

# 2020 Gartner Market Guide for Security Orchestration, Automation and Response (SOAR) Solutions

The security technology market, in general, is in a state of overload, with pressure on budgets, staff shortages and too many point solutions. Customers often cite problems with an overload of events or alerts, complexity and duplication of tools. As a general practice, automation promises to solve many of these problems and, in cybersecurity, SOAR is the primary vehicle for this functionality.

Gartner defines security orchestration, automation and response (SOAR) as solutions that combine incident response, orchestration and automation, and threat intelligence (TI) management capabilities in a single platform. SOAR tools are also used to document and implement processes (aka playbooks, workflows and processes); support security incident management; and apply machine-based assistance to human security analysts and operators. Workflows can be orchestrated via integrations with other technologies, and automated to achieve desired outcomes, such as:

- Incident triage
- Incident response
- TI curation and management
- Compliance monitoring and management