

Buyer Ready Packet

Aurora Command proof pack export (demo sample)

Generated: 2026-01-04

Classification: Demo sample

What this is

This packet is a demo sample of a buyer ready export used in security reviews. It focuses on clarity, citations, and fast verification.

How to use it

- Start with the question and answer set to see how claims map to evidence IDs.
- Use the evidence index to locate supporting artifacts quickly.
- Use the Trust Center for controlled sharing, watermarking, and access logs.

Scope (sample)

Product	Aurora Command
Export type	Buyer ready packet (demo sample)
Primary contact	security@auroracommand.ai
Review focus	Identity, encryption, monitoring, incident readiness

Reviewer reality

Reviewers do not want a story. They want proof they can validate quickly.

- Every claim should have a citation.
- Every citation should point to evidence with a capture date.
- If evidence is stale, call it out and show a refresh plan.

Question and answer set (sample)

Question	Answer (sample)	Evidence ID
Do you enforce MFA?	Yes. MFA is required for privileged access and strongly encouraged for all users.	IAM-001
Is data encrypted at rest?	Yes. Stored data is encrypted at rest. See architecture overview for the model.	ENC-002
Do you have centralized logging?	Yes. Security relevant events are logged and alerting is configured for critical events.	LOG-003
Do you run tabletop exercises?	Yes. Tabletop exercises are performed on a defined cadence and action items are tracked.	IR-004

Where the evidence lives

Each evidence ID maps to an artifact in the binder export or a Trust Center document.

Evidence index (sample)

Evidence IDs make it easy to validate claims and keep follow ups scoped.

Evidence ID	Artifact	Location	Captured	Expires
IAM-001	User roster export	Binder export	2026-01-02	2026-04-02
ENC-002	Encryption configuration summary	Architecture_Overview.pdf	2026-01-01	2026-07-01
LOG-003	Alert routing summary	Binder export	2025-12-29	2026-03-29
IR-004	Tabletop after action report	Tabletop_AAR.pdf	2025-12-05	2026-12-05

Next steps

- If you need additional artifacts, request access through the Trust Center.
- For time sensitive reviews, ask for a deal room link with an expiration date.

Buyer-ready packet appendix (sample)

How reviewers can validate quickly • Generated 2026-01-04

How to use this packet

Start with the index and citations. Reviewers can validate claims by following evidence IDs to exports and timestamps. When a question is sensitive, access can be gated under agreement rather than emailed as an attachment.

What makes evidence defensible

Every artifact should have an ID, capture date, scope notes, and a refresh cadence. Prefer exports/logs from systems of record over screenshots. When something is missing, document it as an owned exception with a target date.

How to request follow-ups

Reply with the question IDs or evidence IDs you need. We provide deltas (new IDs) rather than resending full attachment sets, so the reviewer always looks at one current packet.

Scope and boundaries (sample)

What is covered vs excluded • Generated 2026-01-04

In scope

Aurora Command production environment and the systems used to operate and secure it (identity, logging, CI/CD, ticketing, monitoring).

Identity scope

Workforce identity controls are in scope. Customer authentication may be customer-managed depending on deployment; scope is stated in each answer block to prevent over-claims.

Data scope

This sample uses sanitized data categories and avoids internal identifiers. Real packets should include a precise data inventory summary and retention/deletion overview.

Control coverage summary (sample)

What is covered now vs gated • Generated 2026-01-04

Identity and access

Covered: MFA enforcement (IAM-001), access reviews (IAM-002), privileged role inventory (IAM-003).

Logging and monitoring

Covered: retention configuration (LOG-001), alert routing summary (LOG-003), admin audit log excerpt (LOG-010, agreement-required).

Secure SDLC

Covered: branch protection rules (SDLC-001), deploy approvals evidence (SDLC-002).

Evidence index excerpt (sample)

Artifact IDs, freshness, and owners • Generated 2026-01-04

Index (excerpt)

IAM-001 MFA enforcement export (captured 2026-01-02; cadence quarterly). LOG-001 log retention configuration export (captured 2026-01-02; cadence quarterly). IR-001 incident response playbook (captured 2025-12-15; cadence annual). VND-001 subprocessor list (captured 2026-01-02; cadence quarterly).

Freshness

Reviewers follow up when evidence is stale. Make capture dates and cadence explicit in the index so the reviewer can trust what they are reading without a meeting.

Incident readiness snapshot (sample)

Exercises and follow-through • Evidence IDs: IR-004, IR-010

Tabletop cadence

Tabletop exercises are scheduled semiannually. Each session produces an after-action report (AAR) and remediation items with owners and due dates.

What we track

Decision ownership, communication cadence, evidence preservation, and follow-through. Gaps become remediation tasks that are tracked to closure with proof.

Example gap

Logging retention ownership was unclear. Owner assigned and a retention configuration export was added to the evidence binder (LOG-001).

Vendor and subprocessor transparency (sample)

Downstream risk management • Evidence IDs: VND-001, VND-010

Subprocessors

A current subprocessor list is shareable at early stages. It includes data categories and a review cadence (VND-001).

Vendor review trail

High-risk vendors are reviewed with a questionnaire, evidence index, and a recorded decision (approve/approve-with-conditions/reject). Conditions are time-boxed and tracked (VND-010).

Sharing model

Sensitive vendor reports can be gated behind agreement with time windows and access logs, rather than emailed as attachments.

Reviewer FAQ (sample)

Common follow-ups and how to handle them • Generated 2026-01-04

Do you have SOC 2 / pen test reports?

When available, these are typically agreement-required. Access is time-boxed and logged. The packet includes enough scope and evidence IDs for initial validation without the report.

How do we know evidence is current?

Every artifact is timestamped with a capture date and a refresh cadence. If something is stale, it is flagged and refreshed as a delta rather than silently replaced.

Can we get more detail on architecture?

Yes. A deeper engineering appendix can be gated for security reviewers. Sanitized exports and diagrams are preferred over narrative-only answers.

Answer format (sample)

A structure reviewers can verify • Generated 2026-01-04

1) Scope (always)

Start by stating what's in scope and what's excluded. If customer auth is customer-managed, say so. If a control applies only to workforce systems, say so.

2) Answer (short, precise)

Use 2–6 sentences. Avoid marketing language. Make each claim specific enough that proof exists (and is indexed).

3) Proof (required for claims)

List Evidence IDs and capture dates (e.g., IAM-010 captured 2026-01-02; LOG-010 captured 2026-01-03). If a report is agreement-required, cite the access instructions (SOC2-001).

Delta updates and versioning (sample)

How to reduce back-and-forth • Generated 2026-01-04

Ship one packet link

Send one packet link once. When follow-ups arrive, respond with deltas: new Evidence IDs and a short note (what changed, why, when captured).

Avoid attachment floods

Email attachments cause version drift (final_v7.pdf). Instead, publish a current index and append new evidence IDs over time.

Time-box follow-ups

If something is missing, log it as an owned exception with a target date (and compensating controls). Reviewers prefer an explicit plan over vague promises.

Redaction and sensitive info (sample)

Public-ready sharing without over-claims • Generated 2026-01-04

Prefer exports you can sanitize

Export from systems of record (IdP, logging platform, CI) and redact identifiers. Keep the control signal (what is enforced, for whom, and when) intact.

Use tiered sharing

Default to Public (safe), Gated (sensitive operational details), and Agreement-required (reports like SOC 2, pen test summaries). Log access and enforce time windows.

Keep scope explicit

When you redact, do not remove scope context. Reviewers need to know environment, time period, and ownership to trust evidence.

Evidence capture checklist (sample)

What to export for defensible proof • Generated 2026-01-04

Identity

Export MFA enforcement and privileged role membership (IAM-010, IAM-003). Capture access review records (IAM-002) with reviewer and result.

Logging and monitoring

Export retention configuration and an admin audit log excerpt (LOG-001, LOG-010). Include alert routing and escalation paths (LOG-003).

SDLC and change control

Export branch protection rules and deploy approval trails (SDLC-001, SDLC-002). Reviewers trust exports more than screenshots.