kaspersky

Утечки данных в Даркнет

Пошаговое руководство по реагированию

Анна Павловская

Старший аналитик Digital Footprint Intelligence

Оглавление

Мониторинг дарквеба

80%
форумы

10%
мессенджеры

5%
onion

5%
форумы с закрытым доступом

- Глобальные тенденции
- Последствия атак
- Злоумышленники с навыками скрипт-кидди
- Старые утечки

- Хактивизм
- Уязвимости нулевого дня
- Утечки данных

- Планы злоумышленников (продажа доступов в инфраструктуру)
- Скомпрометированные учетные записи сотрудников
- Инсайдерская активность

500 000+ сообщений ежедневно

Достоверные данные

Только критические инциденты – без фейков или публичной информации

Законные основы

Информация полученная из внешних источников (Дарквеб форумы и блоги)

Требующие реакции

Инциденты требующие незамедлительного реагирования

Безвозмездно

Информация со всеми деталями и рекомендациями от экспертов

Какая была реакция?

1

Что делать, если ваша компания была упомянута в даркнебе?

2

Кто ответственный за обработку инцидента?

Утечки данных

Доступ в инфраструктуру

Скомпрометированные аккаунты

Конфиденциальная и чувствительная информация

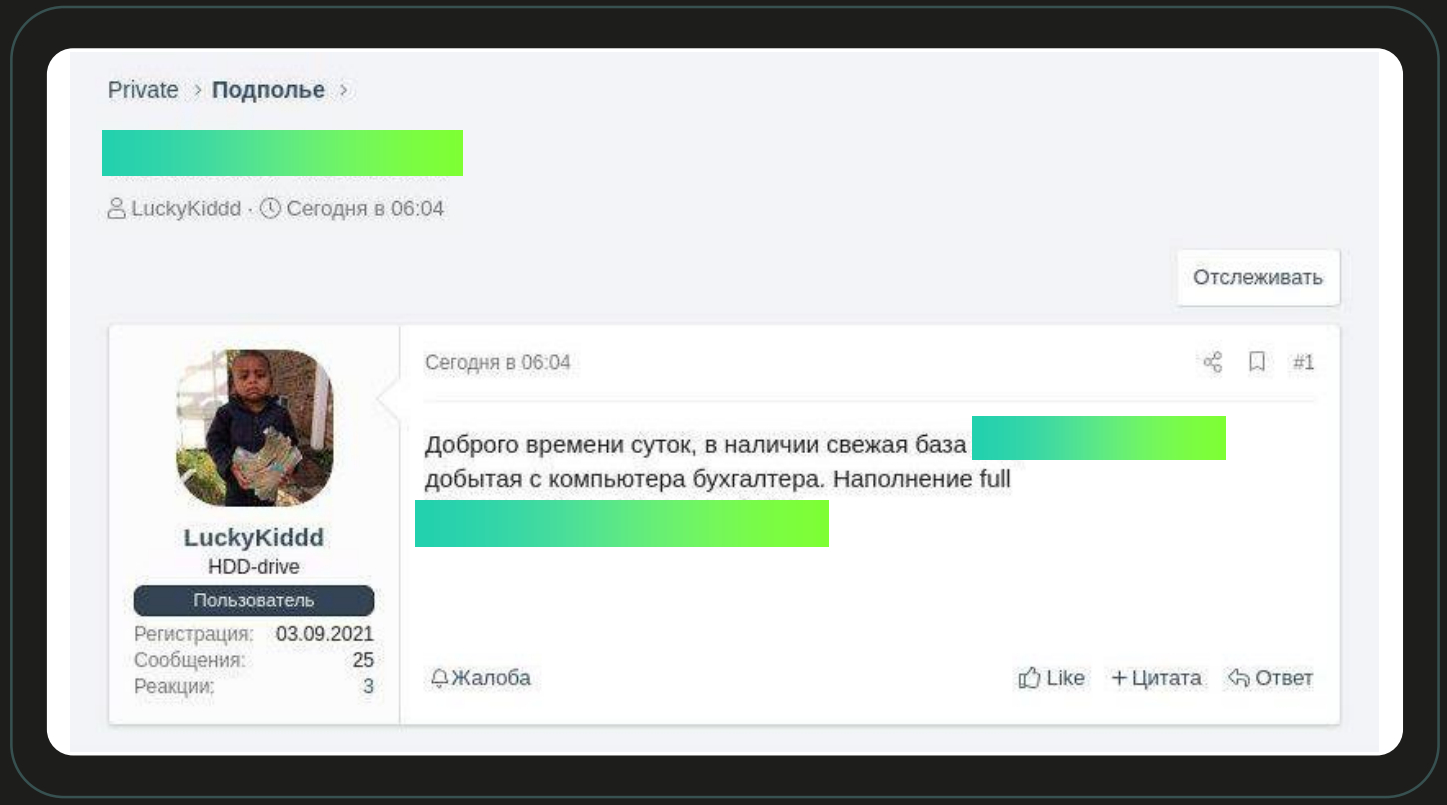
Базы данных, содержащие персональные данные, информацию о банковских картах, учетные записи

Финансовые документы

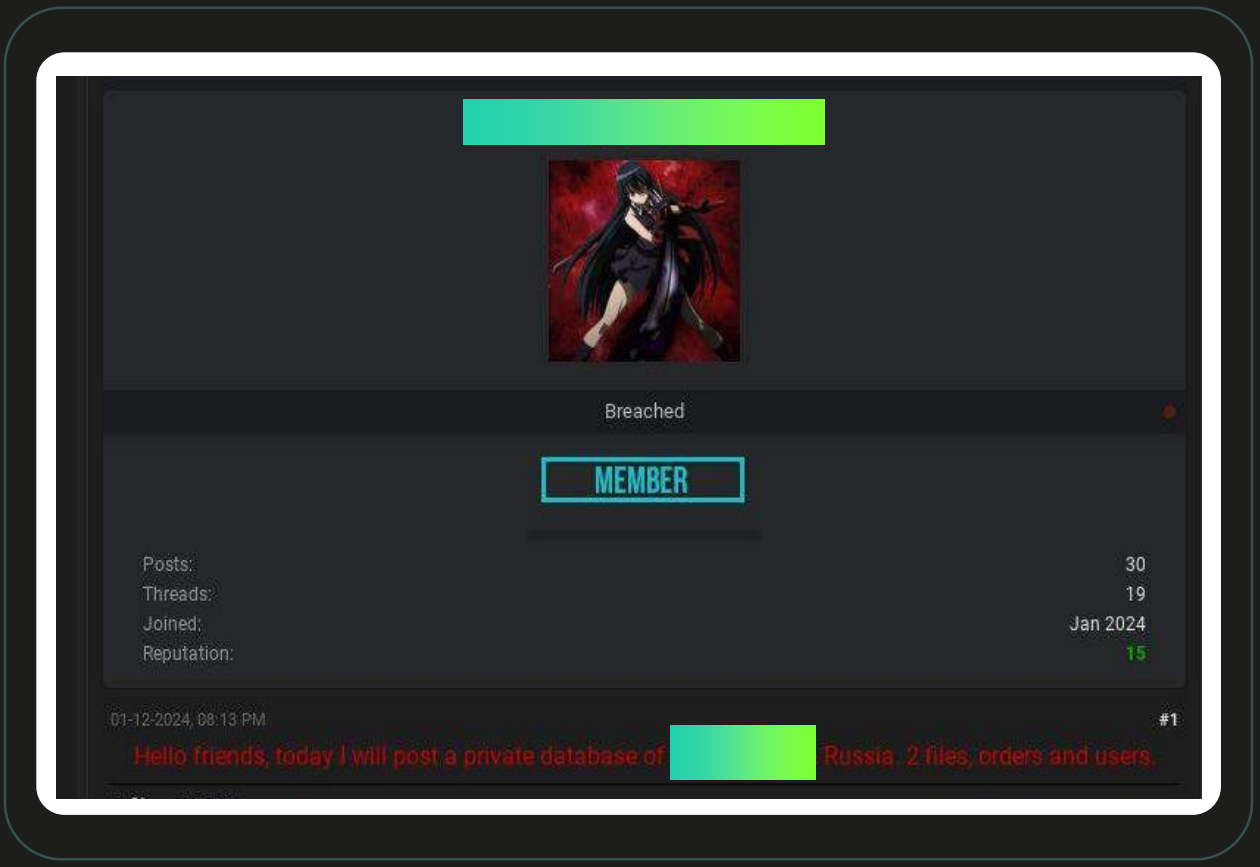
Интеллектуальная собственность

Внутренние документы

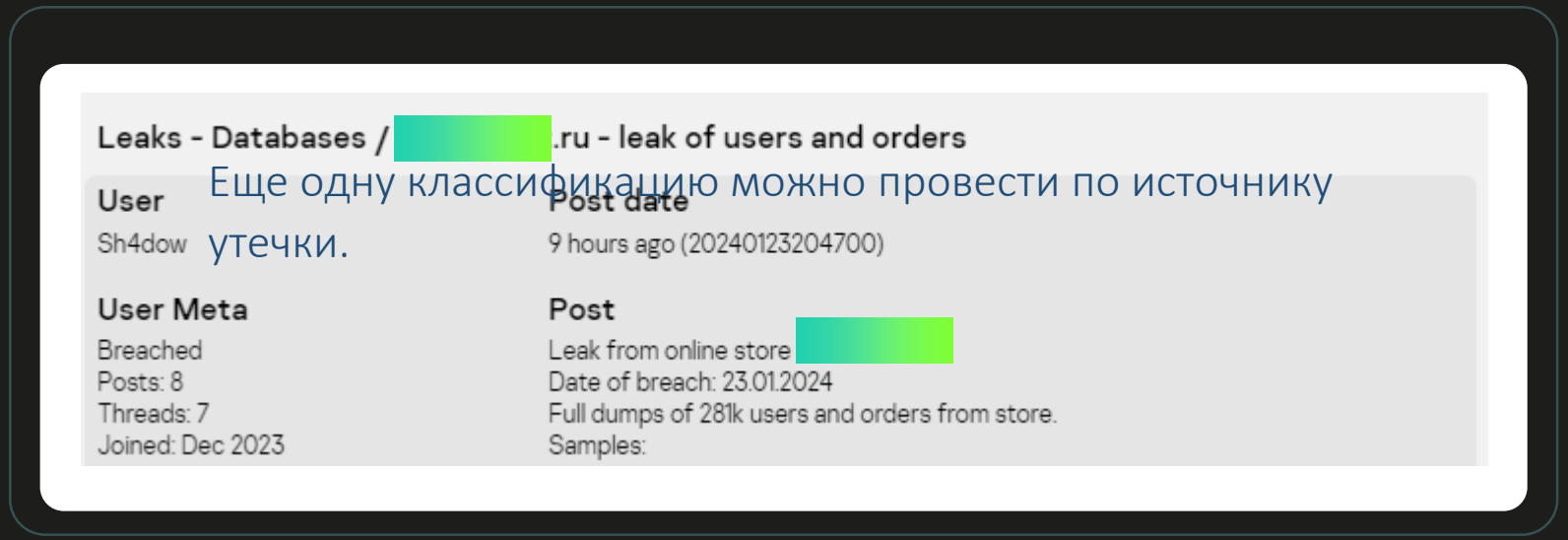
Представляют угрозу компании и ее сотрудникам



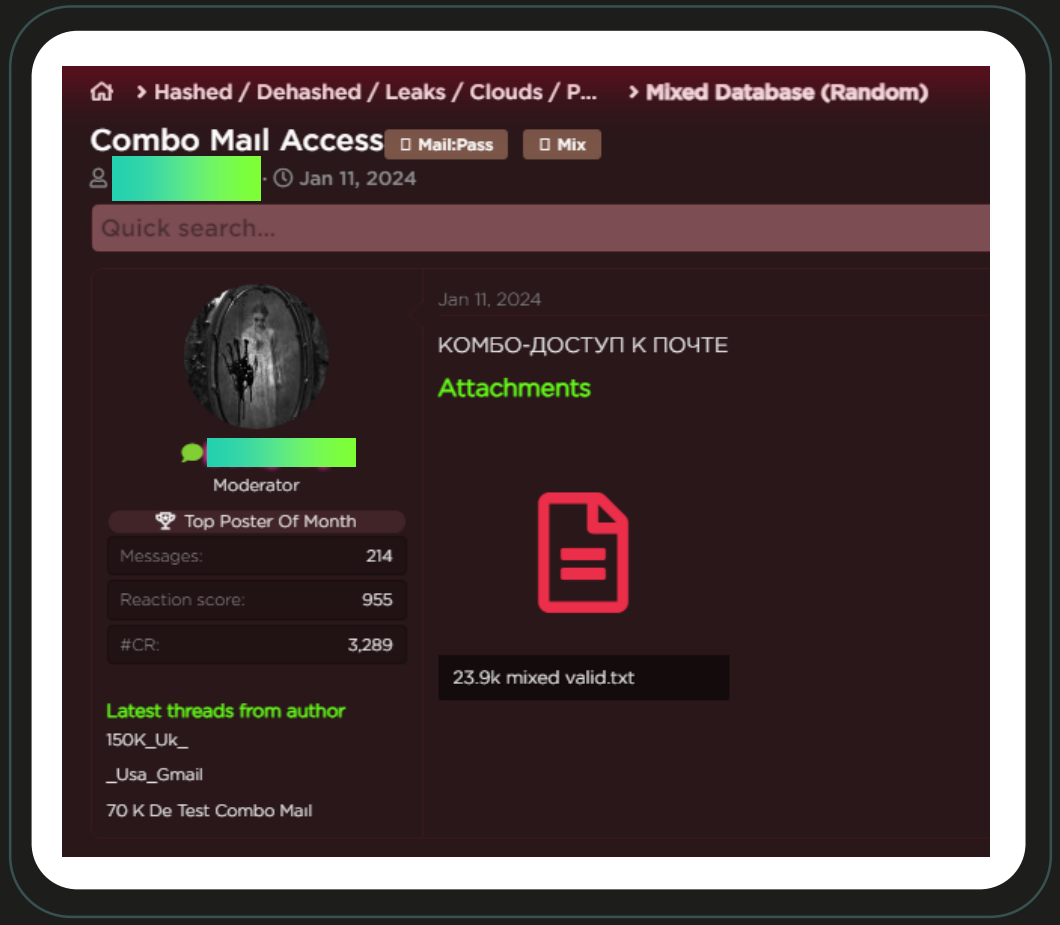
Представляют угрозу клиентам и заказчикам



Утечка определенной компании



Комбинированные утечки



Доступ к серверам, базам данных, и другим важным компонентам инфраструктуры:

1

RDP доступ

- local admin
- domain admin
- user

2

VPN + RDP

3

Другие типы доступа

Никаких упоминаний названий компаний

Обычно собщения в дарквебе не содержат названий компаний

Страна / регион | Индустрия | Доход | Размер

#2
I will advise you to remove the company name. No one will want your access of the company is aware.

Доступ в инфраструктуру

Post

Доступ: VPN Cisco
Есть DA полученый с простого юзера.
Доступ в ESXi, Veam, NAS
Данных на 30ТБ
700+ PC в сети, страхуют популярные компании, киберстраховки
Цена 3000$ покупка.
Tox для связи -
844618BF19132399FB64DC23E2FF63A70C285628151FAE77EC390D6DB7FFCB2193784B58A4AE
Все провожу строго через гаранта.

Доступ в инфраструктуру

RDP
USA
ZOOM/REV = 7KK
Level = Administrator Rights
Commercial & Residential Construction, Construction
Network = Workgroup
System = Windows 2016
AV = Windows Defender + Sentinel Agent
Extra : In Folder C:/ There is Login/Password to SonicWall / WPA / And Godaddy (I Didn't Checked Credentials For validation)
I think The Workgroup Server Belongs to the IT Exmployeer
App 600-700 GB of data Invoices/documents/scans etc + Quickbooks backups

start 500
step 250
blitz 1000

pps 12 h

Garan Forum Escrow ++ Accepted !!

Логин / адрес электронной почты + пароль

Публичные утечки

Базы с ограниченным доступом

Инфостилеры

Тип аккаунта

- Пользователь Active Directory
- Сотрудник
- Служебная учетная запись
- Администратор
- Тестовая учетная запись
- Клиент
- Партнер
- Подрядчик
- Поставщик

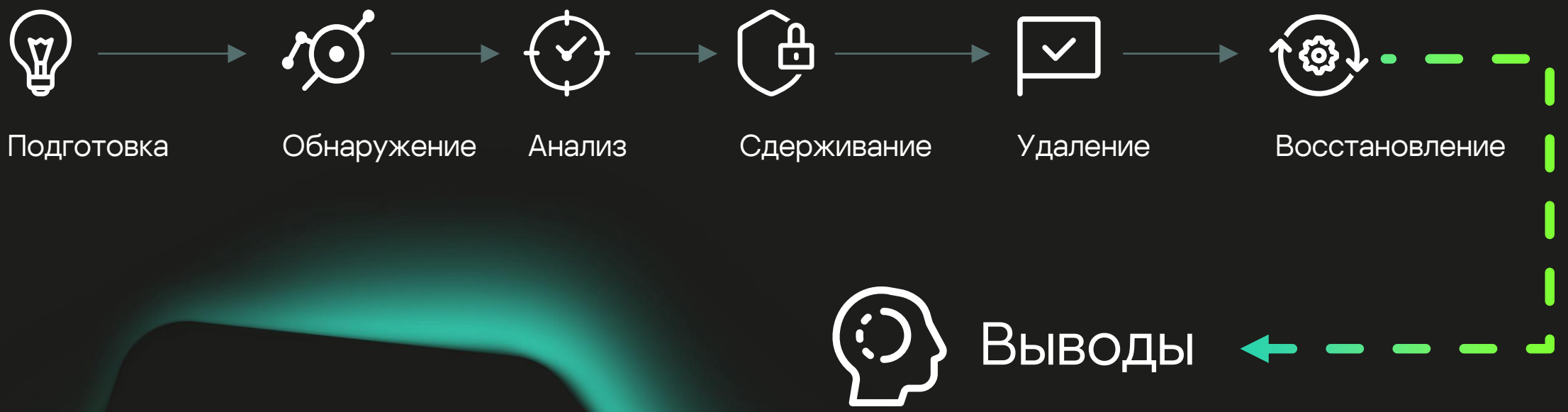
Скомпрометированное устройство

- Сервер базы данных
- Личное устройство
- Корпоративная рабочая станция

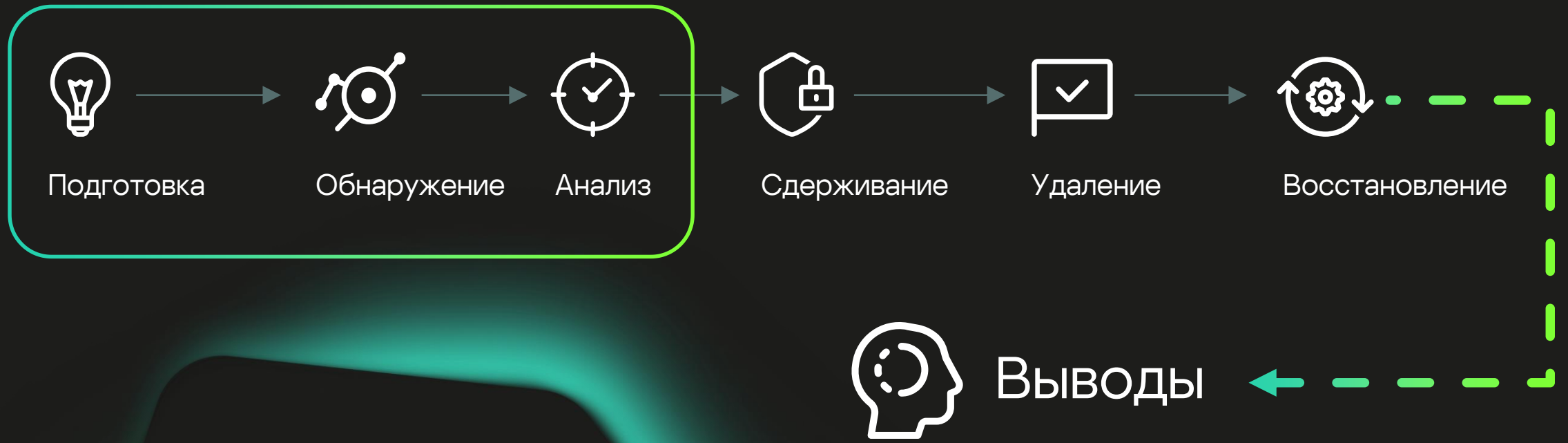
Ресурс аутентификации

- Корпоративный ресурс
- Внутренний ресурс
- Публичный ресурс
- Клиентский портал

Жизненный цикл реагирования на инциденты



Жизненный цикл реагирования на инциденты



Подход к реагированию на дарквеб инциденты

Подготовка

Подготовьте людей, процессы и технологи, необходимые для управления дарквеб инцидентами

Обнаружение

Определите сценарии обнаружения сообщений в дарквеб и необходимые инструменты и сервисы

Анализ

Расследуйте сообщение и оцените уровень угрозы

Верификация

Подтвердите угрозу и начните процесс реагирования на инцидент

Плейбук реагирования на инцидент

Подход к реагированию на дарквеб инциденты

Подготовка

Подготовьте людей, процессы и технологи, необходимые для управления дарквеб инцидентами

Обнаружение

Определите сценарии обнаружения сообщений в дарквеб и необходимые инструменты и сервисы

Анализ

Расследуйте сообщение и оцените уровень угрозы

Верификация

Подтвердите угрозу и начните процесс реагирования на инцидент

Плейбук реагирования на инцидент

CTI аналитик

- Первоначально обрабатывает данные об обнаружении сообщения в дарквебе
- Подтверждает угрозу
- Оценивает уровень угрозы
- Передает инцидент в SOC команду

SOC аналитик

- Расследует обнаруженный инцидент
- Проверяет угрозу в защищенной среде
- Создает инцидент информационной безопасности

Специалист по реагированию

Выполняет необходимые действия по реагированию на инцидент

1

Создание системы мониторинга с нуля

Ответственный создает:

- Список дарквеб ресурсов для мониторинга
- Выделенную инфраструктуру для доступа к дарквеб ресурсам
- Специализированные аккаунты, имитирующие пользователей дарквеб ресурсов

2

Использование готового решения

Область мониторинга

	Параметр	Интервал обновления	Лайфхак
1	Полное / официальное наименование	Каждый месяц, M&A	Разные языки
2	Сокращенное наименование и аббревиатуры	Каждый месяц, M&A	
3	Ключевые партнеры / поставщики, наименования и основные домены	Каждый месяц, M&A	
4	Домены и поддомены	Каждую неделю, новые регистрации	Экранирование
5	Диапазоны IP адресов	Каждую неделю, новые регистрации	
6	Имена руководителей и представителей компании	Каждый месяц, изменения в организационной структуре	
7	Данные о местоположении (страна, регион) и индустрия	Каждые 6 месяцев, случаи FP	Проверка ложноположительных срабатываний
8	Бренды и продукты	Каждые 3 месяца, новые продукты	

Подход к реагированию на дарквеб инциденты

Подготовка

Подготовьте людей, процессы и технологи, необходимые для управления дарквеб инцидентами

Обнаружение

Определите сценарии обнаружения сообщений в дарквеб и необходимые инструменты и сервисы

Анализ

Расследуйте сообщение и оцените уровень угрозы

Верификация

Подтвердите угрозу и начните процесс реагирования на инцидент

Плейбук реагирования на инцидент

Автоматическое оповещение

В дарквебе упомянуто название компании

Упоминание в дарквебе корпоративного IP-адреса или диапазона IP-адресов

Упоминание в дарквебе имен или адресов электронной почты сотрудников

Упоминание в дарквебе бренда или продукта компании

Упоминание в дарквебе партнера или поставщика компании

В дарквебе упомянут домен компании

Домен компании упомянут в базах скомпрометированных учетных данных

Упоминание в дарквебе профиля похожей компании (действующей в том же регионе и/или отрасли)

Подход к реагированию на дарквеб инциденты

Подготовка

Подготовьте людей, процессы и технологи, необходимые для управления дарквеб инцидентами

Обнаружение

Определите сценарии обнаружения сообщений в дарквеб и необходимые инструменты и сервисы

Анализ

Расследуйте сообщение и оцените уровень угрозы

Верификация

Подтвердите угрозу и начните процесс реагирования на инцидент

Плейбук реагирования на инцидент

Расследуйте угрозу и оцените риск

Проанализируйте источник сообщения

Проанализируйте профиль автора сообщения

Проанализируйте активность автора

Проанализируйте новизну, цену, модель распространения и тип предложения

Определите первоисточник сообщения

- Форумы
- Мессенджеры
- Приватные блоги
- Блоги вымогателей
- Новостные агрегаторы
- Социальные сети

Если есть много постов с одинаковым сообщением, первое упоминание должно быть проанализировано в первую очередь

Создайте профиль злоумышленника

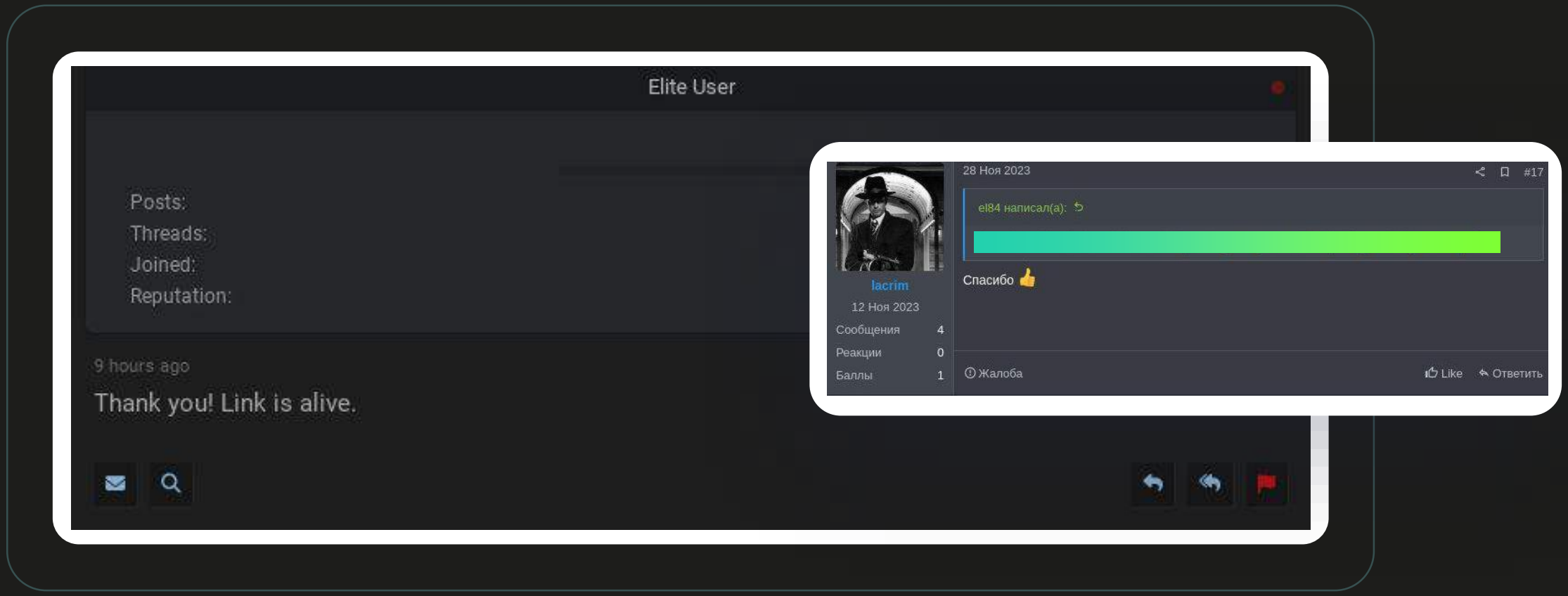
- Рейтинг
- Предыдущая активность
- Успешная активность
- Участие на других форумах
- Поддержка сообщества
- Область интересов

Анализ профиля автора сообщения

Предыдущая активность

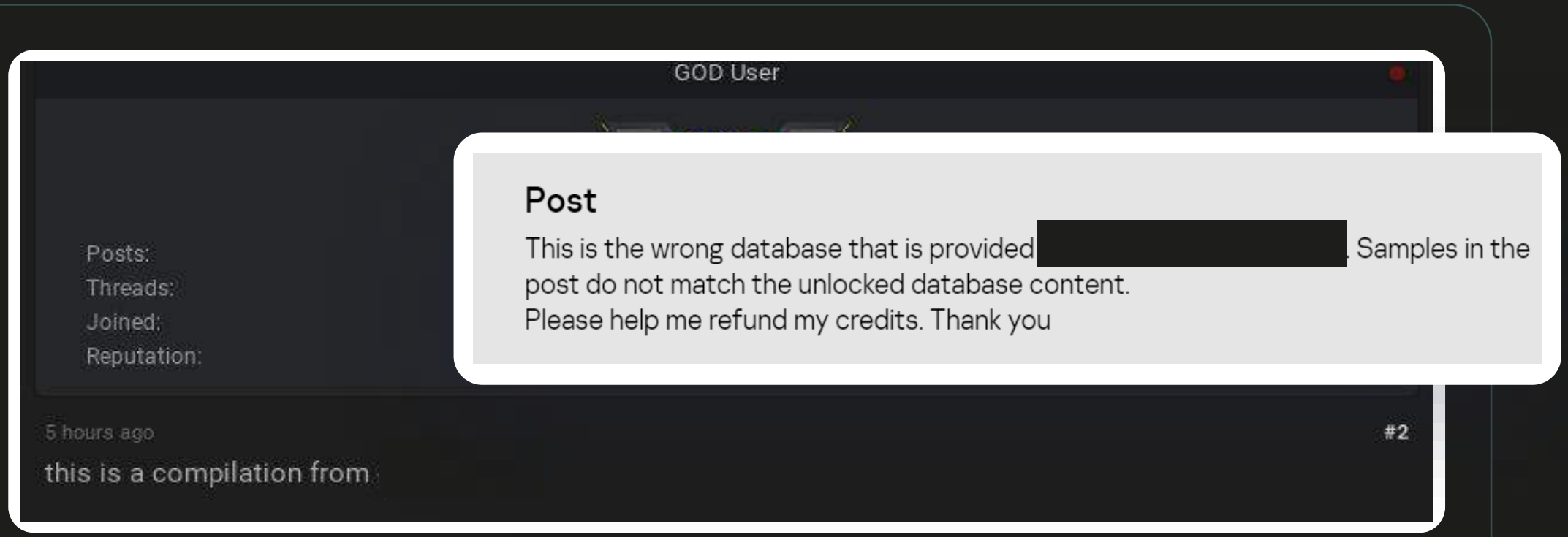
Рейтинг

Поддержка сообщества

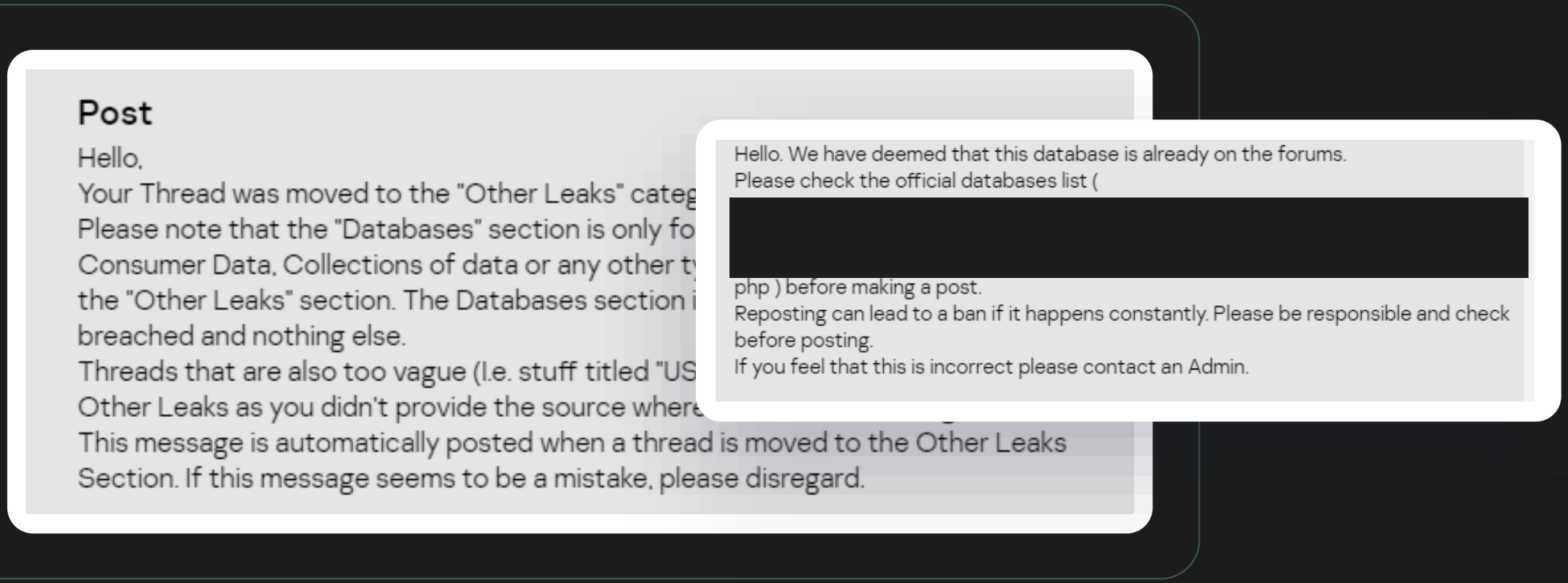


Комментарии от других пользователей

Комментарии от других пользователей

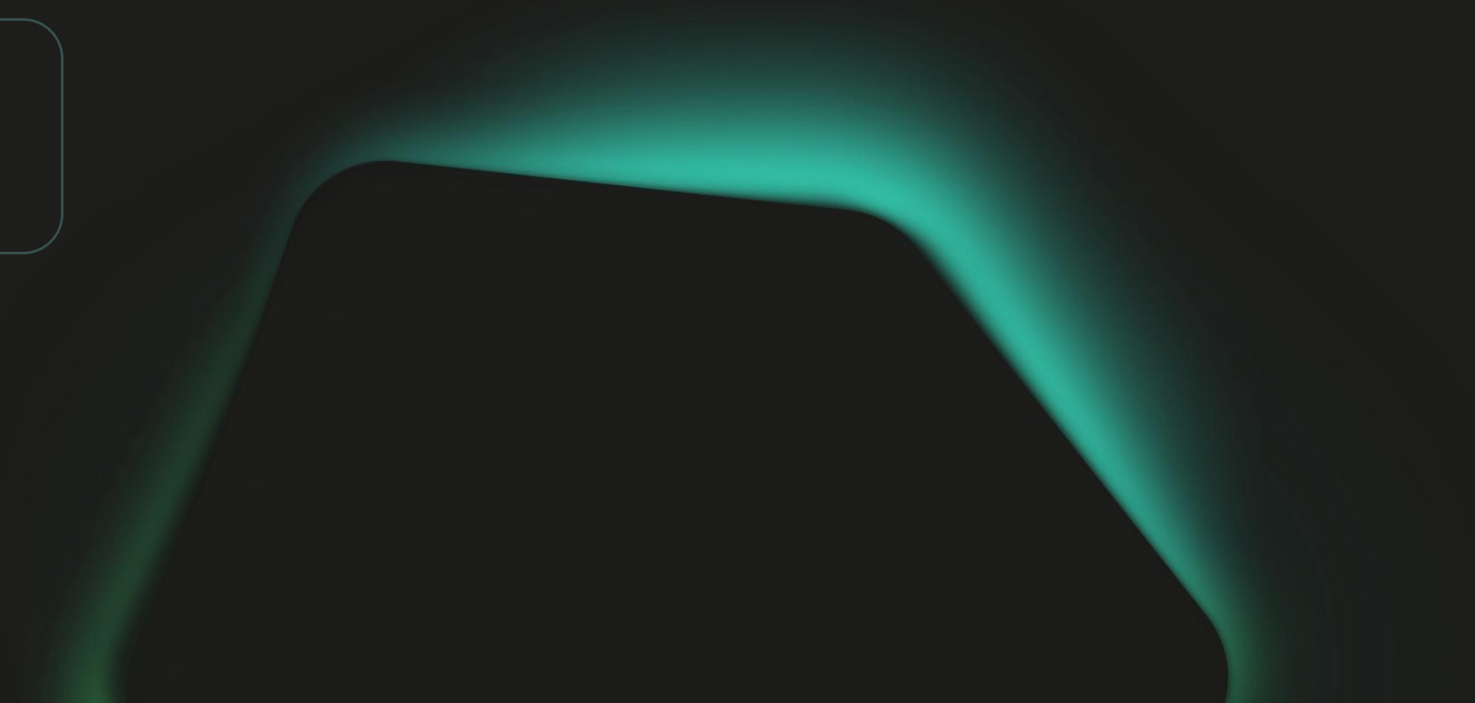


Модераторы форумов



Оцените риск от публикации в дарвебе

- Дата публикации
- Новизна
- Предлагаемый контент
- Условия сделки
- Цена



Подход к реагированию на дарквеб инциденты

Подготовка

Подготовьте людей, процессы и технологи, необходимые для управления дарквеб инцидентами

Обнаружение

Определите сценарии обнаружения сообщений в дарквеб и необходимые инструменты и сервисы

Анализ

Расследуйте сообщение и оцените уровень угрозы

Верификация

Подтвердите угрозу и начните процесс реагирования на инцидент

Плейбук реагирования на инцидент

Утечки данных

Our team of security researchers has meticulously conducted a comprehensive assessment of the company's intranet and extranet networks, revealing the existence of approximately sixty significant vulnerabilities. Through these vulnerabilities, we were able to gain access to and retrieve highly sensitive data belonging to company employees, critically classified documents, as well as password-protected database records. Furthermore, we successfully extracted a substantial volume of data amounting to 16GB from the Active Directory service.


```
[{"employeeNumber"
02T04:14:00
"firstName"
Supervisor","emplo
```

Доступ в инфраструктуру

$75

Role: Global Administrator Azure Active Directory with PIM roles, Intune Admin, Auth admin etc

Access type: Azure Active Directory

Domain [redacted]

Users: 9[redacted]

Licenses: Enterprise Mobility + Security E5; Microsoft Power Automate

Скомпрометированные аккаунты

Domain\

user@mail.com

123456

passw0rd

user001

Admin

2023!

admin

Первая коммуникация

Руководство

Оперативное оповещение высшего руководства — обязательно

СМИ

Подготовьте публичное заявление в сотрудничестве с юридическим отделом и отделом по связям с общественностью

Регулирующие органы

Информируйте регулирующие органы в соответствии с законодательством

Заинтересованные стороны

Уведомите пользователей, если требуется реакция с их стороны

Коммуникация со СМИ

Инциденты вредят репутации, но лучше заявить об утечке первым.

Правильная коммуникация показывает, насколько серьезно вы относитесь к безопасности и защите заинтересованных сторон.

Создание инцидента ИБ

CTI Аналитик

- Обнаружение угрозы
- Профиль злоумышленника
- Оценка риска
- Верификация

Создание инцидента ИБ

Специалист по реагированию на инциденты

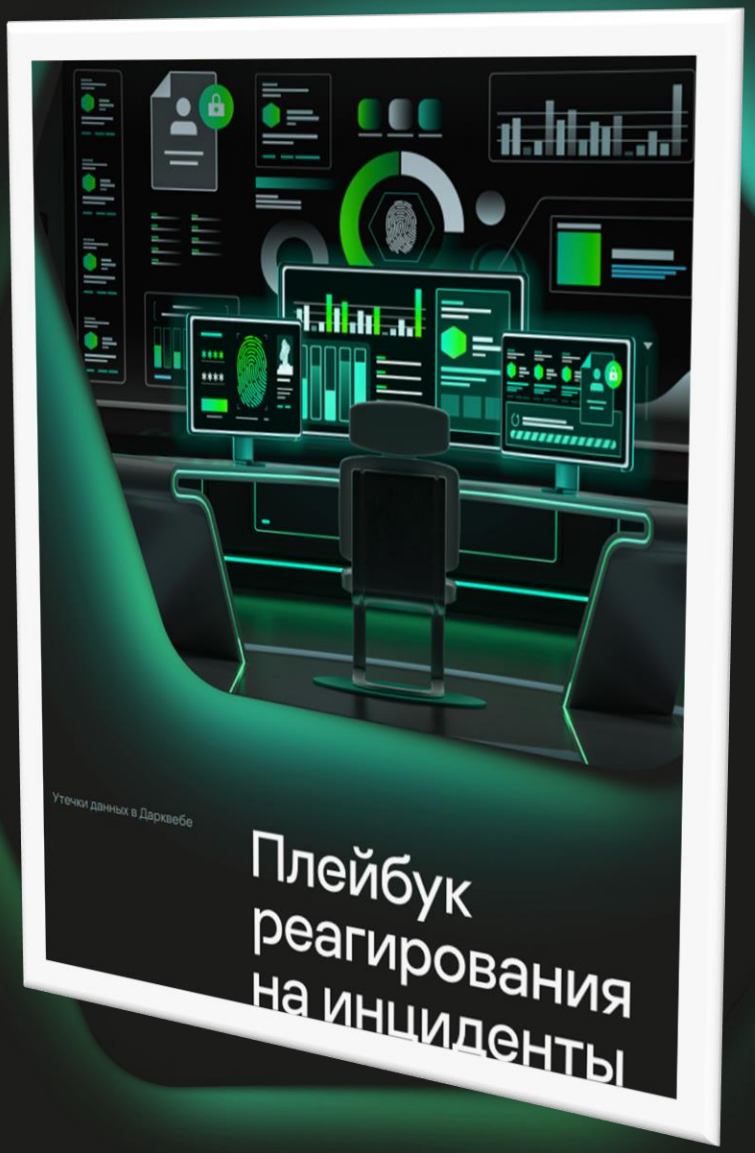
- Расследование
- Плейбук реагирования на инцидент

Скачайте плейбук

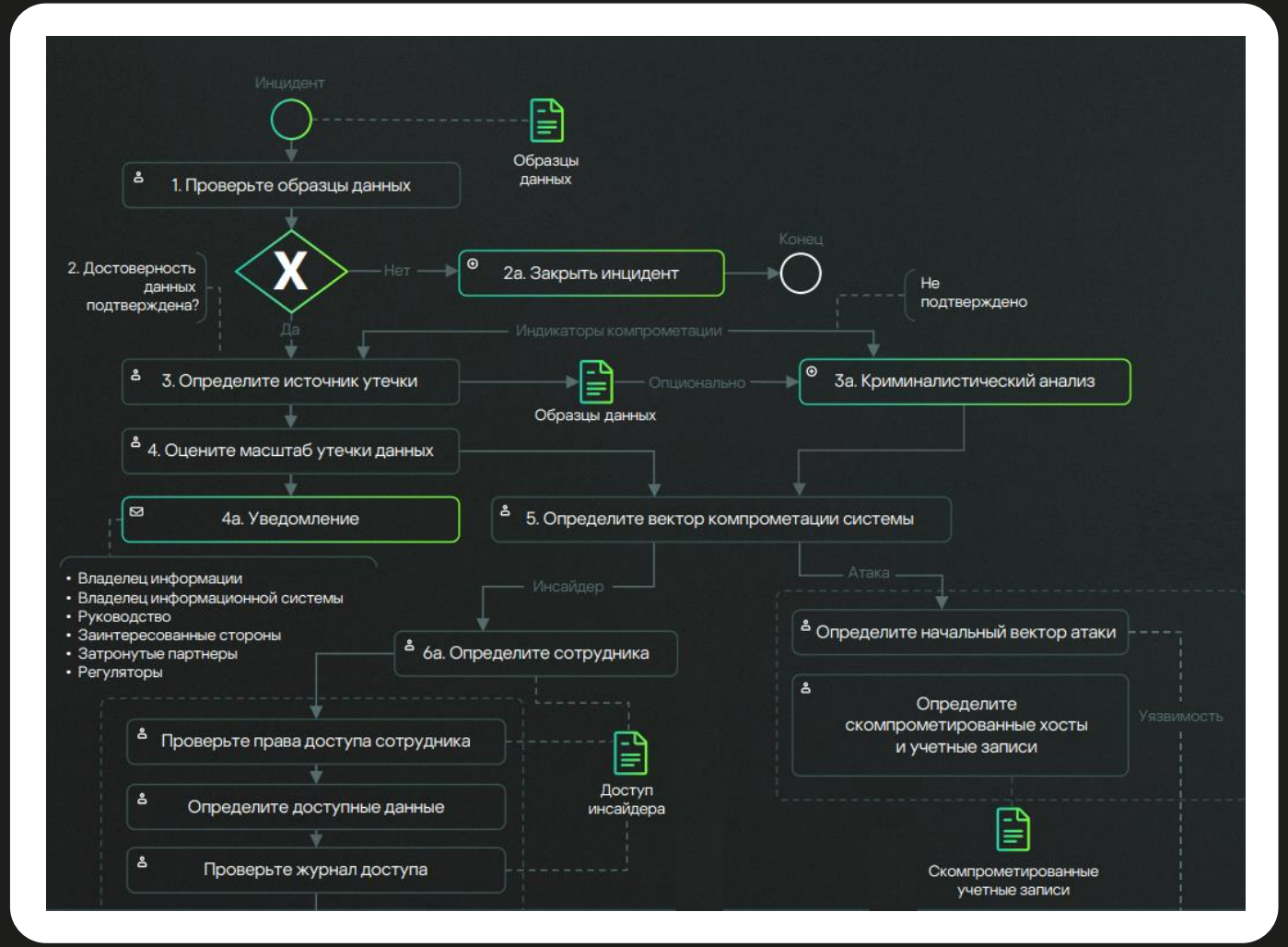
Сценарий утечки данных

Сценарий продажи удаленного доступа

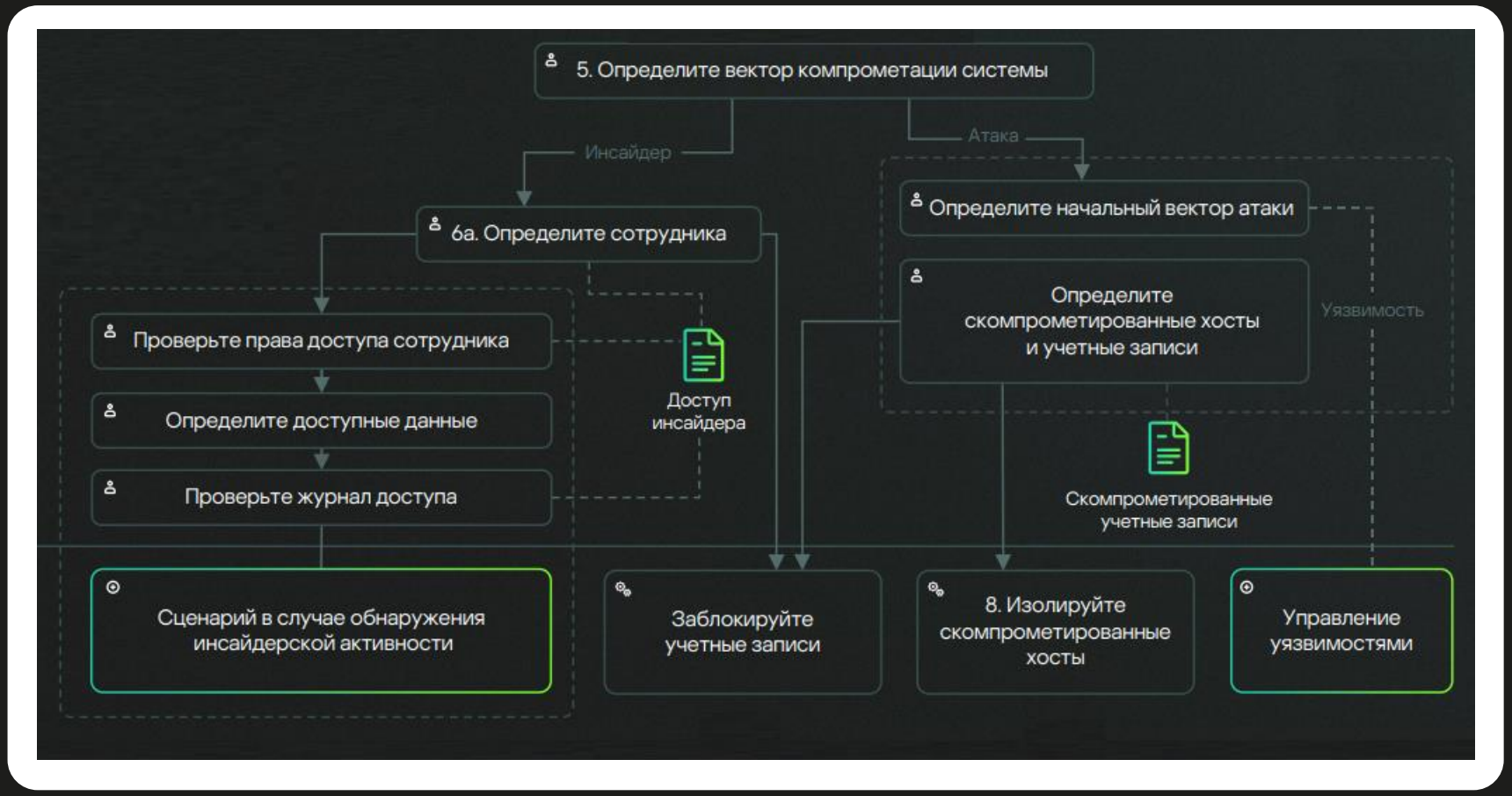
Сценарий компрометации учетных записей



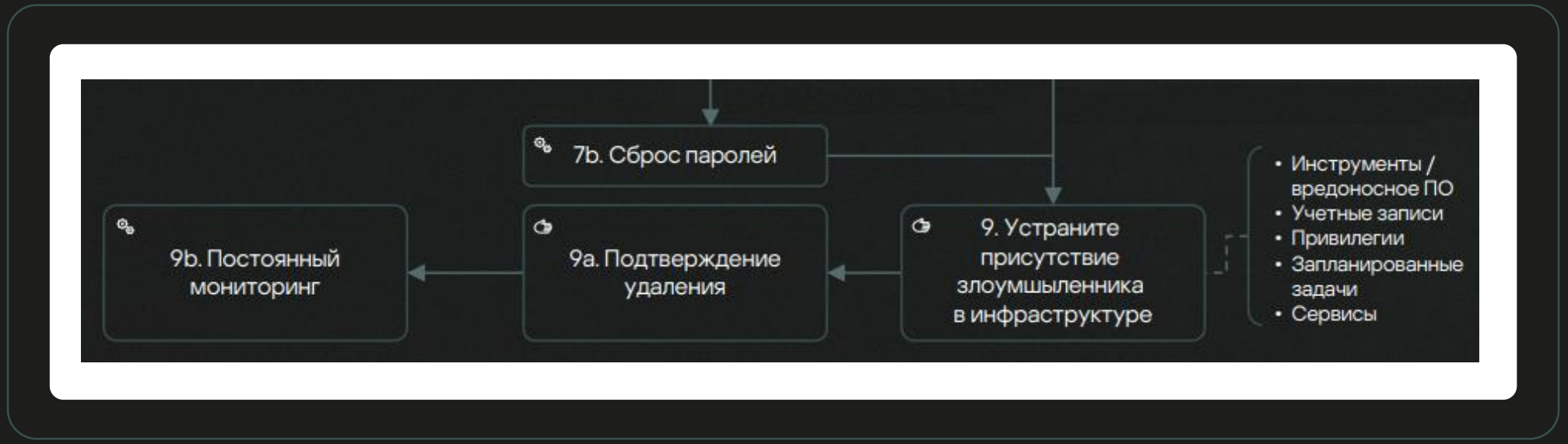
Сценарий Утечки данных. Расследование



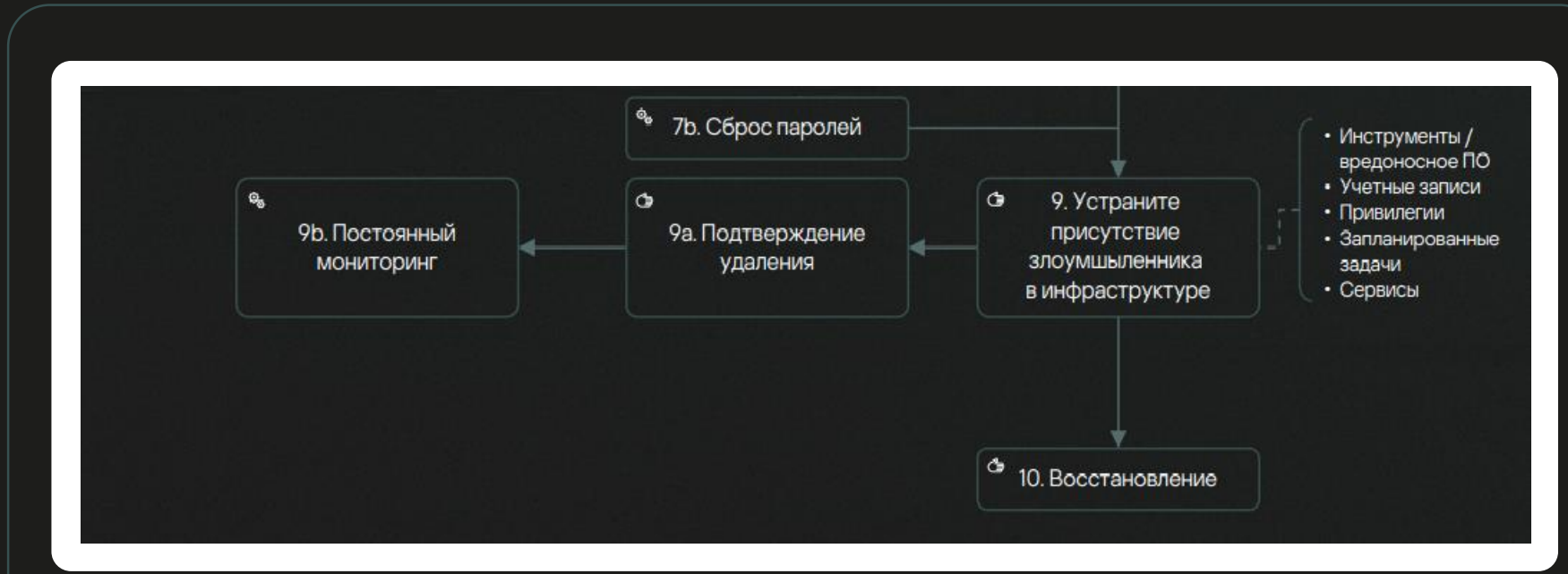
Сценарий Утечки данных. Сдерживание



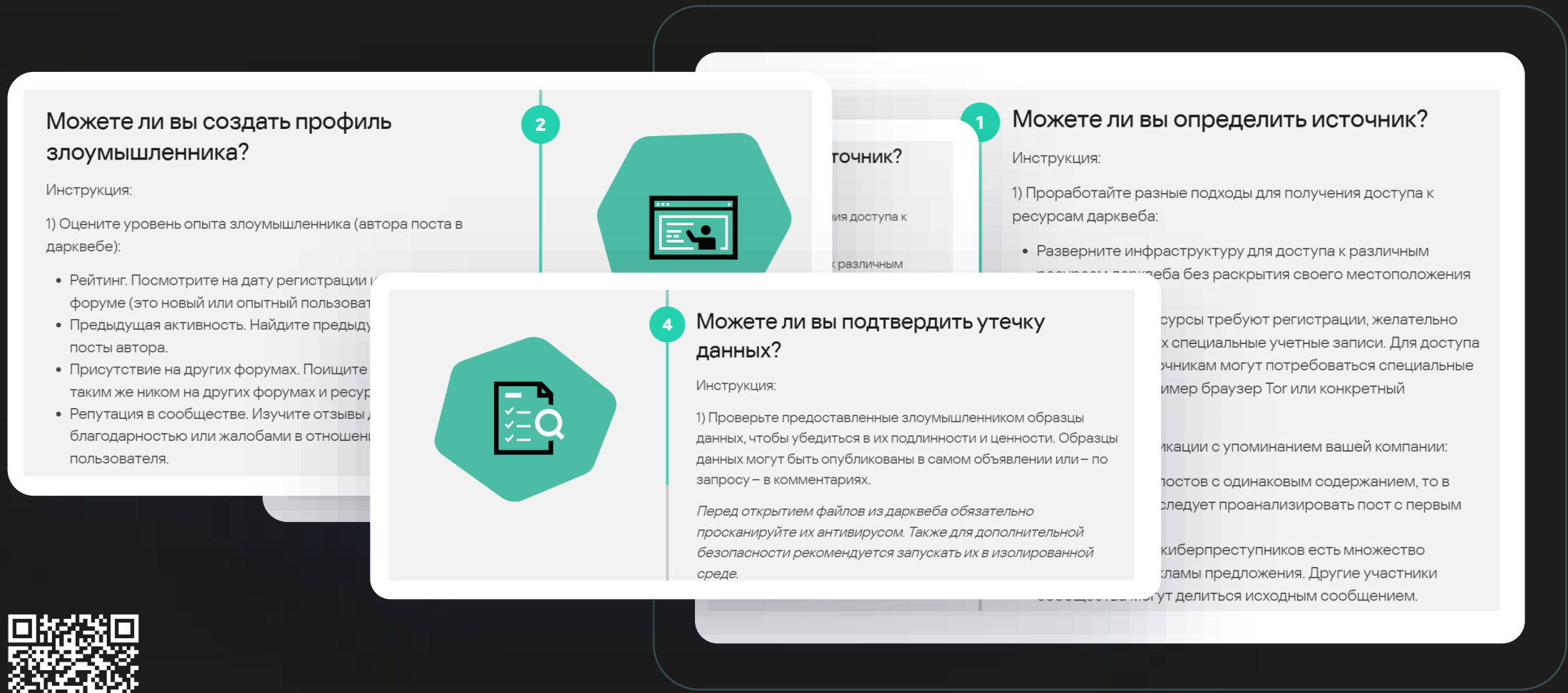
Сценарий Утечки данных. Удаление



Сценарий Утечки данных. Удаление



Используйте гайдлайн



Можете ли вы создать профиль злоумышленника?

Инструкция:

1) Оцените уровень опыта злоумышленника (автора поста в дарквебе):

- Рейтинг. Посмотрите на дату регистрации и
форуме (это новый или опытный пользоват
- Предыдущая активность. Найдите предыду
посты автора.
- Присутствие на других форумах. Поищите
таким же ником на других форумах и ресур
- Репутация в сообществе. Изучите отзывы
благодарностью или жалобами в отношени
пользователя.

Можете ли вы подтвердить утечку данных?

Инструкция:

1) Проверьте предоставленные злоумышленником образцы данных, чтобы убедиться в их подлинности и ценности. Образцы данных могут быть опубликованы в самом объявлении или – по запросу – в комментариях.

Перед открытием файлов из дарквеба обязательно просканируйте их антивирусом. Также для дополнительной безопасности рекомендуется запускать их в изолированной среде.

Можете ли вы определить источник?

Инструкция:

1) Проработайте разные подходы для получения доступа к ресурсам дарквеба:

- Разверните инфраструктуру для доступа к различным
еба без раскрытия своего местоположения

сурсы требуют регистрации, желательно
х специальные учетные записи. Для доступа
очникам могут потребоваться специальные
имер браузер Tor или конкретный

икации с упоминанием вашей компании:

постов с одинаковым содержанием, то в
следует проанализировать пост с первым

киберпреступников есть множество
кламы предложения. Другие участники
гут делиться исходным сообщением.

Если расследование инцидента невозможно ресурсами существующей команды — привлеките квалифицированных отраслевых экспертов

Мы всегда рекомендуем не платить киберпрес-тупникам

20%

людей, заплативших выкуп, не получили свои файлы обратно

Назначьте ответственных лиц.

Создайте процедуры для SOC.

Настройте дарквеб мониторинг.

Спасибо за внимание!

Вопросы

https://dfi.kaspersky.ru/