RAPID7 VS SUMO LOGIC

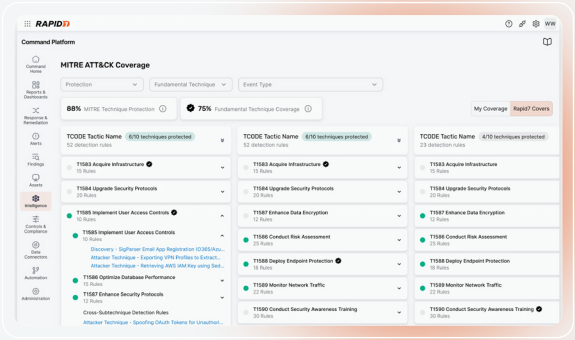
Turn Complete Visibility Into Stronger Protection, Faster Response, and Fewer Blind Spots.

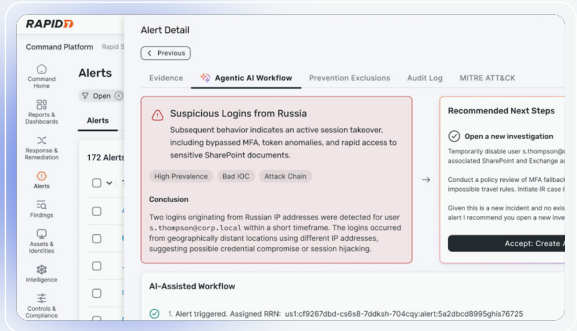
While Sumo Logic offers a cloud-native SIEM with log analytics and scalability, it often leaves teams with gaps in detection, automation, and risk management. This is due to a significant lack of core features such as restricted Security Orchestration, Automation, and Response (SOAR) functionality in lower-tier plans, inadequate reporting and export options, difficulties with data aggregation, filtering, visualization, and a steep learning curve with a less intuitive interface.

Rapid7 Incident Command closes those gaps with unified visibility, native automation, and actionable threat intelligence — empowering SOCs with the context and tools needed to accelerate every investigation. For teams who want more than just log storage and dashboards, Rapid7 delivers a truly holistic platform for modern SOC operations.

Holistic Security, Not Just Logs

Rapid7 Incident Command combines logs, assets, cloud telemetry, advanced investigation and automation, and adversary context into one platform for a complete picture. Sumo Logic can perform log ingestion and search, but its SIEM is limited when it comes to exposure visibility, Attack Surface Management, and integrated threat intelligence.



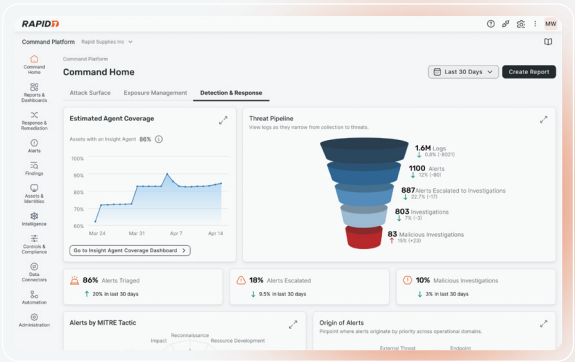


Analyst-Friendly AI and Automation

Unlike Sumo Logic's reliance on manual tuning and limited UBA, Incident Command delivers out-of-the-box UBA/ABA detections, AI-powered log search, automated triage, and AI-driven workflows all proven by thousands of customers in the Rapid7 SOC — accelerating investigations from day one.

Faster Time-to-Value and Higher Satisfaction

Rapid7 earns consistently higher marks for ease of deployment, intuitive workflows, and customer support — helping SOCs realize value faster. Sumo Logic's steep learning curve and complex queries often slow adoption.



It's Not Just About Checking More Boxes, But We Do Anyway

USE CASE / FEATURE	DETAILS	RAPID7	SUMO LOGIC
Cloud-Native Scalability	Scalable SaaS architecture that effortlessly scales with growing data and environments.	✓	✓
Strong UBA Capabilities	Combines user behavior analytics with AI-driven anomaly detection to surface risky activity in real time.	✓	Limited Customizability
Vast Integration Library	Hundreds of out-of-the-box connectors across security, IT, and cloud.	✓	✓
AI-Powered Log Search	Use natural language to accelerate investigations with faster insights and no complex language learning curve.	✓	✓
AI Triage & Agentic AI Workflows	AI alert triage and agentic workflows reduce analyst workload and accelerate investigations.	✓	X
Attack Surface Management	Continuous internal and external asset visibility to eliminate blind spots.	✓	X
Remediation Hub	Automatically prioritize various risk signals across hybrid environments and get suggested remediation actions.	✓	X
Detection Library Mapped to MITRE ATT&CK®	Rich library of prebuilt detections mapped to the MITRE ATT&CK framework.	✓	✓
Integrated Threat Intelligence	Native enrichment from threat intelligence for real-time and vetted attacker, campaign, and IOC context.	✓	Limited
Integrated SOAR	Built in automation and orchestration playbooks	✓	X
Deception Technology	Native deception tools lure adversaries and accelerate investigations.	✓	X
DFIR & Remote Remediation	Integrated digital forensics and endpoint interrogation tooling with malicious artifact clean up.	✓	X

Driving Real-World Customer Impact

A consulting firm providing IT services to a diverse client base needed to modernize its security operations. Their team managed vulnerabilities and incidents across multiple environments but struggled with manual workflows, limited real-time visibility, and siloed tools. To protect both internal systems and client projects, they sought a solution that could centralize detection and streamline vulnerability management to provide actionable insights without adding operational overhead.

Challenges Faced:

- **Manual Vulnerability Management:** Security processes were heavily manual, making it difficult to manage vulnerabilities efficiently across client projects.
- **Lack of real-time detection:** Without continuous monitoring, threats could go undetected during nights, weekends, or vacations.
- **Complex security stack:** The firm needed a platform that could integrate easily with existing tools to streamline both incident response and vulnerability management.

Benefits of the Rapid7 Solution:

- **Enhanced visibility & behavioral insights:** The SIEM's timeline capability gave the team rich insights into user activity without requiring deep manual investigation.
- **Smoother deployment & integration:** Deployment was simple and fast, with seamless integration into existing technologies (e.g., Cisco Meraki, Microsoft 365) and consolidated reporting in one interface.
- **Time savings for the team:** Automation delivered by the SIEM and vulnerability management platform saved the team around four hours weekly, freeing them for higher-value work.
- **Improved security posture:** Continuous monitoring and automated alerting enabled faster detection and response, strengthening the security of both the firm and its clients.
- **Real-time threat intelligence:** With access to up-to-date vulnerability and zero-day threat guidance, the team could patch faster and stay ahead of emerging risks.

"The automation provided by the SIEM and the accompanying platform saves me at least four hours per week, allowing my team to focus on strategic tasks rather than manual data gathering and analysis." — Director of IT, Consulting Firm

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.