
STANDOFF
ПРАВИЛА

Содержание

1. О киберучениях на платформе Standoff 365

Standoff 365 — это социальная платформа, позволяющая общаться и обмениваться опытом, киберполигон для проведения киберучений и исследовательская площадка для проверки защищенности систем и оборудования. В основе платформы лежит технология, позволяющая быстро развертывать информационную инфраструктуру и подключать к ней внешние системы и оборудование.

Платформа позволяет проводить киберучения Standoff для исследования атак на информационную инфраструктуру и приложения, а также для реагирования на инциденты. На платформе разворачиваются сегменты полигона. В них воссоздаются информационные системы и процессы, характерные для предприятий определенной отрасли — торговых фирм, банков, телеком-операторов, промышленных предприятий. Каждая отрасль может включать в себя один или несколько сервисов, которые регулируют деятельность организации или обеспечивают ее информационную безопасность. Сервисами могут быть, например, почтовый сервер, FTP-сервер, база данных клиентов, система документооборота, межсетевой экран, система управления светофорами, ветрогенераторы.

В Standoff предусмотрены два типа участников — атакующие и защитники. Цель атакующих — реализовывать критические события, например парализовать работу АСУ ТП или получить доступ к конфиденциальной информации. Задача защитников — своевременно выявлять и расследовать инциденты, а также реагировать на действия хакеров и вводить меры защиты от атак.

Атакующие за свои действия получают баллы, а действия защитников оцениваются в виде метрик.

Информация о ходе киберучений, оценки действий участников и задания отображаются на платформе Standoff 365, доступ к которой предоставляет организатор.

2. Правила для атакующих

Этот раздел содержит правила участия в киберучениях, а также информацию о подготовке к ним и подключении к полигону.

В этом разделе

2.1. Подготовка

Для участия в киберучениях пользователю нужно зарегистрировать аккаунт на сайте standoff365.com и подать заявку. После того как заявка будет одобрена организатором, каждый участник команды сможет подключиться к инфраструктуре киберполигона, используя данные из своего личного кабинета.

2.2. Подключение

Для доступа к киберполигону участнику нужно перейти на вкладку **Доступ и ресурсы** на платформе Standoff 365 и следовать инструкциям в разделе **Настройка VPN-подключения**.

2.3. Ход киберучений

В ходе киберучений атакующие должны находить уязвимости, реализовывать критические события, выполняя предоставленные задания, и получать за это баллы.

Разрешается атаковать только сервисы информационной инфраструктуры, расположенные по адресам, предоставленным организаторами. Атаки на адреса, не входящие в список предоставленных, не учитываются при начислении баллов. Сервисы, расположенные за пределами инфраструктуры, предоставленной организаторами, не входят в рамки полигона, и атаковать их запрещено.

> Внимание! За использование служебных учетных записей или попытку получения доступа к ним организаторы могут отстранить участника от киберучений.

> Внимание! За атаку на адреса, не входящие в предоставленный список, организаторы могут отстранить участника от киберучений. Кроме того, участникам запрещается проводить DoS- и DDoS-атаки на службы, сервисы и приложения инфраструктуры полигона. Организаторы могут отстранить от киберучений участника, осуществляющего такие атаки.

> Внимание! За рассылку фишинга сотрудникам Positive Technologies (например, по электронной почте или в Telegram) организаторы могут отстранить участника от киберучений.

Баллы можно получать следующими способами:

— **За реализацию критических событий.** Задания могут быть связаны, например, с получением конфиденциальной информации, отключением одного или нескольких сервисов или несанкционированным изменением информации на тестовом сайте.

— **За нахождение уязвимостей.** Участник может представить отчет об уязвимостях, найденных в информационной инфраструктуре.

Чтобы получить техническую поддержку, участнику следует направить обращение через Telegram-бот для атакующих. Специалисты техподдержки отвечают только через такие заявки.

> **Примечание.** Участники могут создать запрос в техподдержку для проверки работоспособности вектора атаки. Специалисты техподдержки не отвечают на другие вопросы, связанные с векторами атаки.

2.4. Задания

В киберучениях в качестве заданий используются приближенные к реальности ситуации. Задание дано в карточке уязвимости или критического события, там же указано, сколько баллов будет начислено за выполнение.

2.5. Получение баллов

Баллы за выполнение заданий начисляются автоматически. На основе полученных баллов формируется рейтинг участников.

> Внимание! Организаторы вправе дисквалифицировать участника, если он пытается выдать отчет другого участника за свой.

В этом разделе

2.5.1. Баллы за реализацию критических событий

Чтобы заработать баллы за реализацию критического события, нужно сдать соответствующий отчет на платформе Standoff 365.

Если в отчете недостаточно информации о том, как было реализовано критическое событие, отчет не принимается и баллы не начисляются. В этом случае организаторы оставляют комментарий с замечаниями к сданному отчету. После исправления недостатков отчет можно сдать повторно.

Чем выше уровень сложности задания, тем больше баллов можно получить. Расчет баллов динамический: участник или команда, реализовавшие критическое событие первыми, получают максимальный балл, каждая последующая реализация события другими участниками приносит на 15% меньше баллов. Количество баллов уменьшается до тех пор, пока не достигнет 40% от значения, указанного в задании. С этого момента все последующие участники получают это минимальное количество баллов.

Таблица 1. Пример расчета баллов за реализацию критического события

Первая реализация	1000 баллов (максимальное значение)
Вторая реализация	850 баллов
Третья реализация	722 балла
Четвертая реализация	613 баллов
Пятая реализация	521 балл
Шестая реализация	443 балла
Седьмая реализация и последующие	400 баллов (минимальное значение)

2.5.2. Баллы за поиск уязвимостей

Чтобы заработать баллы за найденную уязвимость, нужно сдать соответствующий отчет на платформе Standoff 365. В отчете необходимо привести пример эксплуатации уязвимости и — в зависимости от типа обнаруженной уязвимости — получить баннер с версией СУБД, прочитать локальный файл, отправить произвольный HTTP-запрос или показать вывод команд `ipconfig/ifconfig`, `whoami` или `id`.

Принимаются отчеты только об определенных типах уязвимостей: локальном повышении привилегий (LPE) до root, удаленном выполнении кода (RCE), внедрении SQL-кода (SQLi), обходе каталога (Path Traversal), подмене запросов на стороне сервера (SSRF), внедрении внешних сущностей XML (XXE).

3. Правила для защитников

Этот раздел содержит информацию о подготовке к киберучениям, подключении к полигону и правила участия в киберучениях для команды защитников.

В этом разделе

3.1. Подготовка

Команда защитников заранее (обычно за месяц) получает доступ к полигону и может с ним ознакомиться. Команде предоставляются конфигурационные файлы, данные учетных записей для подключения и другая информация, необходимая для участия.

При ознакомлении с инфраструктурой полигона команды защиты получают доступ к сканеру уязвимостей. Учетные записи от объектов инфраструктуры для запуска инвентаризации и сканирования защитникам выдают организаторы. Команда может использовать любой другой сканер уязвимостей, но должна установить его самостоятельно.

После ознакомления с полигоном команда предоставляет организаторам список средств защиты, которые она планирует использовать, а также схему их размещения. В общем случае команды ограничены следующими классами средств защиты: межсетевые экраны следующего поколения (NGFW), межсетевые экраны уровня веб-приложений (WAF), системы security information and event management (SIEM). Использование иных средств защиты согласовывается с организаторами отдельно.

3.2. Подключение

Для доступа к киберполигону участнику нужно перейти на вкладку **Доступ и ресурсы** на платформе Standoff 365 и следовать инструкциям в разделе **Настройка VPN-подключения**.

3.3. Ход киберучений

Основная цель защитников — обнаружение и расследование инцидентов, вызванных действиями атакующих. В ходе киберучений команда защитников получает опыт защиты инфраструктуры в условиях, максимально приближенных к реальным. Помимо этого, защитники могут участвовать в киберучениях в режиме реагирования. В этом случае их цель — пресекать действия команд атакующих. Для этого защитники могут использовать в качестве инструмента защиты MaxPatrol EDR и такие методы, как блокировка трафика, изоляция узла, перенаправление DNS-запросов и другие. При этом защитникам запрещается полностью блокировать ресурсы других команд и совершать действия, которые могут помешать проведению киберучений.

Киберучения ограничены по времени. Оставшееся до конца киберучений время отображается на платформе Standoff 365.

Для оценки действий команд защитников учитываются количество зафиксированных инцидентов и среднее время расследования одной атаки.

Чтобы получить техническую поддержку, участнику следует направить обращение через Telegram-бот для защитников. Специалисты техподдержки отвечают только через такие заявки.

В этом разделе

Количество обнаруженных инцидентов (см. раздел 3.3.1)

Среднее время расследования атаки (см. раздел 3.3.2)

3.3.1. Количество обнаруженных инцидентов

Перед командой защитников в первую очередь стоит задача выявления инцидентов на защищаемых ими предприятиях. В процессе противостояния команды защитников могут сдавать отчеты о выявленных ими инцидентах.

Отчеты оцениваются организаторами. Если в отчете недостаточно информации, организаторы не принимают такой отчет и оставляют соответствующий комментарий к нему на игровом портале. Отчет можно скорректировать и сдать повторно.

В истории защищаемого объекта на платформе Standoff 365 будет периодически обновляться информация о том, какое количество инцидентов зафиксировано командой защитников.

3.3.2. Среднее время расследования атаки

После того как организаторы примут отчет о реализации критического события от атакующих, защитникам становится доступна информация о том, какое критическое событие было реализовано. Задачей защитников становится расследование этого события и сдача отчета. На игровом портале появляется таймер, который ведет отсчет времени расследования.

Отчеты оцениваются организаторами. Если в отчете недостаточно информации о действиях атакующих, отчет не принимается, о чем делается пометка на игровом портале. По оставленному организаторами комментарию команда защитников может провести дополнительное расследование, доработать отчет и повторно отправить его на проверку.

После того как организаторы приняли от команды защитников отчет о расследовании реализации критического события, фиксируется время, за которое расследование было выполнено. При этом время, которое отчет находился на проверке у организаторов, не учитывается.

Глоссарий

Standoff

Открытые киберучения, которые проводятся несколько раз в год и могут быть приурочены к конференции по информационной безопасности.

Standoff 365

Платформа для специалистов по информационной безопасности, которая включает в себя киберполигон, программы bug bounty, социальную сеть, тематические блоги и платформу для организации CTF-соревнований.

Standoff 365 Киберполигон

Часть платформы Standoff 365 для проведения киберучений. Может состоять из одного и более сегментов полигона. В киберучениях участвуют атакующие и защитники. На киберполигоне можно увидеть, как реализуются кибератаки, и в безопасной среде оценить масштабы их последствий.

атака

Комплекс действий атакующих, приводящий к реализации критического события. По итогам успешной атаки «красные» сдают отчет о реализации критического события.

атакующие

Команда или отдельный участник, целью которых являются поиск уязвимостей и реализация критических событий на полигоне.

задание

Описание целей, которых должны достичь участники.

заявка на участие в киберучениях

Сообщение о намерении команды участвовать в офлайн-киберучениях. В заявке указываются роль команды (атакующие или защитники), капитан команды, состав участников. Подается админом группы. После подачи рассматривается организатором киберучений.

инцидент

Одиночное действие атакующих, направленное на нарушение доступности, целостности или конфиденциальности информации. По итогам расследования «синие» сдают отчет об отдельных инцидентах.

киберучения

Комплекс мероприятий, организуемый для повышения уровня подготовки и развития навыков специалистов по информационной безопасности.

критическое событие

Событие, в результате которого становится невозможным достижение операционных и стратегических целей организации или которое приводит к длительному нарушению ее основной деятельности. На платформе Standoff 365 цель атакующих — реализовать критические события, а цель защитников — расследовать случаи их реализации.

организатор киберучений

Пользователь платформы Standoff 365, имеющий права для создания киберучений и для рассмотрения заявок команд на участие в офлайн-ивенте.

отчет о расследовании реализации критического события

Отчет команды защитников, содержащий описание предполагаемых действий, выполненных атакующими для реализации критического события.

отчет о реализации критического события

Отчет атакующих, содержащий описание действий, которые позволили реализовать критическое событие.

отчет об инциденте

Отчет команды защитников, содержащий описание зафиксированного действия атакующих, влияющего на доступность, целостность и конфиденциальность информации.

отчет об уязвимости

Отчет атакующих об обнаруженной уязвимости.

сегмент полигона

Отдельная виртуальная часть инфраструктуры киберполигона, в которой воссоздаются информационные системы и процессы, характерные для предприятий определенной отрасли.

сервис

Объект инфраструктуры киберполигона, который управляет тем или иным процессом в информационной системе.

уязвимость

Недостаток в системе, используя который, можно намеренно нарушить целостность, доступность и конфиденциальность информации.

Standoff 365 — это социальная платформа, позволяющая общаться и обмениваться опытом, киберполигон для проведения киберучений и исследовательская площадка для проверки защищенности систем и оборудования. В основе платформы лежит технология быстрого развертывания и доступа к информационной инфраструктуре и подключения к ней внешних систем и оборудования.

На киберполигонах Standoff воссоздается инфраструктура реальных предприятий различных отраслей мировой экономики. Атакующим и защитникам будет предоставлена возможность отработать свои навыки на объектах транспортной, нефтяной, добывающей и энергетической промышленности. Помимо этого, кибербитва развернется вокруг систем умного городского хозяйства, финансовых структур и многого другого.

Участие в Standoff 365 позволяет протестировать возможность реализации кибератак и оценить масштабы их последствий в безопасной среде, получить новые знания и практические навыки выявления кибератак и противодействия им, изучить сценарии реагирования на известные и неизвестные риски, исследовать взаимосвязи кибербезопасности и бизнеса.

org@standoff365.com standoff365.com