

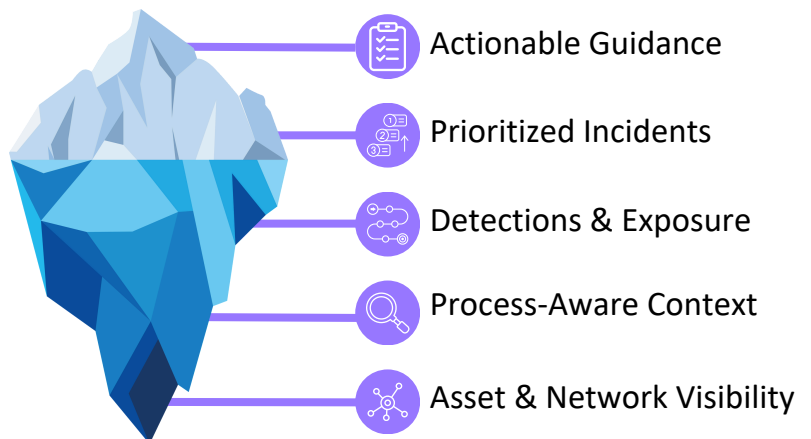
# When Every Alert Needs Investigation, You Need to Know Where to Start

**Security analysts are on the hook for OT threats, but most platforms weren't built for that job. SageOne is.**

Security teams are expected to monitor and respond to OT threats with the same speed and clarity they apply in IT. But most of the tools they're given weren't built for OT systems, assets, or workflows. Instead of visibility, they get noise. Instead of answers, more dashboards. Analysts are left triaging alerts with too little context and too much guesswork.

## The Real-World Problem

Analysts get the alerts, but they can't see what they're tied to—asset inventories are incomplete, event logs are disconnected from real activity on the floor, and when it's time to investigate, they're forced to either pull in OT teams manually or piece together a story from general-purpose tools. Either way, response slows and risk lingers.



## Why It Matters

### Alert Fatigue

When teams can't verify what's real or where to begin, alerts pile up, response slows, and trust in the system erodes.

### Increased Risk

The longer an incident or vulnerability remains unaddressed without context, the more it spreads or, worse, it gets missed entirely.

### Leadership Pressure

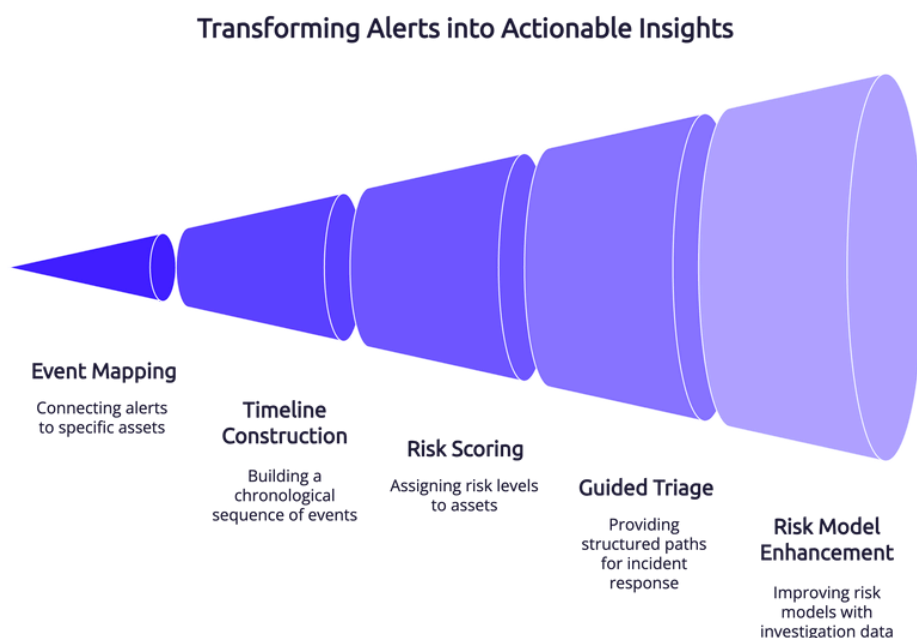
Security leaders want faster decisions. Analysts want clearer data. And no one wants another tool that adds more questions than it answers.

## | The SageOne Approach

SageOne transforms raw alerts into actionable information. It maps events to the assets involved, builds a timeline of what happened, and shows how the threat unfolded—all in one view. You get asset-specific risk scoring and guided triage paths, without having to jump between tools or tabs.

Instead of managing alerts, you're investigating incidents. Instead of wondering where to start, you already have the context. That's what gets issues resolved, not just logged.

From Analyst to Governance: Every investigation feeds SageOne's risk model, so security leaders don't just see incidents, they see how risk is evolving across assets and sites

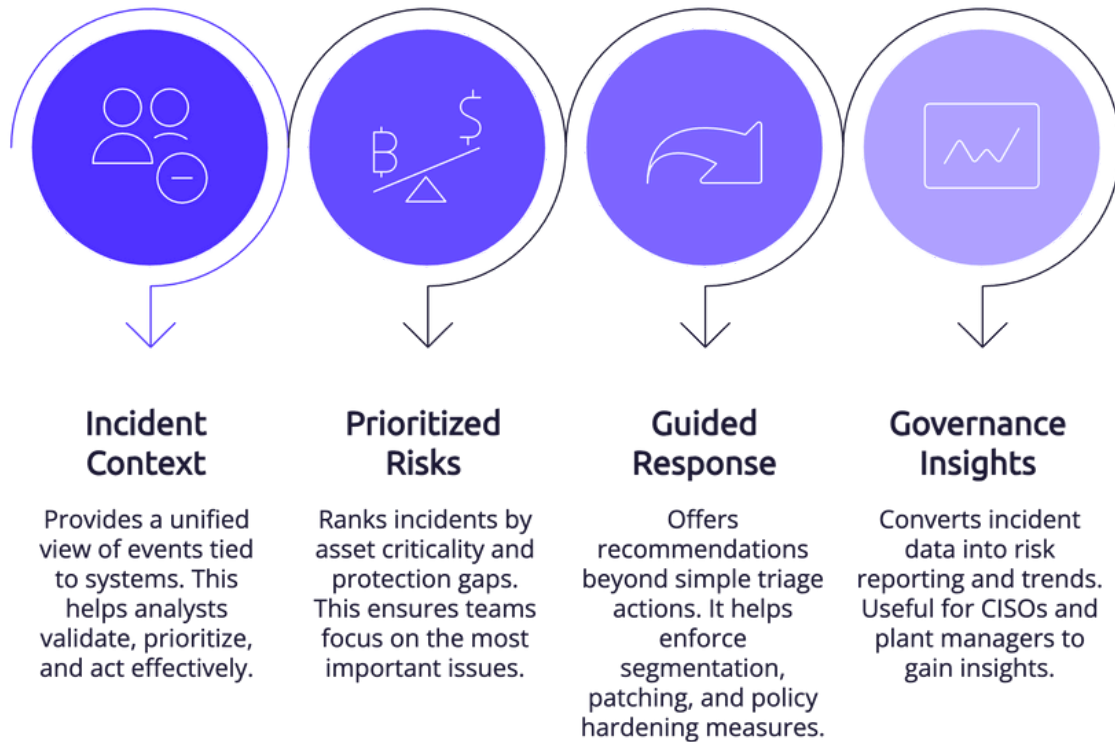


## | More Than Just Triage

SageOne helps analysts move faster but it also helps them work smarter. It reduces alert fatigue by connecting signals to the assets that matter. It adds trust to the data passed between IT and OT teams. And it supports structured triage across sites without forcing teams to learn another complex platform. That means fewer false starts, less back-and-forth, and more time spent solving the issues that count.

By connecting alerts to asset-level risk, SageOne builds trust between SOC analysts, OT engineers, and security leaders — everyone works from the same source of truth.

## What Makes SageOne Different



## Take the Next Step

SageOne gives security analysts the visibility and context to investigate OT threats faster, but that's only part of the story. See how the platform also supports other critical roles and challenges across your OT environment:

- [Secure Without Disrupting](#): How site teams reduce risk without triggering reboots or downtime.
- [Protect Legacy Systems](#): How engineers can defend aging assets, without changing how they work.
- [Full Technical Overview](#): SageOne's architecture, deployment model, and key capabilities.

→ [Explore SageOne](#)

→ [Contact Us](#)