Playbook Design Service

Let us refine and optimize your manual incident response processes into documented workflows and automated playbooks, so your SIEM can be utilized to its fullest extent, reducing your workload, and increasing your ROI on security controls.

/logpoint

What is Playbook Design Service?

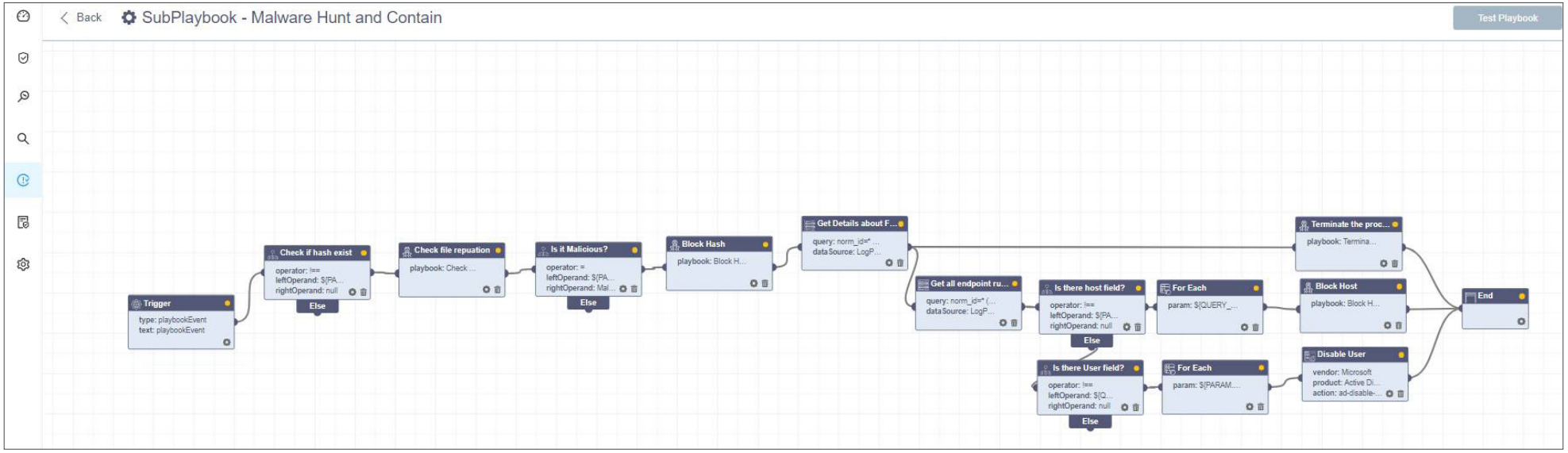
SOAR launches an automated investigation and response, and performs actions for any incident that has a pre-defined playbook.

Playbooks allow you to balance the amount of manual and automated work and free up your analysts' time to enable them to focus on what is important so that when a major threat arises you can be sure it will not go unnoticed.

SOAR can be complex to use, especially, when organizations lack specific expertise or resources in order to define and optimize their incident response processes.

Logpoint Playbook Design Service aids in transforming manual processes into automated playbooks individually tailored to each customer. Our service encompasses a complete playbook lifecycle, starting from understanding the company's needs and architecture, all the way to the creation, development and testing of the playbook, making sure it is ready to be launched in production.

In addition to creating playbooks for specific use cases, our experts can deliver playbook migrations and enhancements from 3rd party SOAR solutions, and options for custom-built processes.



Malware Hunt and Contain playbook

/logpoint

Why you need Playbook Design Service

Enabling SOAR for growing organizations

Deploying SOAR can be challenging even for experienced teams, however taking advantage of Playbook Design Service enables growing organizations to start using SOAR quickly and efficiently. Logpoint GS experts assist you with defining and optimizing incident response processes, transferring your manual processes into automation and orchestration to get the most out of your SIEM solution while reducing your workload and minimizing alert fatigue.

Playbook migration and continuous optimization

Our service ensures continuous support and enhancement of playbooks as well as biweekly meetings to accommodate new Use Case creation.

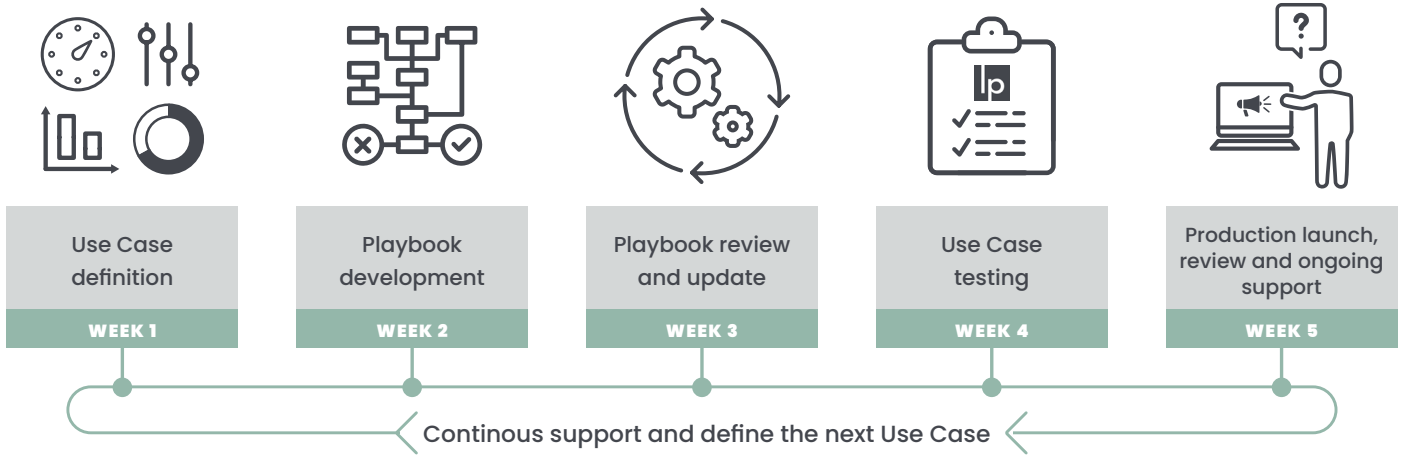
We constantly optimize your incident response processes. Furthermore, we provide migration of existing playbooks and automation of existing processes.

Four times faster, personalized process

Our service lifecycle is rapid and tailored to each customer. It takes approximately 4 weeks to define and create a Use Case up to launching it in production, followed by continuous optimization and testing.

Using Logpoint GS experts, with experience in designing, building and deploying playbooks, adds efficiency and order to the process, improving speed and precision.

Rapid and personalized service lifecycle



/logpoint

You're in the hands of experienced security researchers

Our Playbook Design Service is delivered by an experienced team of security experts specialized in different SOAR and SOC processes.

Our skilled team is experienced in recommending and building processes, along with assisting customers in creating automated playbooks.

Playbook Design Service is provided by the Logpoint Global Services team.

Logpoint provides two levels of service to match your needs

Deliverable	Basic	Advanced
Use Case definition	1× / month	1-2× / month
Documented playbooks and workflows	Yes	Yes
Product Actions (Rest APIs)	Publicly available products with RestAPI	Custom-defined products support
Playbook migration / optimization support	Yes	Yes
Custom-built Python scripts	No	Yes

For more information, contact Logpoint:
https://www.logpoint.com/en/contact/

APRIL 2022 01

/logpoint