



Как ускорить возврат инвестиций при внедрении SOAR?

Алексей Комаров,
Уральский центр систем безопасности

Деньги: экономическая отдача SOAR



Примером экономической отдачи SOAR может служить кейс реагирования на предполагаемые фишинговые письма*

Наименование	До внедрения SOAR	После внедрения SOAR	Ожидаемая экономия
Фишинговых писем в день	45	45	
Средняя почасовая заработная плата для аналитика уровня L1	\$37,11	\$37,11	
Время реагирования на одно письмо	90 минут	40 секунд	89 минут 20 секунд
Ежедневная стоимость обработки писем	\$ 2 504	\$ 18	\$ 2 486 в день
Ежегодная стоимость обработки писем	\$ 515 824	\$ 3 708	\$ 512 116 в год

* - Measuring the ROI of Security Orchestration and Response Solutions, Splunk, 2021

Что мы предлагаем?

Средство по автоматизации создания автоматических сценариев обнаружения и реагирования (автоматический playbook) на основе графов знаний по кибербезопасности

Для чего мы это предлагаем?



Трудности внедрения SOAR - сроки и стоимость:

- + Шаблонные автоматические сценарии обнаружения и реагирования (автоматический playbook) дают мало ценности и завязаны на экосистеме вендора
- + Экспертиза накапливается медленно, когда строится только на реальных кейсах
- + Разработка и поддержка playbook – длинный, итерационный процесс, в который вовлечены несколько участников
- + Внедрение и сопровождение SOAR требует участия специалистов высшей квалификации



Организации, внедряющие SOAR / **СОАРоСтроители**

- Организации, с применением SOAR оказывающие услуги по реагированию
- Организации, внедряющие SOAR как для собственного SOC, так и при использовании внешнего SOC



Организации, приобретающие аутсорсинговые услуги по реагированию / **СОАРоПользователи**



СОАРoСтроители

- Меньше затраты на внедрение SOAR
- Выше конкурентные преимущества → Больше Заказчиков → Больше денег



СОАРoПользователи

- Быстрее внедрение → Быстрее финансовая отдача
- Качественнее результат → Ниже ущерб
- Кастомизация в рамках стандартной услуги → Ниже стоимость услуги

Что это дает? Тоже деньги, но косвенно



Выше точность автоматического playbook → Ниже частота ложноположительных срабатываний → Больше событий обрабатываются теми же ресурсами



Лучше покрытие → Меньше поверхность атаки, не закрытой техниками обнаружения → Ниже риски



Меньше время создания автоматического playbook → Быстрее процесс обновления



Систематизация процесса построения автоматических playbook'ов → Выше информативность при выборе варианта действий → Быстрее обучается персонал SOC

Как мы это делаем? Коротко

Экспертная система поддерживает разработку автоматических playbook «на лету» (вплоть до режима реального времени – т.е. прямо в ходе развития инцидента) и основана на применении графов знаний в области кибербезопасности: MITRE D3FEND, OSSEM, STIX, графового представления репозиторий уязвимостей ПО.

Как мы это делаем? Подробнее



- Онтология ИБ описывает внешние (техники атак, защитные меры, уязвимости, IoC) и внутренние (активы, СрЗИ) знания по кибербезопасности
- На ее основе специальное ПО строит единое пространство состояний и решений, реализует алгоритм поиска путей в данном пространстве с учетом введенных ограничений
- Результатом работы этого ПО является сценарий (playbook) который может быть прочитан человеком и выполнен в SOAR
- Каждый из разработанных playbook опирается на унифицированный список скриптов (коннекторов)
- Скрипты работают в модели данных, заданной онтологией ИБ

Живой пример: фишинговая атака



**Анализ
фишингового
письма**



Подтверждение
тактики Initial Access

**Анализ
вложений**



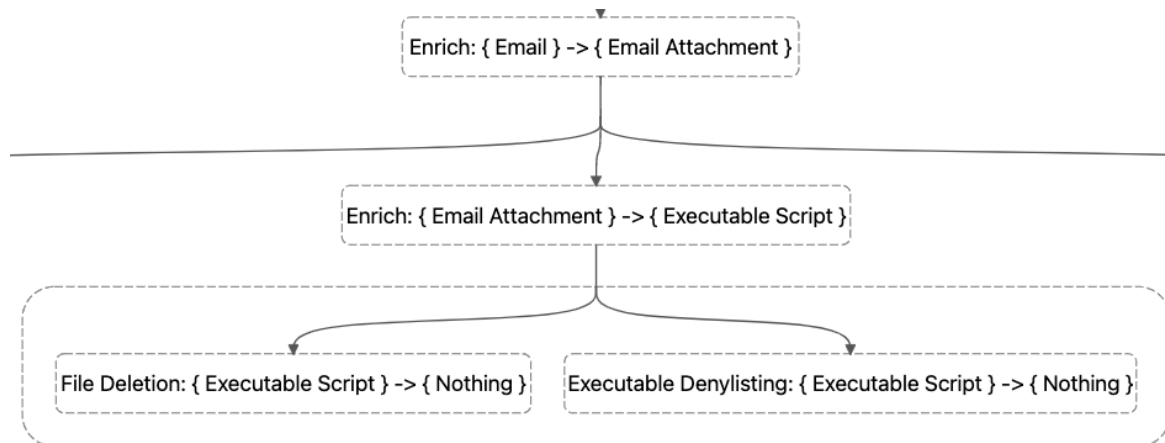
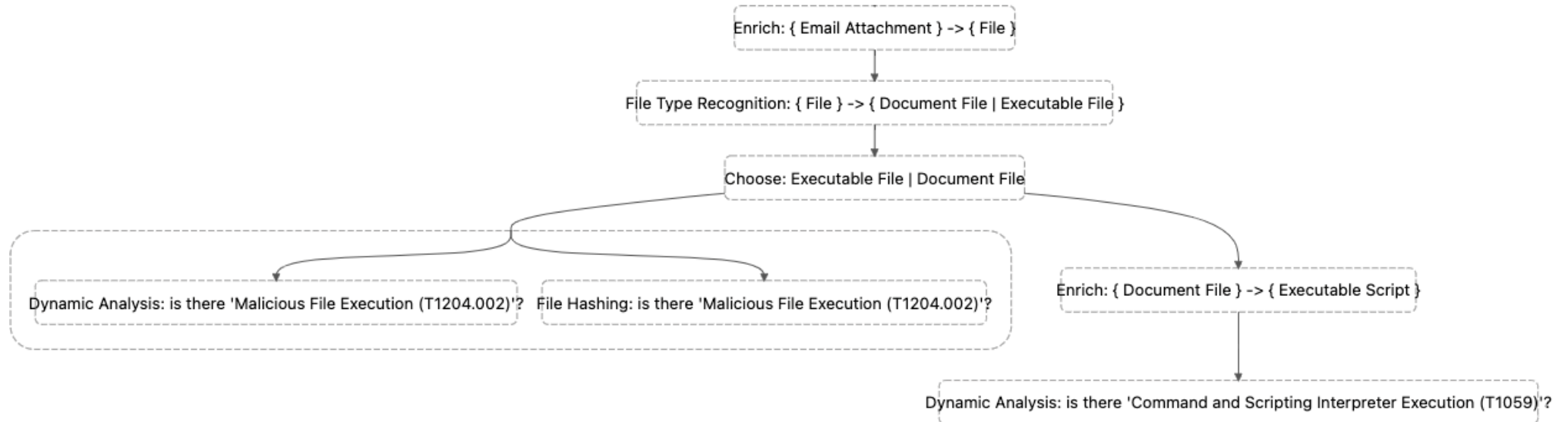
Подтверждение
тактики Persistence

**Реагирование на
фишинговое письмо**

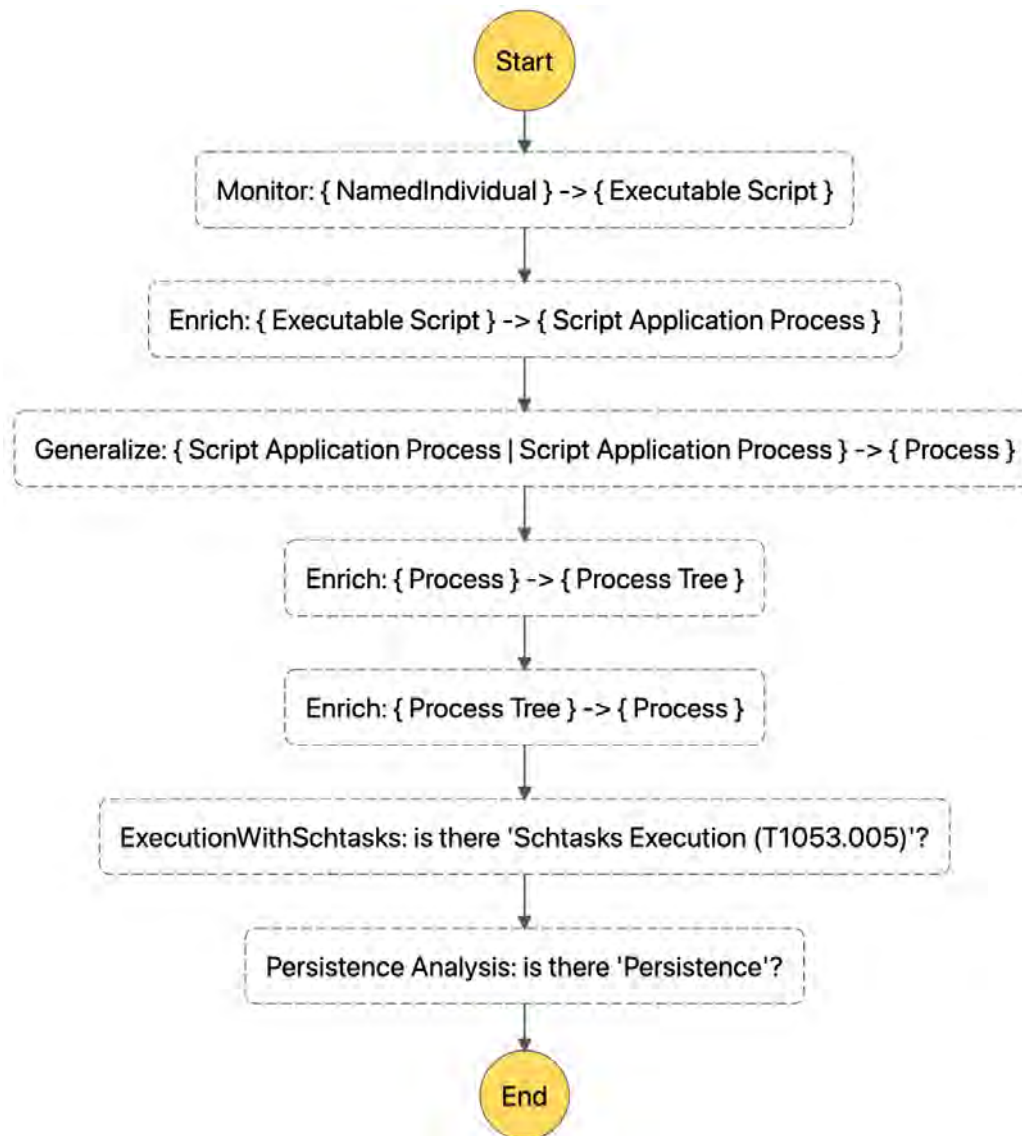


Блокировка атаки

Живой пример: плейбуки



Живой пример: плейбуки



Приглашение к сотрудничеству и контакты



Алексей Комаров

региональный представитель УЦСБ в Москве

akomarov@ussc.ru

УРАЛЬСКИЙ ЦЕНТР
СИСТЕМ БЕЗОПАСНОСТИ | **USSC.RU**