Когда нужно автоматизировать пентест?

Валерий Филин
Технический директор

CITUM – экспертный дистрибьютор

Добрый день, коллеги.

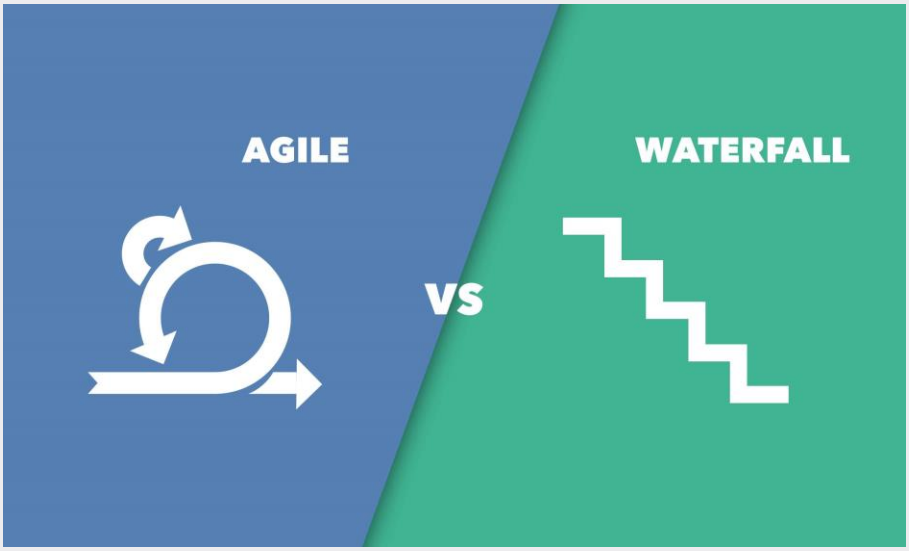
Сегодня мы поговорим о различных подходах к построению ИБ в организации, о том, что такое тест на проникновение, и когда его нужно автоматизировать.

Подходы к управлению ИБ (1/2)

- Каскадная модель управления

или

- Гибкая модель управления



Каскадная vs Гибкая (Agile) модель управления безопасностью

- **Каскадная модель** управления подходит для случаев, когда весь объем задач заранее известен, изменения маловероятны, и проектная команда слабо связана между собой. Классический порядок построения ИБ - комплексная оценка активов, создание профиля злоумышленника и модели угроз, анализ рисков по всем активам, выбор стратегий работы с рисками, внедрение средств защиты, внедрение процессов управления ИБ, оценка эффективности системы в целом. В случае с каскадной моделью построение эффективной ИБ с нуля занимает годы. На определенном этапе внедряется сканер уязвимостей для анализа рисков, связанных с уявзимостями в ПО. Внедрение одного только сканера занимает месяцы, а после внедрения анализ отчетов сканера и исправление всех критичных уязвимостей требует существенных трудозатрат на постоянной основе. В итоге на протяжении месяцев нельзя с уверенностью сказать, что сеть организации эффективно защищена. А даже после эффективного внедрения сканера и процесса патч-менеджмент остается риск взлома: ошибки в конфигурации сети, небезопасное пользовательское поведение. Закрыть эти пробелы может регулярное практическое тестирование защищенности.
- **Гибкая модель** призвана быстро планомерно инкрементально повышать эффективность ИБ с минимальными издержками за счет постоянной проверки результата.

*- В современных условиях быстро меняющегося ландшафта угроз предпочтительнее **гибкая модель** управления безопасностью. Как "разработка через тестирование" и инкрементальные релизы в гибкой методологии разработки позволяют выпустить рабочий продукт гораздо быстрее, так же и "построение ИБ через тестирование" с инкрементальными исправлениями позволяют организациям получить быстрый существенный прирост уровня защищенности.*
Если организация выбирает для себя гибкую модель управления ИБ - ей в первую очередь необходим эффективный инструмент постоянного тестирования защищенности.

Подходы к управлению ИБ (2/2)

- Эшелонированное построение защиты

  или

- Бережливое построение защиты

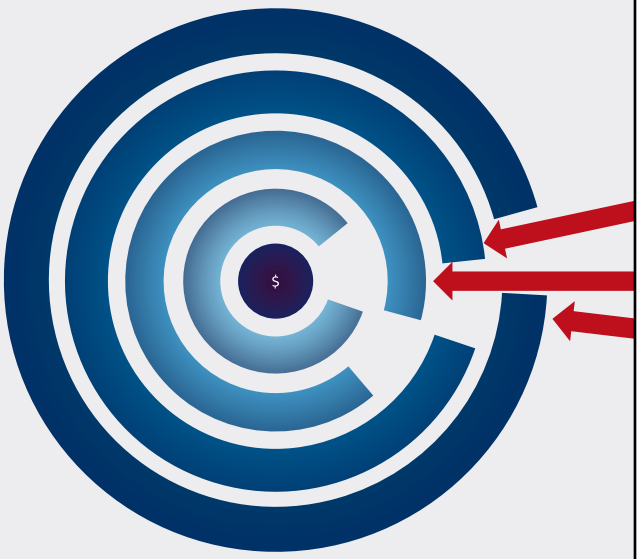
Эшелонированная vs Бережливая (Lean) система защита
Гибкая модель управления перекликается с **бережливым подходом** к построению ИБ.
- **Стандартный эшелонированный подход** к безопасности: внедрить несколько эшелонов защиты (NGFW/IPS, Web Gateway, Email Gateway, AV, NGAV, EDR) и предпочтительно с движками от разных производителей. Совокупная стоимость такой системы - немалая. Трудозатраты на обучение персонала и последующую эксплуатацию огромные. И эффективность по сути сильно зависит от того, насколько регулярно и полноценно используются все внедренные решения. Протестировав защищенность сети в комплексе, мы можем понять, какие решения работают эффективно, а какие требуют оптимизации.
- **Бережливый подход**: внедрять только то, что обязательно нужно именно сейчас с учетом состояния сети, развернутых систем, имеющихся уязвимостей, ошибок в конфигурации и поведения реальных пользователей.

- В современных условиях (кризис, урезание бюджетов) предпочтительнее именно бережливый подход. Как узнать, куда именно сейчас необходимо направить ресурсы в первую очередь? Необходимо не просто оценить теоретический уровень риска на основе статических данных от сканера. Необходимо протестировать

на практике все элементы окружения и средства безопасности и выявить реальные слабые места. Возможно, внедрение нового защитного средства не является срочной задачей - если предотвратить угрозу позволит оптимизация существующих решений или исправление некорректной конфигурации в сети.

Эффективность ИБ

- Эффективность защиты от массовых угроз

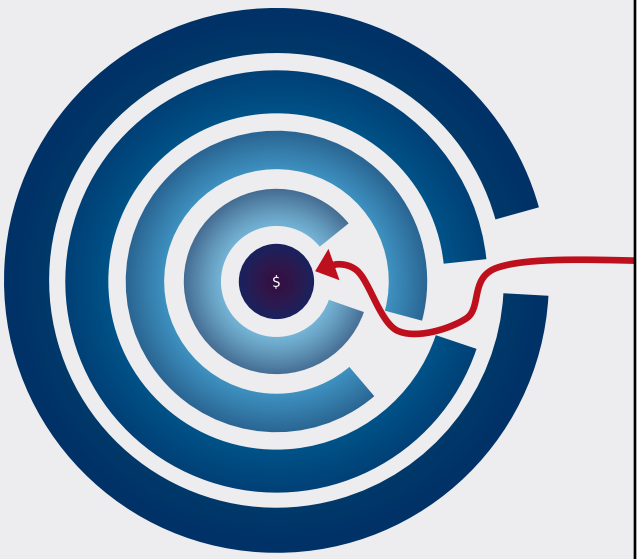


Краеугольный камень ИБ - эффективность.

Как в любой другой дисциплине лучше уметь что-то одно, но делать это на 100% качественно, чем владеть 10 различными инструментами и приемами, но только в теории.
Если в нашей эшелонированной защите применяется 5 решений, и каждое из них работает на 90%, интуитивная математическая оценка эффективности - 99,999%. Для массовых угроз это, возможно, верно.

Эффективность ИБ

- Эффективность защиты от массовых угроз
- Эффективность защиты от направленных атак



Для целенаправленных атак - наша сеть защищена настолько эффективно, насколько хорошо работает самое слабое звено, то есть в данном случае - 90%.

Важно понимать всю цепочку атаки: какие эшелоны защиты могут сработать. Что если где-то неэффективный рубеж?
Как оценить эффективность? Как найти слабое звено?

Тестирование на проникновение

- Конкретная сеть
- Конкретные начальные условия
- Конкретная цель
- Активная эксплуатация
- Подтвержденные векторы атак
- Релевантные рекомендации

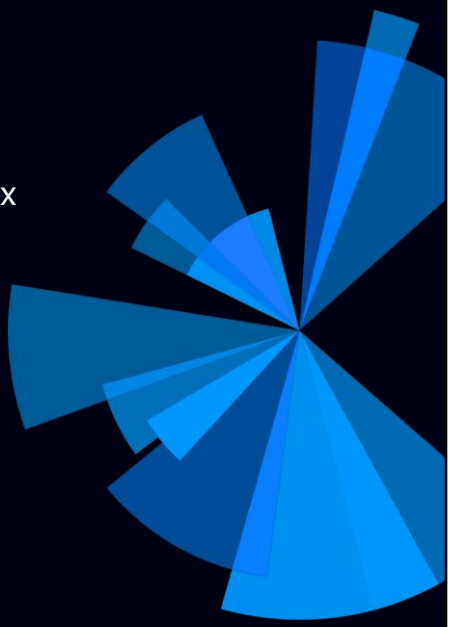
PCYSYS – платформа для автоматизации пентестов

На протяжении последних 20 лет золотым стандартом проверки защищенности организации является тест на проникновение (пентест). Тестирование на проникновение - единственный способ _реально_ оценить уровень защищенности с учетом всех применяемых технологий и процессов ИБ.
Большинство организаций выполняют ручной пентест с привлечением внешнего консультанта или своими силами. Но теперь существует способ выполнять этот процесс автоматически.

Для начала давайте определимся с тем, что мы будем называть пентестом.
Тест на проникновение (пентест) *– метод оценки защищенности сети путем активной эксплуатации найденных слабых мест в окружении. Конечная цель пентеста – демонстрация максимального количества подтвержденных сценариев угроз (векторов атак) в конкретной сети в конкретный момент времени. Результат пентеста – набор подтвержденных векторов атак, перечень рекомендаций по исправлению, релевантный конкретной сети организации.*

Ценность пентеста

- Релевантные данные:
  - реальная проверка сети в «боевых» условиях
  - полная картина развития атаки
  - подтвержденный результат эксплуатации
- Что можно протестировать?
  - надежность доменных политик
  - качество управления привилегиями
  - безопасность ключевых сетевых настроек
  - эффективность средств защиты
  - эффективность процессов реагирования
  - безопасность ценных активов
  - классические бинарные уязвимости



PCYSYS – платформа для автоматизации пентестов

Что дает пентест?

- реальная эксплуатация уязвимостей
- полные векторы атак
- подтвержденный технический результат

Что можно протестировать?

- эффективность парольной политики на практике
- качество управления привилегиями пользователей
- безопасность ключевых настроек сетевой инфраструктуры
- эффективность средств защиты (антивирус, NGFW, HIPS, EDR)
- эффективность процессов реагирования при наличии SOC
- надежность сегментации сети
- к каким данным может получить доступ злоумышленник в различных сценариях
- классические уязвимости также применяются, но далеко не всегда

Именно доступность автоматизированного пентеста позволяет теперь эффективно реализовать гибкий и бережливый подход к управлению ИБ

- Скорость анализа: быстрое получение значимых результатов
- Мгновенный повторный анализ после внесения исправлений
- Непрерывная оценка защищенности: *важно понимать, что в условиях динамично меняющихся современных сетях поверхность атаки не может быть статичной, каждый день в сети могут появляться новые пользователи, устройства или программы, открываться уязвимости, добавляться или исчезать средства защиты – всё это приводит изменению ландшафта угроз в конкретной сети и проведение пентеста 1 раз в год в отдельном сегменте сети недостаточно для обеспечения высокого уровня защищённости. Процесс анализа и устранения брешей в кибер-защите должен быть непрерывным и охватывать всю сеть.*
- Произвольное масштабирование теста
- Экономия ценного человеческого ресурса *на всех этапах: от анализа защищённости, до внедрения исправлений, патчей и устранения мисконфигурации в сети*
- Максимально целостная/последовательная оценка: моделирование полных векторов атак с охватом в ширину и в глубину,

воспроизводимость
- Неразглашение информации об уязвимостях и векторах атак третьим лицам

Алгоритмы - машине, человеку – творчество!

Человеческий мозг и машина - разные вещи, и нужно понимать сильные и слабые стороны обоих.

Мозг хорошо решает трудные творческие задачи, но плохо масштабируется.

Машина хорошо выполняет предложенные ей алгоритмы.

Любой пентестер-консультант работает по определенным плейбукам. Плейбук есть не что иное как алгоритм. Очевидно, машина справится с такой работой быстрее и надежнее, чем человек.

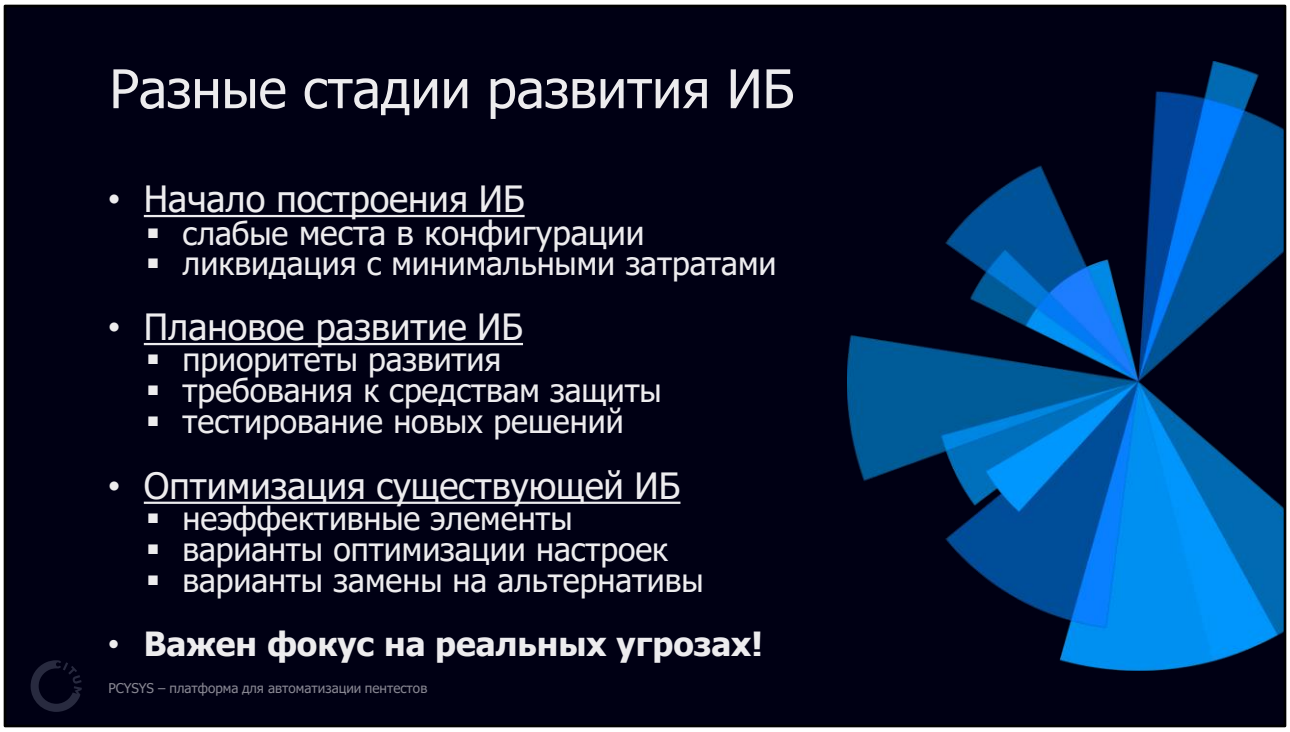
Если задача - точечно проверить потенциальный ущерб для сети от реализации эксплойта на новую 0-day уязвимость - ваш выбор человеческий пентест. Но такой точечный пентест будет априори дорогим, за счёт разработки специализированного кода.

Если задача - регулярно тестировать защищенность сети в комплексе, с учётом всех средств и техник защиты, и в полном масштабе - вам нужна машина.

Так когда же необходимо внедрять автоматизацию пентеста?
Ответ на этот вопрос: сейчас.
Если вы склоняетесь к гибкой модели управления и бережливому построению ИБ, автоматизация пентеста - инструмент оперативного практического тестирования защищенности - ваш главный ориентир в плане оценки эффективности ИБ.
А если вы применяете каскадную модель управления и эшелонированное построение защиты, автоматизация пентеста потребует незначительных дополнительных инвестиций и при этом позволит поднять процесс управления уязвимостями на принципиально новый уровень.

В современных условиях (экономическая ситуация в стране, снижение курса рубля, приостановка многих бизнес-процессов в связи с пандемией) особенно важно экономить средства и ресурсы.
Вместе с тем количество угроз на фоне кризиса только увеличилось.
Перевод сотрудников на режим удаленной работы существенно расширил поверхность атаки: злоумышленник может попасть во внутреннюю сеть организации, предварительно скомпрометировав удаленное рабочее место пользователя, слабо защищенное и неподконтрольное службам ИТ организации.
То есть, требования к защите растут, а возможности инвестиций в

ИБ снижаются.
Автоматизированный пентест позволит быстро обнаружить неэффективные элементы защиты и выбрать наиболее экономичный способ оптимизации ИБ: например, (1) устранить 2-3 наиболее критичные уязвимости в окружении, сократив подтвержденный технический ущерб от вероятной атаки в несколько раз, или (2) оптимизировать настройки существующих средств ИБ без дополнительных финансовых вложений.
Кроме того, регулярный анализ защищенности позволит быть уверенными в безопасности корпоративной среды, несмотря на серьезное давление со стороны внешних факторов.



Конкретные примеры на разных стадиях становления ИБ

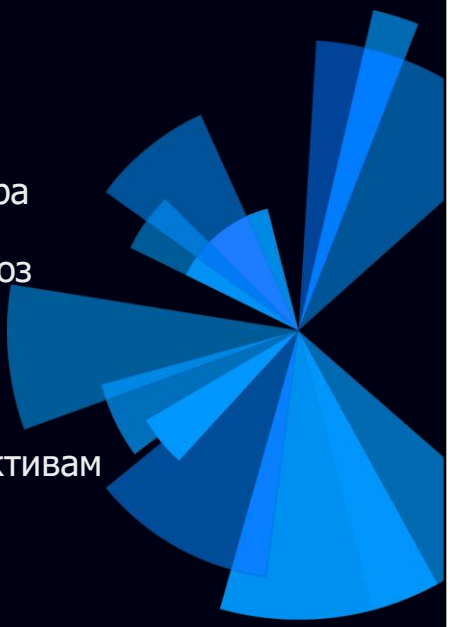
1. Начало построения ИБ в организации. Начинать анализировать защищённость целесообразно уже тогда, когда будет развёрнута ИТ-инфраструктура (домен, АРМ, серверы) и базовые средства кибер-защиты (антивирусы и МСЭ). На этом этапе средства автоматического анализа защищённости позволяют выявить базовые недостатки в кибер-защите, определить поверхность атаки и максимально закрыть её минимальными средствами, внося изменения в инфраструктуру и используя уже имеющиеся инструменты ИБ для закрытия уязвимостей, не устранимых в оперативном режиме.
2. Плановое развитие ИБ. В ходе развития корпоративных ИБ-комплексов заказчики сталкиваются с вопросом приоритизации: какие инструменты, когда и для закрытия каких именно угроз необходимо покупать? Как формализовать задачу для новых инструментов ИБ и проверить качество их работы? Платформа автоматизации пентеста позволит приоритизировать процесс, фокусируя внимание на фактически подтверждённых угрозах, а также протестировать новые инструменты "в бою" перед покупкой.
3. Оптимизация существующей ИБ. Заказчики, использующие обширный перечень ИБ-инструментов всё время сталкиваются с вопросом об их эффективности. Как проверить, что инвестиции в ИБ-работают? Как

узнать, какой инструмент нужно дополнительно настроить, а какой - заменить? Есть 2 пути: 1) реактивный, когда мы отталкиваемся от выявленных инцидентов ИБ и 2) проактивный, когда мы не ждём ИБ-инцидентов или ущерба, а заранее выявляем все слабые места и исправляем их.

Pcysys PenTera – первая в мире полностью автоматическая платформа автоматизации тестов на проникновение.
Ежедневное тестирование защищенности теперь доступно каждому.

Преимущества PenTera

- Не требует экспертных знаний
- Не требует постоянного участия оператора
  Быстрое получение ценных результатов
- Проверка самых актуальных техник и угроз
- Безопасная эксплуатация
- Полное представление о векторе атаки
- Высокоуровневая категорийная оценка
- Тестирование специфичных сценариев
- Демонстрация векторов атак к ценным активам
- Экономически эффективный подход



PCYSYS – платформа для автоматизации пентестов

Все преимущества автоматизации + дополнительные уникальные:

- Не требует экспертных знаний для выполнения пентеста
- Не требует участия оператора – экономит человеческий ресурс
- Ценные результаты доступны быстрее, чем от консультанта или штатного специалиста
- Оценка защищенности с использованием самых современных техник и с учетом актуальных угроз
- Безопасная эксплуатация
- Полное представление о картине развития атаки: исходная точка, детальная информация о каждом шаге, подтвержденный результат
- Высокоуровневая оценка защищенности организации по категориям
- Тестирование специфичных сценариев угроз (например, имитация заражения конкретной системы в сети)
- Демонстрация всех достижимых векторов атак, угрожающих ценным активам
- Организация процесса повышения защищенности самым экономически эффективным образом

Остались вопросы?

Мы готовы на них ответить:
vfilin@citum.ru
+7(903)765-3862

Подробнее о Pcysys PenTera – на нашем сайте:
https://citum.ru/pcysys

Если вы хотите узнать больше о решении Pcysys PenTera, вы можете обратиться к коллегам в Axxtel для организации продуктовой презентации.
На нашем сайте вы также всегда сможете запросить презентацию или тестирование PenTera.

Если у вас остались какие-либо вопросы по теме сегодняшнего вебинара – мы готовы ответить.