

Radar AI Incident Management

When AI goes wrong, turn a cross-functional event into a structured response.

AI governance sets the rules. Security and monitoring help identify and reduce risk. But when an AI system contributes to an adverse event, organizations still need to understand what happened, coordinate the right teams, and maintain a clear record of the response. Radar AI Incident Management provides a purpose-built process for managing AI incidents consistently.

THE CHALLENGE & WHY NOW

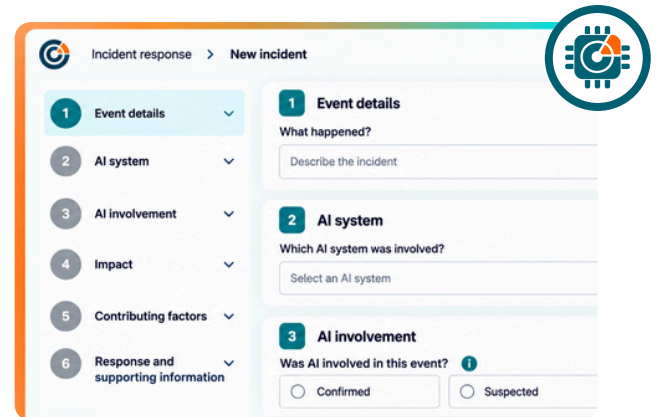
When something goes wrong, where does the incident go?

AI incidents don't fit neatly into traditional privacy, security, or compliance processes. They can quickly involve multiple teams, different types of harm, and evolving obligations.

Organizations need a consistent way to answer:

<i>What happened?</i>	<i>What was impacted?</i>
<i>Which AI system was involved?</i>	<i>Who owns the response?</i>
<i>How did AI contribute?</i>	<i>What actions were taken?</i>

Radar AI Incident Management gives teams one structured place to capture those answers and maintain the incident record.



PLATFORM CAPABILITIES & FEATURES



Dedicated AI Incident Process

Manage AI incidents as their own first-class category instead of forcing them into workflows built for something else.



AI-Specific Intake

Capture the AI system involved, your organization's relationship to it, incident context, impacts, and potential harms.



Investigation & Evidence

Document findings, supporting evidence, mitigation, and corrective actions in one place.



Cross-Functional Response

Bring privacy, legal, compliance, security, product, risk, and business teams together around a shared incident record.



Complete Documentation

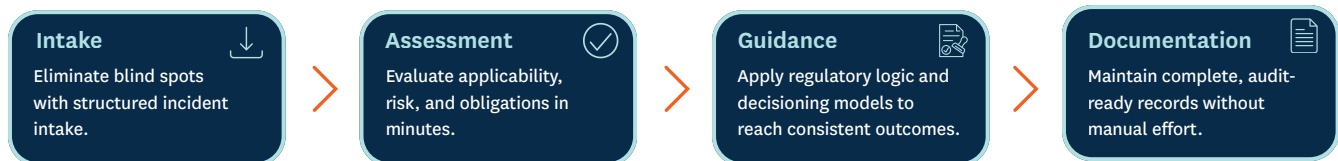
Maintain a consistent record of what happened, what was investigated, and what actions were taken.



Ready for What's Next

Establish a structured process now while AI regulations and industry practices continue to evolve.

THE APPROACH



COMMON AI INCIDENT SCENARIOS

Harmful Outputs

Inaccurate, misleading, or harmful AI-generated content or decisions.

Bias & Discrimination

AI behavior that creates unfair or discriminatory outcomes.

Sensitive Data

Exposure, misuse, or inappropriate processing of sensitive information.

Unexpected AI Actions

Autonomous or unintended actions outside expected boundaries.

Policy & Control Failures

AI operating outside organizational policies, guardrails, or approved use.

WHY RADARFIRST

For more than a decade, RadarFirst has helped leading organizations operationalize complex incident and regulatory decisions through structured, repeatable, and defensible processes. Radar AI Incident Management extends that proven approach to a new category of incidents purpose-built for AI.