Утечки данных в Даркнете

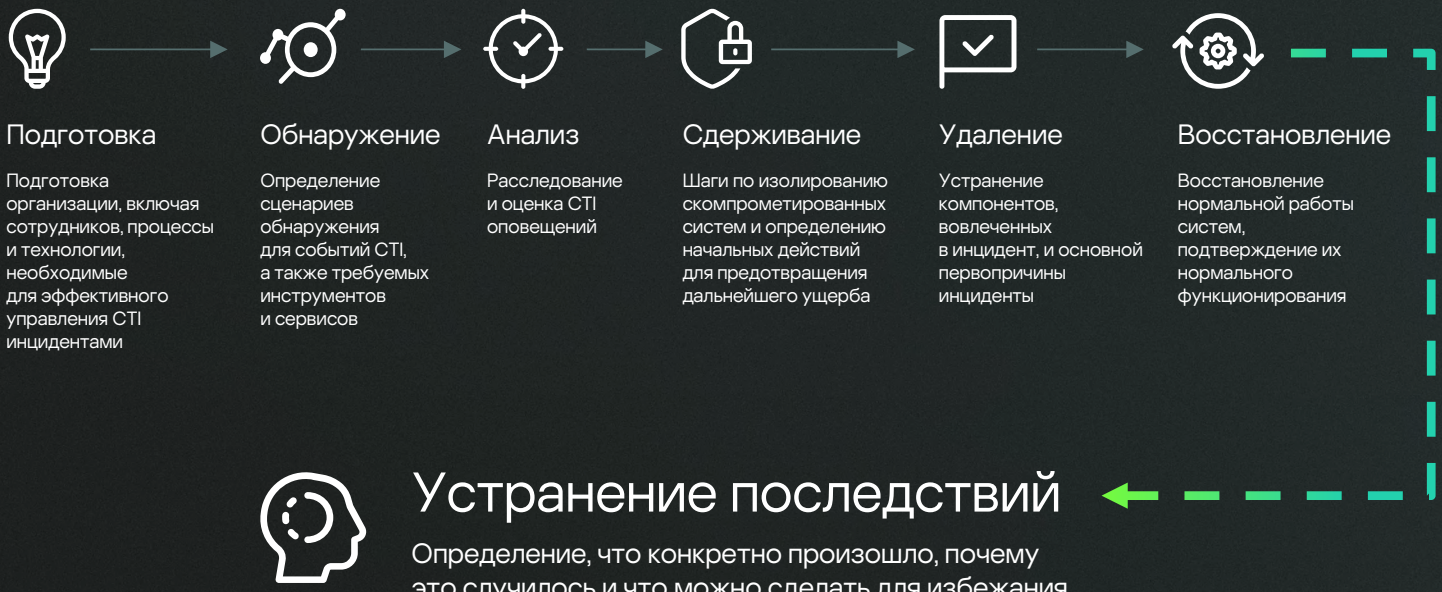
Плейбук реагирования на инциденты

kaspersky активируй будущее

Содержание

Введение

Используя распространенный подход к реагированию на инциденты безопасности из NIST Framework, жизненный цикл реагирования на инциденты, связанные с Даркнетом, можно разделить на семь этапов, которые показаны на рисунке ниже.



С точки зрения управления инцидентами, Cyber Threat Intelligence (CTI) является ценным источником информации о потенциальных инцидентах информационной безопасности (ИБ). При этом анализ угроз, связанных с Даркнетом, включает дополнительные шаги для анализа и проверки обнаруженной информации, а также оценки уровня угрозы ИБ.

После подтверждения инцидента ИБ, SOC команда может реагировать на угрозу с использованием подходящих сценариев реагирования на инциденты ИБ. В настоящем документе мы рассмотрим процедуру реагирования на инциденты, связанные с Даркнет угрозами, с привлечением следующих команд:

1. Аналитики Threat Intelligence (CTI)
2. Команда центра мониторинга и реагирования (SOC)
3. Специалисты по реагированию на инциденты ИБ (IR)

В зависимости от структуры команды кибербезопасности, рассматриваемые роли могут быть объединены или разделены, но общая процедура останется прежней.

Когда дело касается мониторинга Даркнета, организации необходимо проконсультироваться с профессиональными юристами и соблюдать законы и нормативные требования, которые действуют в соответствующем регионе. Кроме того, подход к кибербезопасности и защите данных должен выстраиваться с учетом требований к прозрачности и соблюдению этических норм. Если у вас возникнут трудности на любом этапе, обращайтесь к экспертам по угрозам Даркнета и реагированию на инциденты ИБ. Вы можете продолжать двигаться по рекомендованным шагам, но их помощь позволит эффективнее справиться с угрозой ИБ.

Роли и обязанности

Данная процедура была разработана в качестве образца для следующих специалистов по информационной безопасности:

Роли	Обязанности
Аналитик CTI	Осуществляет первоначальную обработку CTI оповещений, проверяет найденную информацию, оценивает угрозы на основе внешней информации, передает результаты в центр мониторинга и реагирования (SOC).
Аналитик SOC	Тщательно исследует CTI данные, проверяет угрозу в защищенной среде, создает инцидент информационной безопасности.
Специалист по реагированию на инцидент ИБ	Выполняет необходимые действия по реагированию на инцидент информационной безопасности.

Матрица распределения ответственности (Responsible, Accountable, Consulted, Informed – RACI)

Действие	CTI	SOC	IR
1. Подготовка и настройка механизма обнаружения	R	C	C
2. Обработка и оценка CTI оповещений	R	I	I
3. Расследование	C	R	I
4. Сдерживание	I	I	R
5. Удаление	I	I	R
6. Анализ полученного опыта	C	C	R

R — Responsible, A — Accountable, C — Consulted, I — Informed

Подготовка

Настройте мониторинг Дарквеб ресурсов для идентификации упоминаний вашей компании или информации, связанной с вашей компанией:

- Названия компании / дочерних компаний + партнеров / поставщиков
- Сокращенные названия / аббревиатуры
- Домены компании / дочерних компаний + партнеров / поставщиков
- Диапазоны IP-адресов
- Отрасль / географическое положение

Составьте список заслуживающих внимания Дарквеб ресурсов, где вы будете искать информацию.

Разверните инфраструктуру:

- VPN, Tor
- Внешние виртуальные хосты для получения данных
- Зарегистрируйте на форумах специальные учетные записи для сбора аналитических данных. Некоторые форумы требуют регистрации учетной записи, что затрудняет доступ к ресурсу для представителей правоохранительных органов или исследователей и ограждает от обычных посетителей.

Kaspersky Digital Footprint Intelligence

Или используйте решения, разработанные специально для таких задач, например Kaspersky Digital Footprint Intelligence.

Обнаружение

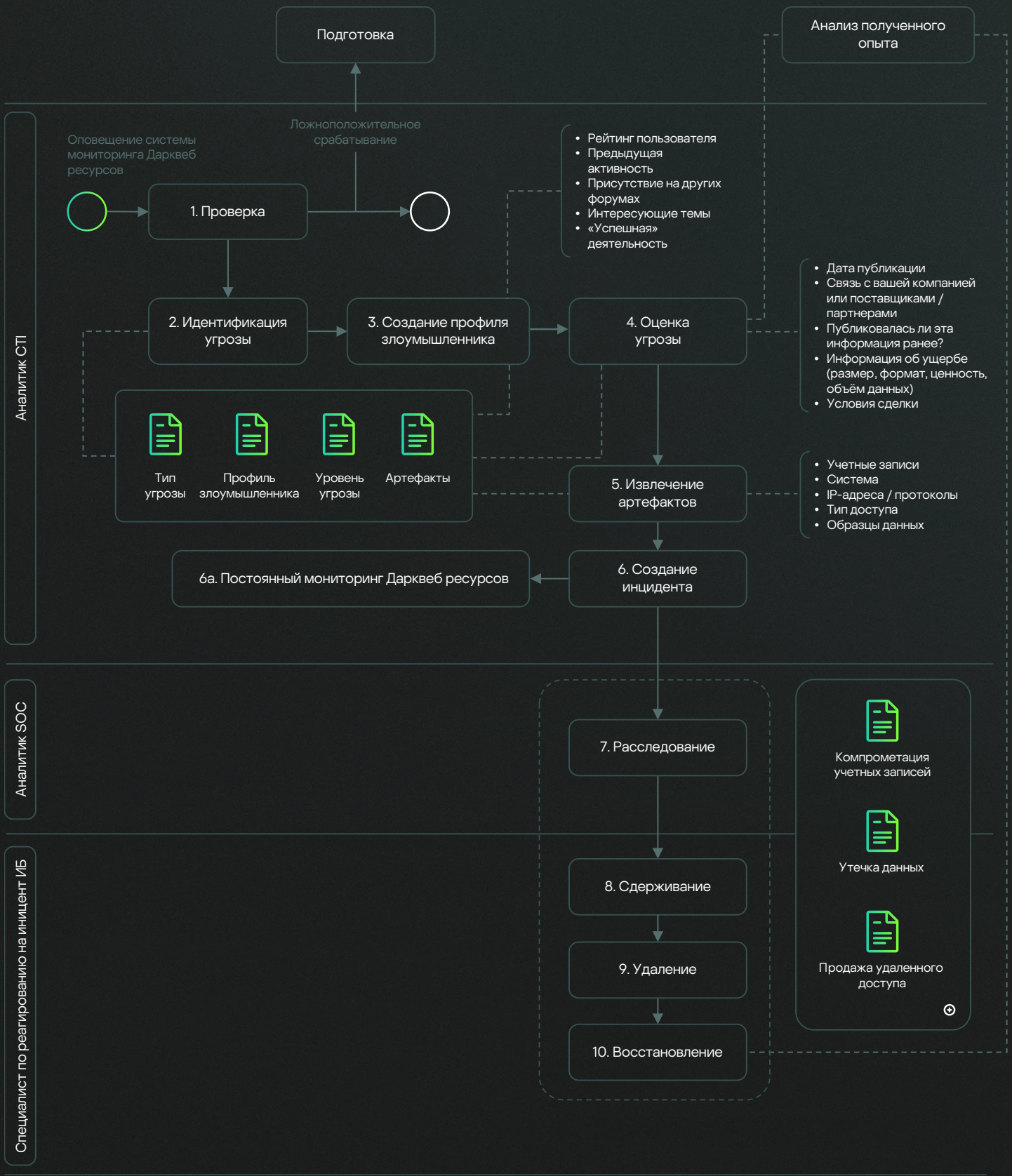
Обнаружение CTI угроз обычно включает отправку автоматического оповещения в случае обнаружения определенной информации в Дарквеб или дампах данных. Достоверность найденной угрозы может быть различной в зависимости от типа оповещения.

	Тип оповещения	Способы эффективного мониторинга
1	В Дарквеб упомянуто название компании	Отслеживайте упоминания названия, аббревиатуры или сокращенного названия компании в Дарквеб
2	В Дарквеб упомянут домен компании	Отслеживайте упоминания доменов компании в Дарквеб
3	Домен компании упомянут в базах скомпрометированных учетных данных	Отслеживайте упоминания почтовых доменов компании в дампах, содержащих скомпрометированные данные учетных записей
4	В Дарквеб упомянут профиль похожей компании	Иногда злоумышленники для маскировки своей личности и действий не упоминают точное название, но приводит определенные характеристики компании (регион /отрасль / размер / доход / типы информационных систем)
5	Аналогично пунктам 1–4	Тот же набор оповещений, что и выше, но в результате отслеживания упоминаний партнёров, поставщиков, субподрядчиков или других лиц с доступом к вашей инфраструктуре

Специальные сервисы для мониторинга Дарквеб, такие как Kaspersky Digital Footprint Intelligence, осуществляют мониторинг оповещений всех типов, упомянутых в таблице.

Процедура реагирования на инцидент ИБ

Процедура начинается с этапа «Анализ» процесса реагирования на инциденты ИБ.



Шаг	Описание

1 Проверка

Первым шагом обработки CTI оповещения является проверка обнаруженной информации. Это особенно важно для данных, достоверность которых невозможно подтвердить напрямую. Пункты проверки:

- Прямые упоминания компании с соответствующими подтверждениями.
- Оцените косвенные данные (упоминания географического положения, отрасли, размера, дохода, списка информационных систем компании), если компания не упоминалась.
- Найдите первоначальные сообщения – многие сообщения переопубликовываются. Если Даркнет ресурс, где первоначально были упомянуты данные, известен, но сообщение не удается найти, возможно, оно было удалено, а данные проданы.
- Составьте полный список упоминаний.

2 Идентификация угрозы

Определите тип угрозы. Какая информация продается? Возможные варианты:

- Скомпрометированные учетные записи
- Удаленный доступ
- Скомпрометированные данные компании

3 Создание профиля злоумышленника

Создайте новый профиль злоумышленника (или обновите существующий), содержащий следующую информацию:

- Дата регистрации автора публикации на форуме (или ином Даркнет ресурсе).
- Рейтинг автора (если на форуме поддерживается такая функция).
- Предыдущая активность. Другие сообщения/предложения от автора публикации.
- Присутствие на других форумах. Существует ли пользователь с таким же именем на других Даркнет ресурсах?
- Репутация в сообществе. Проверьте взаимоотношения автора с другими участниками. Проверьте реакции и комментарии на сообщения автора.
- Интересующие темы. Связана ли текущая тема с основной областью интересов автора?
- «Успешная» деятельность. Есть ли доказательства успешной продажи предыдущих предложений от автора?

На основе собранных данных создайте или обновите профиль злоумышленника.

4 Оценка угрозы

Оцените риск, связанный с угрозой:

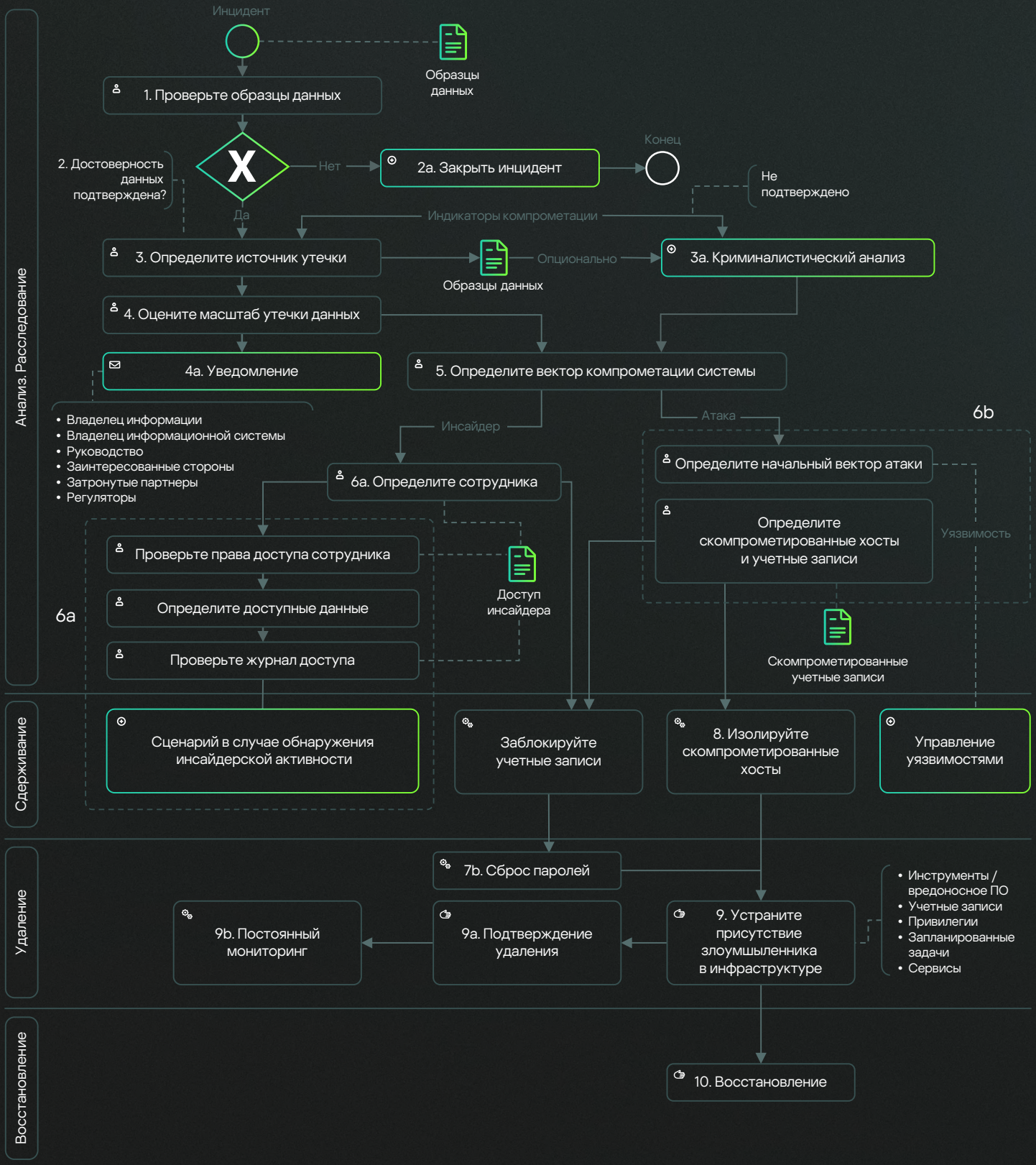
- Проверьте дату предложения.
- Проверьте, не публиковалась ли эта информация ранее.
- Проанализируйте цену предложения, объем и ценность данных, а также типы доступа или учетных записей.
- Проанализируйте условия сделки: предлагаются данные бесплатно, выставлены на продажу всем желающим или только одному покупателю?

Проверьте, относится ли информация к вашей компании или третьим сторонам (партнерам / субподрядчикам/поставщикам и т. д.).
На основе собранных данных определите уровень угрозы.

Шаг	Описание
5	**Извлечение артефактов** Определите всю ценную информацию в предложении. Основные артефакты для поиска: • Имена учетных записей • Упомянутые информационные системы и приложения • IP-адреса / протоколы • Тип доступа • Образцы данных
6	**Создание инцидента** Создайте инцидент информационной безопасности для дальнейшего расследования командой центра мониторинга и реагирования (SOC). С этого момента результаты CTI обрабатываются в соответствии со стандартными процедурами реагирования на инциденты ИБ.
7 – 10	**Расследование, Сдерживание, Удаление, Восстановление** Следующие шаги рабочего процесса выполняются командой SOC и группой реагирования на инциденты ИБ и определяются соответствующим сценарием согласно типу выявленной угрозы: • Продажа скомпрометированных учетных записей ⟶ Компрометация учетных записей • Продажа удаленного доступа ⟶ Продажа удаленного доступа • Продажа данных компании ⟶ Утечка данных

Сценарии реагирования

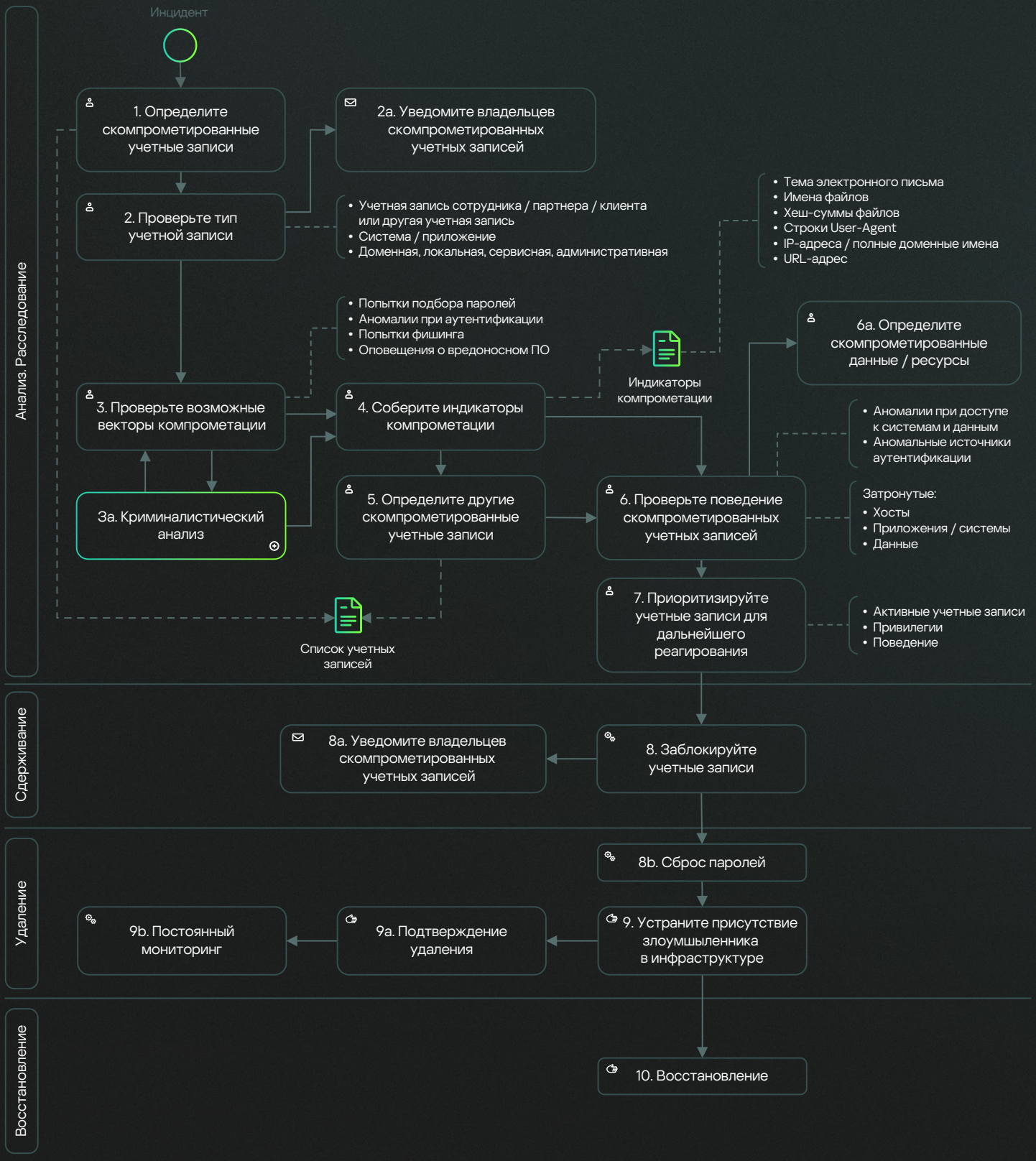
Сценарий «Утечка данных»



Шаг	Описание
1	**Проверьте образцы данных** Проверьте образцы скомпрометированных данных на предмет принадлежности вашей компании.
2	**Подтвердите достоверность данных** Если проверка показала, что скомпрометированные данные не принадлежат вашей компании или являются недостоверными, инцидент следует закрыть как ложноположительное срабатывание.
3	**Определите источник утечки** На основе образцов данных составьте список информационных систем, которые обрабатывают эти данные. Обращайте внимание на формат, метаданные и технические поля, если таковые имеются (некоторые системы могут обрабатывать те же данные, но в других форматах).
3a	**Проведите криминалистический анализ** Если возможно, инициируйте процедуры цифровой криминалистики для выявленных систем. Это поможет определить, не взломал ли злоумышленник другие системы.
4	**Оцените масштаб утечки данных** Определите потенциальный масштаб атаки, проанализировав список скомпрометированных информационных систем и данные, которые ими обрабатывались.
4a	**Уведомите заинтересованных ответственных лиц** в соответствии с матрицей оповещения. Стандартный список заинтересованных лиц в случае утечки данных: • Владельцы информационных систем и ресурсов • Владельцы информации • Руководство • Затронутые партнеры • Регуляторы, если в отношении скомпрометированных данных применяются нормативно правовые акты • Клиенты
5	**Определите вектор компрометации систем** Проведите тщательное расследование, чтобы определить вектор компрометации систем. Это могут быть действия инсайдера или атака.
6	**Инициируйте соответствующие процедуры расследования в отношении выявленного вектора компрометации** На основе результатов этого расследования составьте список затронутых / скомпрометированных учетных записей и список скомпрометированных хостов.

Шаг	Описание
6a	В случае действий инсайдера: • Определите сотрудника, являющегося инсайдером. • Определите уровень доступа инсайдера для всех систем компании. • Определите все данные, потенциально доступные инсайдеру. • Проверьте журналы действий инсайдера, чтобы определить дополнительные права доступа и тип информации, которая запрашивалась этим лицом. • Инициируйте установленную в компании процедуру в случае обнаружения иснайдерской активности.
6b	В случае атаки определите начальный вектор атаки и цепочку атаки внутри вашей инфраструктуры. Составьте список систем, которые полностью или частично контролируются злоумышленником. Если обнаружено использование уязвимостей, инициируйте соответствующие процедуры управления уязвимостями для предотвращения их дальнейшего использования.
7	**Заблокируйте учетные записи** Независимо от начального вектора атаки, заблокируйте все скомпрометированные или инсайдерские учетные записи. Кроме того, перед разблокировкой учетных записей выполните сброс их паролей.
8	**Изолируйте скомпрометированные хосты** В случае атаки изолируйте все хосты, которые контролируются злоумышленником.
9	**Устраните присутствие злоумышленника в инфраструктуре** Выполните различные действия по удалению злоумышленника из инфраструктуры в соответствии с полученными результатами. Контролируйте удаление злоумышленника из инфраструктуры посредством постоянного мониторинга выявленных индикаторов компрометации (IOCs). В случае инсайдерской угрозы настройте мониторинг попыток доступа с использованием всех учетных записей инсайдера.
10	**Восстановление** Проведите процедуры восстановления.

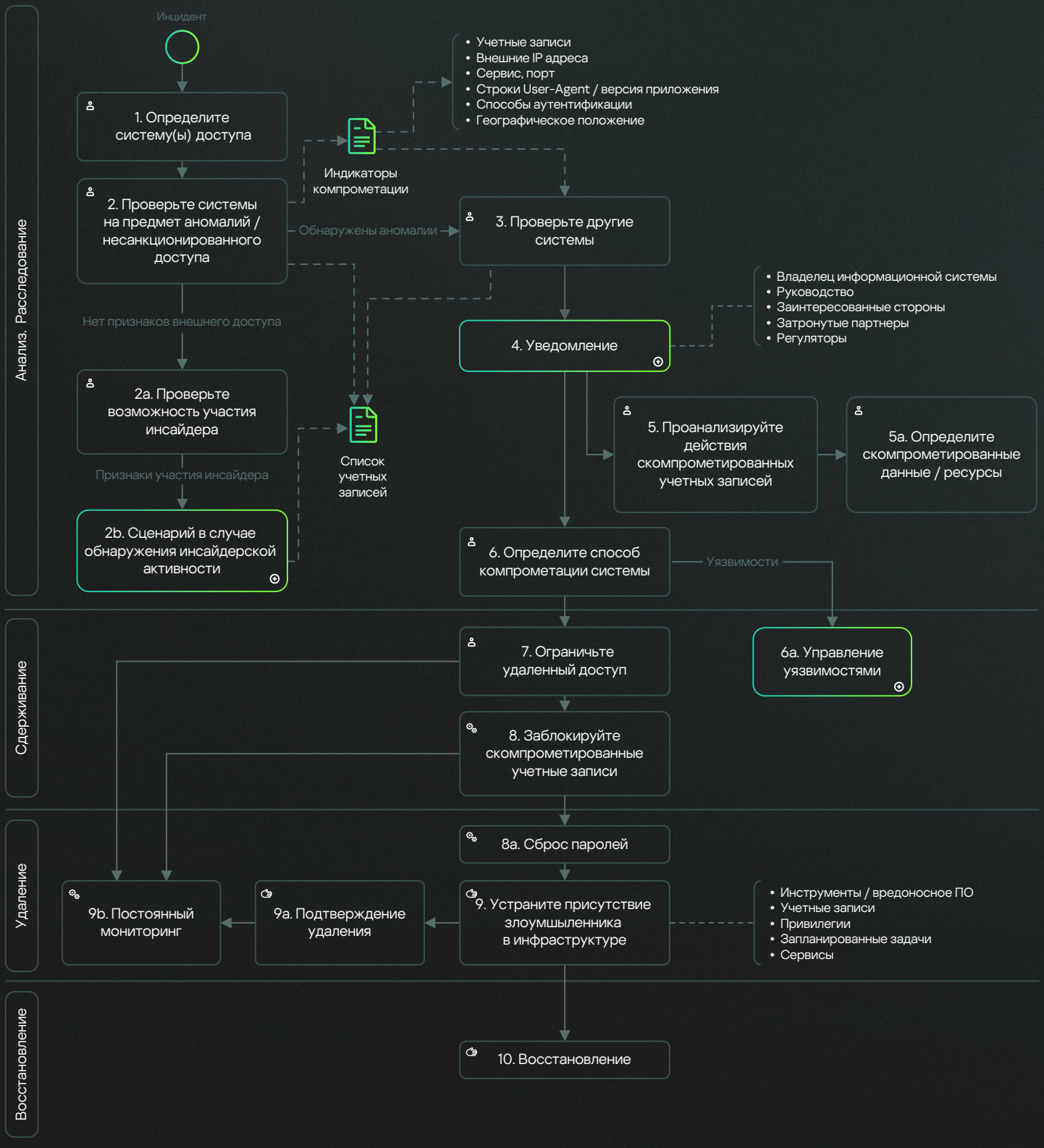
Сценарий «Компрометация учётных записей»



Шаг	Описание
1	**Определите скомпрометированные учетные записи** На основе полученной информации (тип доступа, информационная система) определите скомпрометированные учетные записи и (или) системы.
2	**Проверьте типы учетной записи** • Учетная запись сотрудника / партнера / клиента или другая учетная запись • Система / приложение, для которой использовалась учетная запись • Доменная / локальная / сервисная / административная учетная запись
3	**Проверьте возможные векторы компрометации** Проанализируйте журналы авторизации учетных записей на предмет следующей информации: • Попытки подбора паролей • Аномалии при аутентификации (нетипичные хосты / системы, способы аутентификации, протоколы, клиентские приложения и т. д.) • Попытки фишинга затронутых пользователей Проверьте наличие оповещений о вредоносном ПО и EDR оповещения для хостов, связанных со скомпрометированными учетными записями.
3a	**Проведите криминалистический анализ** Если учетные записи были скомпрометированы посредством компрометации информационных систем, инициируйте процедуры криминалистического анализа скомпрометированных систем. Это поможет определить начальный вектор атаки и индикаторы компрометации.
4	**Соберите индикаторы компрометации** для выявленных скомпрометированных систем и учетных записей. Индикаторы компрометации могут включать: • Темы фишинговых писем • Имена файлов вредоносного ПО • Хеш-суммы файлов вредоносного ПО • Строки User-Agent веб-клиентов, которые использовались вредоносным ПО • IP-адреса / полные доменные имена • URL-адреса, к которым обращались пользователи
5	**На основе собранных индикаторов компрометации** определите другие скомпрометированные учетные записи.
6	**Проверьте поведение и историю доступа для скомпрометированных учетных записей** на предмет аномалий в способах аутентификации, а также в доступе к системам и данным. Определите затронутые: • Хосты • Приложения / системы • Данные

Шаг	Описание
7	**Приоритизируйте учетные записи для дальнейшего реагирования** на основе следующего: • Период действия учетной записи • Привилегии учетной записи • Признаки использования злоумышленниками
8	**Заблокируйте учетные записи** Заблокируйте скомпрометированные учетные записи.
8a	**Проинформируйте владельцев учетных записей** о компрометации и предпринятых действиях.
8b	**Выполните сброс паролей** скомпрометированных учетных записей перед их разблокировкой.
9	**Устраните присутствие злоумышленника в инфраструктуре** Выполните различные действия по удалению злоумышленника из инфраструктуры в соответствии с полученными результатами. Контролируйте удаление злоумышленника из инфраструктуры посредством постоянного мониторинга выявленных индикаторов компрометации (IOCs).
10	**Восстановление** Проведите процедуры восстановления.

Сценарий «Продажа удаленного доступа»

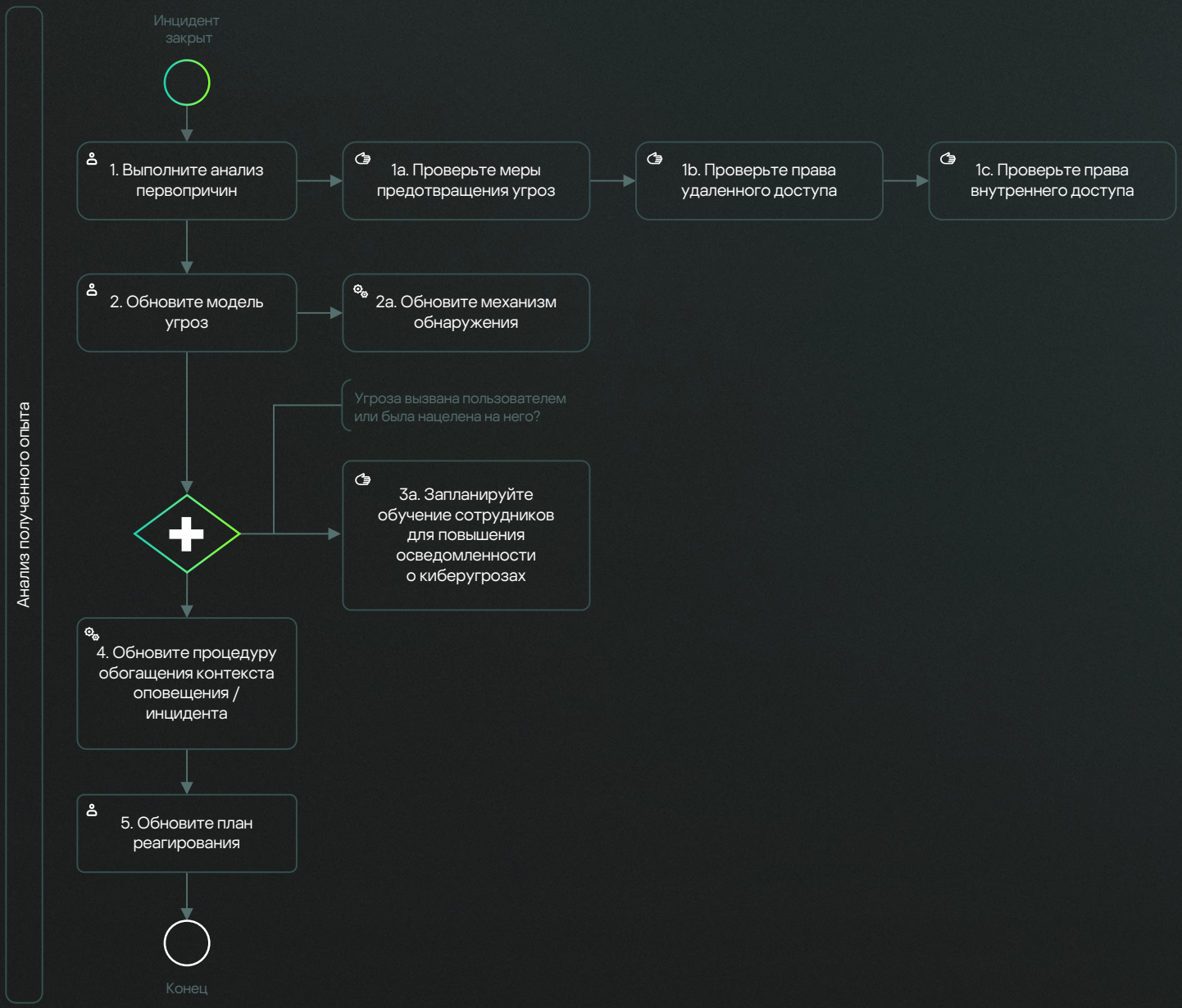


Шаг	Описание
1	**Определите системы** На основе предоставленной информации (тип и реквизиты доступа) определите системы, доступ к которым выставлен на продажу.
2	**Проверьте системы на предмет аномалий / несанкционированного доступа** Для выявленных систем проведите анализ журналов доступа и поиск аномалий. В случае обнаружения аномалий соберите индикаторы компрометации для проверки полученного доступа. Список стандартных индикаторов: • Имена учетных записей • Внешние IP-адреса или пулы IP-адресов • Сервисы, порты, протоколы • Строки User-Agent, цифровые следы приложений • Способы аутентификации • Профиль географического положения
2a	**Проверьте возможность участия инсайдера** Если нет признаков аномального доступа к системе, проведите расследование, исходя из предположения, что доступ продается инсайдером. Определите сотрудников с требуемым уровнем доступа и проверьте их активность.
3	**Проверьте другие системы** Выполните поиск собранных индикаторов компрометации в журналах доступа других систем
4	**Уведомите соответствующих заинтересованных лиц** в соответствии с матрицей оповещения. Стандартный список заинтересованных лиц для уведомления о компрометации систем: • Владельцы информационных систем и ресурсов • Руководство • Затронутые партнеры • Регуляторы, если в отношении затронутой системы применяются их нормативно правовые акты
5	**Проанализируйте действия скомпрометированных учетных записей** Проанализируйте действия и поведение скомпрометированных учетных записей. Проверьте, нет ли признаков того, что учетные записи уже используются злоумышленниками. Для каждой скомпрометированной учетной записи составьте список ресурсов, систем и данных, к которым через нее обращались.
6	**Определите вектор компрометации системы** Проведите тщательное расследование, чтобы определить вектор компрометации системы. Это могут быть действия инсайдера или атака.

Шаг	Описание
7	**Ограничьте удаленный доступ к скомпрометированным системам** В зависимости от важности системы и доступа к ней для сдерживания атаки можно применять различные подходы: • Полностью отключите удаленный доступ. • Задействуйте двухфакторную аутентификацию. • Ограничьте удаленный доступ определенными IP-адресами / сетевыми сегментами / группами пользователей.
8	**Заблокируйте учетные записи** Заблокируйте скомпрометированные учетные записи.
8a	**Выполните сброс паролей** скомпрометированных учетных записей перед их разблокировкой.
9	**Устраните присутствие злоумышленника в инфраструктуре** Выполните различные действия по удалению злоумышленника из инфраструктуры в соответствии с полученными результатами.
10	**Восстановление** Проведите процедуры восстановления.

Анализ полученного опыта

Этап «Устранение последствий инцидента» для CTI угроз включает стандартные задачи по анализу полученного опыта на основе результатов расследования инцидента ИБ, а также некоторые особые шаги для обновления информации о ландшафте угроз и корректировки CTI оповещений.



Шаги по устранению последствий инцидента:

Шаг	Описание
1	**Выполните анализ первопричин** обстоятельств, которые привели к инциденту. Этот шаг включает составление списка мер и средств контроля, которые не были использованы, и подготовку плана действий для предотвращения возникновения подобных инцидентов в будущем. Ключевые элементы: • Меры предотвращения угроз • Права удаленного доступа • Права внутреннего доступа
2	**Обновите базовую модель угроз** с использованием новой информации. Обновите уровни угроз. Этот процесс включает следующее: • Обновление уровней опасности для определенных злоумышленников • Пересмотр профиля угроз для затронутых систем Также этот шаг часто включает разработку и внедрение новых механизмов обнаружения.
3	Проанализируйте природу угрозы и возможность ее возникновения в результате ошибки внутреннего пользователя. Если ответ положительный, запланируйте соответствующий тренинг по осведомленности пользователей.
4	**Обновите процедуру обогащения контекста оповещения / инцидента** Проанализируйте, какие данные были пропущены на каждом шаге обработки CTI оповещения и инцидента ИБ. Обратите особое внимание на шаги, которые включали обмен информацией между командами. Запланируйте действия, чтобы в следующий раз обеспечить требуемый контекст.
5	**Обновите план реагирования** Обновите текущую процедуру и сценарии с учетом выявленных недостатков и требуемых улучшений.

Приложение. Пояснения к диаграммам

В следующей таблице представлена справочная информация по элементам диаграмм, которые использовались в описанных выше сценариях.

Категория	Элемент	Описание
Событие		Начальное событие: указывает, с чего начинается конкретный сценарий.
Событие		Конечное событие: указывает, где заканчивается сценарий.
Задача		Действие интеграции, которое может быть автоматизировано.
Задача		Действие, выполняемое вручную аналитиком T1/T2/T3 в соответствии с определенными инструкциями.
Задача		Задача, назначенная аналитику или другому участнику.
Шлюз		Можно выбрать только один из путей на основе логики рабочего процесса.
Шлюз		Можно выбрать несколько путей без установленного порядка приоритета.
Вспомогательная процедура		Свернутая вспомогательная процедура, которая выполняется отдельно для поддержки процесса выполнения сценария.