Siemplify vs Resilient an IBM Company

Fast, Comprehensive Threat Investigations. No Add-ons Required

Having an investigation disrupted due to the lack of a capability is frustrating. Even worse is when the ability exists in the product but requires an additional license. Security teams face more than enough challenges daily, the last thing they need is to worry if their SOAR product will allow them to access all its capabilities. Siemplify delivers a fully-enabled threat-centric SOAR platform that will never slow down an investigation. With built-in automated alert grouping and a robust library of response actions included, analysts will fly through cases like never before. See how Siemplify and IBM Resilient stack up on these critical capabilities.

Capability	Siemplify	Resilient	Considerations
Integrations	180 + integrations available	100+ integrations available	Integrations drive SOAR capabilities, ensure your security stack products are supported and those integrations can be freely used
SOAR Approach	Threat-centric	Alert orchestration	SOAR solution must address key challenge in the SOC, too many alerts
Intended User	Designed for analysts of all skill levels, with built-in capabilities aimed at security engineers and architects	Designed for security engineers	Ensure the SOAR selected maps to your current and expected resources, no sense is deploying a solution that only a fraction of the team can use
Objective	Turning individual alerts into threat-centric cases comprised of multiple related alerts speeding investigations	Automate and orchestrate alerts	Alert overload is killing your SOC efficiency, choose a solution that addresses this problem first and foremost
Playbooks and Automation	Flexible and easily customizable playbooks with thousands of actions from hundreds of products available, no coding required	Playbooks will require security engineer configuration as well as add-ons to enable certain capabilities	Understanding your capabilities to build and manage playbooks should significantly influence your SOAR selection.
Collaboration and Crisis Management	Streamline the tactical and strategic responses to a successful attack ensuring all stakeholders inside and outside the SOC are working as a team.	Disaster recovery add-on available for additional license	Compromises are stressful times for organizations, having one "source of truth" for all response actions will eliminate confusion and missteps
Machine Learning Use	Used to aid prioritizing cases, assigning analysts, investigations, and case tagging	Use of machine learning is not clearly definable	Machine learning, when combined with SOAR, drives improvements across the SOC
Metrics and Reporting	Track and analyze a wide range of SOC KPIs across people, process and technology	Alert-based reporting available	With real-time SOC analytics, SOC managers can make data-informed eliminating ambiguity
Pricing	Per-user pricing, no limitations on actions, playbooks, or integrations	Sold on a subscription or perpetual basis with additional licenses required for add-ons	Cost concerns ideally should not influence the investigation process