CS Code Evidence Pack

Demo App 2.0.0

Buyer-facing release evidence for restricted and offline software deployments.

Services	Ports	SBOM Components	Vulnerabilities
4	1	4	0

Generated locally. Source code does not leave the customer environment by default.

Executive Summary

- This pack provides release evidence for Demo App 2.0.0, generated from local scan outputs.

- It covers 4 detected service(s), 1 exposed port mapping(s), 11 environment variable reference(s), 7 potential external endpoint reference(s), and 4 SBOM component(s).

- Current risk posture: Change review. Deployment-relevant changes are present and should be reviewed by security/operations.

- The pack is designed for buyer security and operations review; it is not a replacement for customer-specific penetration testing, code review, accreditation or deployment acceptance.

Risk Cards

Critical	High	Endpoints	Posture
0	0	7	Change review: Deployment-relevant changes are present and should be reviewed by security/o

What This Pack Proves

- The pack can be generated locally without a SaaS connection.

- Deployment evidence covers services, ports, environment variable names, endpoints, dependencies and vulnerabilities.

- Generated metadata and scanner/report artefacts include SHA-256 checksums for receiver-side integrity verification.

- Standard dashboard upload is metadata-only and excludes source code, raw reports, file inventories and release ZIPs.

- Update-diff evidence highlights release-to-release changes.

Approval Considerations

- 1 new service(s), 0 removed service(s).

- 1 added port mapping(s), 1 removed port mapping(s).

- 3 added environment variable(s), 1 removed environment variable(s).

- 6 added endpoint reference(s), 3 removed endpoint reference(s).

- 3 added component(s), 2 removed component(s).

- 0 new vulnerability finding(s), 2 resolved finding(s).

Services

Service	Image	Build	Ports
web	local build	.	8081:80
worker	python:3.12-slim		
telemetry	alpine:3.20		
dockerfile	local build	.	

Ports

Service	Mapping	Source
web	8081:80	docker-compose.yml

Environment Variables

Name	Source	File	Service
API_BASE_URL	docker_compose_environment	docker-compose.yml	web
STRIPE_KEY	docker_compose_environment	docker-compose.yml	web
QUEUE_NAME	docker_compose_environment	docker-compose.yml	worker
TELEMETRY_ENDPOINT	docker_compose_environment	docker-compose.yml	telemetry
API_BASE_URL	env_file	.env.example	

Name	Source	File	Service
STRIPE_KEY	env_file	.env.example	
DATABASE_URL	env_file	.env.example	
FEATURE_TELEMETRY	env_file	.env.example	
OIDC_AUTHORITY	env_file	.env.example	
API_BASE_URL	variable_pattern	docker-compose.yml	
STRIPE_KEY	variable_pattern	docker-compose.yml	

Scanner Exclusions

Files intentionally excluded before local evidence summaries were generated.

Path	Source	Pattern
.env.local	default_sensitive_exclude	.env.local
secrets/runtime.env	default_sensitive_exclude	secrets/**

External Endpoints

Term	File	Line	Context
https://	.env.example	1	API_BASE_URL=https://api.vendor.example/v2
https://	.env.example	5	OIDC_AUTHORITY=https://login.microsoftonline.com/demo-tenant/v2.0
https://	config/app.yml	2	issuer: https://login.microsoftonline.com/demo-tenant/v2.0
https://	config/app.yml	3	license_endpoint: https://license.vendor.example/check
https://	config/app.yml	4	telemetry: https://telemetry.vendor.example/collect
https://	docker-compose.yml	10	API_BASE_URL: ${API_BASE_URL:-https://api.vendor.example/v2}
https://	docker-compose.yml	19	TELEMETRY_ENDPOINT: https://telemetry.vendor.example/collect

SBOM Summary

Component	Version	Ecosystem	Licence
fastapi	0.115.14	pypi	unknown
pydantic-settings	2.10.1	pypi	unknown
requests	2.33.0	pypi	unknown
/home/arctic/cs-code-packagemanager/examples/demo-compose-app-v2/requirements.txt	not specified	file	unknown

Top Vulnerabilities

None detected.

Changed Components

Change	Component
Added	/home/arctic/cs-code-packagemanager/examples/demo-compose-app-v2/requirements.txt | | file
Added	pydantic-settings | 2.10.1 | pypi
Added	requests | 2.33.0 | pypi
Removed	/home/arctic/cs-code-packagemanager/examples/demo-compose-app-v1/requirements.txt | | file
Removed	requests | 2.32.3 | pypi

Integrity And Checksums

SHA-256 checksums cover generated metadata and scanner/report artefacts. Evidence exports and ZIP containers are excluded. Verify with: cscode checksums PACK_PATH --verify.

File	Category	Size	SHA-256
README.md	buyer-evidence	2287	ada3e4c104c6bc7dbee1e19a3d6b1b68b39ff6c4d2b4d4c40fc1c351536d036e
environment-variables.json	metadata	2077	a72ca9691b850d3cf9da463e232eea6824ec945e79d105c0ded43da1c5d9e135

File	Category	Size	SHA-256
excluded-files.json	generated-artifact	627	1893424a12169aaf8c54879436e902475a9399ee7260d909c150b71c996c595f
excluded-files.md	generated-artifact	435	425ab5aa256ebd078a8d56a877ad6d0800ed52805e4c8288f006eae0004581a
external-endpoints.json	metadata	1437	5267f6a9df586de8f9ea62063b91e5b9ca3295e0a2e19f9dd914f15614eefefd
files-scanned.json	metadata	779	d9129c108ef54c96916911af41351397ba291eb53fd7cc25a70e30bf2c9eea3c
ports.json	metadata	122	95b9b4d6bd374386f2ab7b70671e7970a91a9eb327ccdfb54066d47da7c3d236
release-diff.json	buyer-evidence	2134	f32a70e1bf3e18b5e3b88afde04c659a629b1fd9c380cfc483512aae2865f3d8
release-diff.md	buyer-evidence	1866	919d193a74007e32f5fecc28a02ff3876a35d8ad8a70910bc5e2e3f62b6161be
release-manifest.json	metadata	1092	2ef25aa50c8dd515ccd07adae729c8de62b79d0d33225c4a9acdfc10d468891c
sbom/images/telemetry-alpine-3.20.cyclonedx.json	sbom	50939	395485e26b6c2edb10f37b5d85737a53c90139f4619189ae77556afb8accd365
sbom/images/worker-python-3.12-slim.cyclonedx.json	sbom	938347	2dfd90c1f05ea9a51f4ffb2b9e8b52aa0b780f23a0e053391bd89b768def33bb
sbom/sbom-summary.json	sbom	646944	20a6c7d7ee0dcecd88d89250e0e00a99f040922f87aa78ccf6fd5971d74e4e70
sbom/sbom.cyclonedx.json	sbom	6545	bc0fba562bd925338d417446f04263e16005f54b2ba949ff344e917050c36400
scan-summary.json	metadata	603	72761ff251e6122f3364d81cbdae1e9dbf0c0ac32ce2659089cb2565b7c02805
security/vulnerability-report.json	vulnerability-reporting	5687	946e8ecc44c03ba3cf0f9d927a31ce4790bbdc293939ee391e2fdc8fe911e4a4
security/vulnerability-summary.json	vulnerability-reporting	247	45d32d4437a31ca2baa8d30a8eba65758eb014bb681c6630ebd2b6de65d2a67
security/vulnerability-summary.md	vulnerability-reporting	138	b44d9f7e9f6f18b6a17bc267a46bbbc5dacad0e6bf0cf8787b25bb56e4d220e6
services.json	metadata	843	7949238a13cec146a62b98b4ed5b5deb6ab23895432b02585a3309485cec44c

Install Guide

- Confirm Docker Engine and Docker Compose are installed on the target host.

- Copy this release pack and the approved release artefacts to the restricted deployment environment.

- Load container images from the approved offline image bundle. Image bundle generation remains a customer-specific step in this MVP.

- Create or update the deployment `.env` file using the environment variable list in this pack.

- Run `docker compose up -d` from the approved release directory. Compose env files referenced: .env.example.

- Verify service health using the product health endpoint or the buyer-approved operational checklist.

Rollback Guide

- Stop the current release using the buyer-approved service stop procedure.

- Restore the previous approved release pack and deployment artefacts.

- Restore previous environment/configuration files from the approved backup.

- Load the previous container image bundle if images are not already available locally.

- Start the previous release with the approved Docker Compose command.

- Verify service health and record rollback approval notes.

Known Limitations

- Scanner results are limited to files available at scan time and the scanner tools/databases installed locally.

- External endpoint detection is conservative and flags potential references for review; it is not a network egress proof.

- Environment variable evidence lists names and sources, not secret values.

- Container image loading, operational health checks and site-specific deployment approvals must be attached by the vendor or buyer team.

Recommended Next Actions

- Review endpoint, environment variable and port changes with security/operations before deployment.

- Attach buyer-specific install, health-check and rollback evidence before formal acceptance.

- Record approval notes, exceptions and reviewer identity in the release workflow.

- Review newly added components for licence/security acceptability.

Generated Artefacts Appendix

Artefact
README.md
checksums.json
checksums.md
environment-variables.json
evidence-pack.html
evidence-pack.md
excluded-files.json
excluded-files.md
external-endpoints.json
files-scanned.json
ports.json
release-diff.json
release-diff.md
release-manifest.json
sbom/images/telemetry-alpine-3.20.cyclonedx.json
sbom/images/worker-python-3.12-slim.cyclonedx.json
sbom/sbom-summary.json
sbom/sbom.cyclonedx.json
scan-summary.json
security/vulnerability-report.json
security/vulnerability-summary.json
security/vulnerability-summary.md
services.json