Siemplify

SOLUTION BRIEF

Playbook Lifecycle Management

Design, develop, simulate and deploy playbooks that turn your SOC into a well-oiled detection and response machine.

Challenge

As your security operations center (SOC) broadens implementation of SOAR technology, you may be finding that the playbooks that interact with the many technologies in your environment are failing to complete successfully, resulting in analysts having to intervene manually to complete investigations. Further, your team may be spending more time applying updates to playbooks to account for changes in your environment as they occur. Unfortunately, many SOAR technologies did not anticipate this challenge and require individual playbook updates. And if your SOC requires a wide variety of playbooks, the time required for these updates can add up quickly.

Solution Overview

Siemplify is the first SOAR provider to introduce Playbook Lifecycle Management, which is the practice of designing, developing, simulating and confidently deploying accurate playbooks into a SOAR production environment. Playbook Lifecycle Management allows SOC teams to develop advanced playbooks from start to finish based on a foundation of knowledge of existing processes.

Implementation focuses on extensive playbook simulations and analyst training to ensure confident deployment and fewer misconfigurations. Once implemented, it provides detailed analytics on playbook effectiveness in real-time, enabling your SOC managers, engineers and architects to understand where to focus improvement efforts.

Platform Capabilities

for Playbook Lifecycle Management

The following features within the Siemplify Security Operations Platform fully enable and simplify Playbook Lifecyle Management:

- ✓ **Playbook Designer**
- ✓ **Triggers**
- ✓ **Actions**
- ✓ **Blocks**
- ✓ **Simulator**
- ✓ **Monitoring**
- ✓ **Analytics**
- ✓ **Dashboards**

Security Operations Value

Drive Continuous Improvement

Effective Playbook Lifecycle Management results in positive operational outcomes via more accurate playbook deployments.

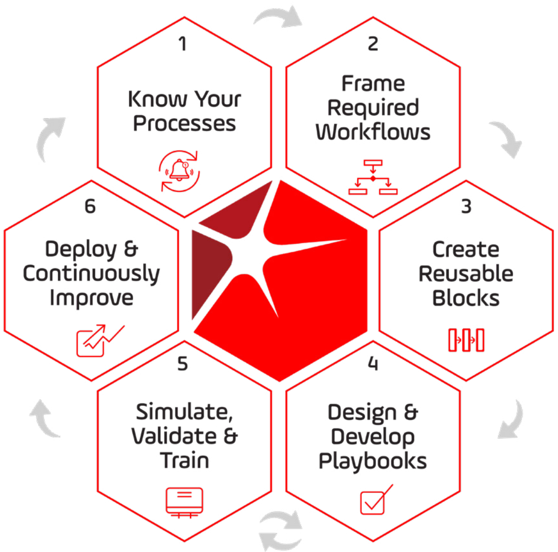
Slow Down to Speed Up

Fully automate the detection and response cycle with limited human involvement so that your SOC can operate at machine speed.

Reduce Analyst Fatigue

Reduce the number of manual intervention points to limit manual misconfiguration risk due to human error or SOC fatigue.

The Playbook Lifecycle


1
Know Your Processes
2
Frame Required Workflows
3
Create Reusable Blocks
4
Design & Develop Playbooks
5
Simulate, Validate & Train
6
Deploy & Continuously Improve

Playbook Lifecycle Management with Siemplify

1. Before Your Start - Know Your Processes

The first step of your automation journey is knowing which alert-types you are going to automate. For example, say you choose "multiple failed login attempts" as the alert-type, then you should gather at least 2-3 of your response workflow examples and note the similarities and differences across them. Explore and understand the events and components such as IP addresses, hostname/domains, file hashes, URLs and so on. This "homework" is foundational to developing any playbooks within Siemplify's SOAR platform.

2. Frame Required Workflow Steps

It's important to review each workflow step to define the actions needed. You can play around with these actions in a test case in Siemplify to be familiar with the way they work and their outputs. You should attempt to understand which entities are going to be affected, from where you are going to retrieve the needed information for input parameters, how you are going to extract that information, and what your expected results are.

Going through this exercise allows you to then categorize the different actions into logical groups of workflow stages such as:

- Triage and Investigation
- Decision and Escalation
- Remediation (or Response)
- Logging (Communication and Ticketing)

3. Create Blocks of Repeatable Workflows

Once you have an alert-type selected and a workflow framed, Siemplify enables you to make them repeatable by using our Blocks feature. Blocks define a set of actions as a self-sustained and independent unit for the reuse of logical steps. Blocks can be saved and used for future playbooks so while it requires some upfront effort it pays off later. A good example of a Block you can build is 'enrichment' as enrichment is the most common stage an alert goes through. With this Block in place, any future updates to your standard enrichment process can be made in one location to affect your broader automation processes.

4. Design & Develop Playbooks

Siemplify supports fast playbook development by using four main components - triggers, actions, flows and blocks. These components are easily dragged into a Playbook Designer area to create your playbooks. Your Playbook triggers are going to decide when to apply the playbook (e.g. on which alert-types). Playbook actions are self-explanatory but they do require some amount of manual configuration to take actions such as adding a comment to a ticketing system or quarantining an endpoint. Flows are logical conditions/branches that can be applied to a workflow at any given point (i.e. manual questions can be added such as "Do you want to quarantine the host?") Blocks, as described earlier, are nested playbooks that will allow you to drop in automated stages like an enrichment step that references your threat intelligence tools.

5. Simulate, Validate & Train Your Team

Siemplify's Playbook Simulator feature allows developers to test out playbooks by turning on a "simulation mode" switch. This lets you test any 3rd party tools under any set of conditions and instantly edit your workflow logic if it fails. The ability to author a step-by-step playbook helps you to execute and inspect its functionality and logic under different scenarios. This includes testing playbooks that include 3rd-party controls that you don't have access to or credentials for. The result is the ability to test playbook logic and behavior as well as train your analysts on building or editing playbooks without doing any damage to your production environment.

6. Deploy & Continuously Improve

As with any development cycle, whether coding a basic web page or a piece of software, there is an iterative process of continuous improvement. It is not different when developing playbooks in your security operations as there will always be room for improvement. However, the ability to test a playbook and quickly fix any logical errors using the Playbook Simulator is one way Siemplify speeds up this process. Once implemented, Siemplify also provides detailed monitoring and analytics on playbook effectiveness in real-time, enabling SOC managers, engineers and analysts to understand where to focus their improvement efforts.

Siemplify

About Siemplify

The Siemplify Security Operations Platform is an intuitive, holistic workbench that makes security operations smarter, more efficient and more effective. Siemplify combines security orchestration, automation and response (SOAR) with context-driven case management, investigation, and machine learning to make analysts more productive, security engineers more effective, and managers more informed about SOC performance.

Learn more at www.siemplify.co or follow us on Twitter at @Siemplify.

v1

Try it out for free at siemplify.co/community