SWIMLANE

11 questions to ask

when evaluating security orchestration, automation and response (SOAR)

(and how your vendor should answer)

1

Does the platform offer customizable reporting and visualizations?

A SOAR platform should give you the ability to quickly and easily report on any data in whatever format is most applicable.

2

Can dashboard be created to present key performance indicators?

A SOAR solution should give you unlimited ability to create and modify dashboards to display data to fit your needs.

3

Does the platform have built-in case management?

Case management should be more than just a repository. Individual case records should be fully interactive, automatically adapting to show the data you need.

4

How is the platform licensed?

Licensing costs should be predictable and shouldn't increase as you add new integrations or use cases.

5

Does the platform have HA/DR capabilities?

Your SOAR platform should be able to scale to fit any environment and be configured with high availability and disaster recovery capabilities.

6

Does the platform support multi-tenancy?

Strong data segregation is crucial. Your SOAR platform should offer flexible and reliable multi-tenancy options to meet your requirements.

7

Does the solution support role-based access control?

Strong role-based access control should be a necessity to ensure only authorized staff access sensitive data.

8

What is the process for building playbooks and workflows?

Your SOAR solution should have a drag-and-drop UI for building and modifying playbooks without getting bogged down by scripting.

9

Can workflows be customized to your business processes?

A robust workflow builder should work with custom code as well as out-of-the-box content to allow for adaptation to any organizational environment.

10

Is your SOAR content shareable?

All content, including dashboards, reports, case management layouts, playbooks, workflows and integrations should be easily shared and modified.

11

Can actions be triggered both manually and/or automatically?

For certain incident response processes manual steps are required. Your SOAR platform should make manual steps fast and simple, with one-click execution.

swimlane.com