Михаил Кадер
Positive Technologies

Киберполигоны и Кибериспытания

Что, зачем и как правильно их готовить

13.06.2024

Результативная ИБ

1. Оценка практической возможности использования уязвимостей и угроз
2. Формирование перечня и отслеживание недопустимых событий
3. Оценка возможности возникновения и реализации недопустимых событий
4. Контроль результативности (эффективности)
5. Проведение регулярных практических киберучений
6. Регулярный анализ и оценка новых угроз (threat intelligence)
7. Непрерывный процесс выявления и устранения угроз и уязвимостей
8. Непрерывный процесс мониторинга и реагирования на компьютерные инциденты
9. И многое другое ...

КИБЕРПОЛИГОН:
ГДЕ «КРАСНЫЕ» ВСТРЕЧАЮТСЯ С «СИНИМИ»

АТАКИ

Высококвалифицированные исследователи из сообщества

Технологические и бизнес-процессы (2023 – на базе 7 отраслей)

~ 150 возможных атак

Готовая инфраструктура (корпоративная сеть + АСУТП)

Средства мониторинга ИБ

МОНИТОРИНГ
РАССЛЕДОВАНИЕ
РЕАГИРОВАНИЕ

Настройка и сопровождение СЗИ

Судейство, прием «красных» и «синих» отчетов

Мониторинг инцидентов и анализ цепочек атак

ЗАДАЧИ ОНЛАЙН-ПОЛИГОНА

СДЕЛАТЬ АТАКУ ЗАШКАЛИВАЮЩЕ ДОРОГОЙ ДЛЯ ЗЛОУМЫШЛЕННИКОВ,
СОХРАНЯЯ БАЛАНС МЕЖДУ БЕЗОПАСНОСТЬЮ И ЭФФЕКТИВНОСТЬЮ

ЭКСПЕРТИЗА ИБ

- Проверка экспертизы SOC
- Постоянный поток информации о нетривиальных техниках и тактиках атакующих
- Отработка политик и плейбуков
- Где актуально: рост экспертизы внутренней red team

ЭФФЕКТИВНОСТЬ СЗИ

- Достаточность набора СЗИ
- Корректность настроек СЗИ (при изменении набора и настроек — можно сравнивать «было-стало»)
- Возможность пилотирования и сравнения продуктов разных производителей

ЗАЩИЩЕННОСТЬ ИНФРАСТРУКТУРЫ

- Умение ИБ и ИТ слаженно предотвращать, выявлять и реагировать
- Адекватность реагирования (в т.ч. эксперименты с разными степенями харденинга)
- Возможность подключения своей инфраструктуры, оценка ее устойчивости (в т.ч. «было-стало» с разными настройками)
- Постоянное добавление новых объектов инфраструктуры

COMPLIANCE & BEST PRACTICES

- Соответствие требованиям регуляторов по учениям
- Демонстрация передового подхода организации к ИБ — учения как яркое мероприятие
- Проверка уровня реальной защищенности компании (результативная кибербезопасность)

ВСЕ ЭТО — БЕЗ КАКОГО БЫ ТО НИ БЫЛО
УЩЕРБА ДЛЯ РЕАЛЬНОЙ ИНФРАСТРУКТУРЫ

ОТРАСЛЕВАЯ СТРУКТУРА ПОЛИГОНА

ИНФРАСТРУКТУРА 7 ОТРАСЛЕЙ (КОРПОРАТИВНАЯ И ТЕХНОЛОГИЧЕСКАЯ СЕТЬ)

РЕЛЕВАНТНЫЕ ДЛЯ ОТРАСЛЕЙ РИСКИ

1. **Управляющая компания**
   ЖКХ, ритейл, умный город
2. **Транспортная компания**
   Ж/д, дорожная сеть, порт, аэропорт, грузоперевозки
3. **Металлургия**
   Доменная печь, прокатный стан, транспортировка, сбыт
4. **Нефть и газ**
   Добыча, транспортировка, НПЗ, реализация нефтепродуктов, АЗС
5. **Электроэнергетика**
   Генерация (ГЭС, ТЭЦ, ветер, солнце), транспортировка, сбыт
6. **Банковская система**:
   ЦБ (межбанк), традиционный банк, цифровой банк, эквайринг
7. **Атомная отрасль**
   Добыча, обогащение, генерация, захоронение

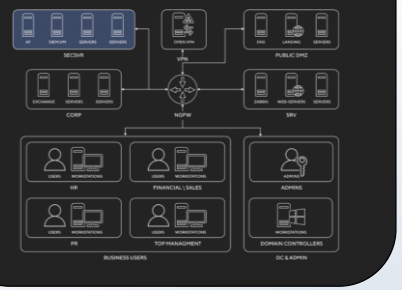
ЗАЩИЩЕННОСТЬ БЕЗ УЩЕРБА ДЛЯ РЕАЛЬНОЙ ИНФРАСТРУКТУРЫ

Суть кибербитвы

> 200
атакующих

Атакуемая инфраструктура

Корпоративная сеть



АСУТП

- ЖКХ и городское управление
- Нефть и газ
- Транспорт
- Электроэнергетика
- Банковская система
- Металлургия
- Атомная отрасль
- ИТ-компания
- Космос

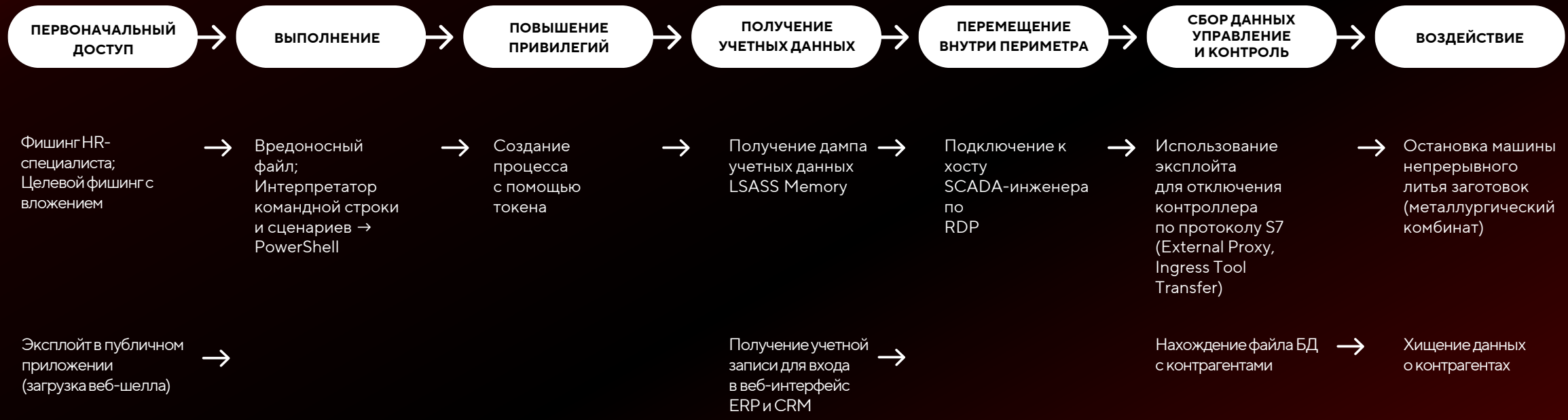
СЗИ

> 80
расследователей

> 20
защитников

ПРИМЕРЫ АТАК, РЕАЛИЗУЕМЫХ НА ПОЛИГОНЕ (1)

Показаны упрощенные цепочки атак, без служебных этапов



ПРИМЕРЫ АТАК, РЕАЛИЗУЕМЫХ НА ПОЛИГОНЕ (2)

Показаны упрощенные цепочки атак, без служебных этапов

Зачем люди проводят неделю на киберполигоне?

Прокачка экспертизы SOC

Мониторинг и расследование

Насмотренность

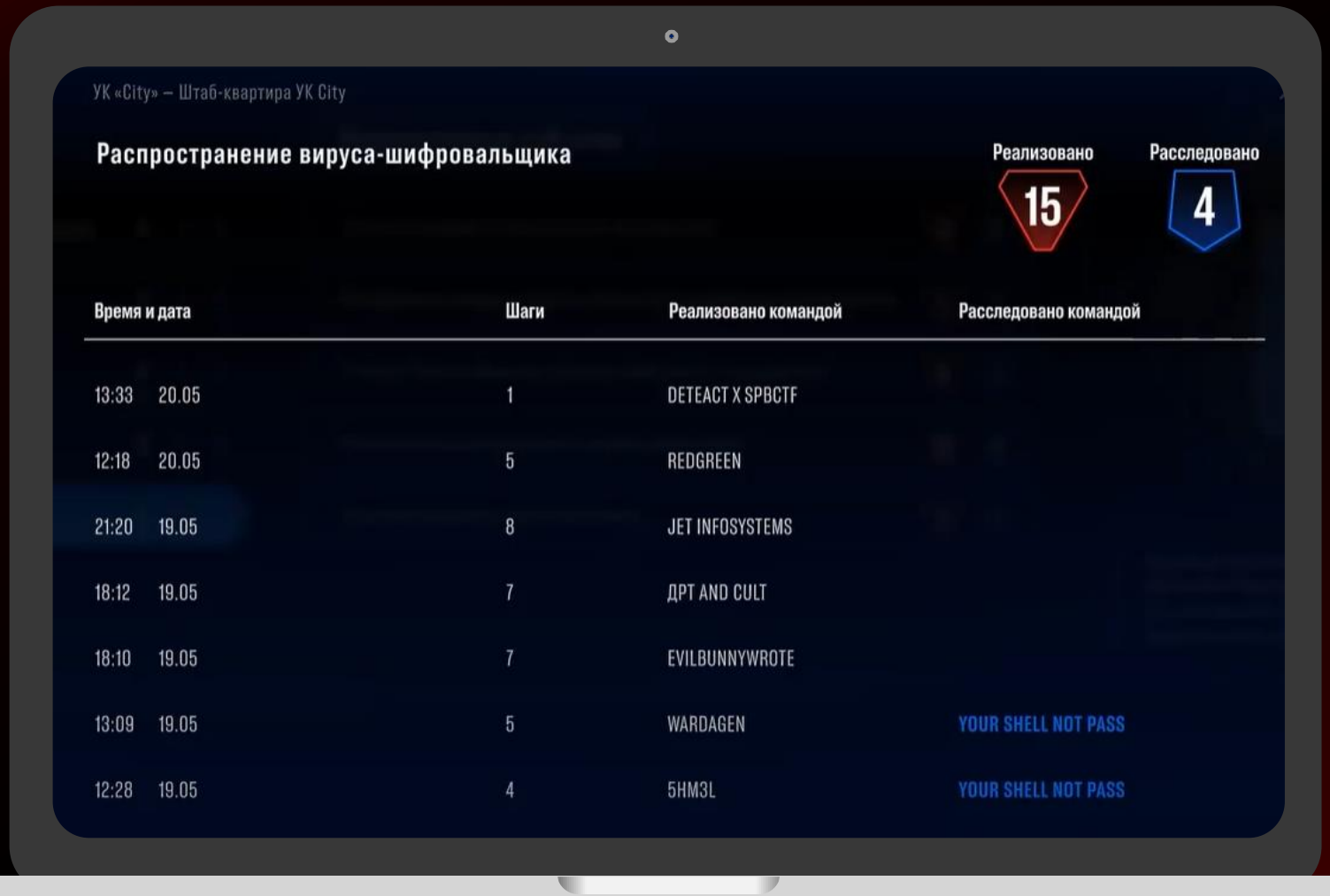
- Соприкосновение с десятками сложных атак и сотней атомарных инцидентов
- Разные тактики и техники атакующих, в т.ч. нетривиальные
- Реализация одного события разными путями

Объективная оценка готовности команды

Практикум по мониторингу

- Отработка умения работать с разными классами СЗИ и разными инфраструктурами
- Использование правил корреляции
- Предварительный анализ сети и проверка гипотез

Реализация одного события разными способами



Прокачка экспертизы ИБ

Реагирование

Укрепление сети и реагирование

- Использование функционала PT xDR и других продуктов
- Блокировка учеток, блокирование входящего и исходящего трафика, разрыв VPN- и SSH-соединения, отзыв ключей для учетной записи, и т.д.

В реагирование лучше «играть» вместе с ИТ

Безопасность vs работоспособность?

- Команда отвечает за работоспособность и доступность сервисов
- Поиск баланса между безопасностью и интересами бизнеса

Развитие команды и процессов

Мониторинг, расследование и реагирование

Развитие сотрудников и ротация

- Доучивание первой линии во вторую и второй в третью
- Определение оптимальных ролей для членов команды

Отладка процессов SOC

- Проверка правильности и достаточности структуры SOC
- Отработка плейбуков

Простой способ экспериментов с процессами и оргструктурой. И мотивация.

Зачем люди проводят на киберполигоне ~~неделю~~ год?

Максимизация эффективности СЗИ

«Выжать максимум из ваших коробок»

Отладка настроек СЗИ

Повышение осведомленности за счет экспериментов с настройками, источниками, правилами

Без ущерба для реальной инфраструктуры

Достаточность набора СЗИ

- Наличие необходимых классов продуктов
- Выбор и пилотирование продукта конкретного производителя (PoC)

Защищенность своей инфраструктуры

Подключение своих сервисов и устройств

- Проверка ключевых систем в условиях множественных атак
- Легкое подключение

Без ущерба для реальной инфраструктуры

Постоянное обновление инфраструктуры

ИБ работает в т.ч. в ситуации постоянного и скрытого от них изменения инфраструктуры

Взаимодействие ИБ и ИТ

Совместная работа для обеспечения киберустойчивости организации

Специфичные сценарии

Для ведомственных регуляторов, холдингов и др.

1

Оценка готовности подведомственных организаций

2

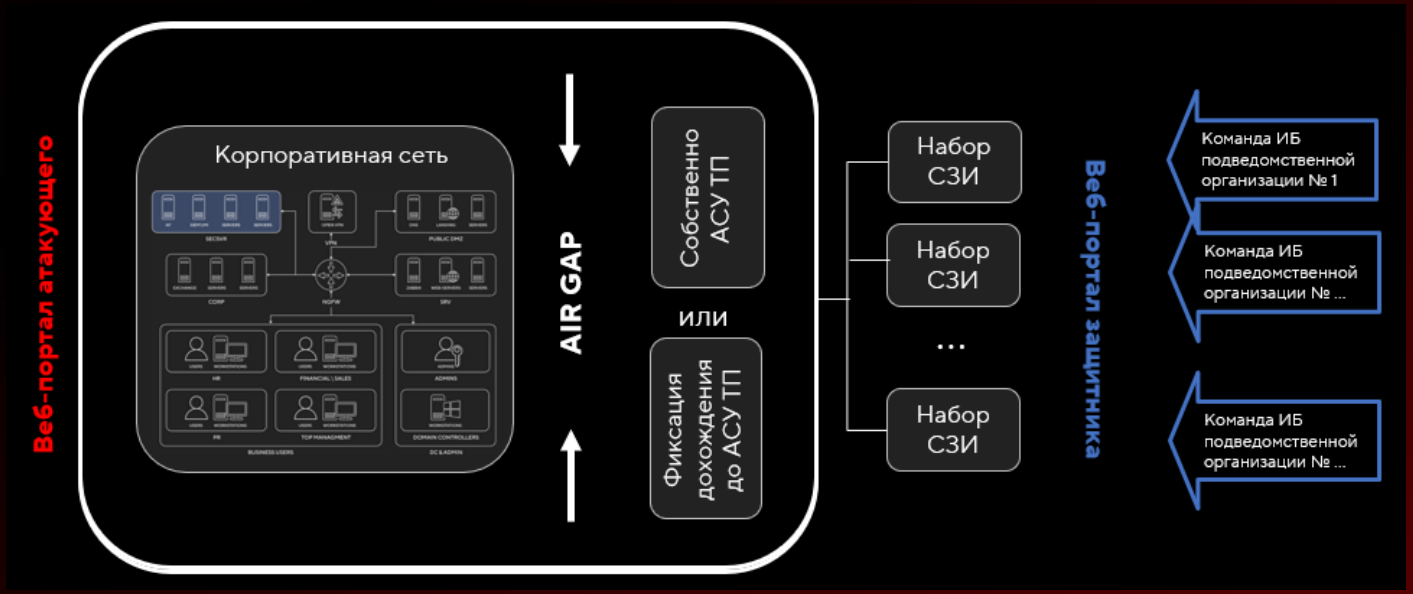
Сертификация SOC

3

Отраслевые кибербитвы

>

Пример отраслевого соревнования



ОНЛАЙН-ПОЛИГОН В ТЕРМИНАХ РЕЗУЛЬТАТА

ОЦЕНЕНА ВОЗМОЖНОСТЬ РЕАЛИЗАЦИИ НЕДОПУСТИМЫХ СОБЫТИЙ

КРИТИЧЕСКИЕ ЭЛЕМЕНТЫ ИНФРАСТРУКТУРЫ ТОЧНО НЕ СОДЕРЖАТ КРИТИЧЕСКИХ ЖЕ (С Т.ЗР. НЕПРЕРЫВНОСТИ БИЗНЕСА) УЯЗВИМОСТЕЙ *

SOC ВЫЯВЛЯЕТ ВСЕ АТАКИ

МЫ МОЖЕМ ЯРКО ПРОДЕМОНСТРИРОВАТЬ, ЧТО ИБ В НАШЕЙ ОРГАНИЗАЦИИ СИЛЬНАЯ: МОЖЕМ ПРОВОДИТЬ ЯРКИЕ МЕРОПРИЯТИЯ, ТУРНИРЫ, ДНИ ИБ

ИБ И ИТ СЛАЖЕННО РАБОТАЮТ, ЧТОБЫ ОБЕСПЕЧИТЬ СВЯЗНОСТЬ ПРОЦЕССА «PREVENT-DETECT-RESPOND-RECOVER»

РАСТЕТ СОБСТВЕННАЯ «КРАСНАЯ» ЭКСПЕРТИЗА

МЫ ТОЧНО УДОВЛЕТВОРЯЕМ ТРЕБОВАНИЯМ РЕГУЛЯТОРА

Кибериспытания

Концептуально новый подход к проверке защищенности от киберугроз – независимые исследователи в режиме 24/7, в условиях постоянно изменяющейся инфраструктуры оценивают защищенность компании от взлома и показывают полную картину кибербезопасности

Что дают кибериспытания

Альтернатива классической услуге пентеста, которая обеспечивает объективную оценку защищенности компании от киберугроз, и может быть организована в кратчайшие сроки

ЭКСПЕРТИЗА ЛУЧШИХ БЕЛЫХ ХАКЕРОВ

Независимые исследователи с разной специализацией в ходе кибериспытаний найдут разные вектора атак и уязвимости, о которых вы не подозревали. Они проверят возможность реализации недопустимых событий в соответствии с критериями, сформулированными совместно со специалистами Positive Technologies

РЕАЛЬНАЯ ОЦЕНКА СИСТЕМЫ ЗАЩИТЫ КОМПАНИИ

Кибериспытания позволяют оценить существующую систему защиты компании в части ее достаточности, эффективности и необходимости доработки. В том числе при планировании расходов на ее создание или модернизацию

БЕЗОПАСНОЕ ИЗМЕНЕНИЕ ИТ-ЛАНДШАФТА

Кибериспытания позволяют быстро и безопасно устранять киберриски и оценивать результаты в процессе всесторонней проверки защищенности вашей компании

Что такое Bug Bounty

Bug Bounty — это процесс поиска уязвимостей в программном обеспечении, веб-приложениях и инфраструктуре компаний с привлечением большого числа внештатных независимых исследователей информационной безопасности

Как работает программа Bug Bounty:

- Организации определяют список исследуемых приложений или ИТ-систем компании, границы работ и уровень критичности уязвимостей
- Независимые исследователи, соблюдая условия программы, ищут уязвимости и направляют отчеты о найденных багах организациям
- За выявленные и подтвержденные уязвимости организации выплачивают независимым исследователям вознаграждения в соответствии с условиями программы
- Компании устраняют уязвимости в соответствии с полученными отчетами, тем самым повышая уровень безопасности своей компании

Решаемые задачи с помощью выхода на Bug Bounty

Поиск уязвимостей 24/7/365

Непрерывная проверка безопасности любого цифрового актива компании — от компонентов ПО и отдельных сервисов до IT-инфраструктуры в целом

Повышение безопасности ИТ-систем компании

Непрерывная проверка безопасности ИТ-систем компании, в том числе необходимый инструмент процесса безопасной разработки

Реальная оценка устойчивости системы к атакам

Поиск слабых мест в безопасности компаний, которые могли не заметить собственные ИБ-специалисты или внешние пентестеры

Повышение квалификации команды ИБ

Обучение команды работе с потоком уязвимостей за счет доступа к экспертизе лучших независимых исследователей кибербезопасности

Рекомендации по выходу на Bug Bounty

Для небольших компаний (до 1 000 сотрудников)

- 5 исследователей в закрытой программе со средними вознаграждениями (до 75 000 рублей за одну уязвимость)

> Поток отчетов на багбаунти полностью управляем

Для больших компаний (более 1 000 сотрудников)

- 50 российских исследователей в закрытой программе со средними вознаграждениями
- 10 000 исследователей со всего мира в публичной программе с высокими вознаграждениями (до 500 000 рублей)

> Поможем настроить программу так, чтобы приходил тот поток багов, который комфортен для устранения

Индивидуальный подход к выходу на Bug Bounty

Приватный режим Bug Bounty

- Программа публикуется в закрытом режиме
- К участию допускается контролируемое количество исследователей, можно выбрать лучших белых хакеров, наиболее активных или исследователей только из России
- Контролируемый поток отчетов от исследователей

Публичный режим Bug Bounty

- Программа публикуется на сайте bugbounty.standoff365.com
- Доступ к программе получают все пользователи, зарегистрированные на платформе Standoff Bug Bounty
- Систему проверяют исследователи с различными специализациями — максимальное покрытие

10 хантеров	20 хантеров	30 хантеров	50 хантеров	100 хантеров	10 000 хантеров
Приватный режим	Приватный режим	Приватный режим	Приватный режим	Приватный режим	Публичный режим

Итоги двухлетней работы платформы Standoff Bug Bounty

	Май 2022 года	Май 2023 года	Май 2024 года	
Старт работы платформы		5232	10102	Зарегистрированных исследователей на платформе
		1956	5180	Отчетов, отправленных багхантерами
		873	2215	Уникальных отчетов багхантеров, принятых заказчиками
		83	252	Выявлено критических уязвимостей

Отзывы тех, кто вышел на Standoff Bug Bounty

«В нашей компании есть информационные сервисы, доступные в интернете, что позволяет сотрудникам успешно выстраивать свои бизнес-процессы. В то же время эти сервисы являются целью для хакеров и точкой входа в случае взлома. Компания неоднократно проводила и будет далее проводить пентесты для проверки своей защищенности. Багбаунти же позволяет провести более точную оценку текущей защиты периметра, так как исследователи 24/7 ищут уязвимости в сервисах. Благодаря площадкам по поиску уязвимостей заказчик получает возможность быть на шаг впереди злоумышленников.»

Александр Шилов, начальник отдела информационной безопасности АО «Новая перевозочная компания»

НОВАЯ ПЕРЕВОЗОЧНАЯ

Варианты участия в Standoff Bug Bounty

> Анализ продуктов или сервисов компании

> Анализ периметра компании

> Реализация критически опасных для бизнеса (недопустимых) событий

Кто уже использует Standoff Bug Bounty (публичные программы)

тинькофф

OZON

минцифры

азбука вкуса

WILDBERRIES

positive technologies

Результат кибериспытаний

Найдены способы причинения ущерба и реализации недопустимых событий компании

Не выявлены способы причинения ущерба компании

Внедрение концепции кибериспытаний в качестве постоянного инструмента оценки защищенности компании

6 месяцев

Рекомендуемый стартовый срок проведения кибериспытаний

Ваши вопросы?