Федор Чунижеков

Старший аналитик исследовательской группы, Positive Technologies

Антон Исаев

Руководитель направления маркетинга метапродуктов, Positive Technologies

phd 2 Positive Hack Days Fest

от ■ positive technologies

Готовы ли российские компании противостоять кибератакам?

Об исследовании

Цель исследования:

Выявить проблемы организаций в вопросах готовности противодействовать кибератакам

Опрос проводился
в I квартале 2024 года

Аудитория:
читатели изданий, telegram-каналов и профессиональных сообществ ИТ и ИБ тематика

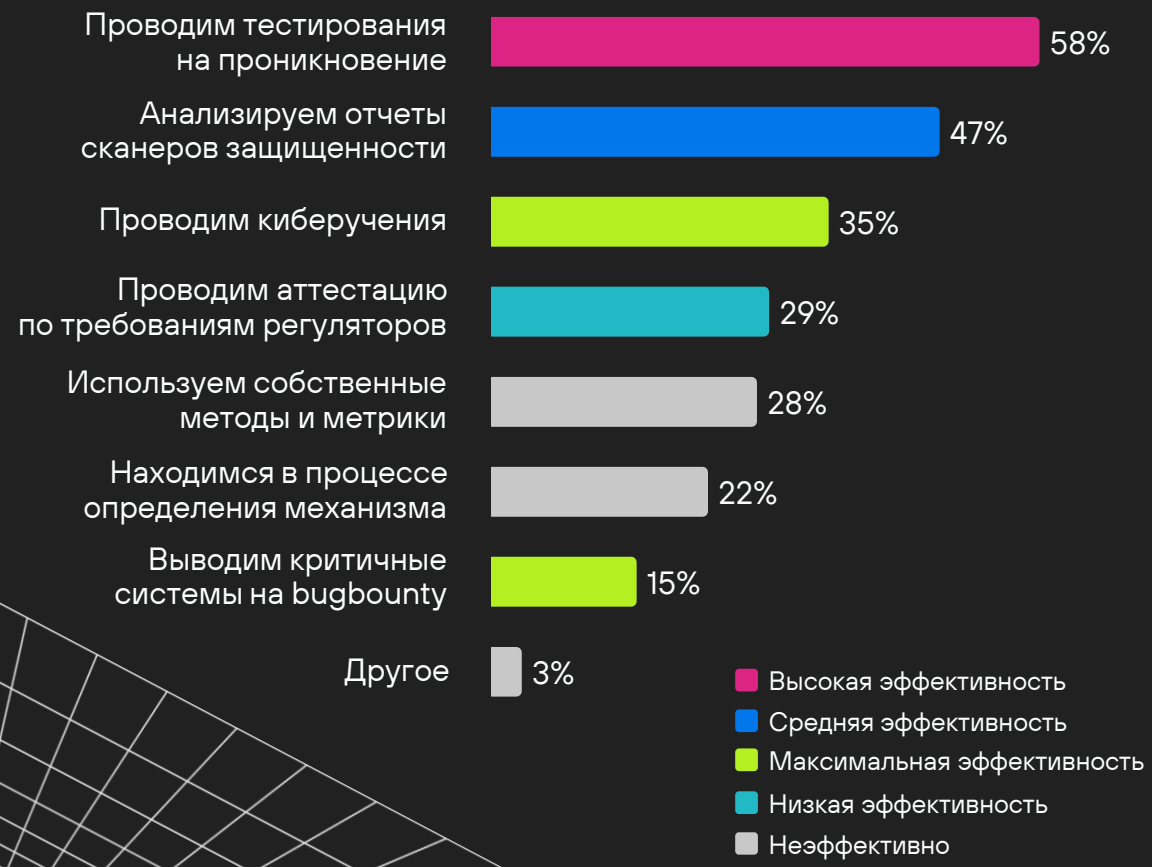
>650
респондентов

>60
представителей организаций


Готовность противостоять кибератакам
Оценивать / Контролировать
Выстраивать / Поддерживать
Методы
Метрики
Усиление защищённости (hardening)
Мониторинг и реагирование

Как организации
оценивают готовность противостоять кибератакам?

Методы оценки готовности противостоять кибератакам (доля участников)



лишь 28%

организаций используют показательные методы оценки: пентесты, киберучения

Как часто

организации проводят оценку готовности противостоять кибератакам?

Периодичность оценки готовности противостоять кибератакам

21% организаций

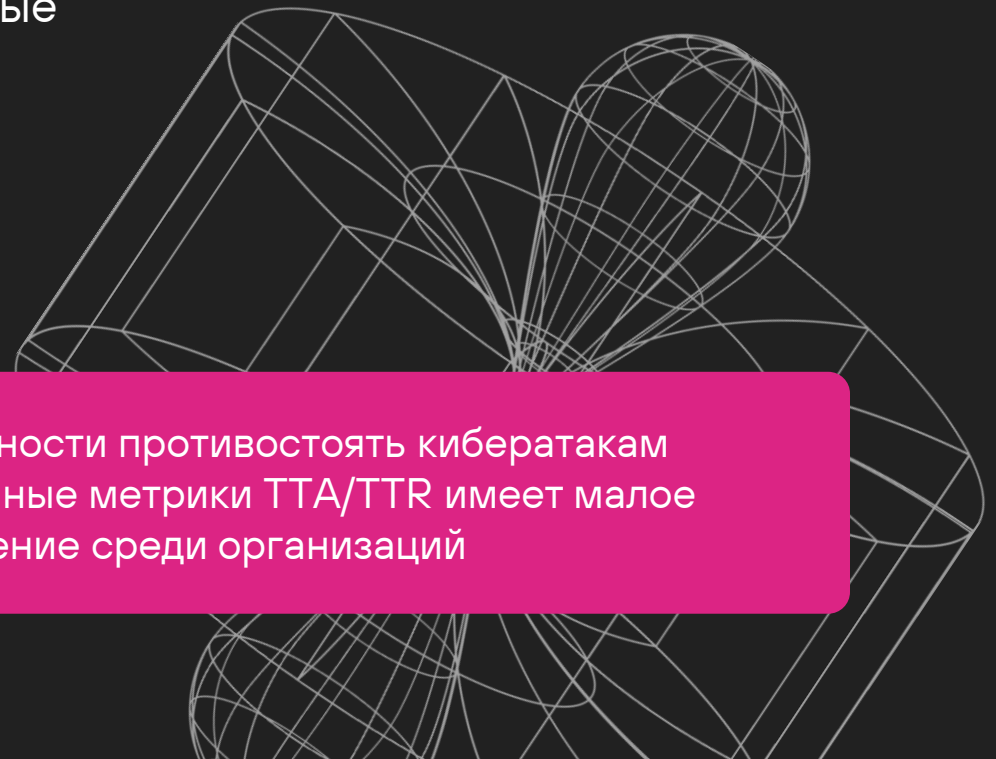
проводят пентест лишь раз в год, либо по запросу

Организации не знают актуальный уровень киберустойчивости в моменты между проведением оценок готовности противостоять кибератакам

Через какие метрики
организации оценивают свою готовность противостоять кибератакам?

только 4%

организаций используют количественные метрики

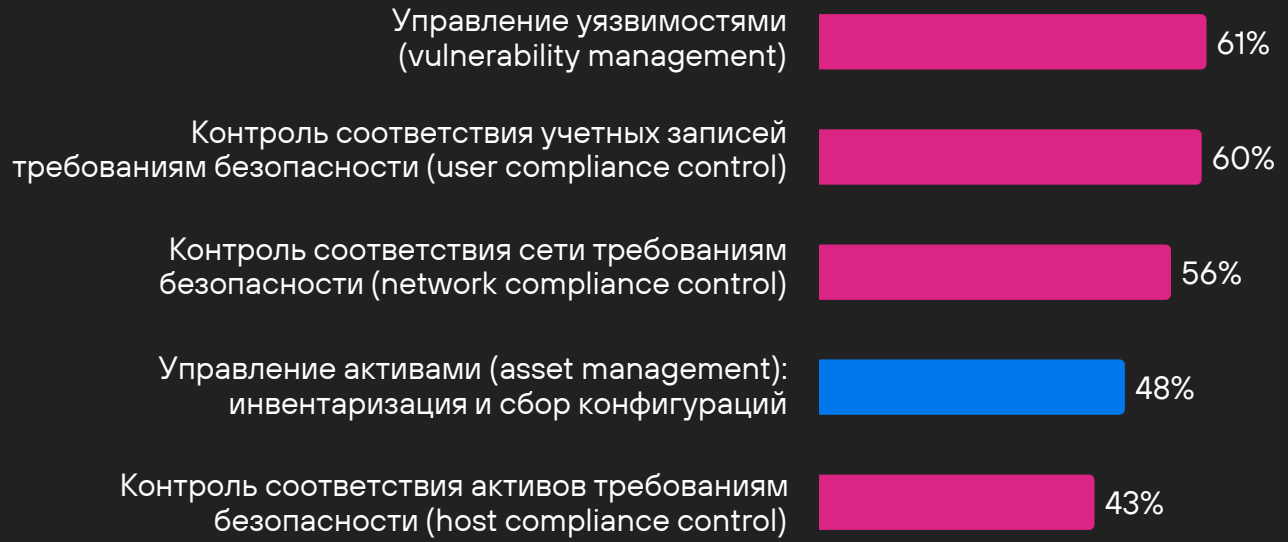


Оценка готовности противостоять кибератакам через временные метрики TTA/TTR имеет малое распространение среди организаций

- Временные метрики обнаружения и реагирования на атаки
- Объем покрытия инфраструктуры средствами защит
- Количество и критичность обнаруженных уязвимостей
- Определение векторов возможных атак злоумышленника
- Другое

Какие процессы
усиления защищённости внедрили/ внедряют организации?

Процессы усиления защищенности инфраструктуры выстроенные/ строящиеся в отделе ИБ



80% организаций
не занимаются полноценным укреплением ИТ-инфраструктуры

52% организаций
проводят харденинг инфраструктуры без внедрения процесса управления активами

70% организаций
приоритизируют задачи харденинга основываясь только на критичности активов

Главная цель укрепления ИТ-инфраструктуры: Удлинить цепочку шагов и действий атакующего, заставить его использовать наиболее сложные, и затратные по времени техники **(увеличить TTA)**

С какими сложностями
сталкиваются организации при выполнении задач по усилению защищенности ИТ-инфраструктуры?

Сложности, с которыми сталкиваются организации при выполнении задач по усилению защищенности ИТ-инфраструктуры

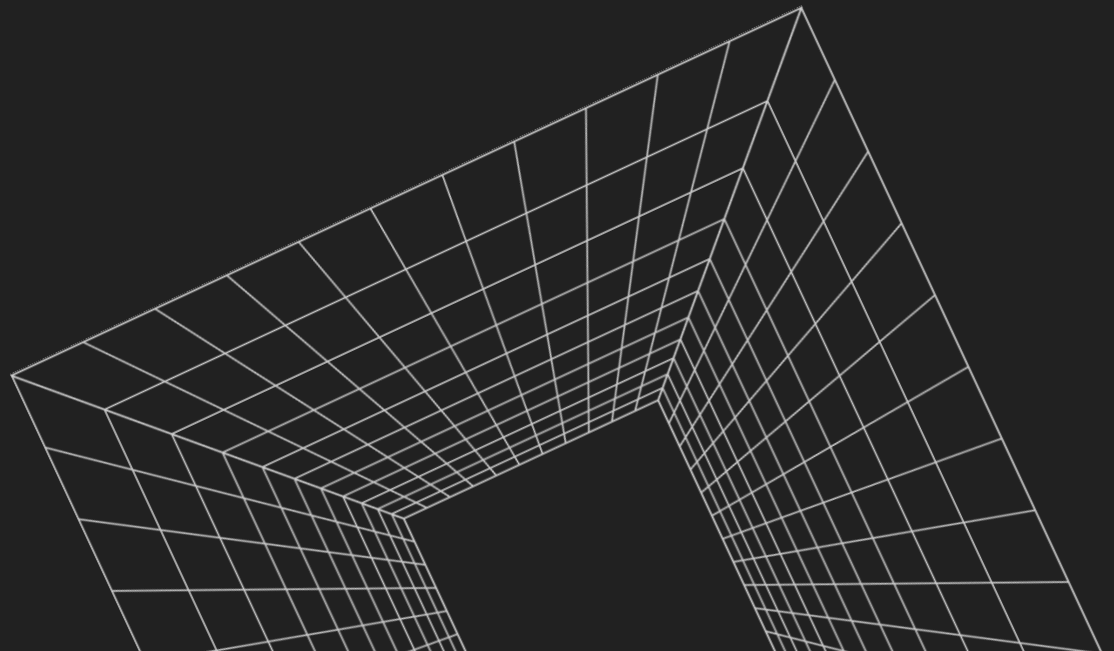
Отсутствие компетенций и времени для выстраивания харденинга в значительной мере влияет на готовность противостоять кибератакам

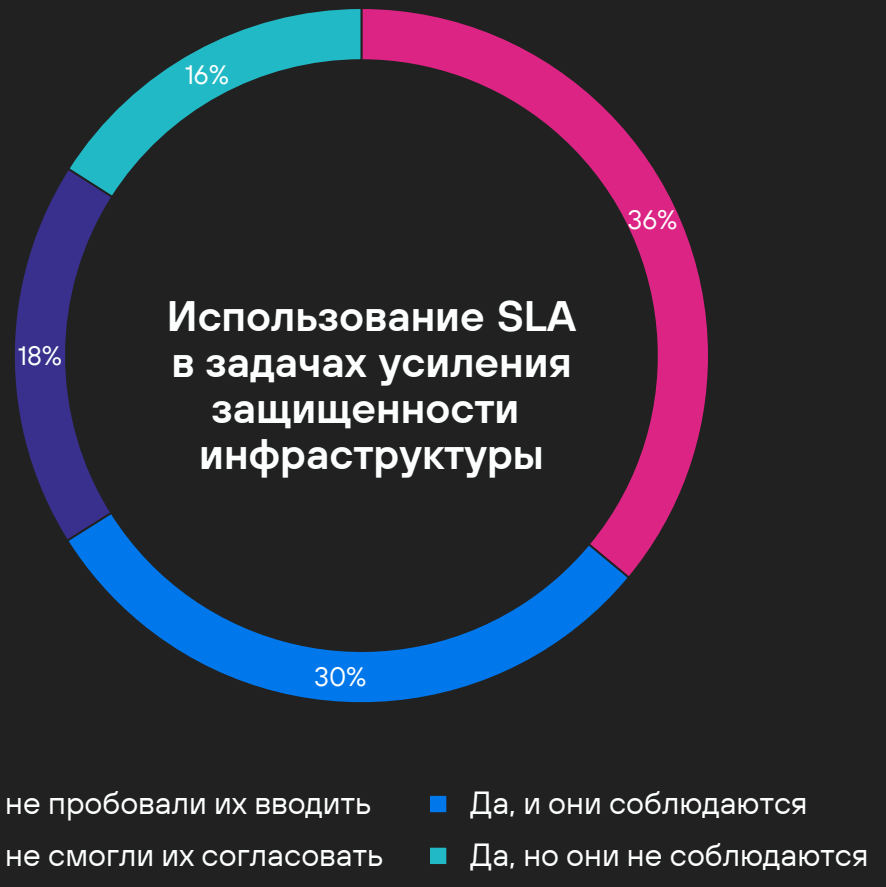
Как обстоят дела

с SLA между ИТ и ИБ в задачах усиления защищенности инфраструктуры?

70% **организаций**

имеют проблемы с формированием регламента взаимодействия между командами ИБ и ИТ в задачах усиления защищенности инфраструктуры

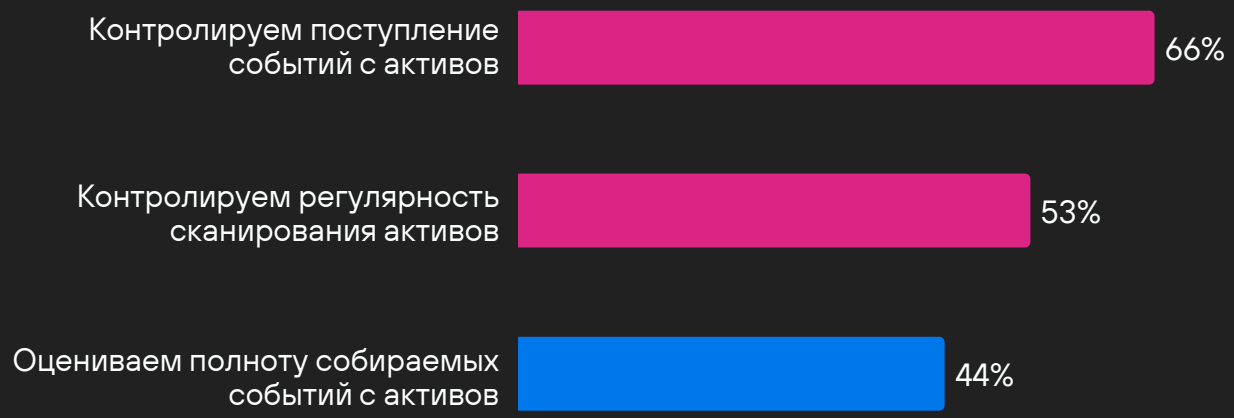




Что отслеживают

организации в средствах мониторинга и защиты инфраструктуры?

Главная цель контроля мониторинга ИТ-инфраструктуры направлена на сокращение времени выявления и реагирования на атаку (сокращение TTD и TTR)



39% организаций

контролируют факт поступления событий с активов, но не их полноту

19% организаций

контролируют факт поступления событий с информационных активов, их регулярность и полноту одновременно

36% организаций

занимаются мониторингом и реагированием 24x7

Проблемы
российский организаций при подготовке к отражению кибератак:

- Малый уровень распространённости объективных методов оценки готовности противостоять кибератакам (с привлечением белых хакеров)
- Выборочное усиление защищённости ИТ-инфраструктуры
- Редкая оценка готовности противостоять кибератакам
- Отсутствие должного внимания контролю мониторинга
- Малое распространение временных метрик (TTA, TTR)

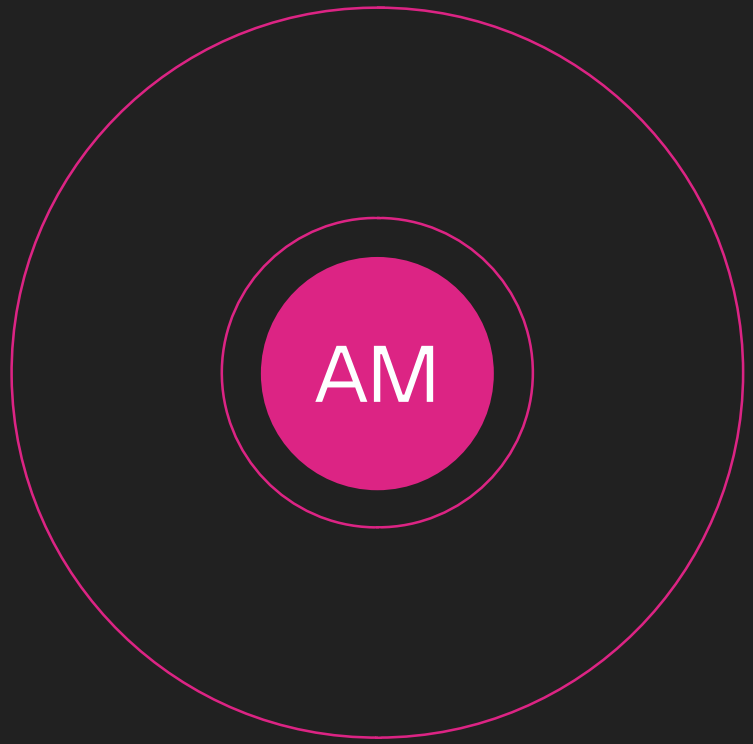
phd 2X pt

Готовимся противостоять кибератакам

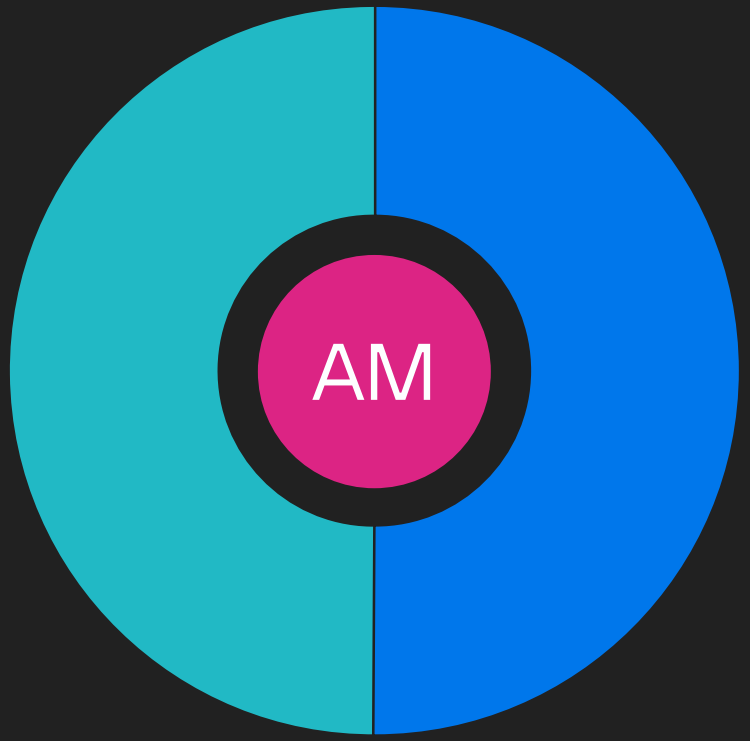
phd 2X pt

Готовимся противостоять кибератакам

Готовимся противостоять кибератакам



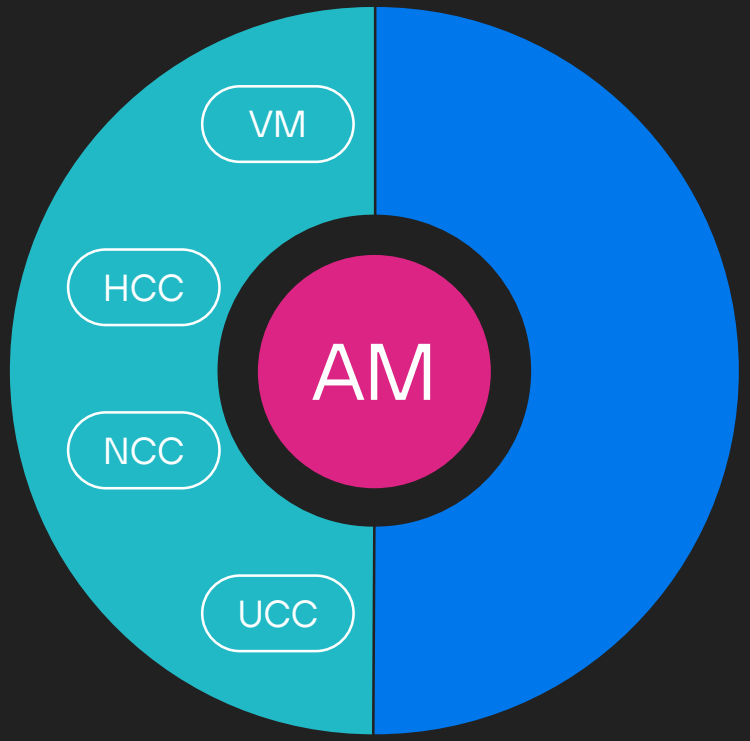
Готовимся противостоять кибератакам



Готовимся противостоять кибератакам

/ Усиление защищённости инфраструктуры (Харденинг)

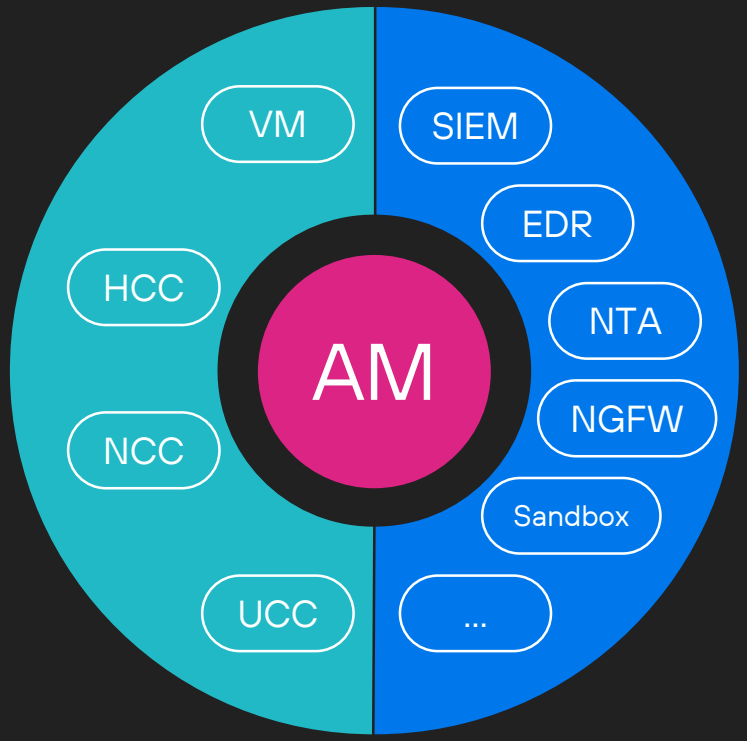
Цель:
сделать действия хакера более трудными, долгими, затратными, а также более «шумными», чтобы заметить его как можно раньше



Готовимся противостоять кибератакам

/ Усиление защищённости инфраструктуры (Харденинг)

Цель:
сделать действия хакера более трудными, долгими, затратными, а также более «шумными», чтобы заметить его как можно раньше



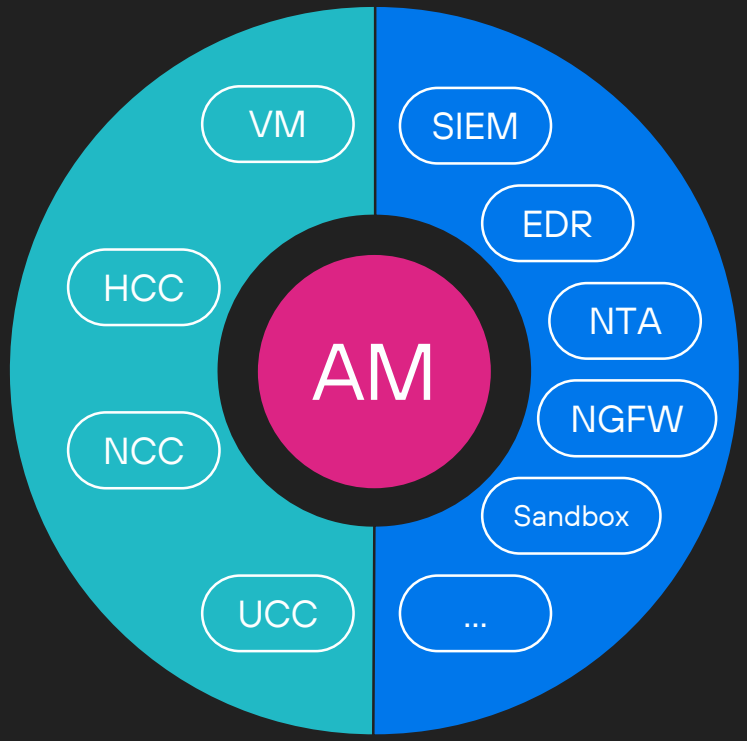
/ Мониторинг и Реагирование

Цель:
настройка средств защиты и их контроль, чтобы точно увидеть действия хакера и иметь возможность для быстрого реагирования

Готовимся противостоять кибератакам

Усиление защищённости инфраструктуры (Харденинг)

Цель:
сделать действия хакера более трудными, долгими, затратными, а также более «шумными», чтобы заметить его как можно раньше



Мониторинг и Реагирование

Цель:
настройка средств защиты и их контроль, чтобы точно увидеть действия хакера и иметь возможность для быстрого реагирования

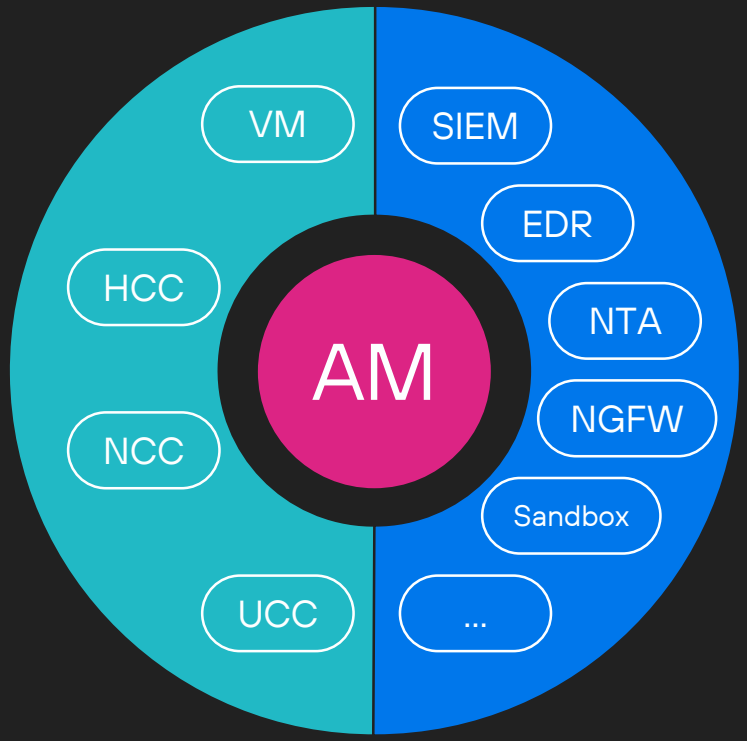
ИТ

ИБ

Готовимся противостоять кибератакам

/ Усиление защищённости инфраструктуры (Харденинг)

Цель:
сделать действия хакера более трудными, долгими, затратными, а также более «шумными», чтобы заметить его как можно раньше



/ Мониторинг и Реагирование

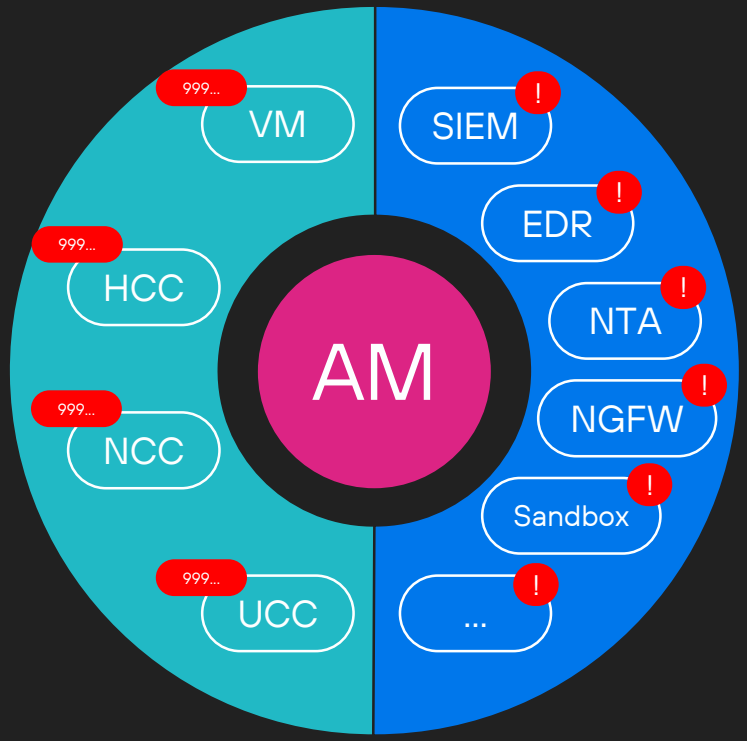
Цель:
настройка средств защиты и их контроль, чтобы точно увидеть действия хакера и иметь возможность для быстрого реагирования

ИТ ⟷ SLA ⟷ ИБ

Готовимся противостоять кибератакам

/ Усиление защищённости инфраструктуры (Харденинг)

Цель:
сделать действия хакера более трудными, долгими, затратными, а также более «шумными», чтобы заметить его как можно раньше



/ Мониторинг и Реагирование

Цель:
настройка средств защиты и их контроль, чтобы точно увидеть действия хакера и иметь возможность для быстрого реагирования

ИТ ⟷ SLA ⟷ ИБ

Готовимся противостоять кибератакам

/ Усиление защищённости инфраструктуры (Харденинг)

Цель:
сделать действия хакера более трудными, долгими, затратными, а также более «шумными», чтобы заметить его как можно раньше

/ Мониторинг и Реагирование

Цель:
настройка средств защиты и их контроль, чтобы точно увидеть действия хакера и иметь возможность для быстрого реагирования

ИТ ⟷ SLA ⟷ ИБ

Готовимся противостоять кибератакам

/ Усиление защищённости инфраструктуры (Харденинг)

Цель:
сделать действия хакера более трудными, долгими, затратными, а также более «шумными», чтобы заметить его как можно раньше

/ Мониторинг и Реагирование

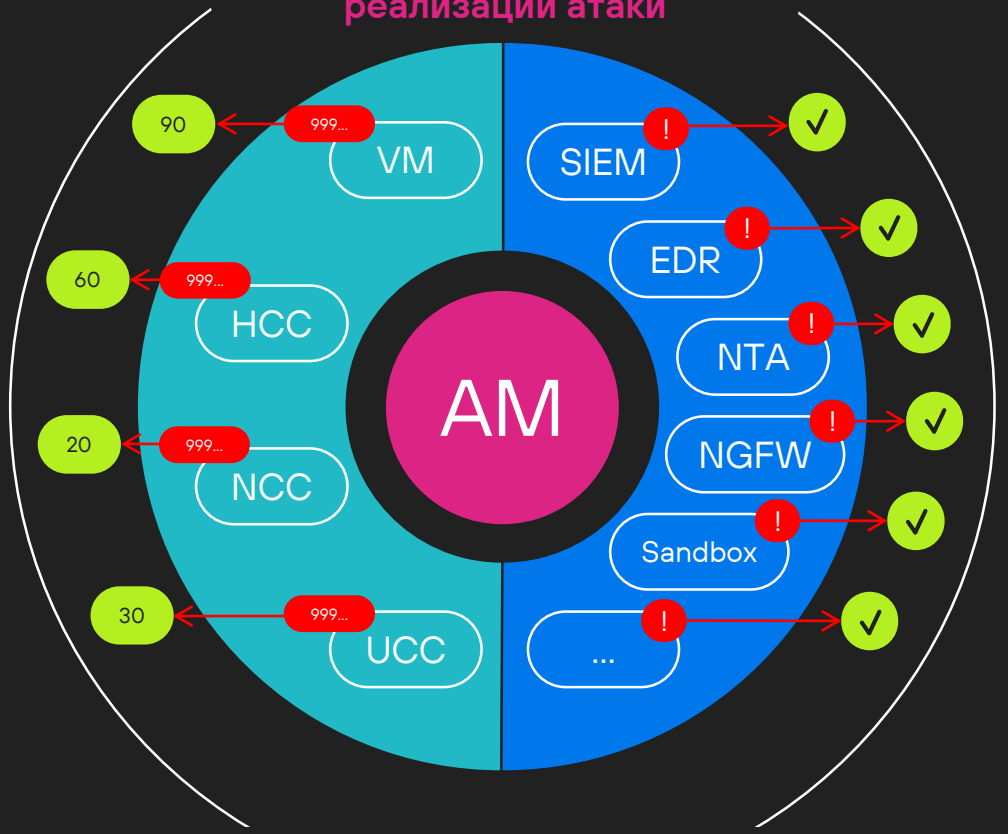
Цель:
настройка средств защиты и их контроль, чтобы точно увидеть действия хакера и иметь возможность для быстрого реагирования

ИТ ⟷ SLA ⟷ ИБ

Готовимся противостоять кибератакам

TTA
Time To Attack

Потенциальные маршруты реализации атаки



/ Усиление защищённости инфраструктуры (Харденинг)

Цель:
сделать действия хакера более трудными, долгими, затратными, а также более «шумными», чтобы заметить его как можно раньше

/ Мониторинг и Реагирование

Цель:
настройка средств защиты и их контроль, чтобы точно увидеть действия хакера и иметь возможность для быстрого реагирования

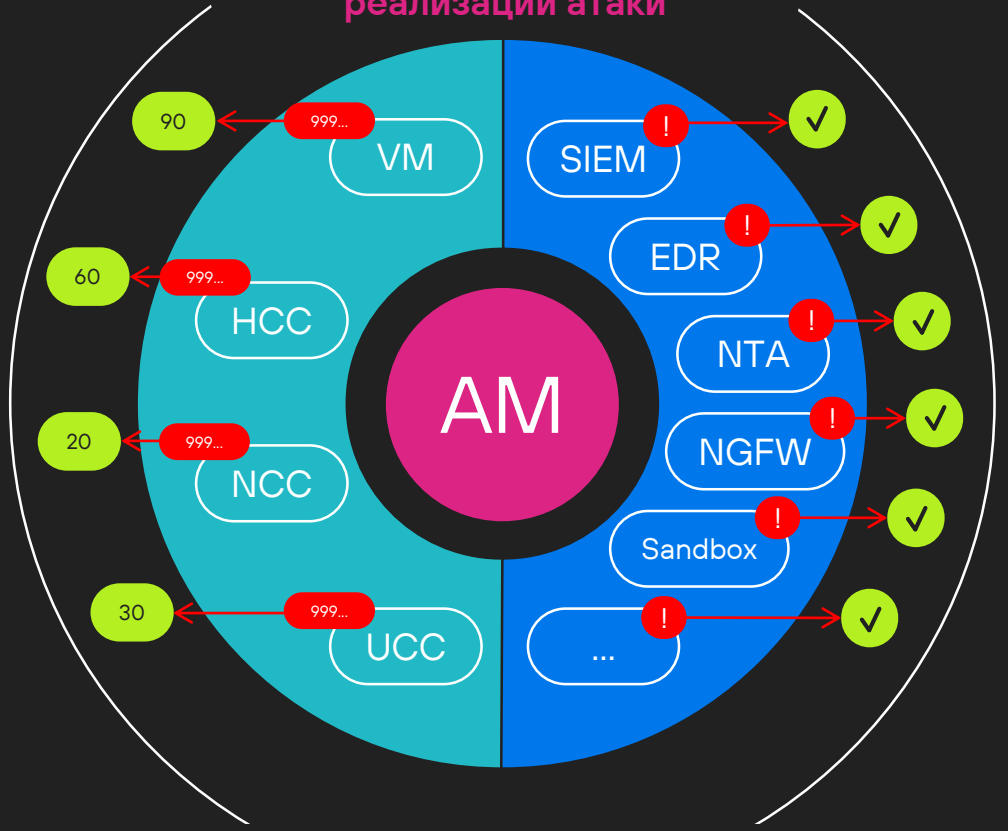
ИТ ⟷ SLA ⟷ ИБ

Готовимся противостоять кибератакам

TTA Time To Attack

TTD + ... + TTR Time To Detect / Time To Response

Потенциальные маршруты реализации атаки



/ Усиление защищённости инфраструктуры (Харденинг)

Цель:
сделать действия хакера более трудными, долгими, затратными, а также более «шумными», чтобы заметить его как можно раньше

/ Мониторинг и Реагирование

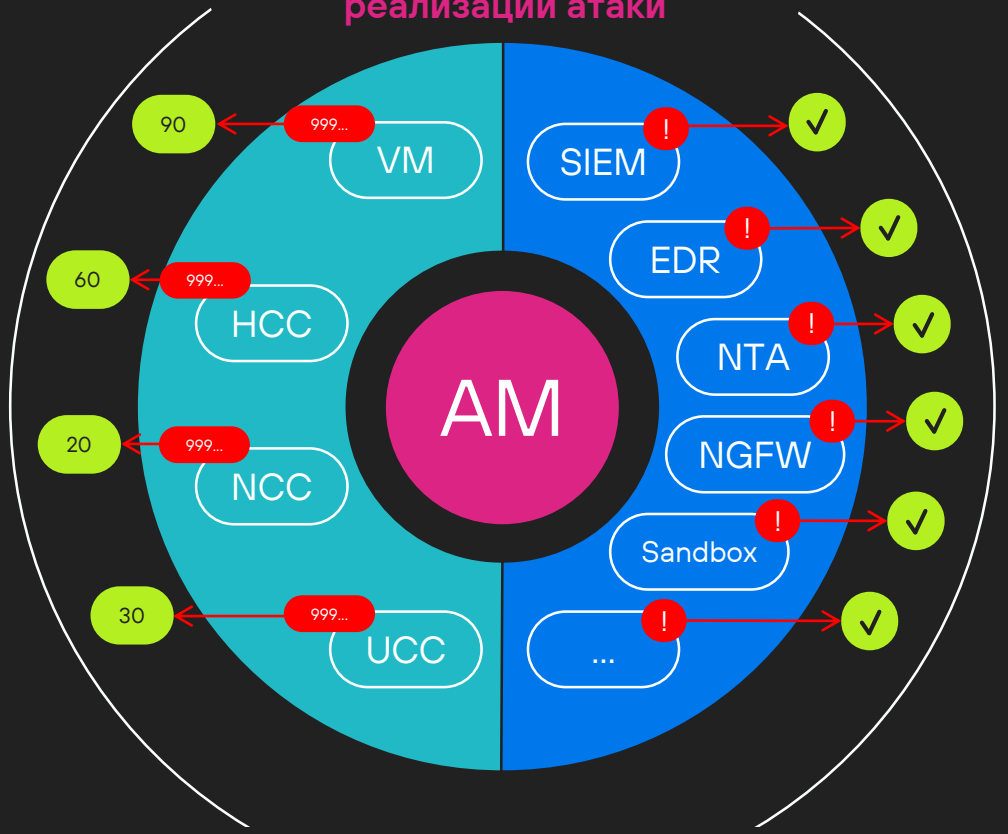
Цель:
настройка средств защиты и их контроль, чтобы точно увидеть действия хакера и иметь возможность для быстрого реагирования

ИТ ⟷ SLA ⟷ ИБ

Готовимся противостоять кибератакам

TTA (Time To Attack) > TTD (Time To Detect) + ... + TTR (Time To Response)

Потенциальные маршруты реализации атаки



/ Усиление защищённости инфраструктуры (Харденинг)

Цель:
сделать действия хакера более трудными, долгими, затратными, а также более «шумными», чтобы заметить его как можно раньше

/ Мониторинг и Реагирование

Цель:
настройка средств защиты и их контроль, чтобы точно увидеть действия хакера и иметь возможность для быстрого реагирования

ИТ ⟷ SLA ⟷ ИБ

Чек-лист

решения для оценки и контроля готовности противостоять кибератакам

1 **Непрерывный поиск потенциальных маршрутов атак внутри инфраструктуры на основе:**

- сетевой достижимости активов
- наличия уязвимостей
- ошибок/недостаток конфигураций ОС/ПО
- ошибок/недостаток сетевой конфигурации
- избыточных привилегий пользователей
- использования техник MITRE ATT&CK
- возможностей удалённого доступа

2 **Расчёт метрик TTA и TTD/TTR для маршрутов атак в реальном времени**

3 **Анализ и приоритизация маршрутов атак:**

- по TTA/TTD/TTR
- по количеству шагов хакера
- по возможностям устранения

4 **Формирование и приоритизация практических рекомендаций на маршрутах атак:**

- устранение / усложнение (харденинг)
- повышение «видимости» хакера и готовности ему противостоять (мониторинг и реагирование)

5 **Установка и контроль сроков реализации рекомендаций (SLA),** исходя из согласованных в организации бизнес-процессов и рассчитанных показателей TTA/TTD/TTR

phd 2 Positive Hack Days Fest

от positive technologies

Спасибо!