kaspersky

How-to-playbook:

пошаговое руководство по разработке сценариев реагирования

Игорь Таланкин

Старший инженер по информационной безопасности «Лаборатории Касперского»

Это заранее определенный набор действий для реагирования на конкретные типы инцидентов ИБ

Playbook = Incident response playbook = Сценарий реагирования

Какая цель достигается сценариями реагирования?

Экономия времени и ресурсов аналитиков

Систематизация и унификация процесса реагирования

Исключение фактора человеческой ошибки

Какие задачи необходимо решить

1. Автоматизация действий по реагированию на инциденты

2. Формализация сценариев реагирования на инциденты ИБ

Чем руководствоваться

ГОСТ Р59712-2022 — Управление Компьютерными Инцидентами

NIST — Computer Security Incident Handling Guide

ISO/IEC 27035 — Information security incident management

НКЦКИ Регламент взаимодействия

С чего начать?

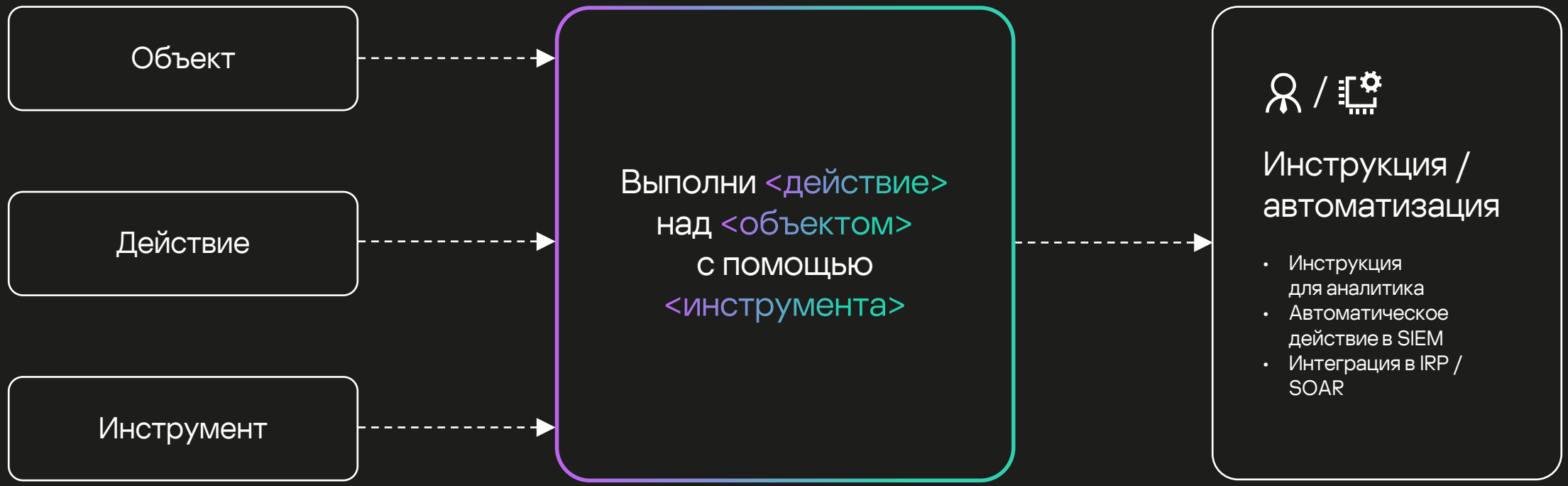
1 Определить роли в SOC, пути эскалации, способы взаимодействия с другими подразделениями и организациями

2 Определить основные фазы процесса реагирования и в чем они заключаются

3 Определить степени критичности инцидентов

4 Определить метрики эффективности процесса реагирования на инциденты

Все действия в плейбуках описываются одной формулой



Определяем объекты

Account

- Password
- Email
- Workstation
- Creation date
- Locked/unlocked
- Enabled/disabled

User

- Full name
- Division
- Department
- Phone number
- Manager
- Account

Host

- Hostname
- IP address
- Owner
- MAC address
- Administrator
- OS
- Software
- Vulnerabilities

Определяем объекты

Event log File, folder, registry key	• Name • Size • Permissions	• Last changed time • Hash • Reputation
Software	• Name • Vendor	• Version • Vulnerabilities
HTTP request	• URL • Domain • Method	• Headers • Body content • Bytes in/out

Определяем объекты

Email	• Sender/recipient • Subject	• Attachment
Network session	• Source • Destination • Protocol	• Duration • Bytes in/out
Process Scheduled task Service, daemon	• Name • Executable file • Arguments	• Creator/Owner • Creation time • Last change time

Определяем действия

restore confirm enrich check remove enable notify revoke bloc

block request explanation get logs report create search verify

isolate kill re-install terminate scan delete escalate disable restore confirm

Определяем инструменты

Network device

- Firewall
- Router, switch
- IDS/IPS
- Proxy server

Infrastructure service

- Active Directory
- DNS server
- Email server
- DBMS

Security system

- Antivirus
- Log management
- SIEM
- Sandbox
- EDR
- WAF
- Scanner

Application

- Web service
- Ticket system

Из чего состоит плейбук

Определяем автоматизации

Форматирование

- Разложить данные из события в поля инцидента
- Выбрать domain из url или email
- Выбрать все ссылки из тела письма

Обогащение

- Запросить данные из whois
- Сделать скриншот подозрительного URL
- Определить репутацию адреса, хеша и т.д.
- Определить ФИО сотрудника по имени пользователя

Получение дополнительной информации

- Скачать файл
- Получить письмо
- Сделать листинг директории
- Получить список запущенных процессов
- Получить содержимое ветки реестра
- Сделать memory dump процесса

Отправка уведомлений и запросов к пользователям

- Выбрать нужный шаблон письма и заполнить его
- Создать тикет с заполнением всех полей
- Отправить письмо

Блокировка

- Добавить адрес в лист SIEM
- Заблокировать адрес на firewall
- Добавить процесс к списку запрещенных на AB

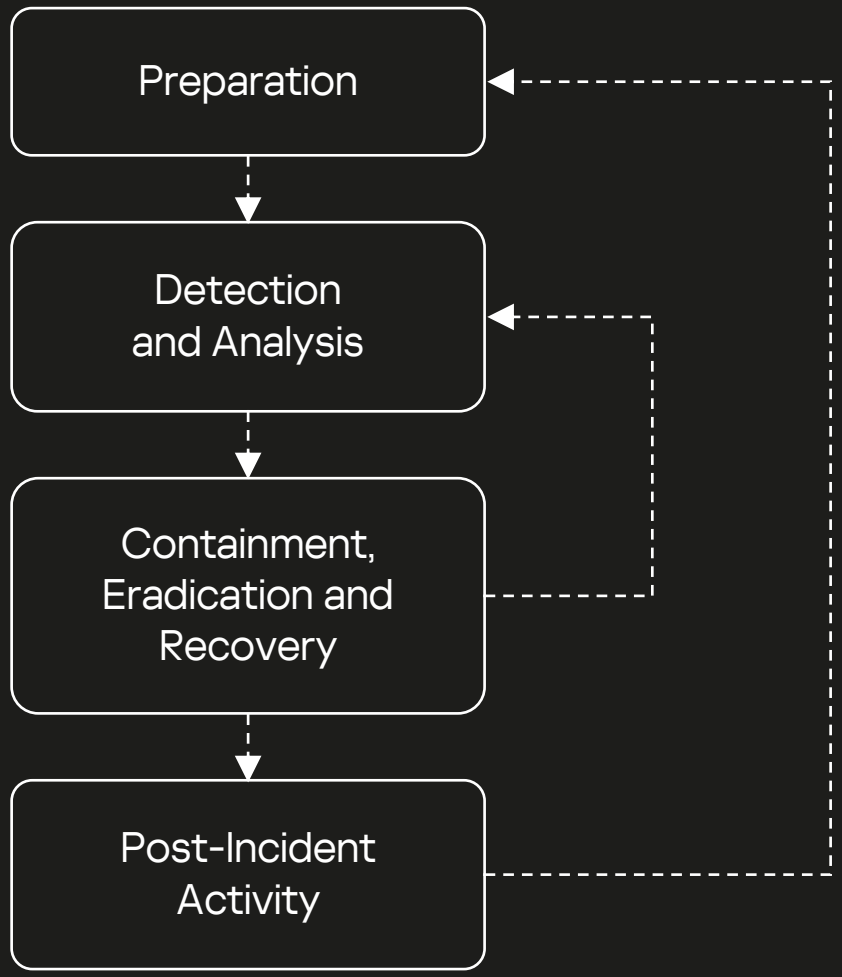
Удаление следов

- Удалить файл
- Изменить настройки системы
- Отозвать права пользователя
- Выполнить скрипт

Пример действий

Жизненный цикл инцидента

- Некоторые шаги могут быть пропущены
- Процесс реагирования может проходить нелинейно
- Стадии подготовки, детектирования и пост-инцидентной активности не реализуются в SOAR/IRP



Preparation

Подготовка необходимых доступов, ресурсов, ПО, контактной информации и т.д.

- Как описать подозрение на инцидент?
- Как взаимодействовать?
- Как производить анализ и расследование?
- Как автоматизировать?

- Формат карточки инцидентов, набор полей и их расположение
- Контактная информация для эскалации и взаимодействия с другими подразделениями или организациями
- Средства для коммуникации
- ПО для проведения расследования и анализа
- Доступ для команды SOC к системам, которые могут понадобиться при реагировании
- Автоматизация. Реализация интеграций, которые помогут выполнять рутинные действия

Detection

Обеспечение сбора телеметрии для анализа и выявления инцидентов

- Как обнаружить инцидент?

- Настройка аудита на источниках
- Настройка сбора и нормализации событий
- Настройка детектирующей логики
- Настройка получения актуальных индикаторов компрометации

Analysis. Documentation

Документирование алерта достаточного для последующего расследования

- Кто нарушитель?
- Кто жертва?
- Что произошло?
- Когда произошло?
- Детали инцидента

- Корректно разложить данные из алерта
- Определить нарушителя и жертву, субъект и объект: хост, аккаунт, email
- Определить что конкретно произошло?
- Зафиксировать дополнительные детали инцидента

- Карточка инцидента

Analysis. Triage

Первичная категоризация и приоритезация инцидентов

- Критичность?
- Тип инцидента?
- Достаточность данных?
- Есть ли похожие инциденты?
- Проверка на false positive

- Оценка потенциального влияния на защищаемую инфраструктуру и необходимость восстановления
- Определение типа инцидента, классификация по MITRE ATT&CK и kill chain
- Удостовериться, что полученных данных достаточно для последующего расследования
- Поиск связанных инцидентов
- Проверка соответствия инцидента логике детектирования

- Приоритет
- Классификация

Analysis. Investigation

Проведение расследования, сбор дополнительных данных, расширение зоны для анализа и определение причины

- Какие события связаны с подозрительной активностью?
- Что является индикаторами компрометации?
- Что мы знаем о затронутых активах?
- На сколько высок риск влияния на инфраструктуру?
- Вектор атаки?

- Поиск связанных событий для получения дополнительной информации о произошедшем
- Определение индикаторов таких как TTP, IP, URL, hostname, account, hash, filename
- Обогащение данными о затронутых активах для получения полной картины происходящего
- Зная затронутые активы и что именно произошло, можно определить риск влияния на доступность сервисов, целостность и конфиденциальность данных, а также, например, возможные репутационные риски

- Скоуп затронутых активов
- IOCs
- Вектор атаки

Analysis. Notification

Оповещение всех заинтересованных лиц

- Кого необходимо оповестить?
- Кто должен быть в курсе ситуации?

- Оповещение владельцев систем, ответственных за системы, руководителя дежурной смены в зависимости от критичности инцидента
- Отправка электронного письма, сообщения в мессенджере, звонок или создания тикета

- Уведомление

Containment

Обеспечить меры по сдерживанию, держать ситуацию под контролем

- Какие превентивные меры можно использовать?
- Какие системы можно использовать для сдерживания вредоносной активности?
- На сколько оправданы меры по сдерживанию, чтобы не нанести большего вреда?
- Кто может посодействовать в разрешении инцидента?

- Определить системы для сдерживания вредоносной активности
- Определить способы изолировать, отключить, заблокировать активы, чтобы предотвратить распространение
- Оценить потенциальный вред для бизнес процессов в случае выполнения превентивных мер
- Определить специалистов из смежных подразделений или сторонних организаций, кто может оказать содействие в более качественном реагировании на инцидент

- Выполнение сдерживающих действий без подтверждения
- Выполнение сдерживающих действий, которые требуют подтверждение аналитика

Eradication

Удалить все следы пребывания злоумышленника в инфраструктуре

- Какие следы вредоносной активности присутствуют в инфраструктуре?

- Удаление артефактов оставшихся после митигации инцидента
- Удаление созданных учетных записей, открытых доступов, созданных файлов и т.д.

- Следы пребывания злоумышленника удалены

Recovery

Восстановление работоспособности системы

- Все ли затронутые активы работают в штатном режиме?
- Какие изменения были внесено в рамках инцидента?
- Как мы можем восстановить работоспособность?

- Определить все ли затронутые системы находятся в работоспособном состоянии
- Откатить все изменения, которые были сделаны злоумышленником, а также в рамках этапа сдерживания инцидента
- В случае невозможности вернуть настройки к изначальному состоянию, необходимо восстановить систему из резервной копии или развернуть её с нуля

- Все системы работают в штатном режиме

Lesson learned

Работа над ошибками

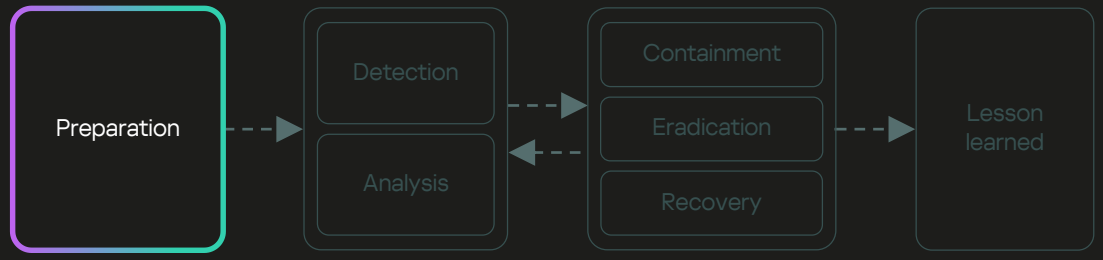
- Как предотвратить подобные инциденты в будущем?
- Как детектировать подобные IoC в будущем?
- Что необходимо внедрить, чтобы улучшить способность обнаружить и противостоять подобным атакам?
- Что нужно сделать иначе в случае повторного инцидента?
- Что было сделано неправильно в рамках реагирования?

- Обновить базу знаний по результатам реагирования на инцидент. Это поможет лучше влиться в процесс новым аналитикам или тем, кто не сталкивался с подобным ранее
- Внести изменения в механизмы обнаружения и предотвращения вторжений, чтобы исключить повторный инцидент в будущем
- Пересмотреть существующий сценарий реагирования и внести предложения по его улучшению

Создадим плейбук «Подозрение на фишинг»

Пришло подозрительное письмо и пользователь
отправил его на проверку в ИБ

Подозрение на фишинг



Preparation

Карточка инцидента

Observables: URL, File name, Email, Domain, Hash, IP address

Attacker: Email, Domain, IP address

Target: Email, Account, Full name, Manager, Department

Инструменты анализа

Доступ к SIEM

Доступ к Sandbox

Доступ к репутационным базам (TI service)

Наличие почтового клиента

Контакты

Сотрудник email – телефон

Администратор почтового сервера

Администратор proxy сервера

Наличие почты, телефона, мессенджера, тикет системы

Автоматизации

Анализ файла в Sandbox

Удаление письма с почтового сервера

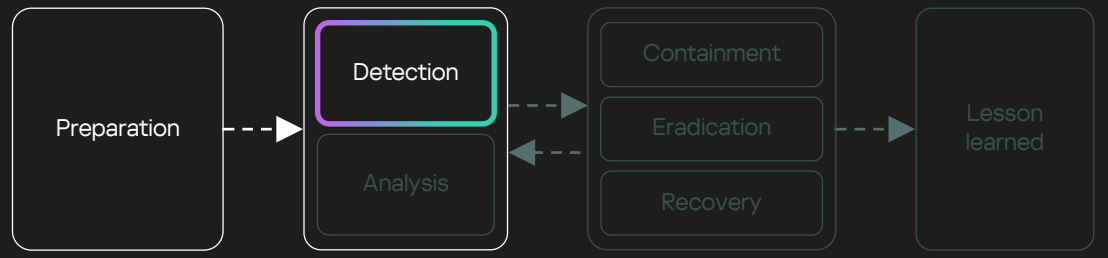
Создание тикета

Отправка письма пользователю по шаблону

* Preparation не является частью плейбука

** Preparation включает в себя много задач, которые не относятся непосредственно к реагированию. Этап стоит рассматривать как чек-лист

Подозрение на фишинг



Detection

Источник данных

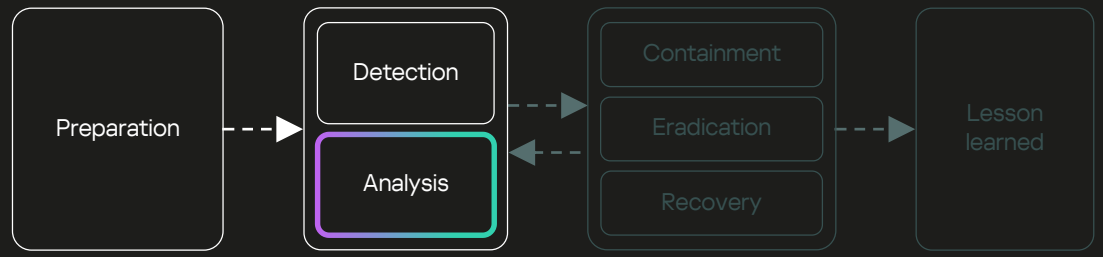
- Научить пользователей отправлять подозрительные письма на единую почту для проверки
- Настроить необходимое логирование

Логика детектирования

- Настройка правил корреляции

* Detection не является частью плейбука

Подозрение на фишинг



Analysis. Documentation

Письмо
от пользователя

Старт

Создание case

- Заполнение обязательных полей: дата, время, тип инцидента, название, ответственный

Анализ/парсинг письма

- Определение email отправителя и получателя
- Получение вложений
- Получение всех ссылок в теле письма

Прикрепление артефактов к case

- Прикрепить подозрительное письмо к case
- Прикрепить все вложения

Заполнение полей в карточке

- Заполнить все имеющиеся данные в карточку для атакующего и цели

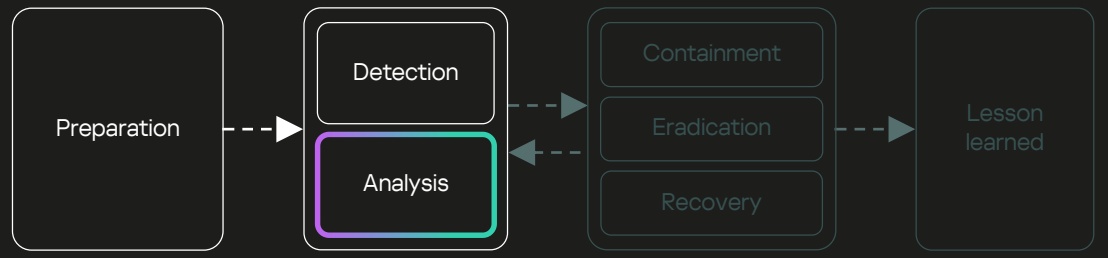
Alert от системы
детектирования

Старт

Создание case

- Заполнение обязательных полей: дата, время, тип инцидента, название, ответственный

Подозрение на фишинг



Analysis. Triage

Проверка корректности данных

- Проверить, что полученные данные действительно соответствуют возможному фишингу
- Проверить наличие минимально необходимых данных для дальнейшего расследования

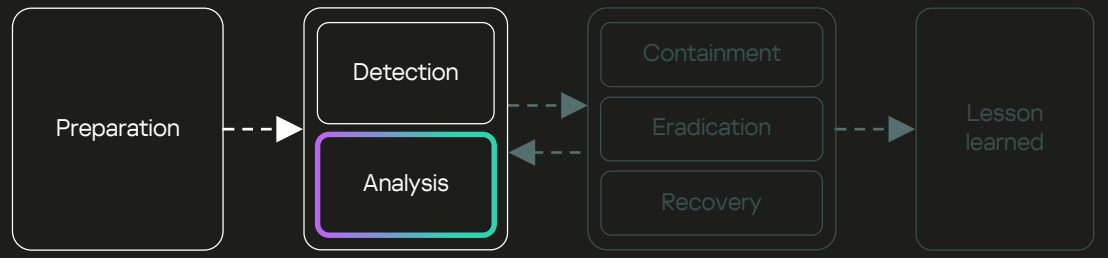
Приоритезация

- Попытаться определить приоритет исходя из полученных данных, чтобы поставить инцидент в очередь при большом потоке

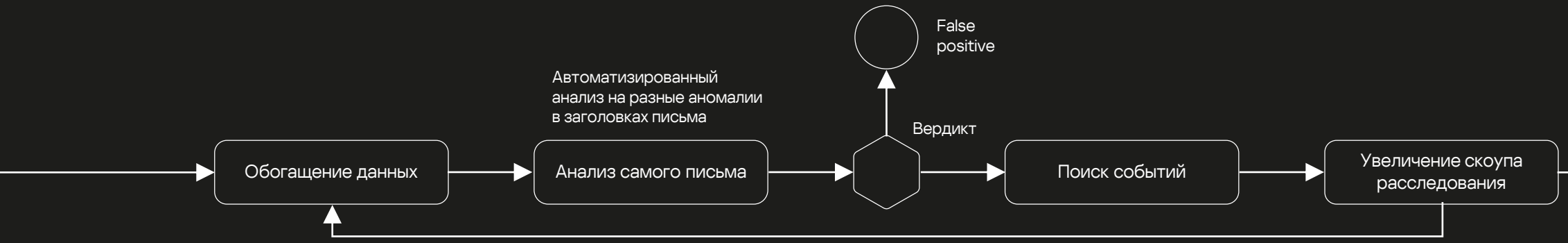
Категоризация

- Заполнить поля, отвечающие за категорию, тип, стадию атаки (kill chain) и т.п.

Подозрение на фишинг



Analysis. Investigation



Данные о жертве

AD: получить данные о пользователе, зная его email

HR: получить данные о сотруднике зная его email или account

CMDB: получить данные о рабочей станции пользователя

Данные об индикаторах

Kaspersky TIP: проверить наличие данных по индикаторам

Получить скриншот страниц по вложенным URL

Sandbox

Kaspersky Sandbox: проверить вердикт по вложениям в письмо

Поиск перехода по ссылкам

Поиск обращения перехода на подозрительный домен/URL

Поиск похожих писем

Поиск писем с этого же адреса/домена

Поиск писем с похожей темой

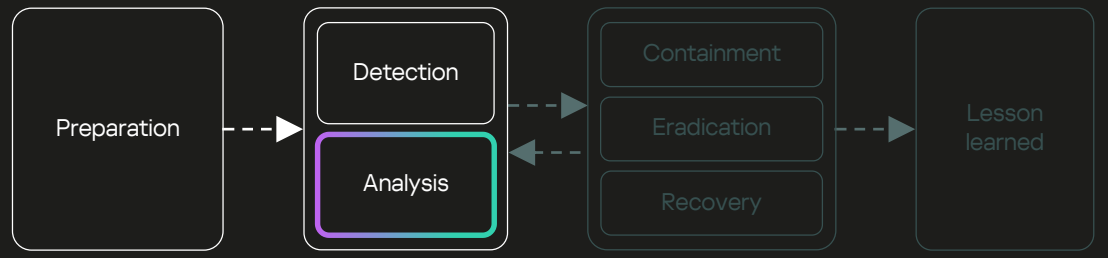
Поиск писем с похожим вложением

Поиск событий с вложением

Поиск событий с именем файла как у вложения

Углубленное расследование в случае обнаружения

Подозрение на фишинг



Analysis. Notification

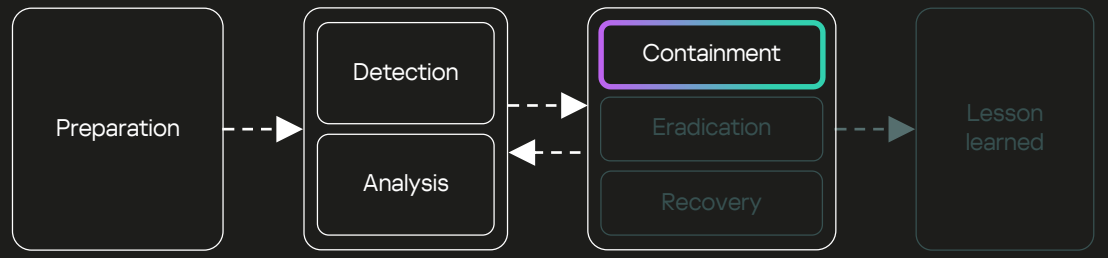
Оповещение цели

- Проверить, что полученные данные действительно соответствуют возможному фишингу

Эскалация на L2, L3, SOC Manager

- Заполнить поля, отвечающие за категорию, тип, стадию атаки (kill chain) и т.п.

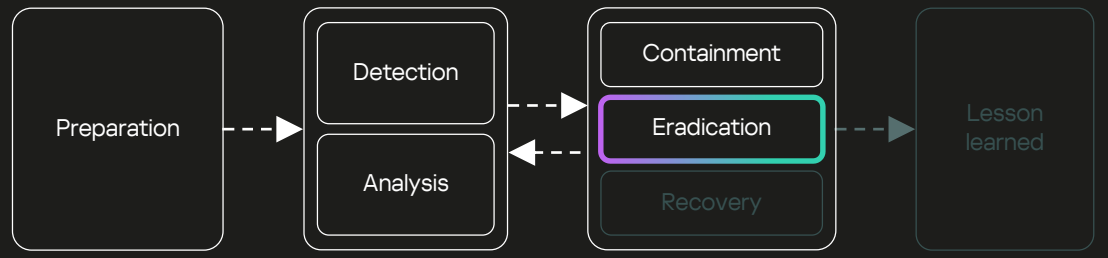
Подозрение на фишинг



Containment

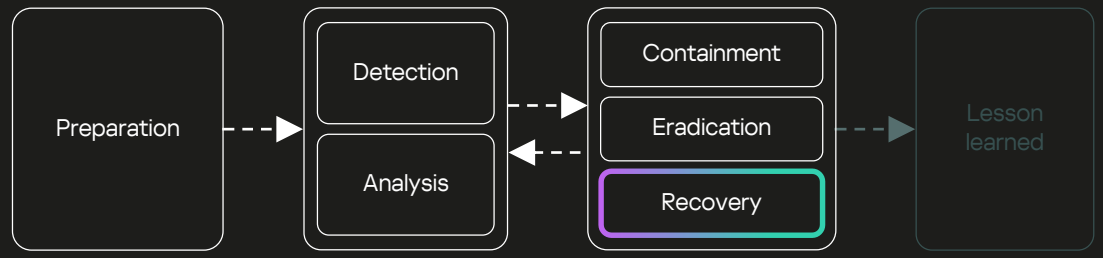
- Добавление URL в KWTS
- Добавление email в KSMG
- Добавление IoC в CyberTrace
- И т.д.

Подозрение на фишинг



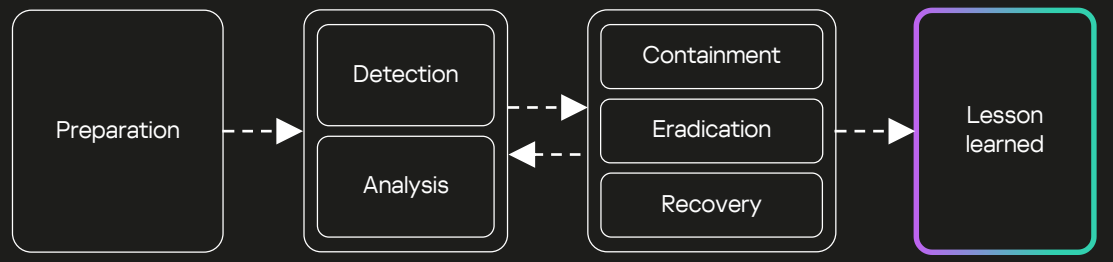
Eradication

Подозрение на фишинг

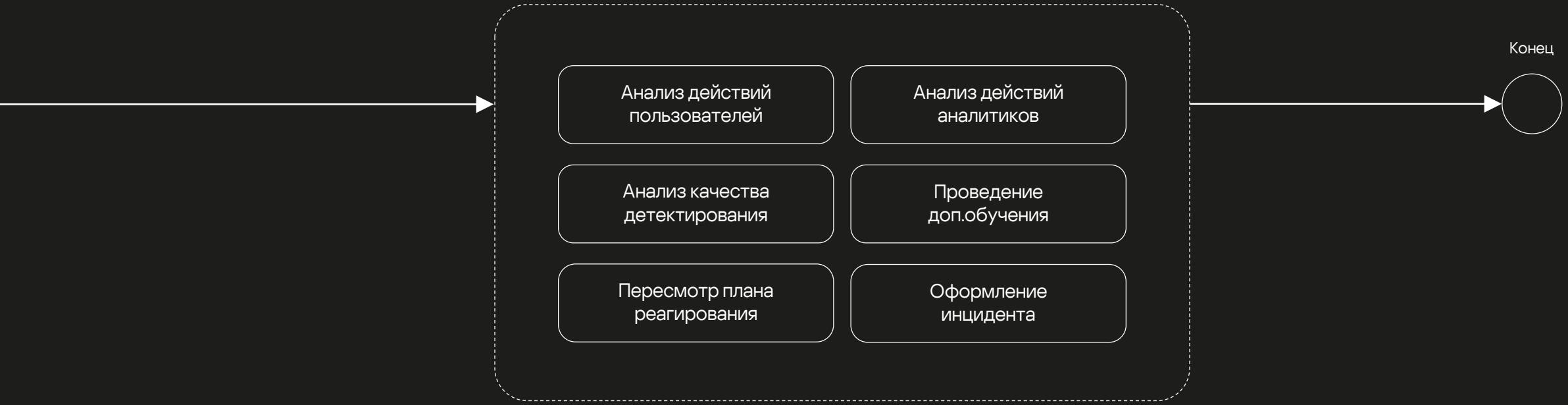


Recovery

Подозрение на фишинг



Lesson learned



Вопросы

Спасибо!