

Model Assurance Attestation

Issued 2026-10-15T03:14:33Z · Template 0.1

nvidia/Qwen3.8-27B-NVFP4

14f1f01bdd7978f942ec9f1ea5cee5788b50ce7ac610bbd2f2a40f6384b30c33
model directory · document SOCAIR-20261015-14f1f01b · issuer socair.ai examples
license Apache License 2.0 (apache-2.0) · declared base Qwen/Qwen3.8-27B

Tier 1 (static)

Promotion: authorized

6 pass 0 fail 0 lead 0 not tested

CHECKS PERFORMED

Check	Looks for	Result	Evidence
-------	-----------	--------	----------

Format and structure

Malformed container structure, unexpected tensors

PASS means: The container parsed, and its tensor data tiles the data section exactly: no unaccounted bytes, overlapping tensors, or duplicate names. For an ONNX model: every tensor holds exactly the data its type and shape need, no two initializers of a graph share a name, external data stays inside the model's directory and fits its file, and every operator is ONNX's own, one of onnxruntime's contrib operators, or a function the model defines. For an OpenVINO IR: every Const lies inside the .bin and is exactly the size its element type and shape take, the Consts cover the .bin with no byte outside them, and every operation OpenVINO builds is in its own opsets. Tensor values are not judged, and an operator library a deployment registers is outside the model. For a Keras model (HDF5 or a .keras archive): every dataset's storage lies inside the HDF5 data, sized by its type and shape, with none overlapping and no data or link in another file, the archive holds only what Keras reads, and the config names no Python bytecode, pickled module, or class or function from outside Keras and TensorFlow (KerasHub, KerasCV, and KerasNLP classes are named). Weight values are not judged. Addresses AML.T0010.003, LLM03

PASS

4 of 4 file(s) PASS; e.g. model-00001-of-00003.safetensors: safetensors layout verified: 1043 tensors tile 9965526000 data bytes exactly, each sized to its shape and dtype; 1 metadata keys

File inventory and payloads	Hidden files, embedded payloads, unexpected executables PASS means: No script, shell command, long encoded blob, or executable signature was found in string metadata values, including every string-array element of 64 bytes or more, and no native executable among the files. Shorter array elements, such as vocabulary tokens, are too short to carry one and are not scanned. An archive among the files counts only when the Pickle opcode scan PASSEd it and read every entry in it: a torch.save checkpoint with nothing outside torch.save's layout. Addresses AML.T0011.000, AML.T0018.002, AML.T0010.003, LLM03	PASS	4 of 4 file(s) PASS; e.g. directory listing: repo: 19 files, 0 scripts inventoried (scripts are expected, not a finding); no pickle file: none is named as one or begins as one (a protocol 2 to 5 stream, or a zip holding a pickle), so no Pickle opcode scan row
Hash, provenance, lineage	Traceable origin: a manifest bound to this hash, from an immutable upstream commit; files that disagree with the uploader's checksum list PASS means: A trusted publisher signature verified over this artifact, or an operator-supplied manifest binds this hash to a repository at an immutable commit. The notes say which; a manifest is the operator's claim, not a signature. No file the scan compared with a SHA-256 list its uploader ships (SHA256SUMS or a .sha256 file) disagrees with it, save Markdown, which is named and not graded; agreement is noted, and the PASS does not rest on it. Addresses AML.T0010.003, AML.T0115.001, LLM03	PASS	origin bound to this artifact's hash, at an immutable commit: repo https://huggingface.co/nvidia/Qwen3.8-27B-NVFP4; revision 482ca0f3832238542f8f5295dde86b5f22711d80; commit 482ca0f3832238542f8f5295dde86b5f22711d80; via airlock pull; publisher signature not established; manifest provenance.json (sha256 979f3f95058fd62f606300a61fb5d7eb2a7b90bfb619cccfdfce321988919f58)

Chat template	Code reach, hidden or obfuscated text, override or content-triggered instructions, and the text the rendered template adds to the prompt PASS means: The template parsed and reaches no Python internals or process execution, and carries no override or concealment language, URL, hidden or obfuscated text, or condition on message content other than a standard content-part type such as text or image. Instructions written as ordinary guidance, or added for a content-part type, are not judged: the notes list the text a template adds for a content-part type, and, when the template rendered, the text it adds to the prompt and whether it matches a reviewed template. Addresses AML.T0018.003, AML.T0051, AML.T0011.000, LLM01, LLM03	PASS	template parsed; no code-execution reach, content-conditional injection, hidden or obfuscated text, or instruction-language lead found. Structural heuristic; not a proof of absence. Rendered on 6 probes/v1 probe conversation(s) with Socair's own Jinja evaluator, modelling transformers' sandbox settings. This template adds to the prompt: "Reasoning effort is set to xhigh. Please think carefully through the task, validate key assumptions, consider plausible ..." (4 of 6); "Reasoning effort is set to xhigh. Please think carefully through the task, validate key assumptions, consider plausible ..." (2 of 6); "</tools>\n\nIf you choose to call a function ONLY reply in the following format with NO suffix:" (2 of 6); "<function=example_function_name>\n<parameter=example_parameter_1>\nvalue_1\n</parameter>\n<parameter=example_parameter_2>\nTh..." (2 of 6); "<IMPORTANT>\nReminder:\n- Function calls MUST follow the specified format: an inner <function=...></function> block must b..." (2 of 6); "XML tags\n- Required parameters MUST be specified\n- You may provide optional reasoning for your function call in natural ..." (2 of 6); and 3 more. Listed for review, not judged. No reviewed template text was available, so it was not compared.
Tokenizer config	Tampered tokenizer tables: special-token ids, token types, control tokens PASS means: The tokenizer tables are internally consistent, and no control token carries instructions. When a canonical reference table for its family is configured (from a feed or SOCAIR_TOKENIZER_REFERENCE), every token was compared with it and no ordinary token differs; the notes say which reference, or that none was configured or matched. Addresses AML.T0018.003, AML.T0011.000, AML.T0010.003, LLM03	PASS	tokenizer.json (sha256 0997f410c57a1f4e, BPE model): 248077 tokens, 33 added (21 special); special-token ids, added-token tables, declared special tokens, and template tokens agree; no token, normalizer, or template injects text. No canonical tokenizer reference was configured, so its tokens were not compared.

Remote code	Python a loader would import: modules a config names (auto_map, custom_pipelines, sentence-transformers and diffusers modules), files loaders import by their path, and the repository files those import PASS means: No config a loader reads names Python in this directory or in another repository (through an auto_map entry, custom_pipelines, a sentence-transformers module, or a diffusers custom pipeline or component), and no file sits where a loader imports one by its path (custom_generate/generate.py, or an inference toolkit's handler.py, pipeline.py, or code/inference.py). Other Python and script files are listed in the notes and not judged: a loader Socair does not model, or a person, can still run them. Addresses AML.T0011.000, AML.T0010.001, LLM03	no loader is told to import code: no auto_map, custom_pipelines, sentence-transformers module outside sentence_transformers, or diffusers custom component in the 10 JSON config(s) read, and no custom_generate/generate.py, handler.py, pipeline.py, or code/inference.py
-------------	---	--

Framework editions: MITRE ATLAS 2026.09, OWASP LLM Top 10 2025.

ASSURANCE LEVEL: TIER 1 (STATIC)

What it is

Static checks on the artifact's bytes and metadata, run offline. No inference is run, and the weights are not evaluated for behavior.

What it means

Each listed check ran on the exact bytes identified by the artifact hash, and each row states what its PASS means. A FAIL carries positive evidence, a LEAD is a suspicious signal that needs a person's review, and a NOT_TESTED names why it was not tested. A FAIL or a LEAD withholds promotion, and no acceptance clears it.

What it does not mean

It is not an assessment of the model's behavior or safety. It does not test the weights for backdoors or poisoning, behavior that appears only after quantization or on particular hardware, or jailbreak susceptibility and harmful capability, and it is not a legal review of the model's license.

Tier 2

Tier 2 (inference on the production node class) did not run.

BOUNDED STATEMENT

For the artifact identified by its hash, the Tier 1 checks that returned PASS found no indicators within their stated scope. Rows marked NOT_TESTED were not examined, for the reason each row gives. Tier 1 runs no inference, so no model behavior was tested. Every surface outside that scope is listed under Out of scope.

OUT OF SCOPE

This attestation does not certify the absence of unknown backdoors.

- Backdoors, trojans, or poisoning in the model weights. Tier 1 reads the weights' layout, never their behavior.

- Triggered, sleeper, or polymorphic behavior. Tier 1 runs no inference.
- Behavior that appears only after quantization, or only on particular hardware or serving stacks, unless Tier 2 ran on the production node class.
- Behavioral safety: jailbreak susceptibility, harmful capability, and bias.
- Malicious behavior that only emerges at runtime under real traffic.
- Artifact formats we do not parse.
- Pickle code execution through a reviewed class's state, loader bugs, parse differentials, a tampered environment, or code carried as data for a later stage to run.
- Chat-template instructions written as ordinary guidance (no override or concealment phrase, URL, hidden or obfuscated text, or condition on message content other than a standard content-part type such as text or image): the text a rendered template adds, and the text a template adds for a content-part type, is listed in the report, not judged, unless the template matches a reviewed template.
- Legal review of a license, and compliance with its usage policies. The license is identified, and checked only against a policy you configure.

Checks not run at this level:

- Forward-pass trigger probes (Tier 2) (Behavior under the production serving stack): not run. Tier 2 (forward-pass, on the production node class) did not run; Tier 1 is static and runs no inference
- Serving-stack differential (Tier 2) (Same artifact behaving differently across stacks): not run. Tier 2 (forward-pass, on the production node class) did not run; Tier 1 is static and runs no inference
- Known-bad hash match (Match against the known-bad artifact denylist): not run. no known-bad list was supplied (SOCAIR_DENYLIST, or a signed feed that carries one), so the artifact's hash was not matched against one

Node classes not tested:

- every node class: Tier 1 is static and ran no inference on any hardware

PROMOTION AUTHORIZATION

Clean-store promotion: authorized · Tier 1 only

Every Tier 1 check PASSED.

VERIFICATION

Signing: DSSE Ed25519 over an in-toto Statement v1

Signer key: 6230d2225405c855da4cfba73cad678651dd6f0221e2739fc9bd3901ffd35e38

Document hash: 22af02da3df842439708530287e9f25a54cc4f22111f52ec0ab541515aaab2f7

A printed report is a claim, not the proof. Check the attestation: socair verify <attestation.dsse.json> --trusted <key.pub> --artifact <file or directory>

Artifact SHA256: 14f1f01bdd7978f942ec9f1ea5cee5788b50ce7ac610bbd2f2a40f6384b30c33

LICENSE STATEMENTS

What the artifact says about its license, and where. A license is identified, never reviewed: this is not legal advice.

LICENSE: "Apache License" · apache-2.0

model card license: "apache-2.0" · apache-2.0

FILES

The artifact SHA256 is the digest of this manifest: every file's hash, size, and path (socair.modeldir/v1).

.gitattributes · other · 1570 bytes · 34448b82c17d60fec9b65b1f093c115ddbaadc04beb1b0140b6bfed2e012a930
 .quant_summary.txt · other · 318035 bytes · 0f8818b69fa46381899bdc72833805409e6ca9771f9c34e5f3dcf4674da9a3a1
 LICENSE · other · 11544 bytes · bbedc3fda3305820b977265f01b8619d87570a6739de3a5582c3464840f1e57a
 README.md · other · 9578 bytes · 2dc5368ce2dda4393818fc3c6e587d588ec7b7f599b1f3a326d97dc271e3866d
 chat_template.jinja · chat_template · 8952 bytes · c3cf9e34abf4f9e36c2d72165aa9c132d3e2a725b6c2586aaa3a8af9d7a81041
 config.json · config · 87506 bytes · 71fa01bb64de20971045cd82a82c0ebb25a54e1b0a3f09ef23cf5479e9c54df8
 generation_config.json · config · 214 bytes · 8a3a817a9d330f6f9e62f048fe62a48594946c4a5c4cb314a8011316d5094986
 hf_quant_config.json · config · 53760 bytes · 5f4aaa9e462ddb26a9790ab459eee69d100b9ade7541f0c86038e925c013f80b
 merges.txt · tokenizer · 3353259 bytes · a9d356d7bdf1ef4949e3e748e95b8e10ad9d4e2e838eddc38a0a7b6b94d1db8d

model-00001-of-00003.safetensors · weights · 9965652544 bytes ·
7d0fd155118901373eb0fd13ed3aae68f95be747bc205be72ebc41739c25ee80
model-00002-of-00003.safetensors · weights · 9985757064 bytes ·
98a7e9486baa860c792c9463a770cb9d017696bdd17606300a5b9334149f4c27
model-00003-of-00003.safetensors · weights · 1970287672 bytes ·
0506ad35dc21469708e7813bd76c592cef08bd0317b4a1fe899745ebe2435271
model.safetensors.index.json · config · 214866 bytes · 7aa103a2582b7d26631988de33dea19e8a308ee9c239e8e14feb374af30905e2
preprocessor_config.json · config · 390 bytes · 27225450ac9c6529872ee1924fcb0962ff5634834f817040f444118116f4e516
processor_config.json · config · 1191 bytes · d89ef49ce9cd37fbf510158e13c1ef063d9286411c1ec9049932dbe0487143b1
tokenizer.json · tokenizer · 12809320 bytes · 0997f410c57a1f4e53b09e4be8f4a172d90edd9564368fb0847030937229b9f3
tokenizer_config.json · tokenizer · 1121 bytes · e5d078b00e6c1223b32444db8c1001dc71d86ceef8ee706b5bf084c3a43a1f9c
video_preprocessor_config.json · config · 385 bytes · 7768af27c1fafa9cc9011c1dc20067e03f8915e03b63504550e11d5066986d13
vocab.json · tokenizer · 6722759 bytes · ce99b4cb2983d118806ce0a8b777a35b093e2000a503ebde25853284c9dfa003

socair.ai examples · No absence guarantee. See the bounded statement and out-of-scope ceiling.