Siemplify vs splunk> phantom

Go Beyond Automation for Faster Investigations

Anyone can provide security automation.Siemplify is the only SOAR provider that groups related alerts into threat-centric cases automatically, eliminating time-consuming, redundant, and efficiency-draining alert-based investigations once and for all. The result: comprehensive investigations with less effort. See how Siemplify and Splunk Phantom stack up on other critical capabilities below.

Capability	Siemplify	splunk> phantom	Considerations
Integrations	180 + integrations available	220+ integrations available	Integrations drive SOAR capabilities, ensure your security stack products are supported and those integrations can be freely used
SOAR Approach	Threat-centric	Automation-Focused	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 focused on automation	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 processes	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	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.	Crisis management not included in the solution	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	Machine learning not included in the product	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	Priced per action executed	Cost concerns ideally should not influence the investigation process