Siemplify

10 Must-Ask Questions

When Choosing a SOAR Solution

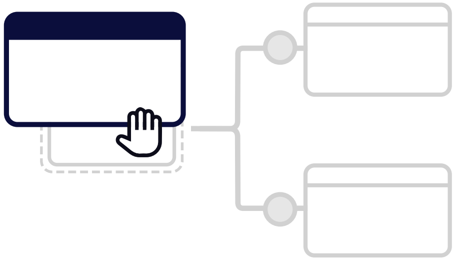
Security orchestration, automation and response (SOAR) platforms address the toughest security operations challenges, provide the basis for a cohesive security ecosystem and enable better response to the growing onslaught of cyber threats.

With an increasing number of SOAR solutions in the market, each with a different approach, here are the 10 questions you should ask when selecting the best SOAR platform for your organization.

1 Does the SOAR platform integrate with my existing security solutions?

WHY IT MATTERS

A good SOAR solution should provide out-of-the-box connectivity for most of the security and IT tools you have already invested in. Ensure the SOAR vendor has a process for rapidly developing integrations for any new or custom technologies you may have.



2 Does the platform enable my analysts to build and customize playbooks?

WHY IT MATTERS

Playbooks create process consistency and predictability.

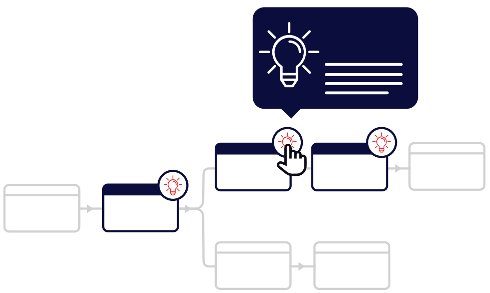
Ensure your SOAR solution makes it easy for analysts at every level - not just engineers - to customize standard playbooks and create new ones with an easy-to-use playbook builder that doesn't require coding abilities.

3 How do analysts investigate cases once a playbook stops running?

WHY IT MATTERS

Some cases can be fully automated using playbooks, but non-trivial cases typically require skilled analyst investigation after a playbook has run.

A good SOAR solution should provide clear, easy-to-use insights and a visual, interactive view of the event for analysts to take better, faster action, reduce dwell time and improve overall security.



4 How does the platform support SOC workflow and collaboration?

WHY IT MATTERS

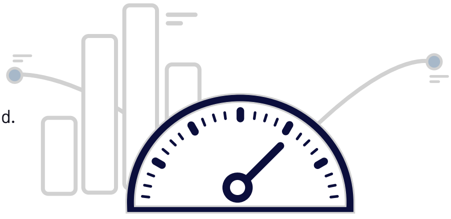
Most SOCs are 24x7 operations, with the need for seamless transition and communication between analysts to effectively handle cases. Your SOAR platform should streamline collaboration, facilitate smooth handoffs and escalations and provide the visibility needed by SOC management to keep tabs on day-to-day activity.

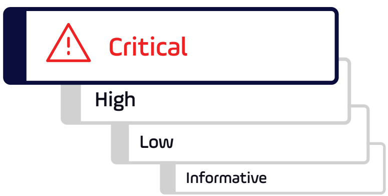
5 How does the platform help me track, measure and improve SOC performance?

WHY IT MATTERS

Reporting is a time-intensive exercise for most SOCs, even when KPIs are well-defined. Security operations teams must track their performance in real-time to understand incident detection and response effectiveness and create plans for continuous improvement.

Be sure your SOAR solution has customizable KPI dashboards and simple, automated reporting that can be tailored for various stakeholders.





6 How does the platform help analysts manage their workload?

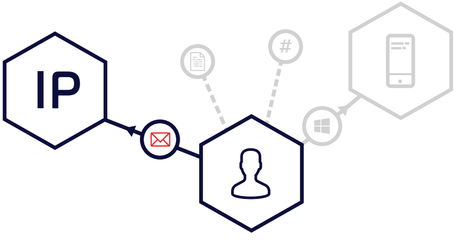
WHY IT MATTERS

Security operations teams must work smarter, not harder. A SOAR platform should not only correlate and consolidate alerts to reduce caseload, but it should also clearly prioritize cases based on criticality, assign cases based on past analyst performance and serve as the hub that analysts use to manage their workday.

7 Will the platform group related alerts?

WHY IT MATTERS

Alert overload is one of the biggest challenges faced by any SOC team today. The ideal SOAR platform must be able to correlate and combine related alerts from multiple tools to minimize false positives and give analysts the ability to address threats holistically with less effort.



8 What context does the platform provide on the different entities in the alert?

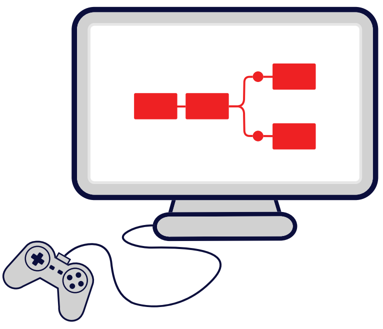
WHY IT MATTERS

Visibility and context are key for analysts to understand and take effective action against a threat. A SOAR solution that clearly shows the relationships between affected entities allows the SOC analysts to get a clear picture of an event and take decisive action quickly.

9 Can we run simulations in the platform to test the efficacy of playbooks?

WHY IT MATTERS

Playbooks are rarely one-and-done. You'll want to test and refine them to maximize their efficacy in responding to an incident. A SOAR solution should allow you to simulate alerts and test your playbooks to continuously improve your incident response processes.



10 Is the pricing model predictable?

WHY IT MATTERS

Pricing models vary, with some solutions basing costs on the number of actions or automations conducted within the platform. Look for solutions with per analyst or per seat pricing that enables your organization to effectively understand and manage annual spend.

siemplify.co 877.487.7222

Siemplify