New Page

> **i Информация:** Приведенная на данной странице информация, является разработкой команды pre-sales и/или AntiAPT Community и НЕ является официальной рекомендацией вендора.

Раздел 1. Что такое плейбук

1.1. ??? ????? ???????

При расследовании инцидентов аналитик SOC часто выполняет одни и те же действия: проверяет источник события, получает информацию об устройстве, запускает дополнительные проверки, изолирует хост или уведомляет ответственных сотрудников. Выполнение этих операций вручную занимает время и увеличивает вероятность ошибки.

Плейбук — это сценарий автоматизации, который позволяет системе самостоятельно выполнить заранее определенную последовательность действий при наступлении заданного события.

Проще говоря, плейбук можно представить как инструкцию:

> **«Если произошло определенное событие, последовательно выполни указанные действия и получи необходимый результат».**

Например, если в системе появился критический алерт, плейбук может:

1. определить устройство, на котором произошло событие;
2. получить сведения о пользователе;
3. изолировать устройство от сети;
4. запустить дополнительную проверку;
5. отправить уведомление ответственному специалисту.

В результате аналитик получает уже обработанный инцидент и может сосредоточиться на принятии решений, а не на выполнении однотипных операций.

1.2. ??? ??????? ??????????? ?? ???????? ????????

Отдельное действие выполняет только одну операцию:

- изолировать устройство;
- получить информацию о процессе;
- отправить уведомление.

Плейбук объединяет множество таких действий в единый алгоритм, где результат одного шага используется следующим.

Именно поэтому плейбуки являются одним из основных инструментов автоматизации реагирования в Kaspersky EDR Expert и OSMP.

????? ????? ????????

При расследовании инцидентов аналитик регулярно выполняет повторяющиеся действия: открывает карточку алерта, получает информацию об устройстве и пользователе, проверяет индикаторы компрометации, запускает дополнительные проверки, изолирует хост или отправляет уведомления.

По отдельности эти операции занимают немного времени, однако при большом количестве событий они превращаются в однообразную рутинную работу. Кроме того, выполнение одинаковых действий вручную увеличивает вероятность ошибки: можно пропустить важный шаг, выбрать неверный объект или просто забыть выполнить необходимую проверку.

Плейбуки позволяют автоматизировать такие сценарии. Вместо того чтобы выполнять каждое действие самостоятельно, аналитик описывает последовательность шагов один раз, после чего система воспроизводит ее при наступлении заданного условия.

Например, при обнаружении вредоносного процесса плейбук может автоматически:

- определить устройство, на котором произошло событие;
- получить информацию о пользователе;
- изолировать устройство от сети;

- запустить IOC Scan;
- отправить уведомление ответственному сотруднику.

В результате все типовые операции выполняются одинаково и без участия аналитика, а специалист может сосредоточиться на анализе инцидента и принятии решений.

????? ?????? ?????? ????????

Плейбуки не заменяют аналитика, а помогают автоматизировать повторяющиеся этапы реагирования. Их можно использовать для решения самых разных задач:

?????????????? ???????????

Выполнение заранее определенных действий сразу после появления алерта или инцидента.

Например:

- изоляция устройства;
- завершение вредоносного процесса;
- запуск дополнительной проверки;
- создание правила блокировки.

?????????? ??????????

Перед выполнением действий плейбук может собрать дополнительные сведения, необходимые для расследования:

- получить информацию об устройстве;
- определить пользователя;
- найти связанные алерты;
- извлечь хэш, IP-адрес или имя процесса.

???????? ???????

Плейбук способен анализировать данные и принимать решения на основе заданных условий.

Например:

- выполнить действия только для критических алертов;
- реагировать только на события определенного правила корреляции;

- запускаться только для устройств из конкретной группы.

??????????? ????????

Один плейбук может объединять несколько независимых операций в единый сценарий, где результат предыдущего шага используется следующим.

```
Получен алерт        |        ▼Получить HostID        |        ▼Получить информацию о
пользователе        |        ▼Изолировать устройство        |        ▼Запустить IOC
Scan        |        ▼Отправить уведомление
```

????? ????? ????????????? ????????

Плейбук имеет смысл создавать, если один и тот же набор действий регулярно выполняется по одинаковым правилам. Если сценарий требует постоянного участия аналитика и принятия решений на каждом этапе, автоматизация может оказаться избыточной.

Практика показывает, что лучше всего плейбуки подходят для стандартных процессов реагирования, обогащения данных и выполнения рутинных операций, позволяя сократить время обработки инцидентов и обеспечить единообразное выполнение действий независимо от того, кто занимается расследованием.

Revision #1
Created 23 June 2026 15:53:13 by Николай
Updated 23 June 2026 16:33:38 by Николай