BUYER EVALUATION GUIDE

Questions worth asking before choosing a critical-event coordination platform.

Use this guide to compare products on operating clarity, governance and evidence rather than feature-count alone.

Incident command	Can the product show who owns the incident, response roles, open actions and current state without relying on chat history?
Shared facts	Can responders distinguish confirmed facts, open questions, proposals and evidence references?
Chronology	Does the incident record preserve a durable sequence of material changes rather than overwrite history?
Handover	Can one shift hand over current state, ownership and outstanding work without rebuilding context from scratch?
Governance	Does the product separate recommendation, approval and execution authority for consequential actions?
Identity and tenancy	Are organisation scope and application entitlement explicit, server-validated and fail-closed?
Communications	If notifications are offered, can the system distinguish sent, received, acknowledged and assistance-request states?
Resilience	What is actually proven about degraded operation, alternate channels, hosting regions and vendor dependencies?
Evidence and audit	What integrity, provenance and export evidence is available, and what legal/compliance claims are explicitly not being made?
Commercial proof	Can the vendor show the current product with synthetic or authorised data without relying on a slide-only demonstration?

How Criticl currently answers

Criticl currently focuses on the incident-command record: incident lifecycle, roles, chronology, follow-ups, linked playbooks, handovers and review. Production identity, shared governance, situational intelligence, reasoning and durable cross-system execution remain explicitly gated integration work.