai-model-ollama-gemma327b)

#	Finding	Impact	Effort	Recommendation
1	Missing categories	High	Medium	Add full STRIDE coverage.
2	No insider threats	High	Low	Include engineer risks.
3	Shallow mitigations	High	Medium	Develop detailed fixes.

Threats & Mitigations Maturity Assessment (husky-ai-model-ollama-gemma327b)

Dimension	Weight	Score	Reasoning
DFD Element Coverage	30%	50	Partial coverage.
Methodology Coverage & Balance	30%	40	Unbalanced and incomplete.
Contextual Accuracy	20%	50	Basic plausibility.
Mitigation Validity	10%	40	Ineffective.
Proportionality & Realism	10%	45	Unrealistic depth.

Threats & Mitigations Total Score (0–100): 40 **Threats & Mitigations Maturity:** ⚠️ Poor

Strategic Recommendations (husky-ai-model-ollama-gemma327b)

26. Expand to full STRIDE categories.
27. Add insider and supply chain threats.
28. Improve mitigation detail.
29. Balance focus areas.
30. Justify with system context.

##

husky-ai-model-openai-gpt-5

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

##

Threat Landscape Snapshot (husky-ai-model-openai-gpt-5)

STRIDE Category	High	Medium	Low	Observations
Spoofing	4	2	1	Credential focus.

Tampering	5	3	1	Poisoning and flows.
Repudiation	1	1	0	Logging.
Information Disclosure	4	3	1	Encryption.
Denial of Service	3	2	1	Resources.
Elevation of Privilege	4	2	0	Cross-zone.

Well-balanced, ML-focused.

Mitigation Quality & Alignment (husky-ai-model-openai-gpt-5)

Control Area	Adequacy	Observations
Relevance & Specificity	✅	Targeted to threats.
Practicality	✅	Feasible.
Completeness & Coverage	✅	Good.
Effectiveness	✅	Root-focused.
Standards Alignment	✅	Strong.
Traceability & Justification	✅	Clear.

Summary Rating: ✅ Adequate

Gaps, Blind Spots & Prioritized Fixes (husky-ai-model-openai-gpt-5)

#	Finding	Impact	Effort	Recommendation
1	Repudiation underdeveloped	Medium	Low	Add more logging threats.
2	Limited supply chain	Medium	Medium	Include dependency risks.
3	No physical threats	Low	Low	Add data center risks.

Threats & Mitigations Maturity Assessment (husky-ai-model-openai-gpt-5)

Dimension	Weight	Score	Reasoning
DFD Element Coverage	30%	85	Strong on key elements.
Methodology Coverage & Balance	30%	80	Balanced, repudiation weak.
Contextual Accuracy	20%	85	Plausible.
Mitigation Validity	10%	85	Effective.
Proportionality	10%	85	Realistic.

& Realism			

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

Strategic Recommendations (husky-ai-model-openai-gpt-5)

31. Strengthen repudiation.
32. Add supply chain threats.
33. Include physical access risks.
34. Refine for emerging threats.
35. Ensure zone-specific focus.

##

husky-ai-model-xai-grok-4-fast-reasoning-latest

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

##

Threat Landscape Snapshot (husky-ai-model-xai-grok-4-fast-reasoning-latest)

STRIDE Category	High	Medium	Low	Observations
Spoofing	2	1	0	Basic.
Tampering	2	1	1	Flows.
Repudiation	0	0	0	Absent.
Information Disclosure	2	1	0	Encryption.
Denial of Service	1	0	0	Limited.
Elevation of Privilege	1	1	0	Sparse.

Unbalanced, limited depth.

Mitigation Quality & Alignment (husky-ai-model-xai-grok-4-fast-reasoning-latest)

Control Area	Adequacy	Observations
Relevance & Specificity	⚠️	Generic.
Practicality	⚠️	Basic.
Completeness & Coverage	⚠️	Gaps.
Effectiveness	⚠️	Low.
Standards Alignment	⚠️	Minimal.
Traceability & Justification	⚠️	Poor.

Summary Rating: ⚠️ Partially adequate

Gaps, Blind Spots & Prioritized Fixes (husky-ai-model-xai-grok-4-fast-reasoning-latest)

#	Finding	Impact	Effort	Recommendation
1	No repudiation	High	Low	Add logging threats.
2	Sparse overall	High	Medium	Expand coverage.
3	Misses ML specifics	Medium	High	Add poisoning threats.

Threats & Mitigations Maturity Assessment (husky-ai-model-xai-grok-4-fast-reasoning-latest)

Dimension	Weight	Score	Reasoning
DFD Element Coverage	30%	60	Partial.
Methodology Coverage & Balance	30%	55	Unbalanced.
Contextual Accuracy	20%	60	Basic.
Mitigation Validity	10%	55	Inadequate.
Proportionality & Realism	10%	60	Fair.

Threats & Mitigations Total Score (0–100): 55 **Threats & Mitigations Maturity:** ⚙️ Fair

Strategic Recommendations (husky-ai-model-xai-grok-4-fast-reasoning-latest)

36. Add repudiation threats.
37. Expand to full STRIDE.
38. Include ML risks.
39. Improve mitigations.
40. Balance categories.

##

husky-ai-model-xai-grok-4-latest

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

##

Threat Landscape Snapshot (husky-ai-model-xai-grok-4-latest)

STRIDE Category	High	Medium	Low	Observations
Spoofing	2	1	0	Basic.
Tampering	2	1	0	Flows.
Repudiation	0	0	0	Absent.

Information Disclosure	1	1	0	Limited.
Denial of Service	1	0	0	Sparse.
Elevation of Privilege	1	0	0	Minimal.

Very limited, unbalanced.

Mitigation Quality & Alignment (husky-ai-model-xai-grok-4-latest)

Control Area	Adequacy	Observations
Relevance & Specificity	⚠️	Vague.
Practicality	⚠️	Simple.
Completeness & Coverage	❌	Major gaps.
Effectiveness	⚠️	Basic.
Standards Alignment	⚠️	Loose.
Traceability & Justification	⚠️	Limited.

Summary Rating: ⚠️ Partially adequate

Gaps, Blind Spots & Prioritized Fixes (husky-ai-model-xai-grok-4-latest)

#	Finding	Impact	Effort	Recommendation
1	Missing categories	High	Medium	Full STRIDE addition.
2	No advanced risks	High	Low	Add ML threats.
3	Shallow depth	High	High	Develop details.

Threats & Mitigations Maturity Assessment (husky-ai-model-xai-grok-4-latest)

Dimension	Weight	Score	Reasoning
DFD Element Coverage	30%	55	Incomplete.
Methodology Coverage & Balance	30%	50	Unbalanced.
Contextual Accuracy	20%	55	Basic.
Mitigation Validity	10%	50	Poor.
Proportionality & Realism	10%	55	Fair.

Threats & Mitigations Total Score (0–100): 50 **Threats & Mitigations Maturity:** ⚠️ Poor

Strategic Recommendations (husky-ai-model-xai-grok-4-latest)

41. Expand STRIDE coverage.
42. Add insider threats.
43. Improve mitigation quality.
44. Include supply chain.
45. Justify with context.

4. Conclusion

The Claude models excel in threats and mitigations with detailed, balanced coverage and strong mitigations, making them suitable for high-maturity environments, while Gemma and Grok variants lag with sparse, unbalanced threats that overlook key areas like repudiation and supply chain risks. The common DFD architecture is 🌟 Good overall, providing a reliable base but needing consistent encryption annotations to better highlight transit vulnerabilities. To elevate the shared architecture, standardize encryption on all internal flows and stores; for per-model threats, prioritize adding comprehensive STRIDE coverage and ML-specific risks like inversion attacks across all variants, starting with the lower-ranked models to achieve uniform adequacy. Next steps include a unified threat model template emphasizing encryption and auditing, followed by validation through red-team exercises.