Innostage Orchestrator

Общее описание

В рамках расследования и реагирования на инциденты ИБ аналитику Центра мониторинга информационной безопасности неоднократно приходится взаимодействовать с разного рода средствами и системами как ИБ, так и ИТ. Подобные однотипные задачи сильно замедляют процесс расследования и реагирования на инциденты ИБ, как в части переключения между различными консолями и интерфейсами, так и согласования действий по реагированию на инциденты ИБ с профильными отделами.

Решение Innostage Orchestrator позволяет автоматизировать типовые операции в части реагирования на инциденты ИБ и воздействия на ИТ-инфраструктуру посредством заранее подготовленных и согласованных с профильными отделами сценариев реагирования. Таким образом, Innostage Orchestrator позволяет автоматизировать типовые операции, которые ранее аналитики Центра мониторинга ИБ выполняли вручную, тем самым значительно сокращая время на сбор необходимых данных для принятия решений и реагирования на инциденты ИБ.

Стоит также отметить, что не все операции нужно автоматизировать полностью и решение позволяет останавливать процесс и ожидать дальнейших действий от оператора. Например, после автоматического сбора исходных данных по инциденту ИБ оператор проводит анализ их достаточности и только после этого принимает решение о необходимости воздействий на ИТ-инфраструктуру.

В Innostage Orchestrator реализован встроенный графический конструктор сценариев, который позволяет оператору самостоятельно формировать сложные, многоуровневые сценарии реагирования на инциденты ИБ и воздействий на ИТ-инфраструктуру, а также, при необходимости, разрабатывать собственные коннекторы к целевым ресурсам.

Схема («звезда»):

- Более 30 разработанных сценариев реагирования
- Встроенный графический конструктор сценариев
- Интеграция через API
- Управление ИТ-инфраструктурой из единого окна
- Не требует установки агентов
- Работа с индикаторами компрометации

Основные преимущества

К основным преимуществам решения Innostage Orchestrator можно отнести следующие возможности:

• запуск автоматизированных типовых сценариев реагирования в области ИБ\ИТ – выполнение блокирующих операций, внесение изменений в настройки безопасности средств защиты, компоненты ИТ-инфраструктуры, прикладные и автоматизированные системы, выполнение обновлений элементов ИТ-инфраструктуры;

• запуск типовых сценариев реагирования на инциденты ИБ и воздействий на ИТ-инфраструктуру по расписанию, предполагающих последовательность активных воздействий на ИТ-инфраструктуру, средства защиты информации (блокировок, отключений, изменений) и проверки индикаторов компрометации;

• наличие коннекторов к целевым ресурсам и более 30 сценариев реагирования из коробки для выполнения заданных Заказчиком сценариев реагирования на инциденты ИБ и воздействий на ИТ-инфраструктуру;

• наличие возможности группировки целевых ресурсов по группам и дальнейший их поиск тегам;

• наличие встроенного гибкого графического конструктора сложных, многоуровневых сценариев реагирования на инциденты ИБ и воздействий на ИТ-инфраструктуру;

• возможность формирования новых и корректировки существующих сценариев реагирования на инциденты ИБ и воздействий на ИТ-инфраструктуру;

• наличие встроенного редактора кода для разработки новых, используя имеющиеся шаблоны, коннекторов к целевым система для автоматизации реагирования на инциденты ИБ и воздействий на ИТ-инфраструктуру;

• наличие инструкции по созданию и тестированию коннекторов к целевым ресурсам для автоматизации реагирования на инциденты ИБ и воздействий на ИТ-инфраструктуру, которые могут быть созданы специалистами самостоятельно;

• наличие возможности тестировать разработанный коннектор для автоматизации реагирования на инциденты ИБ в рамках операций реагирования на инциденты ИБ и воздействий на ИТ-инфраструктуру;

• возможность интеграции с системами класса Incident Response Platform(IRP) и иными системами информационной безопасности в части автоматизации реагирования на типовые инциденты ИБ;

• реализация принципа сервисной изолированности – исключение хранения административных учетных записей в системах класса Incident Response Platform и иных системах ИБ. Защищенное\зашифрованное хранение административных учетных записей осуществляется в вынесенной системе Innostage Orchestrator с возможностью блокирования операций реагирования на отдельные элементы ИТ-инфраструктуры со стороны подразделений, эксплуатирующих ИТ-инфраструктуру;

• фиксация и хранение истории изменения и запусков операций реагирования на инциденты ИБ и воздействий на ИТ-инфраструктуру по итогам выполнения действий в средствах защиты информации и средствах управления ИТ-инфраструктурой.