Как внедрить стандарты безопасной настройки и не поругаться с IT

Кирилл Евтушенко,
генеральный директор ООО «Кауч»

Кто мы

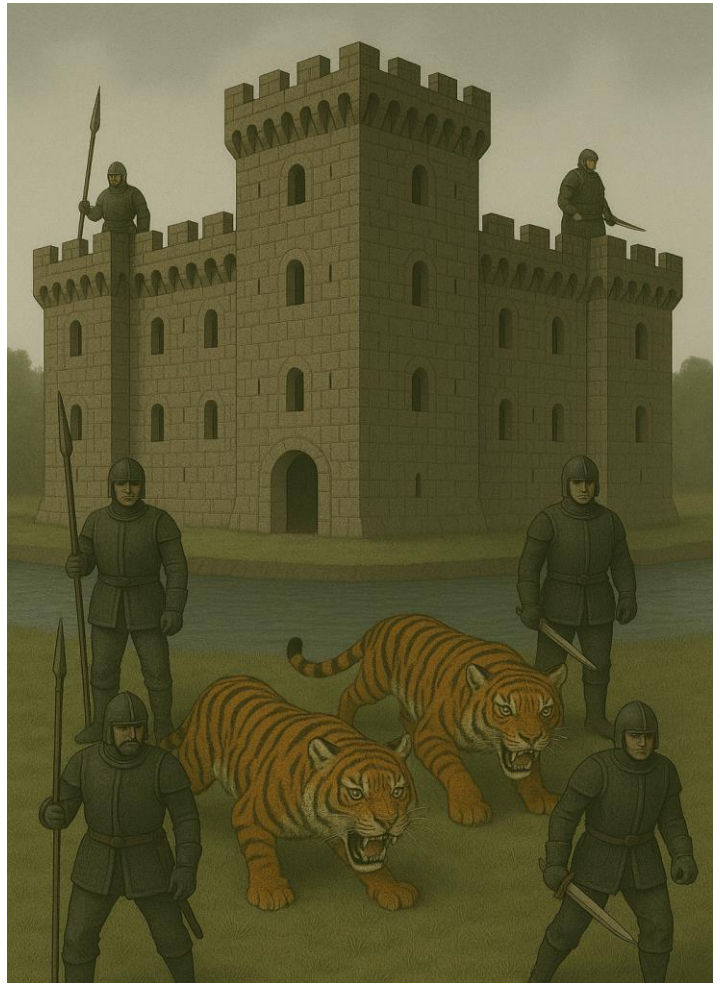
Главные по настройкам 😎

Кто мы

- Аудиторы, консалтеры и пентестеры в душе (и трудовых книжках)
- 10 лет решаем проблемы, связанные с безопасными настройками и их внедрением
- Разрабатываем самую крутую российскую платформу класса Security Configuration Management
- Амбассадоры дружбы ИБ и ИТ

Зачем настраивать безопасно

- Заставляют
  ФСТЭК России, Банк России (ГОСТ Р 57580), НСПК (PCI DSS)…
- Настоятельно рекомендуют
  CIS, NIST, ГОСТ 27001/27002…
- Ломают
  Злые редиски
- Почему бы и нет
  Фундаментальная защита встроенными средствами



Сложно…

- Настроек безопасности **очень** много

  CIS Benchmarks ОС: ~300-400, СУБД: ~200, ППО…
- **ИБ**: не может выполнить задачу безопасной настройки без привлечения ИТ
- **ИТ**: не понимают, за что им это все
- Отчеты сканера уязвимости (aka **ЗЛО**): прилетают

- **Хорошо**: просканировать 1 000 настроек на каждом хосте, чтобы оценить уровень защищённости и GAP
- **Такое себе**: предлагать ИТ-администраторам настраивать на каждом хосте в «боевой» эксплуатации 500-1000 настроек сразу

Тише едешь – д*ѳа*льше будешь

✕ Отказываемся от попытки настроить всё сразу: ограничения времени, ресурсов, возможностей…

☑ За системы и их настройку отвечают живые люди: «красный» отчёт на 500 страниц по каждой системе деморализует, а ещё:

- многое непонятно,
- кажется невыполнимым и бесконечным,
- неясно, достигнут ли результат

Жиза

Как найти друзей после 30

вымученных требований безопасной настройки

Едим слона частями

- При внедрении стандартов конфигурирования первично формируем сокращенный перечень наиболее критичных настроек по каждой системе, чтобы ИТ-администраторы:
  - понимали, что настройка ограниченного количества параметров займет немного времени,
  - сразу осознавали важность и значимость каждой настройки в стандарте,
  - не реагировали остро на попытки «завалить ИБ-шной» работой,
  - ощущали, что поставленные задачи и цели реалистичны, посильны, конечны.
- Можно смотреть на задачи через призму SMART или любых других методологий
- Участники процесса должны иметь возможность «ощущать» результат, поставить ☑, закрыть тикет, выполнить KPI, отчитаться, повысить ЧСВ, получить премию… (нужное подчеркнуть)

Сколько вешать в граммах?

- 30-50 требований на старте в одном стандарте
- Если есть конкретная «обязаловка» (например, PCI DSS) – берем, чтобы не «налететь» на штрафы и санкции
- Самые критичные и понятные с точки зрения важности требования: парольная политика, доступ, логирование и аудит, шифрование и защита данных и пр.
- Стараемся не засовывать в одно требование большие вложенные куски, например, полсотни параметров аудита

- Быстрая настройка базового перечня наиболее важных настроек на всех или на большинстве систем поможет значимо поднять общий уровень защищенности

Маловато будет. Что дальше?

- Регулярно оцениваем прогресс и обновляем стандарты настройки (заодно выполняем регуляторные требования по пересмотру)
- От 1 раза в 3 месяца до 1 раза в год
- Проводим отдельно оценку по каждому типу систем и группе ИТ-администраторов: все могут двигаться с разной скоростью. Оцениваем динамику
- «Отличникам накидываем» побольше, «отстающим» – поменьше
- Выявляем и устраняем причины проблем в процессе

Друзья по несчастью

- «Обязаловка» по безопасной настройке вызывает реакцию
- Можно начинать с небольших «пилотных проектов»: если с каким-то подразделением в ИТ очень хорошие отношения – идём к ним
- Следующие на очереди:
  - секьюрити чемпионы,
  - энтузиасты,
  - гики,
  - эксперты с активной жизненной позицией,
  - ~~медленно бегающие спикеры ИТ-конференций~~
- Успешный пример поможет с меньшими усилиями и более эффективно вовлечь в процесс другие подразделение и ИТ-руководителей

Хотим как лучше

- Согласовываем стандарты с конкретными администраторами
- Проводим тестирование совместно с ИТ: настраиваем тестовые системы и выборку «боевых», идентифицируем и обрабатываем отклонения, собираем обратную связь
- Делаем вместе «рабочие» стандарты, копипаст из отчетов, бенчмарков и стэкэксченьджа «не полетит»
- Объясняем с точки зрения ИБ каждое требование, которое вызывает вопросы
- Разбираемся вместе в проблемах и «трудных местах»
- Не конфликтуем и получаем удовольствие от общего благого дела

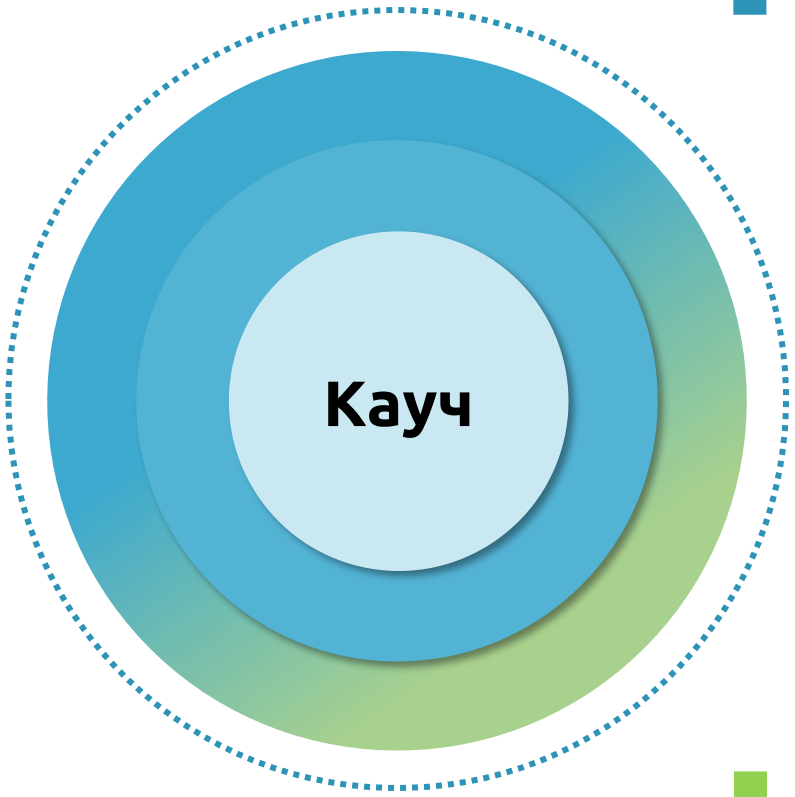
Прорывные технологии

Хорошая новость: мы уже всё «запилили»!

И продолжаем активно пилить дальше

Кауч

All-in-one платформа для управления безопасностью конфигураций



Сканирование на соответствие лучшим мировым практикам

Совместная работа и разделение задач

Настройка ресурсов инструментарием «из коробки»

Создание политик любой сложности

Мониторинг изменений

Единый процесс

Управление безопасностью конфигураций включено в общий процесс мониторинга и реагирования на инциденты

Польза для ИБ

Один инструмент

Можно реализовать техническую часть процесса на базе одного продукта (вне зависимости от размера инфраструктуры)

Меньше трудозатрат

Трудозатраты подразделения ИБ на управление всем процессом и администрирование системы сокращаются до 1-2 часов в день

Экономия времени

Исчезает роль «оператора сканера»: не нужно с утра до вечера обслуживать сканер и пересылать отчеты

Оптимизация затрат

Операционные затраты на реализацию процесса безопасного конфигурирования в разы ниже варианта со сканером уязвимостей и отчетами

Польза для ИТ

Удобство работы

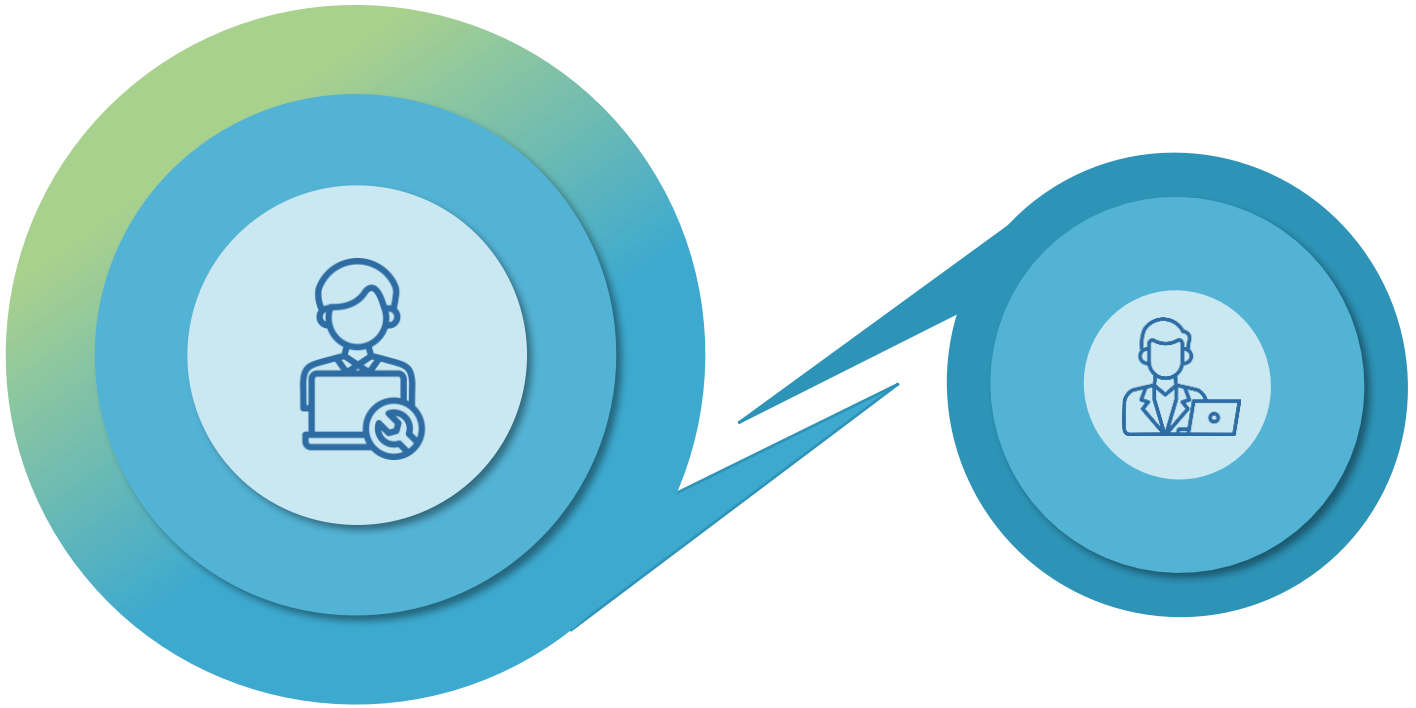
Единственный продукт, который заточен под специфику задач ИТ-службы в процессе безопасного конфигурирования

Меньше трудозатрат

Регулярные трудозатраты ИТ-специалиста на обработку одного требования безопасности сокращаются в 3 или более раз

Не только безопасность

Можно упростить работу не только с ИБ: доступна проверка и настройка любых параметров на всех подключенных ресурсах



Приходите к нам на стенд №11 🙃

А еще нам можно написать:

couch.ru

info@couch.ru