RAPID7

THE 6 CORE USE CASES OF INCIDENT COMMAND

How security teams discover, investigate, contain, and neutralize threats with clarity and speed.

Legacy SIEM tools are expensive, have limited visibility, and are noisy. They create operational silos and lead to slow responses to fast-moving threats. With a next-gen SIEM backbone powered by AI, Rapid7's Incident Command unifies data, threat context, exposure management, and AI triage to help security teams see everything, understand what matters, and act with confidence. Oh, and it's *fast*.

Incident Command breaks down into six critical actions that, when taken together, allow SOC team members to take the strongest command of their attack surface possible.

VISUALIZE

See your entire environment in one view. No blind spots, no silos.

- Unify asset, risk, and telemetry data, regardless of its source
- Eliminate blind spots with native Attack Surface Management (ASM)
- Build continuous, comprehensive awareness of known and unknown assets

Legacy SIEM offers only partial visibility and fragmented tools built in silos. Incident Command quickly locates unknown or misconfigured assets before and after they become attack vectors.

DETECT

Cut through an ocean of noise. Surface real threats and waste no time.

- Reduce alert noise with behavioral analytics and user behavior analytics (UBA)
- Highlight stealthy activity with continuously updated MITRE ATT&CK-mapped detections
- Personalize to your environment with highly adaptable detection-as-code workflows

Legacy SIEM is unadaptable and full of noise. Incident Command lets you catch threats legacy SIEMs miss completely.

IDENTIFY

Know what threats matter and why. Make smarter decisions quickly.

- Accelerate alert classification confidently with AI-powered triage
- Understand the business impact with exposure context and threat enrichment
- Focus on high-risk alerts that could cause material damage to your organization

Legacy SIEM is slow to triage and offers limited threat and business context. Incident Command gets rid of benign alerts with 99.93% accuracy and provides real threat and business context.

INVESTIGATE

Accelerate investigations with full context. Understand the whole attack.

- Correlate evidence across your whole environment to see the entire attack timeline
- Links related events and recommends next steps with AI-assisted investigation
- Make analysis fast and transparent through unified investigation timelines

Legacy SIEM requires manual correlation creating analyst bottlenecks and overload. Incident Command uses AI-assisted investigation to make the right connections fast.

CONTAIN

Stop attacker movement in minutes, not hours. Prevent further damage.

- Save precious seconds by triggering response actions directly from the platform
- Consistently prevent threat movement with automated playbooks and SOAR workflows
- Stop the next attack earlier with preserved forensic evidence via DFIR capabilities

Containing attackers with a legacy SIEM is a slow and manual process. Incident Command's automated and AI-assisted containment immediately puts the brakes on attacks.

RESPOND

Fast, consistent remediation. Move from response to resilience.

- React fast, predictably, and aligned to your hierarchy of risk
- Respond consistently with built-in playbooks and integrated ticketing and AI workflows
- Refine your team's detection logic and response strategies with analyst feedback loops

Legacy SIEMs are slow, manual operations with limited DFIR capabilities. Incident Command lets you respond fast, consistently, and improves itself with each iteration.

WITH INCIDENT COMMAND:

SEE EVERYTHING → DETECT EARLIER → INVESTIGATE SMARTER → RESPOND WITH CONFIDENCE

EXPLORE HOW RAPID7 HELPS YOU STAY AHEAD →

RAPID7