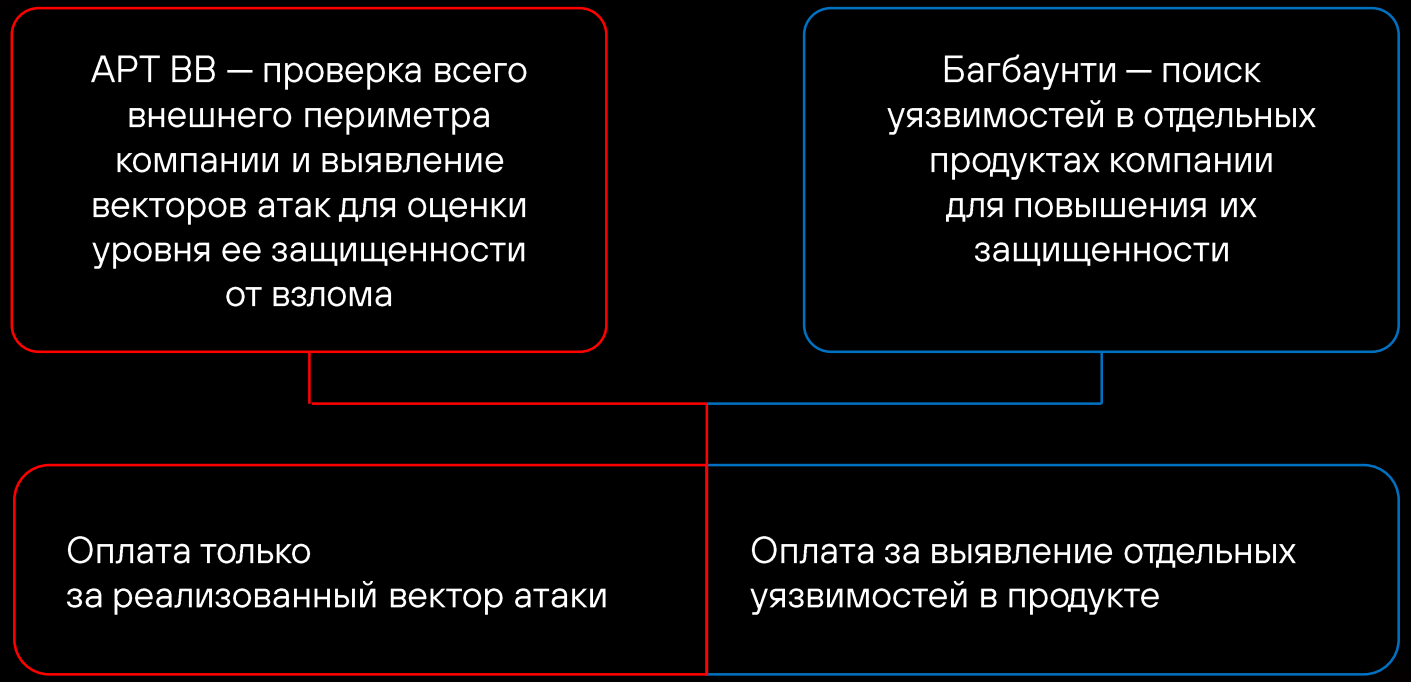
APT Bug Bounty — проверка защищенности на платформе Standoff Bug Bounty

Отличие APT Bug Bounty от классического багбаунти



APT BB — эволюция известных методов: пентеста и red team, новый подход к проверке защищенности от киберугроз, при котором независимые исследователи в режиме 24/7 в условиях постоянно изменяющейся инфраструктуры оценивают защищенность компании от взлома

APT BB vs. пентест vs. red team vs. ASV-сканирование

Параметр	Инструментальное сканирование (ASV)	Пентест	Red team	APT BB
Цель работ	Проверить сетевые службы и узлы на наличие уязвимостей с помощью автоматизированных методов	Оценить возможность проникновения в систему или повышения привилегий с учетом выстроенной системы защиты информации	Оценить возможность проникновения в систему путем моделирования APT-атаки с учетом выстроенной системы защиты информации	Оценить реальный уровень защищенности компании. Оценить возможность проникновения в систему путем проведения реальных атак. Оценить возможность реализации недопустимых событий компании. Оценить эффективность системы защиты информации, выявления киберинцидентов и реагирования на них или эффективность работы подразделения по защите информации согласно заданным метрикам
Модель нарушителя	Внешний	Внешний или внутренний	Внешний	Внешний или внутренний
Необходимость СЗИ	Да	Да	Да	Да
Необходимость SOC	Нет	Нет	Да	Да
Время проведения работ	До 2 недель	До 1 месяца	2–3 месяца	Постоянно, в режиме 24/7/365
Количество исследователей	2–3	5–10 на одну систему	15–25	Не ограничено

Основные преимущества

Это следующий этап повышения защищенности компании, которая прошла все уровни подготовки. APT BB содержит элементы пентеста, проверки силами red team и ASV-сканирования, при этом позволяет:

- оценивать защищенность компании постоянно, получая актуальную информацию об уязвимостях и возможных векторах атак
- экономно расходовать бюджет компании — во время проведения APT BB оплата производится за результат (за успешную реализацию недопустимого события), а не за время работы специалистов
- применять более широкий набор исследовательских инструментов и техник
- получить возможность быстро 24/7/365 проверять инфраструктуру на предмет новых уязвимостей (0-day, 1-day) и оперативно устранять их сразу после появления

В отличие от классической проверки силами red team, APT BB объединяет участие несколько команд, что позволяет за то же время получить наибольшие результаты и выявить несколько векторов атак

Это способ получить информацию об уязвимостях до того, как их обнаружит злоумышленник и использует против компании

Что дает проведение APT BB на платформе Standoff Bug Bounty

Альтернатива red team и классическому пентесту, которая обеспечивает объективную оценку защищенности компании от киберугроз и может быть организована в кратчайшие сроки

Экспертиза лучших этичных хакеров

Независимые исследователи с разной специализацией в ходе APT Bug Bounty найдут векторы 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

APT Bug Bounty позволяют оценить существующую систему защиты компании в части ее достаточности, эффективности и необходимости доработки, что важно среди прочего для планирования расходов на ее создание или модернизацию

Безопасное изменение ИТ-ландшафта

APT Bug Bounty позволяет быстро и безопасно устранять киберриски и оценивать результаты в процессе всесторонней проверки защищенности вашей компании

Недопустимые события

При подготовке к APT BB формулируются значимые для компании недопустимые события, реализация которых приведет к значительному ущербу или другим критическим последствиям

Пример недопустимого события	Пороговое значение	Критерий реализации недопустимого события
Доступ к данным VIP-клиентов	Недопустимо	▪ Предоставление скриншота или выгрузки данных из целевой системы с информацией о VIP-клиенте (номера счетов, номера карт) и совершаемых им операциях ▪ Демонстрация возможности совершения банковских операций от лица VIP-клиента
Невозможность авторизации в экосистеме	Недопустимо	▪ Демонстрация доступа к целевым системам с максимальными привилегиями ▪ Добавление исполняемого файла с вредоносным кодом на сервер

Процесс запуска программы APT BB

1 Определение недопустимых событий

Определяются НС компании и критерии их успешной реализации (совместно со специалистами Positive Technologies)

2 Анализ старта

Специалисты Positive Technologies оценивают инфраструктуру компании и дают рекомендации, чтобы проверка была максимально качественной

3 Запуск

Формируется программа*, которая размещается на платформе Standoff Bug Bounty (в публичном или закрытом режиме). Привлекаются лучшие исследователи — с учетом особенностей инфраструктуры компании и профиля ее деятельности

4 Оценка защищенности исследователями

Исследователи ищут векторы проникновения в инфраструктуру, выполняют цепочки шагов атаки, применяя различные подходы, и создают отчеты о реализованных (в том числе частично) атаках

5 Рассмотрение результатов

Подводятся итоги, анализируются результаты и формируются предложения по повышению защищенности. В отличие от работы red team, процесс APT BB в формате кибериспытаний может быть непрерывным и проходить с привлечением наибольшего количества команд

* Программа включает описание недопустимых событий и критериев их реализации, скоуп, требования к исследователям, перечень запрещенных действий, условия выплаты вознаграждений исследователям и требования к оформлению отчетов.

Результат

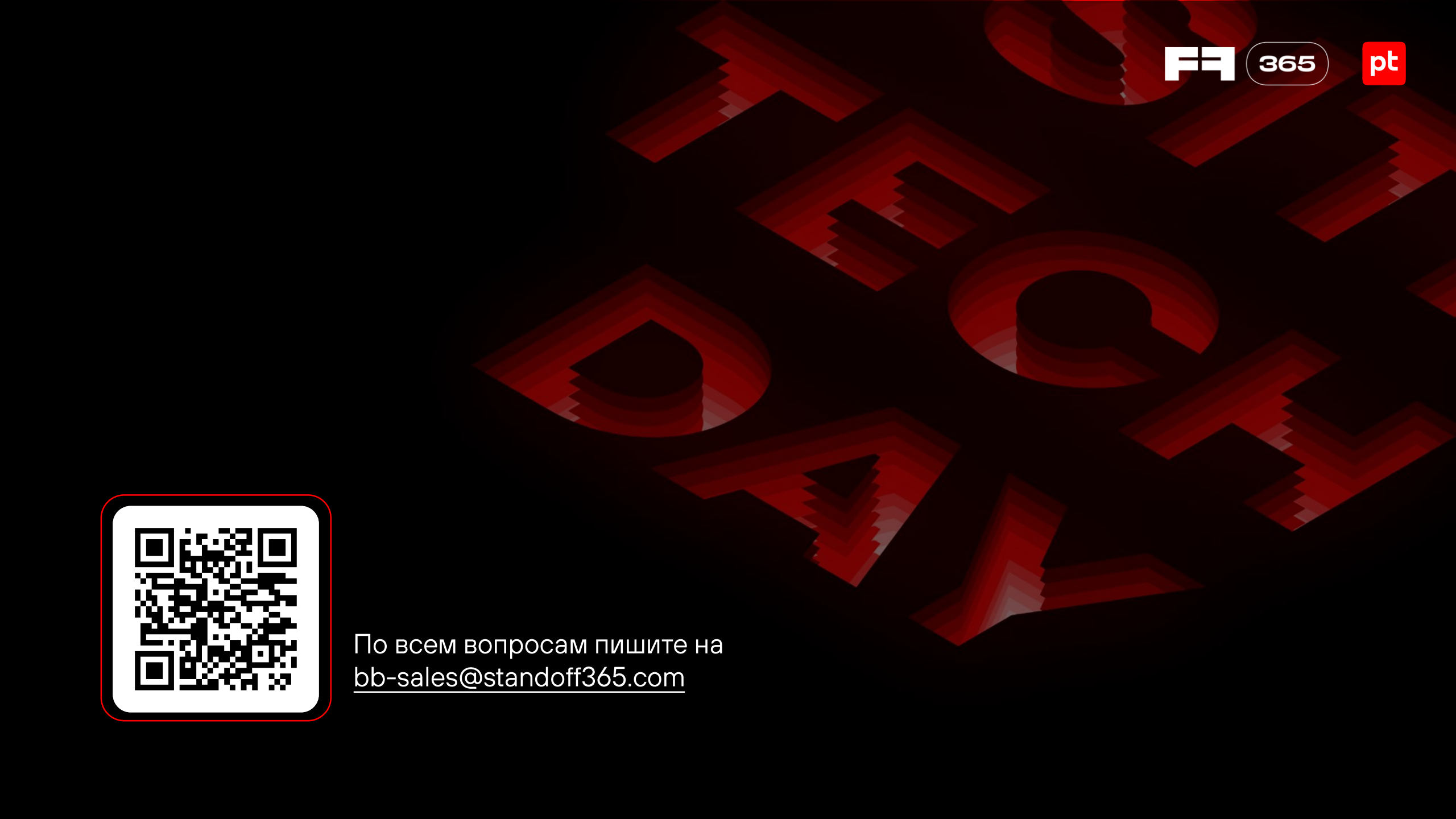
Найдены способы причинения ущерба и реализации недопустимых для компании событий

Способы причинения ущерба компании не выявлены

APT Bug Bounty внедрен в качестве постоянного инструмента оценки защищенности компании

6 месяцев

Рекомендуемый срок проведения программы



По всем вопросам пишите на
bb-sales@standoff365.com

Спасибо!