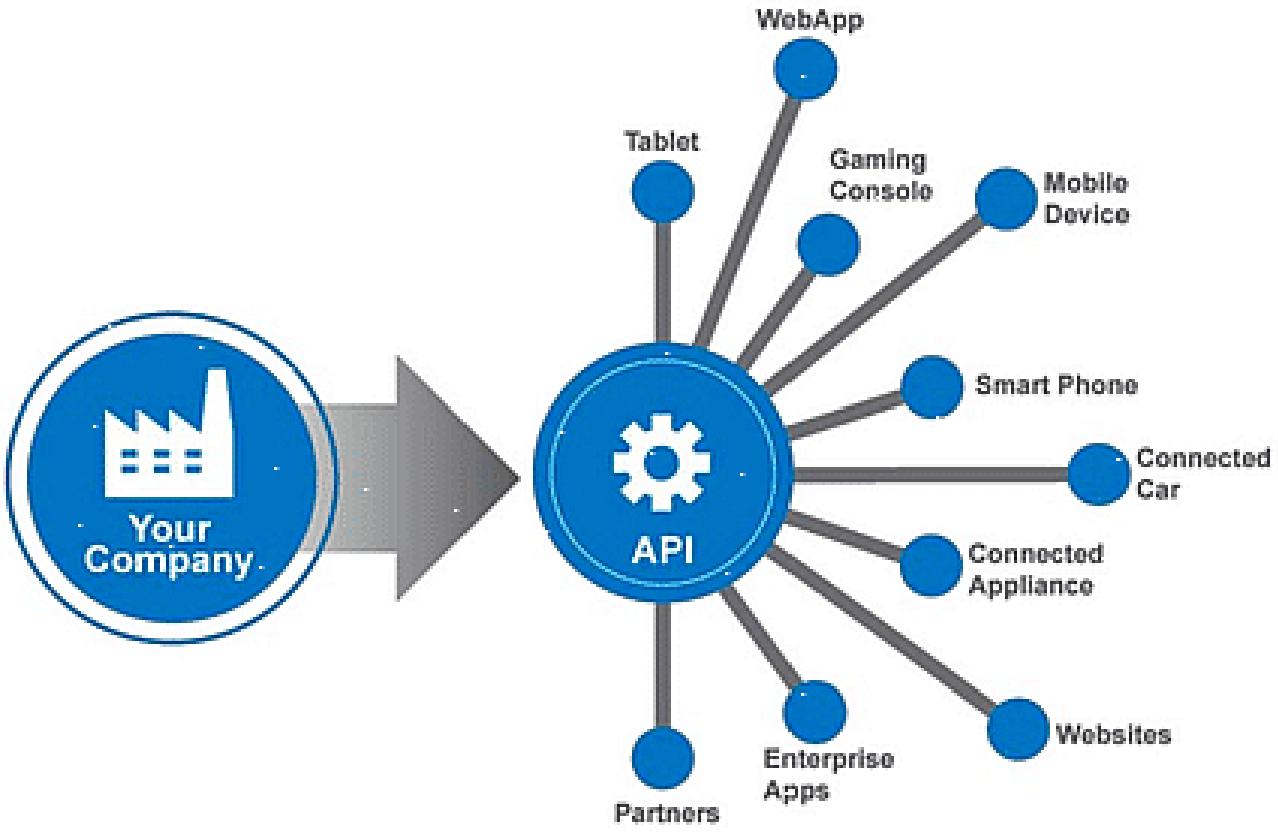
Зачем и как защищать конечные точки API?

Описание

Как вы защищаете свой API? Сейчас эпоха взрыва цифровой экономики, и огромные объемы данных поступают через API. Бизнес, игры, образование, погода, наука, искусство. Что ни назови, все работает на API. Для мира, так сильно зависящего от API, удивительно мало внимания уделяется безопасности. Для разработчиков достаточно стандартных настроек их фреймворков; или, что еще хуже, когда фреймворки не используются, они думают, что следуют практикам безопасности. Для системных администраторов безопасность по умолчанию, предлагаемая их инфраструктурой или поставщиком услуг, – это то, на что они полагаются. Не самое приятное зрелище, как по мне.



Нет нужды говорить, что на карту поставлено очень многое, что мы понимаем только тогда, когда происходит что-то по-настоящему ужасное.

Инструменты для повышения уровня защиты API

Существует несколько инструментов, которые могут помочь нам проверить уязвимости, а еще лучше – предложить первую линию обороны, когда речь идет о защите API. Однако следует помнить, что в конечном итоге ни одна стратегия безопасности не является идеальной. Приведенные ниже инструменты защиты API могут многократно повысить уровень безопасности API, поэтому их рекомендуется использовать.

AppTrana

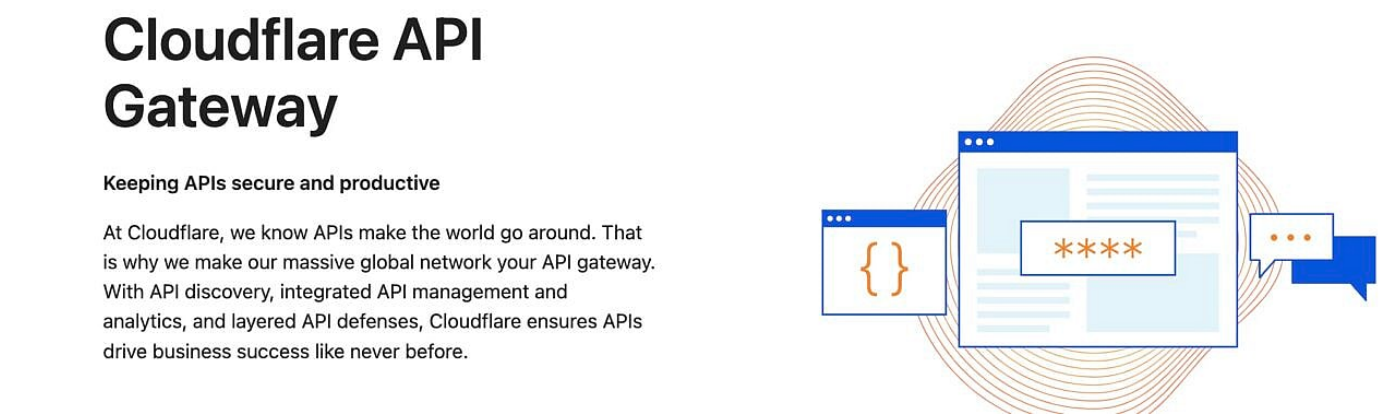
Специальные функции AppTrana по защите API предлагают комплексное решение, основанное на оценке рисков, для защиты от широкого спектра угроз API, включая OWASP API top 10, атаки DDoS и ботов на основе API, встроенные угрозы, утечку данных и т. д. Благодаря неограниченному автоматическому сканированию API,

подкрепленному ручным pen-testing, решение постоянно отслеживает степень риска для укрепления системы безопасности. Защита API от AppTrana обеспечивает наиболее комплексное решение благодаря сочетанию функций обнаружения рисков, обнаружения угроз API, политик позитивной безопасности API, политик DDoS для API, модулей ботов для API и функций обнаружения API.

Обнаружение API обеспечивает полную видимость вызовов API, включая недокументированные и теневые API, чтобы понять поверхность атаки API. Эта специализированная защита API собирает информацию о пользователях, поведении при использовании API, активности угроз, карты вызовов API и многое другое, чтобы продемонстрировать состояние защиты с помощью аналитики в режиме реального времени. Используя Indusface AppTrana, вы можете генерировать специальные политики для API, чтобы блокировать злоупотребления, связанные с API, в режиме реального времени.

Cloudflare

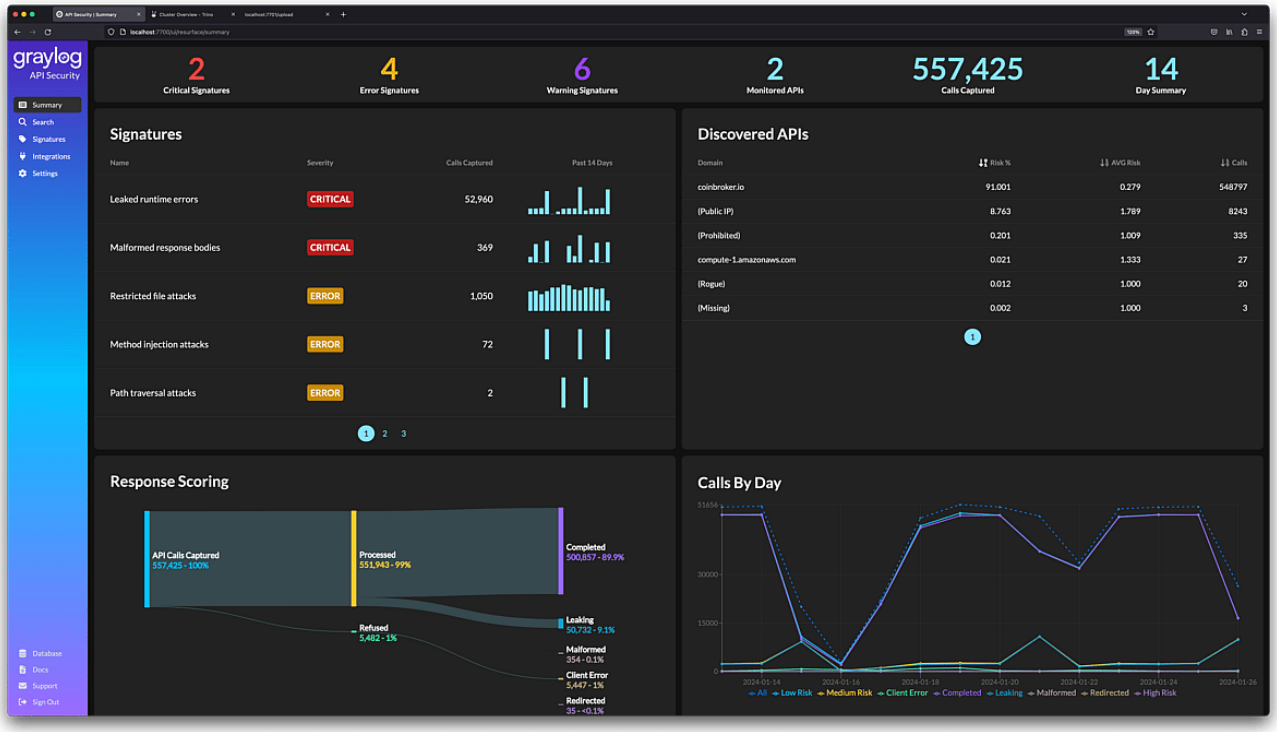
Передовой брандмауэр веб-приложений (WAF) Cloudflare имеет решающее значение для обеспечения безопасности и эффективности приложений и API. Он защищает от DDoS-атак, блокирует несанкционированный доступ ботов, обнаруживает вредоносные данные и сканирует браузер на предмет атак на цепочки поставок.



Обширная всемирная сеть Cloudflare обеспечивает передачу огромного количества трафика через шлюз API. Чтобы обеспечить безопасность своих API, Cloudflare использует комплексную систему, включающую обнаружение API, интегрированное управление API и аналитику, а также многоуровневую защиту API. API Gateway обеспечивает безопасное и эффективное управление API, включая обнаружение, безопасность уровня 7, взаимный TLS, положительную защиту API, обнаружение злоупотреблений и конфиденциальных данных. Он облегчает идентификацию и мониторинг конечных точек, защищает от атак, реализует аутентификацию, проверяет схемы OpenAPI и предотвращает утечку данных. Cloudflare API Gateway защищает от рисков OWASP API.

Graylog API Security

Graylog API Security обеспечивает мониторинг API в режиме реального времени, обнаружение угроз и оперативное устранение последствий, чтобы удовлетворить растущие потребности организаций в безопасности, где традиционные решения, такие как WAF и API-шлюзы, оказываются неэффективными.



Graylog API Security – это облачно-нативная архитектура для самоуправляемых частных облачных или локальных внедрений, обеспечивающая обнаружение утечки данных через API. Это единственное самоуправляемое решение для API, которое перехватывает всю полезную нагрузку как запросов, так и ответов API. С помощью Graylog API Security практикующие специалисты получают:

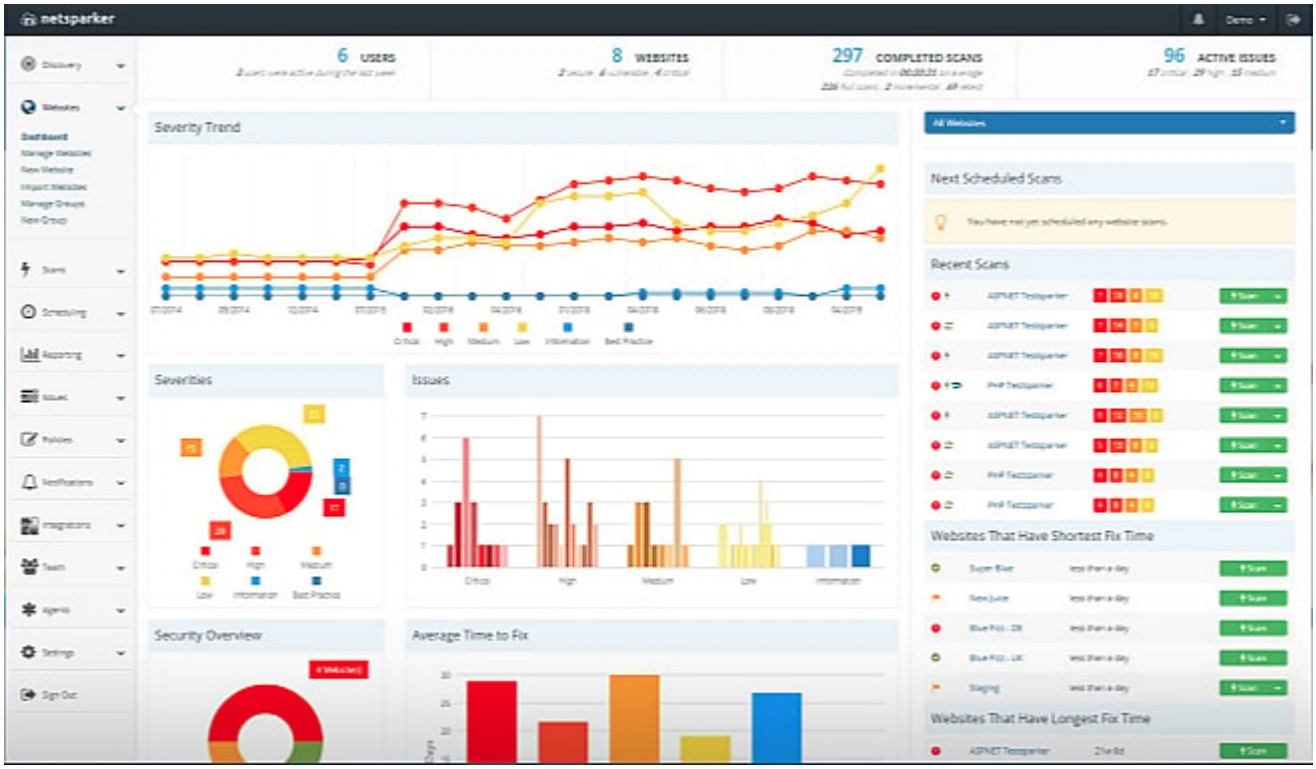
- **Обнаружение API:** Автоматическое обнаружение и категоризация API для целенаправленного мониторинга
- **Оценка рисков:** Приоритет оповещений на основе их относительного риска для организации
- **Полноценный захват:** Захват всей полезной нагрузки API-запросов и ответов, создание легкодоступного хранилища данных для обнаружения атак в режиме реального времени и поиска криминалистических данных.
- **Анализ угроз в режиме реального времени:** Опережайте возникающие угрозы благодаря постоянному мониторингу API и готовым сигнатурам угроз
- **Управляемое устранение:** После обнаружения угрозы Graylog API Security автоматически предоставляет полезную и понятную информацию по устранению последствий
- **Высокоуровневые сведения:** Представленные на сводной приборной панели, они могут способствовать продуктивным обсуждениям в компании, поскольку

API часто находится на стыке DevOps, сети, безопасности и команд разработчиков приложений.

Graylog API Security работает внутри периметра для защиты от инсайдеров и аутентифицированных злоумышленников, маскирующихся под легитимных клиентов и партнеров для получения доступа к конфиденциальным данным.

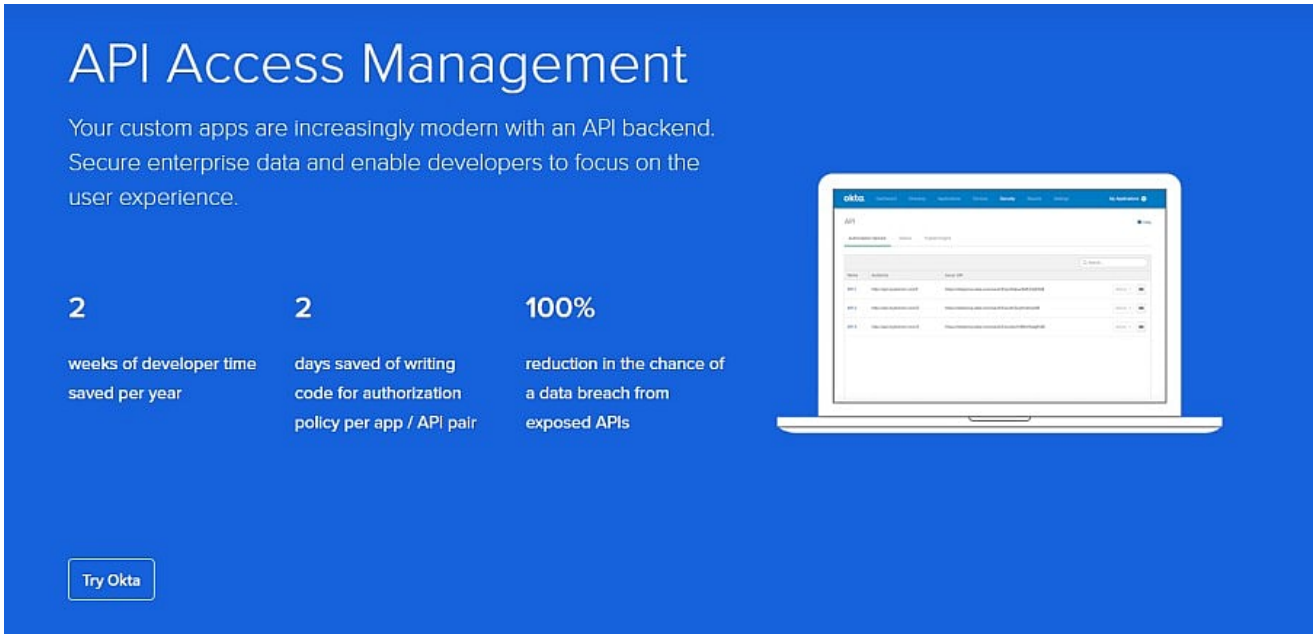
Invicti

Компания Invicti использует принцип “сканирования на основе доказательств”. Проще говоря, часто бывает так, что нестандартные условия работы сети или некоторые малоизвестные особенности поведения API интерпретируются как лазейки в системе безопасности, которые впоследствии оказываются неверными. При этом тратятся ресурсы, так как все уязвимости, о которых сообщается, необходимо просканировать еще раз вручную, чтобы убедиться, что они не являются ложными срабатываниями. В Invicti утверждают, что инструмент способен предоставить достаточно убедительное доказательство концепции для отчетов, устраняя сомнения относительно найденных слабых звеньев.



В списке их клиентов такие компании, как Sony, Religare, Coca-Cola, Huawei идругие, и вы можете быть уверены, что эти люди делают что-то правильное .

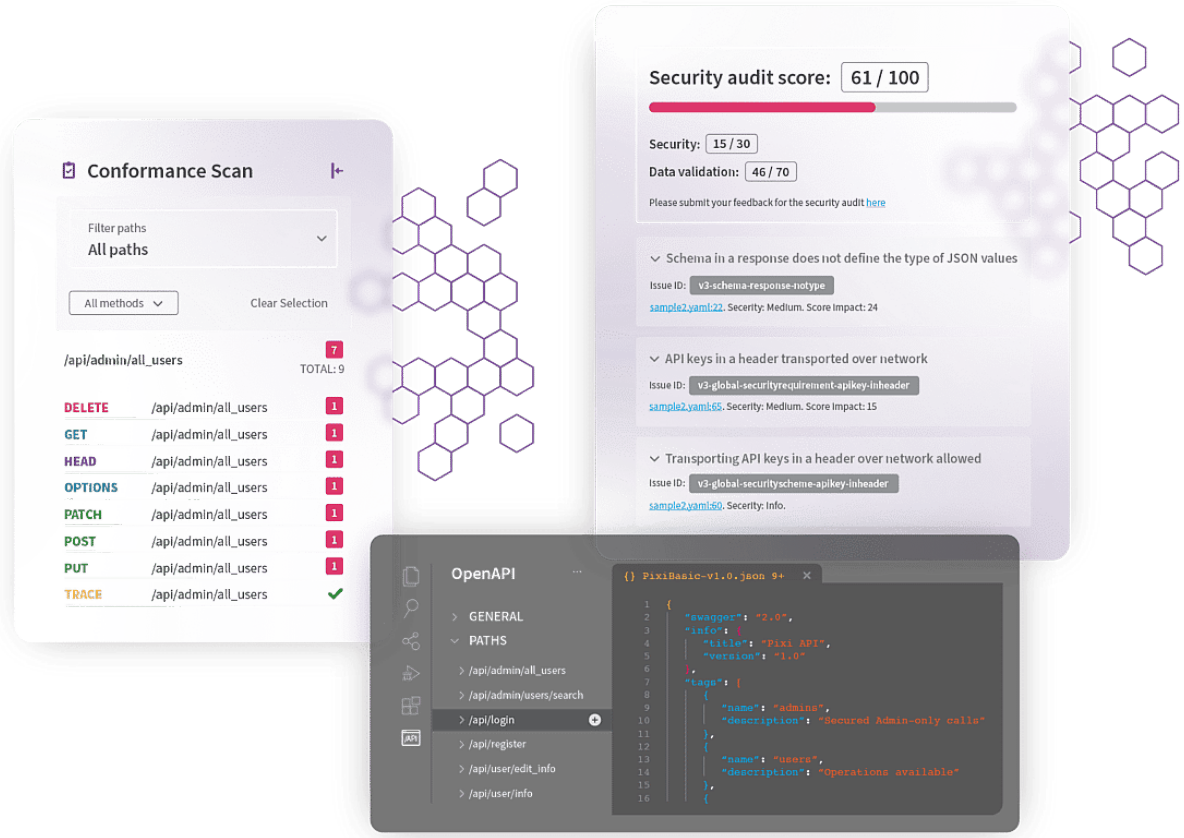
Okta



Попробуйте Okta, чтобы ваши разработчики могли сосредоточиться на улучшении пользовательского опыта, а также эффективно защитить корпоративные данные. Она предлагает авторизацию OAuth 2.0 и предназначена как для мобильных, так и для веб-приложений. Она также совместима со сторонними службами управления API. Используйте Okta для создания, аудита и поддержания всех политик доступа к API с помощью удобных и специально разработанных консолей без необходимости использования пользовательских кодов. Она обеспечивает дополнительную гибкость, поэтому вам не придется защищать свои API с помощью дополнительных экземпляров шлюзов. Okta включает в себя политики, основанные на идентификации, для контроля различных типов пользователей и сервисов под одной крышей. Определяйте доступ в зависимости от профилей пользователей, сетей, групп, согласий и клиентов. Расширяйте токены, используя динамические данные из ваших внутренних систем, чтобы ускорить интеграцию и обеспечить беспрепятственную миграцию. Она обеспечивает централизованное администрирование API и позволяет защищать ресурсы API. Okta уделяет особое внимание безопасности, позволяя защищать доступ между различными микросервисами.

42crunch

42Crunch – это платформа безопасности API для разработчиков, позволяющая легко интегрировать меры безопасности в конвейер разработки API, обеспечивая проактивное тестирование, исправление и защиту от разработки до выполнения. Платформе доверяют такие ведущие бренды, как Verizon, Ford, Bridgestone, Allianz и др.

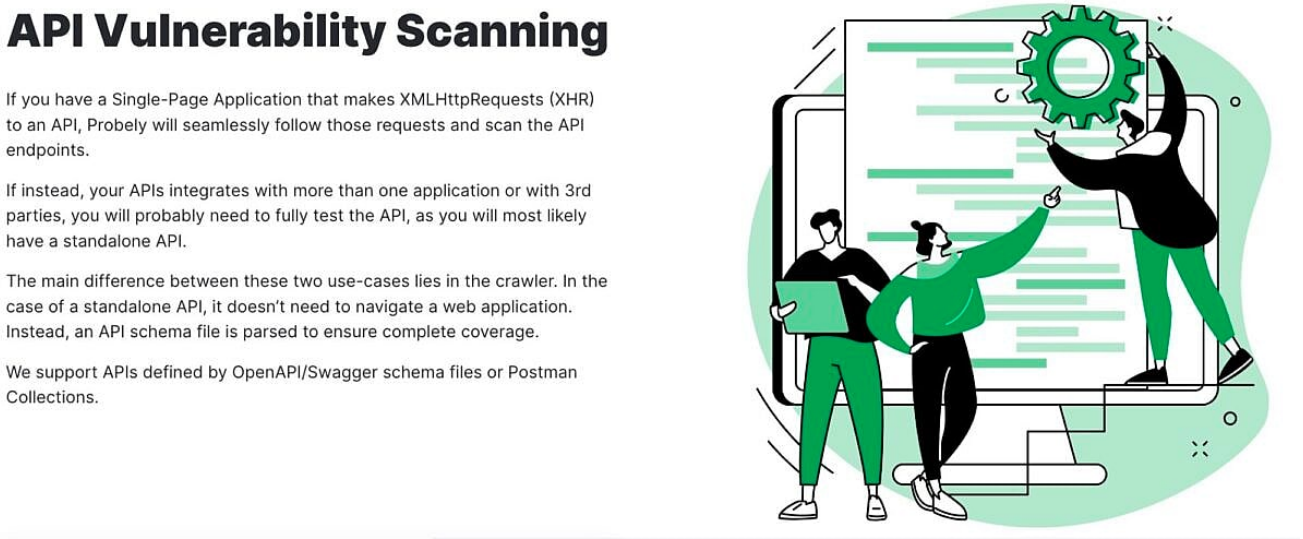


Компания утверждает, что это единственная платформа, которая обеспечивает управление безопасностью и соответствие требованиям от разработки до выполнения. Для этого используется API Audit, который выполняет 300 проверок безопасности; API Scan, который обнаруживает уязвимости во время тестирования и выполнения; и API Protect, который обеспечивает соблюдение политик безопасности API во время выполнения с помощью небольшого, контейнерного микро-API брандмауэра. Инструменты тестирования безопасности API от 42Crunch помогают обнаружить слабые места в безопасности API, а защита API обеспечивает безопасность во время выполнения программы с помощью проверки содержимого, обнаружения угроз, контроля трафика и микрофайервола API. Более 800 тысяч разработчиков используют инструменты 42Crunch для API.

Probely

Probely – это сканер уязвимостей, используемый SaaS-компаниями, разработчиками,

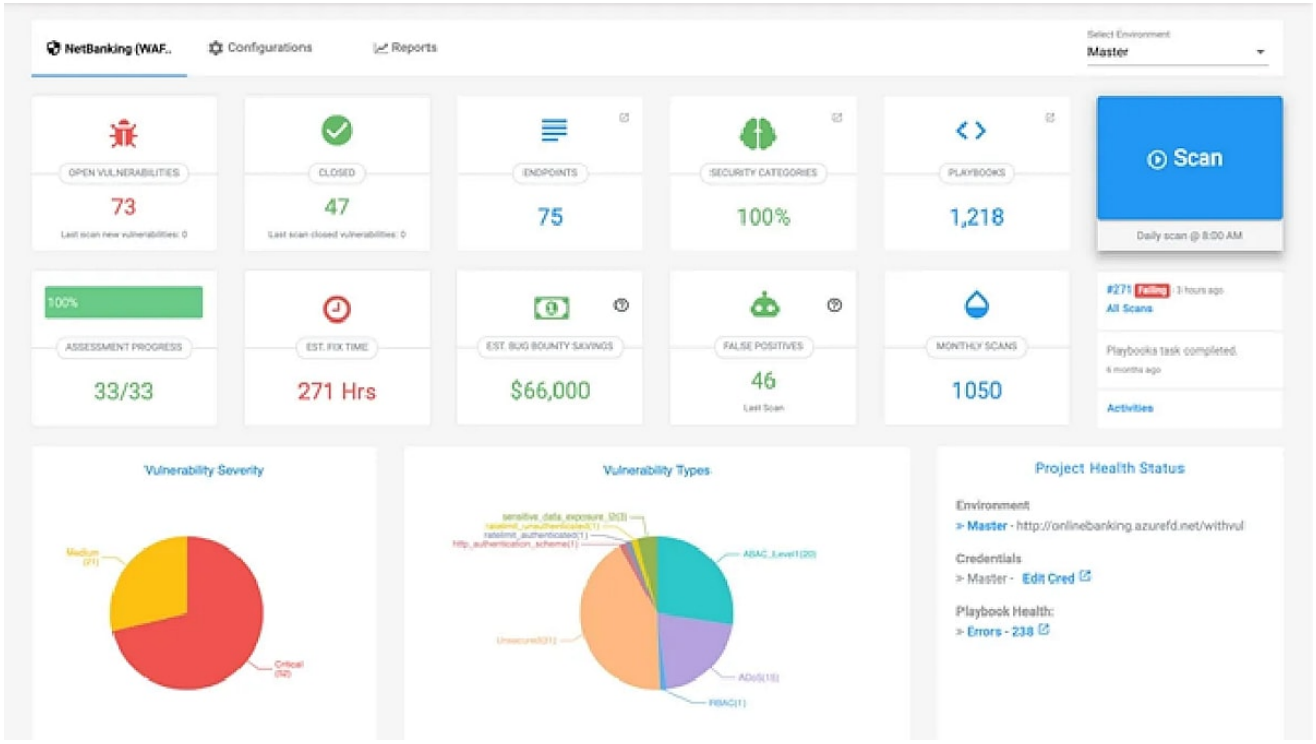
командами безопасности, DevOps и специалистами по соблюдению нормативных требований. Он сканирует веб-приложения и API, находит уязвимости и предлагает подробные отчеты о том, как их устранить.



Некоторые ведущие компании, такие как Olx, Trend Micro и Entertainment Partners, доверяют этой платформе, которая поддерживает различные веб-приложения и API, включая микросервисы и самостоятельные API, соответствующие спецификации OpenAPI (Swagger) или коллекции Postman. Probely предоставляет документированный API и адаптирует степень серьезности уязвимости в зависимости от контекста. Он интегрируется с конвейерами CI/CD, автоматизирует тестирование безопасности веб-приложений и API и синхронизируется с платформами отслеживания проблем. Он обеспечивает соответствие таким стандартам, как PCI-DSS, OWASP TOP 10, ISO27001, HIPAA и GDPR. Попробуйте его бесплатно в течение 14 дней.

APIsec

APIsec – это автоматизированная платформа для проактивного и непрерывного тестирования безопасности API. Она повышает доверие клиентов, тщательно проверяя обновления и релизы, чтобы обеспечить безопасность производственной среды. Платформа автоматизирует комплексное тестирование безопасности API на протяжении всего жизненного цикла разработки программного обеспечения (SDLC). Она позволяет обнаруживать, анализировать и выполнять сценарии атак на API до начала производства.



APIsec помогает избавиться от повторяющегося ручного тестирования сторонних разработчиков, автоматизируя тестирование безопасности API. APIsec легко интегрируется с платформами CI/CD, тикетов и коммуникаций, обеспечивая бесперебойную работу. Согласование тестов на проникновение в API с оценкой рисков позволяет выявлять проблемы безопасности на ранних стадиях, сокращая технический долг при разработке приложений. Платформа предлагает бесплатный сканер неаутентифицированных API для выявления неправильной конфигурации и других базовых недостатков безопасности. Она также предлагает бесплатные курсы, такие как основы безопасности API и экспертное первичное тестирование API; если вы заинтересованы, вы можете посетить APIsec University.

Cequence

Cequence – это отмеченная многими наградами платформа для обнаружения, инвентаризации, проверки соответствия и динамического тестирования API. Платформа помогает выявлять и предотвращать мошенничество, атаки, эксплойты и утечки данных в режиме реального времени.

Она предлагает комплексное решение для выявления поверхностей атак на API с целью обеспечения защиты от угроз, а также соответствия нормативным требованиям. Платформа легко интегрируется с существующей инфраструктурой API и безопасности. Cequence утверждает, что сэкономила миллионы долларов и миллиарды пользователей, обеспечив при этом безопасность транзакций. Среди ведущих компаний, использующих эту платформу, – RBS, American Express, Ulta Beauty, PoshMark, T-mobile, Telstra и другие. Среди основных возможностей платформы – обнаружение и оценка рисков API, устранение последствий воздействия чувствительных данных, предотвращение захвата учетной записи и оценка рисков API. Платформа предлагает бесплатную оценку безопасности API.

Зачем нужно защищать конечные точки API?

Нам нужно защитить конечные точки, потому что от этого зависит бизнес. Отсутствие защиты конечных точек API приводит к следующим нежелательным последствиям для бизнеса.

Потеря бизнеса. Это очевидно. Если кому-то удастся взломать ваши конечные точки API, это приведет к остановке всего процесса. Нарушение безопасности также может занять много времени на восстановление, что в переводе на язык бизнеса означает самоубийство. Хотя большинство компаний, скорее всего, не пострадают от часа или двух простоя, для некоторых это недопустимо. Представьте себе, что валютная биржа не работает в течение нескольких минут!

Вопросы соответствия. Отсутствие надлежащей защиты API может привести к

серьезным неприятностям, в зависимости от того, с какой географией или отраслью вы имеете дело. Например, если вы обслуживаете банковскую отрасль (особенно в ЕС), то обнаружение небезопасных API приведет к серьезным юридическим проблемам и нарушениям нормативных требований. Настолько, что это может даже означать конец вашего бизнеса.

Потеря репутации. Быть взломанным достаточно болезненно само по себе, но если новость становится достоянием общественности, то имидж вашего бренда будет безвозвратно потерян. Например, Sony уже несколько раз подвергалась очень серьезным взломам, и в кругах специалистов по безопасности эта компания стала своего рода посмешищем. Даже если фактическая потеря данных или денег не произойдет, удачи вам в попытках убедить своих уходящих клиентов .

Раздутые счета за инфраструктуру. Когда ваш API работает на инфраструктуре, он потребляет ресурсы (в основном пропускную способность, процессор и память). Например, если API не защищен должным образом, и злоумышленники могут взаимодействовать с ним, они могут заставить API выполнять много бессмысленной работы (например, выполнять тяжелые запросы к базе данных), что может увеличить ваши счета по разным причинам. На платформах, где включено автоматическое масштабирование ресурсов (например, AWS), результаты могут быть шокирующими (не по теме, но если вы когда-нибудь попадете в подобный суп на AWS, они с пониманием отнесутся к ситуации и быстро отменят завышенный счет – по крайней мере, на момент написания статьи!)

Моральный дух команды. Вы можете подумать, что команда, допустившая эти компромиссы, потеряет моральный дух из-за них. Ну, не совсем так. Возможно, компромиссы произошли из-за слабой безопасности инфраструктуры, что расстроит разработчиков или наоборот. Если это произойдет достаточно часто, у вас на руках окажется культура, о развитии которой вы пожалеете.

Прибыль конкурентов. Допустим, взлом произошел, но реальных потерь не было. Однако ваши конкуренты воспользуются этим инцидентом, чтобы пропиарить свой API и заявить, насколько их API безопаснее (даже если это не так!). И снова удачи в попытках убедить рынок . В общем, последствия нарушения безопасности не ограничиваются потерей денег.

Лучшие практики защиты конечных точек API

К счастью, существуют определенные простые в реализации и хорошо понятные практики, которые вы можете применить к своим конечным точкам API для их защиты. Вот что рекомендуют большинство экспертов по безопасности.

HTTPS всегда. Если ваши конечные точки API позволяют потребителям API общаться по `http` или другим небезопасным протоколам, вы подвергаете их большому риску. Пароли, секретные ключи и информация о кредитных картах могут быть легко украдены, поскольку любая атака “человек посередине” или инструмент для перехвата пакетов может прочитать их как обычный текст. Поэтому всегда делайте `https` *единственным* доступным вариантом. Какой бы тривиальной ни казалась конечная точка, подключение по `http` не должно быть даже вариантом. Сертификат TLS стоит не так уж много: в его можно купить всего за 20 долларов.

Одностороннее хеширование паролей. Пароли никогда не следует хранить в виде обычного текста, поскольку в случае нарушения безопасности все учетные записи пользователей будут скомпрометированы. В то же время следует избегать симметричного шифрования, поскольку любой достаточно изобретательный и настойчивый злоумышленник сможет его взломать. Единственный предложенный вариант – асимметричные (или “односторонние”) алгоритмы шифрования для хранения паролей. В этом случае ни злоумышленник, ни разработчик или системный администратор в компании не смогут прочитать пароли клиентов.

Надежная аутентификация. Почти каждый API имеет свою форму аутентификации, но, на мой взгляд, система OAuth2 работает лучше всего. В отличие от других методов аутентификации, она разделяет ваш аккаунт на

ресурсы и разрешает только ограниченный доступ носителю auth-токена. В то же время еще одна очень хорошая практика – устанавливать срок действия токенов, скажем, каждые 24 часа, чтобы их нужно было обновлять. Таким образом, даже если ваш токен утечет, есть шанс, что 24-часовой срок действия уменьшит последствия утечки.

Применяйте ограничение скорости. Если у вас нет API, которым ежеминутно пользуются миллионы людей, очень хорошей идеей будет установить ограничение на количество обращений клиента к API за определенный промежуток времени. В основном это делается для того, чтобы не допустить появления ботов, которые могут отправлять сотни одновременных запросов каждую секунду и заставлять ваш API потреблять системные ресурсы без всякой на то причины. Все фреймворки для веб-разработки поставляются с промежуточным программным обеспечением для ограничения скорости (а если его нет, то его легко добавить с помощью библиотеки), настройка которого занимает всего минуту или около того.

Удостоверение ввода. Звучит как само собой разумеющееся, но вы удивитесь, узнав, как много API-систем опускаются до этого. Валидация входных данных означает не только проверку правильности формата входящих данных, но и исключение возможных сюрпризов. Простой пример – SQL-инъекции, которые могут уничтожить ваши базы данных, если вы позволите строкам запросов пройти через них с минимальной проверкой или вообще без нее. Другой пример – проверка размера POST-запроса и возвращение клиенту соответствующего кода ошибки и сообщения. Попытки принять и разобрать нелепо большие данные приведут лишь к тому, что API будет просто разрываться.

Обеспечьте фильтрацию IP-адресов, если применимо. Если вы занимаетесь B2B-сервисами и вашими API пользуются компании из разных мест, подумайте о том, чтобы добавить дополнительный уровень безопасности, ограничивающий IP-адреса, которые могут получить доступ к вашему API. Для каждого нового местоположения и нового клиента необходимо будет проверять IP-адрес входящего запроса. Да, это создает дополнительные неудобства при регистрации, но в итоге безопасность становится намного выше, чем может быть достигнута иным способом.

Заключение

На рынке нет недостатка в инструментах для обеспечения безопасности API, будь

то инструменты с открытым исходным кодом, бесплатные или коммерческие, или любая их комбинация. Попробуйте несколько из этого списка и посмотрите, что лучше всего подходит для ваших требований.

Дата Создания
09.05.2024