BI.ZONE

EDRo расследования: как объять необъятное и везде успеть

Антон Степанов

Ведущий специалист по компьютерной криминалистике,
BI.ZONE

BI.ZONE

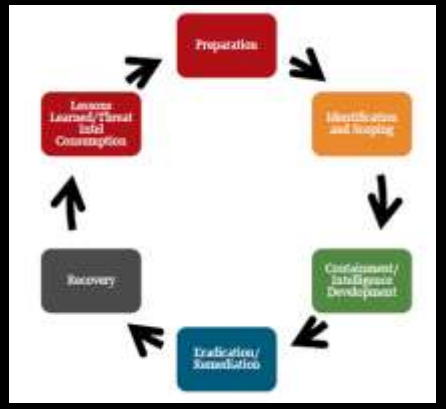
Идеальное расследование

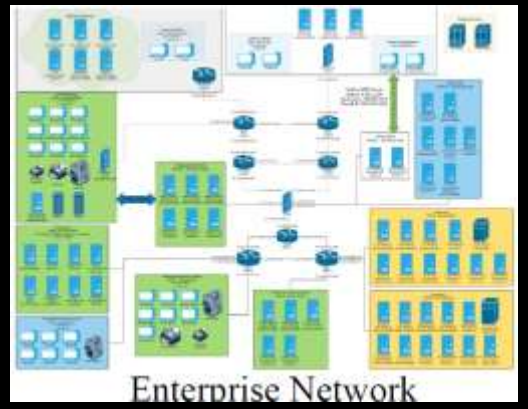
Взгляд со стороны расследователей

DFIR-команда

6 step IR process (SANS)

- Preparation
- Identification and scoping
- Containment
- Eradication/remediation
- Recovery
- Lesson learned





Правоохранительные органы

Изъять все

Спокойно расследовать и изучать каждый вещдок по методике, когда подойдет очередь в экспертном учреждении

BI.ZONE

Идеальное расследование

Взгляд со стороны бизнеса

Быстро вернуть сервисы

Каждый день простоя может стоить сотни миллионов

Обеспечить стабильность работы

Сервисы должны работать без повторных отказов

BI.ZONE

Идеальное расследование

Как совместить подходы **DFIR** и требования бизнеса

EDR
IR

BI.ZONE

Идеальное расследование как услуга

Нужно:

- Восстановить работу

  Сервисы должны максимально быстро возобновить работу

- Не допускать повторных инцидентов

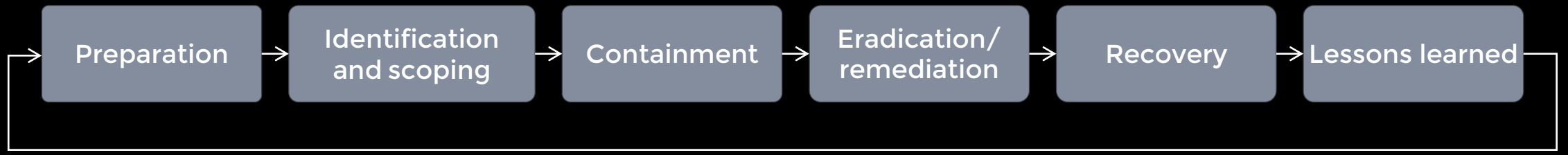
  Если у атакующих остались точки входа, они должны быть найдены и уничтожены

- Провести расследование

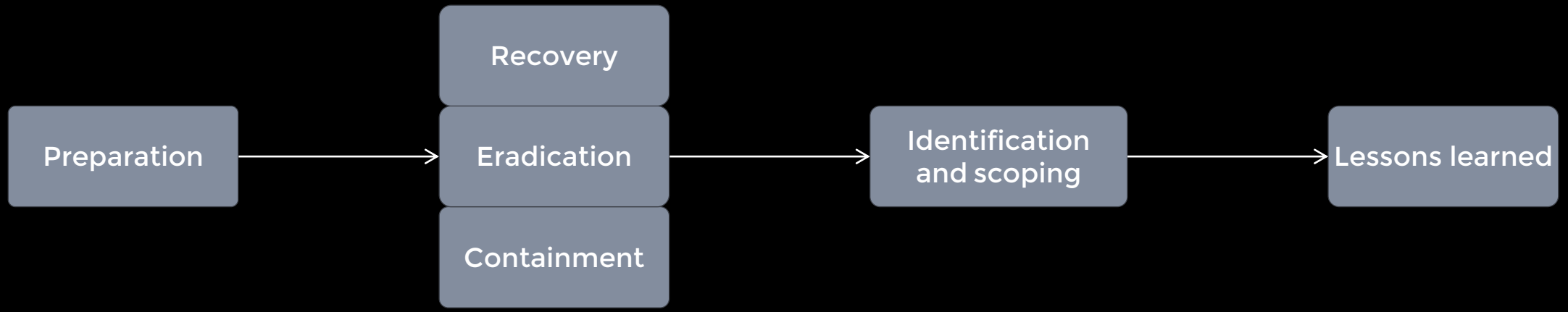
BI.ZONE

Идеальное расследование как услуга

Что должно быть



Что на самом деле



BI.ZONE

Идеальное расследование как услуга

Как мы решали эту проблему на примере двух кейсов с шифрованием

Компания А

- Оказание услуг
- Обширная региональная сеть
- Уровень КБ-зрелости – между низким и средним
- Потери от простоя бизнеса – сотни миллионов в сутки

Компания В

- Телеком-оператор
- Распределенная сеть
- Уровень КБ-зрелости – низкий
- Простой ведущего оператора телеком-услуг в регионе (клиентами являются **>50%** населения региона)

BI.ZONE

1. Как мы действовали

Восстановление инфраструктуры

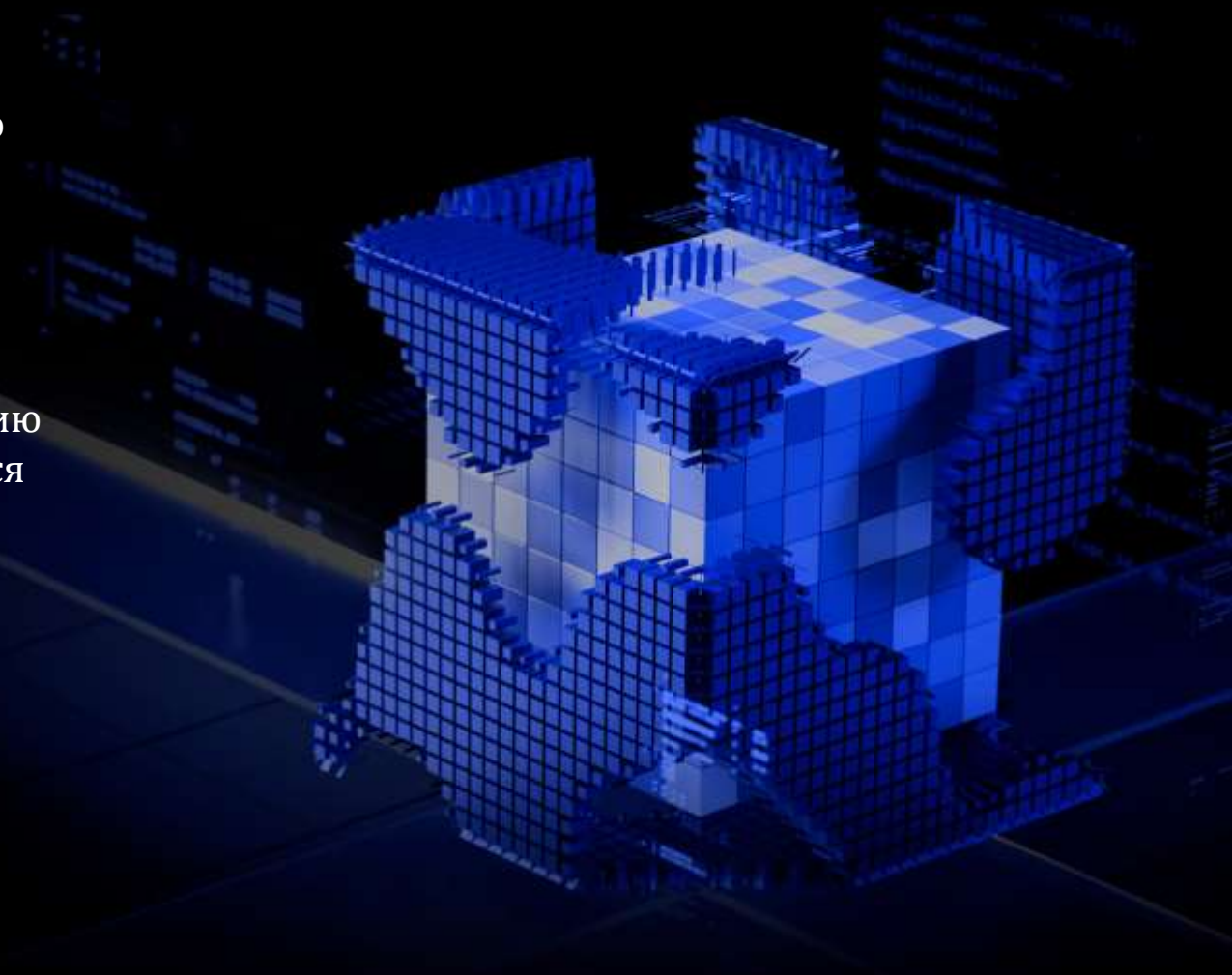
Восстановлением инфраструктуры в состоянии до шифрования занимались интеграторы совместно с клиентами

Защита инфраструктуры и мониторинг

Все восстанавливаемые и вводимые в эксплуатацию хосты защищаются агентами **EDR** и подключаются к мониторингу **SOC**

Расследование

Расследование проводится как классическими методами **DFIR**, так
и при помощи инфраструктуры **EDR**-агентов



BI.ZONE

1. Как мы действовали

День 1

- Восстановление систем
- Установка EDR-агентов во всей инфраструктуре
- Начало исследования систем

День 2

- Анализ телеметрии с EDR-агентов
- Исследование систем и построение килчейна атаки
- Сбор ретроспективных данных со всех систем

День 3

- Настройка сетевой инфраструктуры
- Старт основных сервисов
- Усиленный онлайн-мониторинг событий с EDR-агентов и мгновенное реагирование

BI.ZONE

1. Как мы действовали

День 3 – день 10

- Продолжение активного мониторинга и реагирования
- Ввод в эксплуатацию вспомогательных сервисов с их зачисткой
- Перенастройка инфраструктуры по требованиям КБ

BI.ZONE

2. С чем сталкивались в процессе

Компания А

Попытка удаления файлов виртуальных машин

- Клиенты начали раскатку **EDR**-агентов, но не изолировали часть инфраструктуры от внешних сетей
- Атакующие вновь попали в сеть
- Реакция **SOC**, изоляция хостов
- Атакующие выбиты из инфраструктуры

BI.ZONE

2. С чем сталкивались в процессе

Компания B

Копирование ntds.dit

- На DC заметили копирование ntds.dit
- ntdsutil "ac i ntds" "ifm" "create full c:\root" q q
- Нелегитимные соединения были с почтового сервера, о котором не знали и на котором не стоял агент EDR
- Изоляция хостов – сбор триажей (классический DFIR) – дораскатка агентов на «забытые серверы» + усиленный мониторинг SOC
- Новая атака в процессе расследования атаки старой
- Ретроспективный анализ: такие атаки происходили в инфраструктуре регулярно

BI.ZONE

3. Преимущества гибридного подхода

Преимущества перед DFIR

- Полное покрытие инфраструктуры **EDR**-агентами
- Активная защита и мониторинг в процессе расследования
- Возможность отслеживать все события в режиме реального времени
- Возможность оперативного сбора ретроспективных данных с любой части инфраструктуры
- Гибкость работы, быстрая реакция на любые проблемные ситуации

BI.ZONE

3. Преимущества гибридного подхода

Преимущества для клиента

- Можно спокойно заниматься восстановлением инфраструктуры
- Все восстанавливаемые сервисы сразу заводятся на мониторинг
- Быстрая отработка, реагирование и расследование любых новых атак
- Бесшовный переход на услугу **TDR** после окончания расследования
- Возможность получить дополнительны данные о мисконфигурациях в инфраструктуре
- Пилот сервиса **TDR** в «боевых» условиях

BI.ZONE

Q&A