SOAR Maturity Model

	1	2	3	4	5
Typical Customizations	Out-of-the-box (OOB) playbooks with minimal changes	OOB playbooks adapted to the environment	Mix of OOB and simple custom playbooks	Customized and custom playbooks	Complex custom playbooks
Typical Actions & Responsess	Inform humans	Open tickets; use SOAR as ticketing system	Open tickets with recommended actions; limited automation	Act automatically in many case	Act automatically at scale
Typical Playbook Types	Enrichment playbooks	Simple playbooks, such as for phishing	Automated alert triage playbooks	Playbooks with a mix of automated and human actions	Full-auto playbooks that resolve issues automatically; manual playbooks remain where necessary
Typical Metrics	No formal metrics	Few manually defined metrics	Mix of manual and automated metrics	Mostly automated metrics	Metrics are automated and improved at scale
Automation Coverage	<10% of SOC use cases are touched by automation	10-30% of SOC use cases are touched by automation	30-70% of SOC use cases are touched by or resolved by automation	70-80% of SOC use cases are touched by or resolved by automation	90%+ of SOC use cases are touched by or resolved by automation
Typical Related Security Processes	Adapt a vendor playbook; connect data sources	Playbook customization; more device integration	Playbook content management and refinement; new and action integrations	Playbook creation, refinement and optimization; custom device integration	Robust development and refinement process for playbooks; feedback loops to improve

Google Cloud