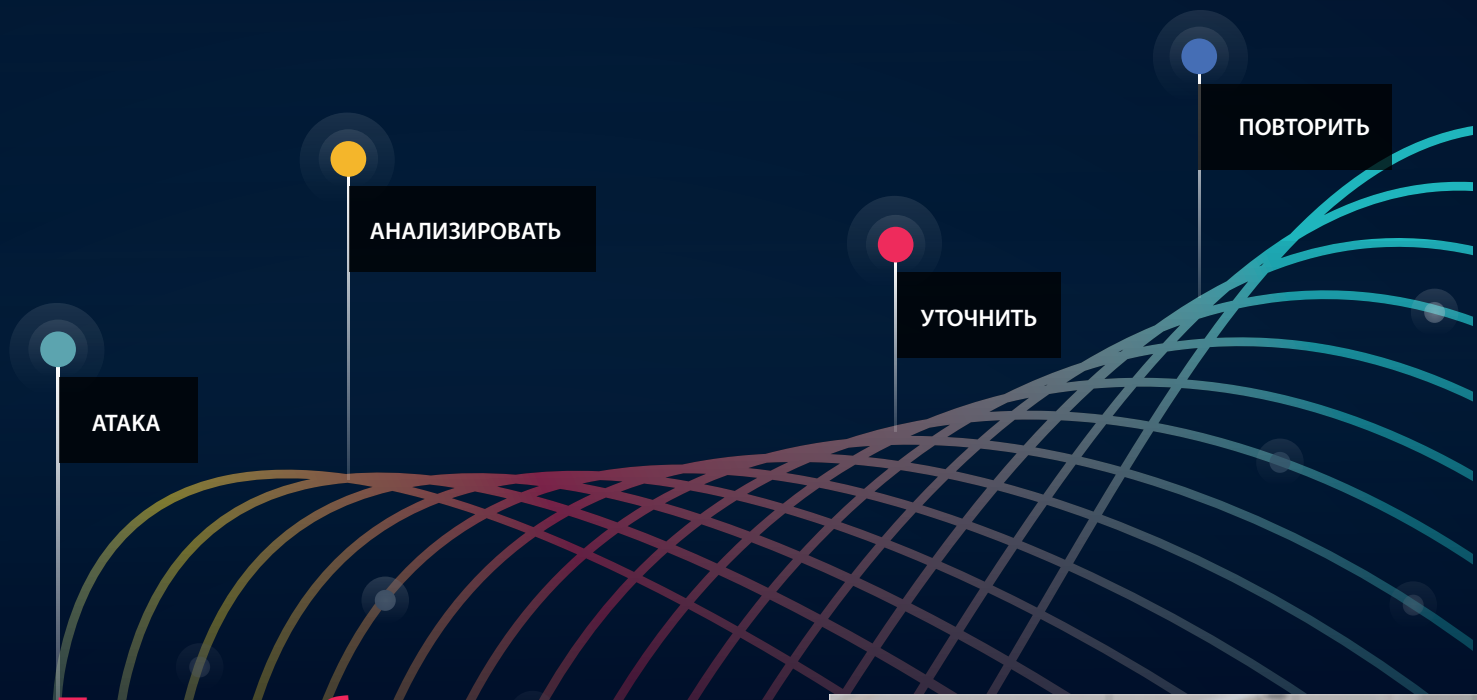
SafeBreach



Проверка безопасности SafeBreach:

Минимизируйте риск, максимизируйте отдачу от ваших инвестиций в безопасность.

Сводка решения

Возможно, вы реализовали десятки проверок безопасности, но этого недостаточно. Вы должны убедиться, что эти элементы управления работают должным образом и должным образом.

Для этого необходимо выполнить проверку аудита безопасности. Это краткое изложение объясняет, почему традиционные подходы не работают. Для этого необходимо выполнить проверку аудита безопасности. Это краткое изложение объясняет, почему традиционные подходы не работают.

Представляем проверку безопасности

Для борьбы с угрозами, исходящими от кибератак, службы безопасности на предприятиях и в государственных учреждениях продолжают внедрять и разрабатывать ряд средств контроля. Однако даже после того, как были сделаны крупные инвестиции и распределены автомобили, работа не завершена. Крайне важно, чтобы команды проверяли свои средства безопасности и обеспечивали необходимую защиту.

Приведите инвестиции в безопасность в соответствие с вашими бизнес-целями с помощью панелей администратора SafeBreach.

- Проверка контроля безопасности
- BAS (моделирование атаки взлома)
- Оценка угрозы
- Оценка облачной безопасности
- Управление уязвимостями

Ограничения традиционных подходов к проверке безопасности

Команды безопасности могут использовать несколько подходов для проверки проверки безопасности. На протяжении многих лет команды могли проводить тестирование на проникновение, упражнения красной команды, сканирование уязвимостей и многое другое. Однако, учитывая все обстоятельства, эти подходы ввели важные ограничения:

Несоответствие. Ручной, индивидуальный характер белого хакерства и подходы красной команды могут подвергнуть бизнес непоследовательности и непредсказуемости в лучшем случае и ошибкам, неточностям и упущениям в худшем.

Минимум инсайтов. Выходные данные таких систем, как сканеры уязвимостей, могут содержать много «шума», выявляя множество проблем, которые могут представлять или не представлять реальную угрозу безопасности. Эти системы могут создавать огромное количество невыполненных работ для перегруженных работой групп безопасности, сталкиваясь с большим количеством проблем, и при этом предлагая минимальные аналитические данные для определения приоритетов.

Высокие затраты. Типы специалистов, необходимых для управления эффективными красными командами или для участия во взломе белых шляп, недостаточны и требуют высокой заработной платы.

Ограниченная частота, объем. Учитывая высокую стоимость и трудности с поиском нужных экспертов, многие организации существенно ограничены в объеме, частоте и продолжительности своих возможностей по проведению такого тестирования. Как правило, тесты на проникновение проводятся периодически, обычно ежегодно или раз в полгода; это означает, что команды получают информацию только в определенное время.

Аутентификация проверки безопасности из Safebreach

SafeBreach

Сегодня, SafeBreach предлагает расширенные функции имитации взломов и атак, которые предоставляют командам эффективный программный способ проверки средств контроля безопасности. В результате платформа позволяет вам решать задачи проверки средств управления вашей организации, преодолевая ограничения ручных трудоемких действий, таких как тестирование на проникновение и построение красной команды. Кроме того, в отличие от других платформ моделирования взломов и атак, SafeBreach позволяет командам автоматически выполнять непрерывные атаки без необходимости нанимать специальные группы для управления платформой.

Платформа SafeBreach безопасно выполняет реальные атаки в производственных средах, чтобы показать, где безопасность может противостоять таким атакам, а где она нуждается в улучшении. Платформа автоматизирует тестирование архитектуры безопасности организации, используя передовую запатентованную технологию, которая может выполнять атаки безопасно и непрерывно.

Завершите объем экосистемы безопасности

С помощью SafeBreach вы можете оценить безопасность всей вашей экосистемы безопасности, включая людей, процессы и существующие технологии. Вы также можете проверить определенные элементы управления во всех этих областях.:

- **Защита от потери данных (DLP).** Убедитесь, что ваши элементы управления VKR настроены правильно, чтобы данные не просочились. Получите информацию, необходимую для максимальной производительности вашего решения ВКонтакте.
- **Управление электронной почтой.** Убедитесь, что ваши проверки электронной почты настроены правильно, чтобы они выявляли все индикаторы нарушений безопасности (LOC), которые, как известно, сигнализируют о проникновении в организацию.
- **Управление конечной точкой.** Убедитесь, что элементы управления конечными точками, включая антивирус, защиту от вредоносных программ, обнаружение угроз и реагирование на конечные точки (EDR) и расширенное обнаружение и реагирование (XDR), правильно настроены для предотвращения или обнаружения вредоносной активности на ваших конечных точках.
- **Сетевое управление.** Убедитесь, что ваши сетевые элементы управления оптимально настроены для защиты от вредоносной активности. Комплексная проверка межсетевых экранов, межсетевых экранов следующего поколения, сегментации, систем предотвращения и обнаружения вторжений, поведения сети и анализа трафика и т. д.
- **Информация о безопасности и элементы управления событиями.** Сопоставьте результаты атаки, чтобы отличить элементы управления, которые обнаруживают или предотвращают атаки, и те, которые терпят неудачу. Сопоставьте соответствующие события и правила для каждой атаки с соответствующими компенсаторными мерами.

- **Управление всемирной паутиной (Web).** Определите, правильно ли настроены ваши веб-шлюзы, прокси-серверы и средства фильтрации URL-адресов для предотвращения или обнаружения вредоносных действий.

- **Управление облаком и контейнером.** Убедитесь, что при миграции в облако правильно настроены элементы управления и элементы управления безопасностью плоскости данных, чтобы максимизировать эффективность вашей облачной стратегии.

После каждой проверки решение SafeBreach создает подробный план исправления, который поможет вам максимально повысить эффективность контроля.

Проверка безопасности: варианты использования

Платформа SafeBreach может помочь вашему бизнесу в решении ряда задач. Ниже приведены лишь некоторые из способов, которыми ваша организация сегодня использует эту платформу моделирования взломов и атак:

- **Делайте авторитетные и основанные на фактах оценки решений.** Сложно полностью оценить и проверить, насколько эффективно новый инструмент защитит ваш бизнес от конкурентов. SafeBreach С его помощью вы можете быстро сделать тысячи ходов в процессе оценки, чтобы убедиться, что вы делаете правильные инвестиции.

- **Оценивать сжатые моментальные снимки.** После того, как вы предприняли шаги по укреплению моментального снимка, вы можете предпринять действия, чтобы быстро оценить эффективность изменений, прежде чем внедрять изменения в рабочую среду. Оцените моментальные снимки и получите подробный план исправления в локальной, виртуальной или облачной инфраструктуре.

- **Выполнять реалистичные сценарии движения для обучения.** Превратите поддельный сценарий из теории в реальность, безопасно выполняя атаки и позволяя командам отслеживать атаки и обучаться реагированию на инциденты.

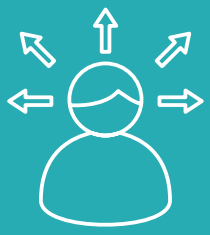
- **Защитите удаленную рабочую силу .** Применяйте критические методы атаки, чтобы быстро выявлять и устранять уязвимости, чтобы вы могли защитить действия и данные своих удаленных сотрудников.

- **Привлекать к ответственности поставщиков услуг безопасности.** Проверьте элементы управления безопасностью всей вашей экосистемы безопасности, чтобы определить решения, которые предотвращают и обнаруживают атаки и полностью пропускают их. Получите возможность привлекать своих поставщиков к ответственности, используя информацию и объективные данные о том, как их решения на самом деле работают в условиях атак.

- **Свести к минимуму потребление ресурсов компьютерной системы.** Часто настольные и портативные компьютеры перегружены слишком большим количеством инструментов безопасности, что снижает производительность системы, срок службы машины и удобство работы пользователей. Выполните атаки на каждый инструмент безопасности, чтобы определить наиболее подходящую комбинацию элементов управления, чтобы вы могли защитить свой бизнес, не утяжеляя свои устройства.

ПРОВЕРКА КОНТРОЛЯ БЕЗОПАСНОСТИ

Выполняйте атаки безопасно



Визуализируйте свое безопасное положение с помощью результатов, основанных на данных

Создает целостное решение для защиты вашего бизнеса

ICT OTD PREFER EXPERIENCE ONLINE Since 2011

OTD BİLİŞİM

SafeBreach: основные преимущества

Платформа SafeBreach для проверки аудитов безопасности, ваши команды могут получить ряд ключевых преимуществ:

- **Уменьшить риск.** Выявляйте уязвимости, лазейки и ошибки до того, как ими воспользуются кибер-злоумышленники. С помощью SafeBreach вы можете выполнять непрерывную проверку , чтобы гарантировать, что новые риски, связанные с новыми методами атак или новыми уязвимостями, возникающими в вашей корпоративной среде, будут быстро идентифицированы и устранены.
- **Усилить безопасность.** Проверяйте эффективность конкретных инструментов, а также всей экосистемы безопасности, включая людей, процессы и доступные технологии. Получите объективную информацию, необходимую для выявления наиболее критических угроз и принятия мер по их устранению.
- **Повышение операционной эффективности.** Оптимизируйте управление и операции, сознательно выявляя и устраняя дублирующие друг друга и неэффективные инструменты.
- **Тщательно оценивайте новые элементы управления.** Тщательно протестируйте возможные решения, чтобы определить, какие из них будут лучше всего работать в вашей среде, прежде чем покупать их.
- **Максимизируйте отдачу от существующих инвестиций.** Объективно оцените различные инструменты на месте и определите, какие из них работают, а какие нет. Таким образом, ваши команды могут максимально эффективно использовать имеющиеся у вас элементы управления и убедиться, что эти системы оптимизированы для обеспечения высочайшего уровня безопасности.

SafeBreach

Заключение

Корпоративная безопасность слишком важна, чтобы полагаться на догадки, спекуляции или принятие желаемого за действительное. Проверка безопасности абсолютно необходима, чтобы убедиться, что команды имеют адекватную защиту и понимают, что делать в противном случае. Кроме того, необходимость проверки мер безопасности имеет решающее значение, но также важна необходимость постоянного и экономичного управления этими усилиями. С SafeBreach ваши команды могут воспользоваться преимуществами передовых возможностей моделирования взломов и атак, которые обеспечивают эффективный программный способ проверки элементов управления безопасностью. Теперь вы можете оценить свои элементы управления и устранить уязвимости, прежде чем они будут использованы в злонамеренных целях.

IT & OT SafeBreach находится в OTD BİLİŞİM!

MALTEPE OFİS Cevizli Mah.
Zuhal Cad. No: 46 Ritim İstanbul
A-1 Blok D:55 34846 Maltepe
Стамбул ТУРЦИЯ

HALKALI OFİS Atatürk Mah.
Güner Sok. B-1 Blok No:
1/1B İç Kapı No: 25734307
Küçükçekmece Стамбул ТУРЦИЯ

T: +90 216 912 10 05 Факс: +90 216 912 10 07 otd.salesgrp@onlineteknikdestek.com

SafeBreach

SafeBreach для безопасности веб-приложений

Разблокируйте полную цепочку смерти с проверкой безопасности веб-приложений без агентов

Веб-приложения — излюбленная цель хакеров. Используя атаки веб-приложений, такие как межсайтовый скриптинг, SQL- инъекция и обход пути, хакеры могут проникать в сети и взламывать их, чтобы украсть конфиденциальные данные или заразить системы вредоносными программами. Предприятия используют брандмауэры веб-приложений (WAF) для обеспечения уровня безопасности, который фильтрует трафик и защищает от злонамеренного поведения, и тем не менее веб-приложения являются вторым наиболее часто используемым методом проникновения для кибератак. Как специалисты по безопасности могут оптимизировать брандмауэры веб-приложений (WAF) и элементы управления приложениями для эффективной защиты от веб-атак?

Платформа SafeBreach создана, чтобы обеспечить «хакерскую визуализацию» состояния безопасности вашей организации, позволяя вам непрерывно и безопасно выполнять атаки, проверять и оптимизировать эффективность ваших средств управления безопасностью, а также расставлять приоритеты по исправлению, чтобы сократить наиболее важные пробелы до того, как произойдет нарушение. . Он также позволяет обеспечить безопасность ваших веб-приложений посредством аутентификации через безагентные брандмауэры веб-приложений (WAF), которые можно быстро и легко развернуть.

SafeBreach для безопасности веб-приложений без использования агентов?

Полная цепочка проверки смерти

Просмотрите поверхность атаки на безопасность веб-приложений в контексте полной цепочки смерти злоумышленника, чтобы понять, как конкретные точки входа влияют на способность злоумышленника достичь своих целей.

Крупнейшая в отрасли книга по тактике движения

Хакерская книга SafeBreach ™ Playbook™ предлагает самый разнообразный набор атак на веб-приложения , в том числе атаки для тестирования большинства из десяти основных угроз безопасности OWASP® Foundation.

Быстрая и простая установка

Safebreach — это функция безагентного тестирования, которая не требует предварительной настройки и может выполняться быстро.

Контекстное представление состояния безопасности веб-приложений

Легко тестируйте свои элементы управления WAF с помощью моделирования атак путем внедрения, атак с использованием межсайтовых сценариев, ошибок шифрования, небезопасного дизайна приложений, удаленного использования уязвимостей веб-приложений, подделки запросов на стороне сервера и т. д.

Полезные отчеты о рентабельности инвестиций для вашего WAF

Используйте настраиваемые информационные панели и функции отчетности, чтобы понимать результаты потенциальных атак на веб-приложения, сообщать о влиянии на бизнес и измерять окупаемость инвестиций в WAF.