КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ИТОГИ

КОД ИБ ИТОГИ | 02 ДЕКАБРЯ 2021

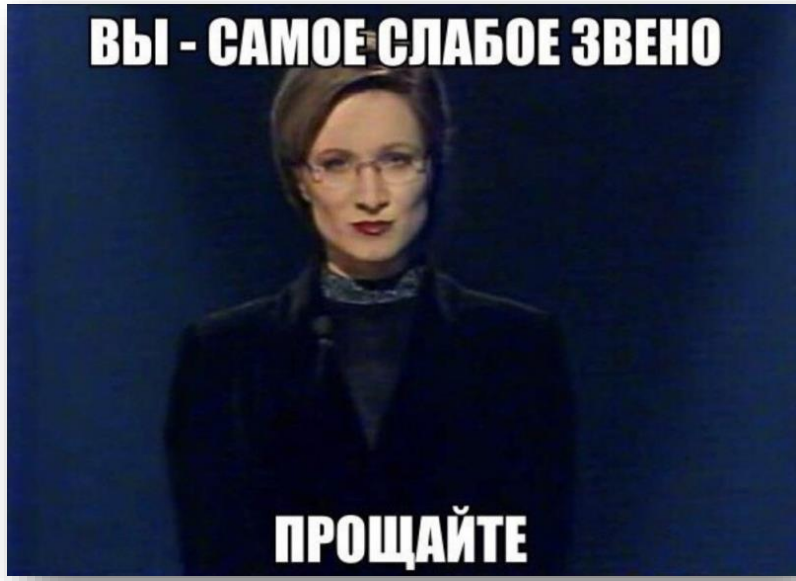
КАК ВОСПИТЫВАТЬ У СОТРУДНИКОВ БЕЗОПАСНОЕ ПОВЕДЕНИЕ

РОМАН ЖУКОВ, PRODUCT SECURITY MANAGER, INTEL

МОСКВА

КАК ИБ ЗАЧАСТУЮ СМОТРИТ НА СОТРУДНИКОВ

1. Сотрудник – слабое звено, брешь, что с него взять.
2. ИБ нужно строго следовать, и так все понятно.
3. ИБ – это вам не другие отделы: строгость и палка.
4. Чтобы сами отделы улучшали ИБ – это утопия.
5. Инциденты, метрики, отчеты – очень секретно.



НЕКОТОРЫЕ МЫСЛИ СОТРУДНИКОВ

1. ИБ-команда – чужая для нашего отдела, как доверять.
2. ИБ – всегда overhead, ведь KPI мои и отдела другие.
3. Меня хвалят за другое, да и босс не говорит про ИБ.
4. Посмотри на мой список задач: вам ИБ или бизнес.
5. Зачем мне это выполнять: нет смысла, кривая инструкция, очередной скучный тренинг.

КАК ВОСПИТЫВАТЬ ПРАВИЛЬНОЕ ПОВЕДЕНИЕ

- Security Champions
- Осведомленность
- Обучение
- Признание

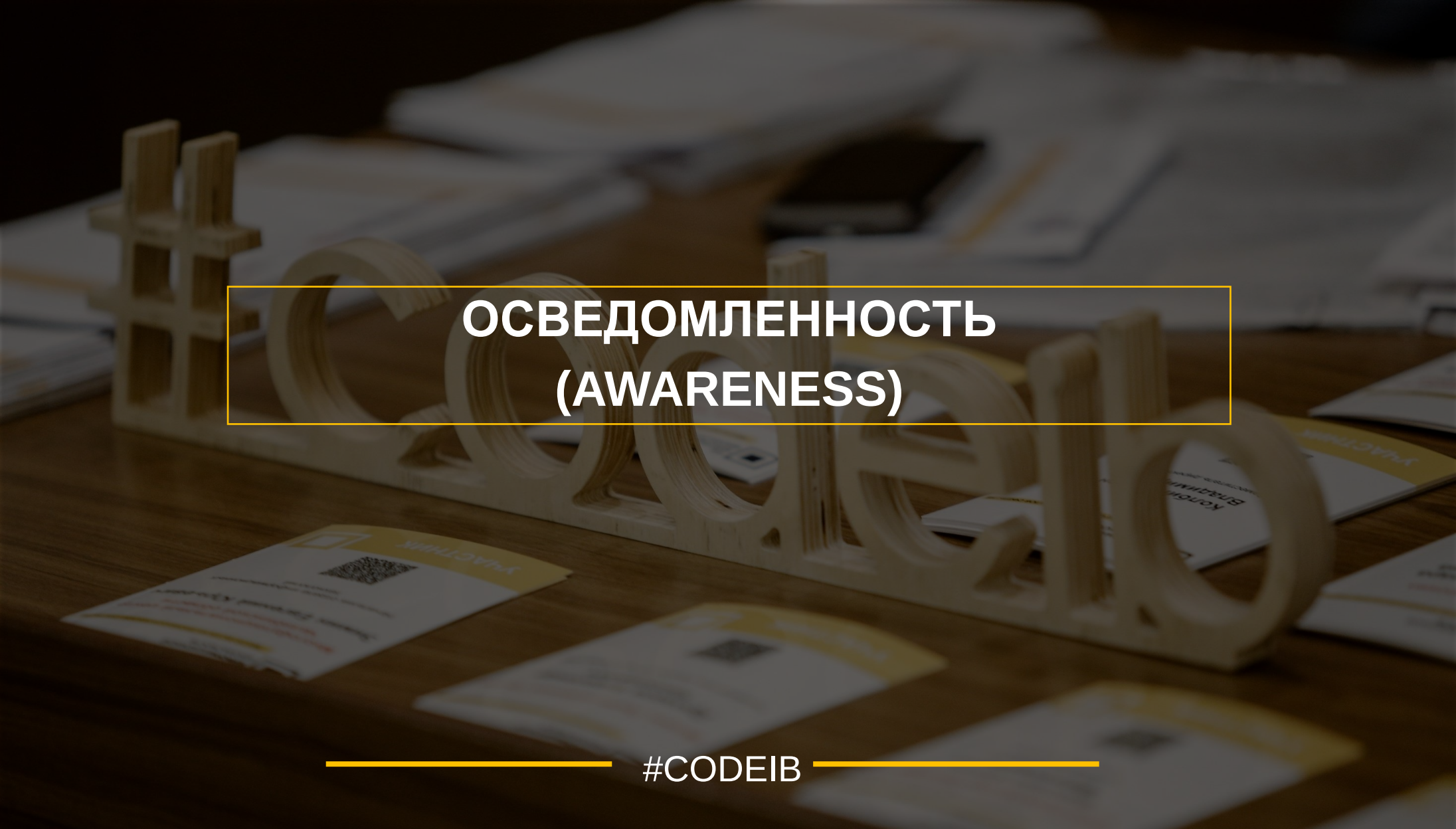

SECURITY CHAMPIONS
#CODEIB

КТО ТАКИЕ SECURITY CHAMPIONS

1. Роль, а не позиция. В первую очередь - «духовная».
2. Авторитетные «адвокаты», а не блокеры.
3. Зачем: ресурсов ИБ-команды еще долго будет не хватать.
4. «Бизнес-партнеры», с которыми команде комфортнее общаться.
5. Комбинируют с «обычной работой», ориентированы на общие цели отдела.

КАК ИСКАТЬ SECURITY CHAMPIONS

1. В идеале - инфлюенсеры, понявшие, что ИБ – часть культуры.
2. Может быть волонтерством, но лучше отдельные KPI.
3. Приветствуются разные техники поощрений, не только з/п.
4. Хороший старт для реально интересующихся ИБ, чтобы потом перейти в ИБ на full time.
5. Для карьеры - очень важная и более заметная роль, чем многие «обычные» роли.

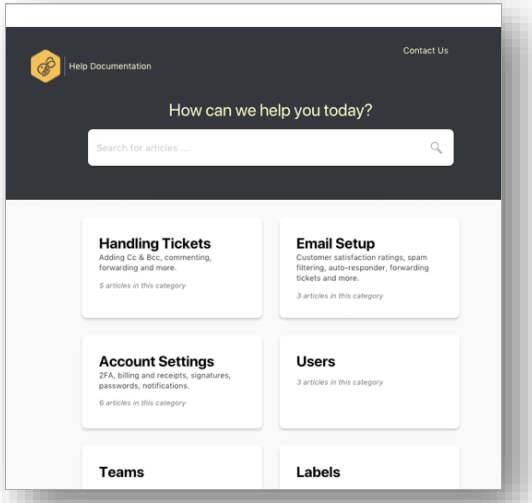


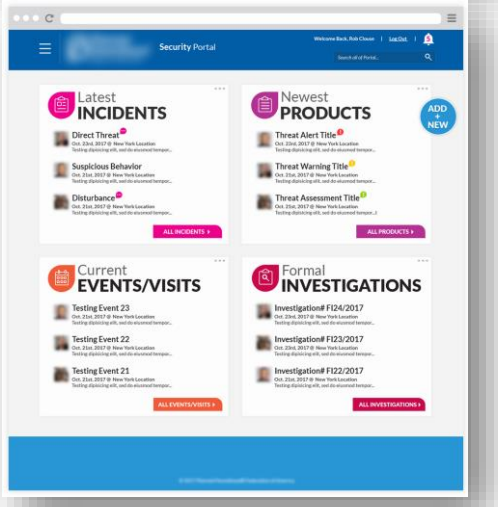
ОСВЕДОМЛЕННОСТЬ (AWARENESS)

#CODEIB

СОЗДАЙТЕ УДОБНУЮ БАЗУ ЗНАНИЙ ИБ

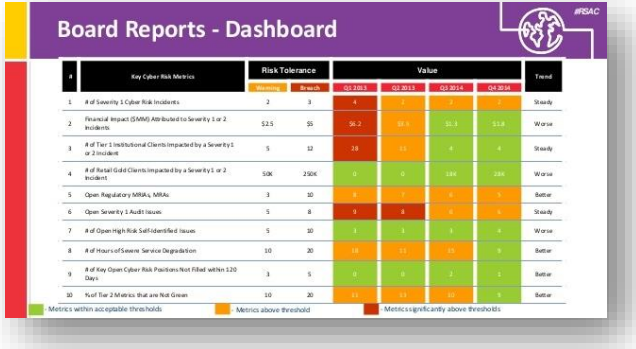
- ✓ Это может быть портал – единая точка входа для всех вопросов (Госуслуги ☺).
- ✓ Разбирайте “реальные жизненные ситуации” и разбейте текстовую политику на простые “Как” и блок-схемы. Например, Как обрабатывать уязвимости, Что сделать для быстрого согласования, Неудобно пользоваться – лайфхаки.
- ✓ Опыт и практика следования ИБ от «заказчиков» – бесценны, не стесняйтесь его рассказывать всем остальным.
- ✓ Организуйте ИБ-community, регулярно собирайтесь.

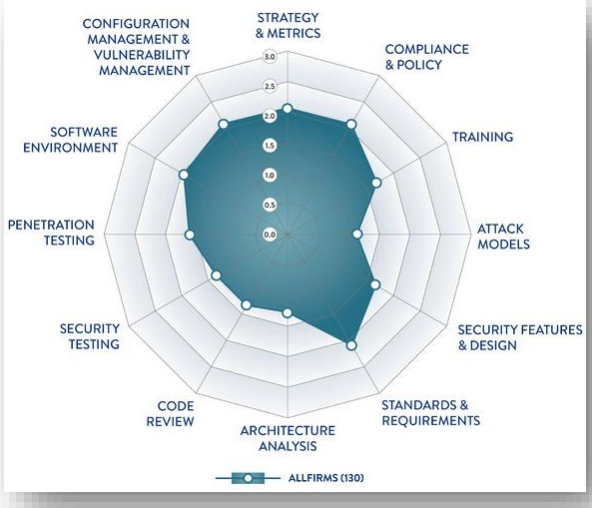


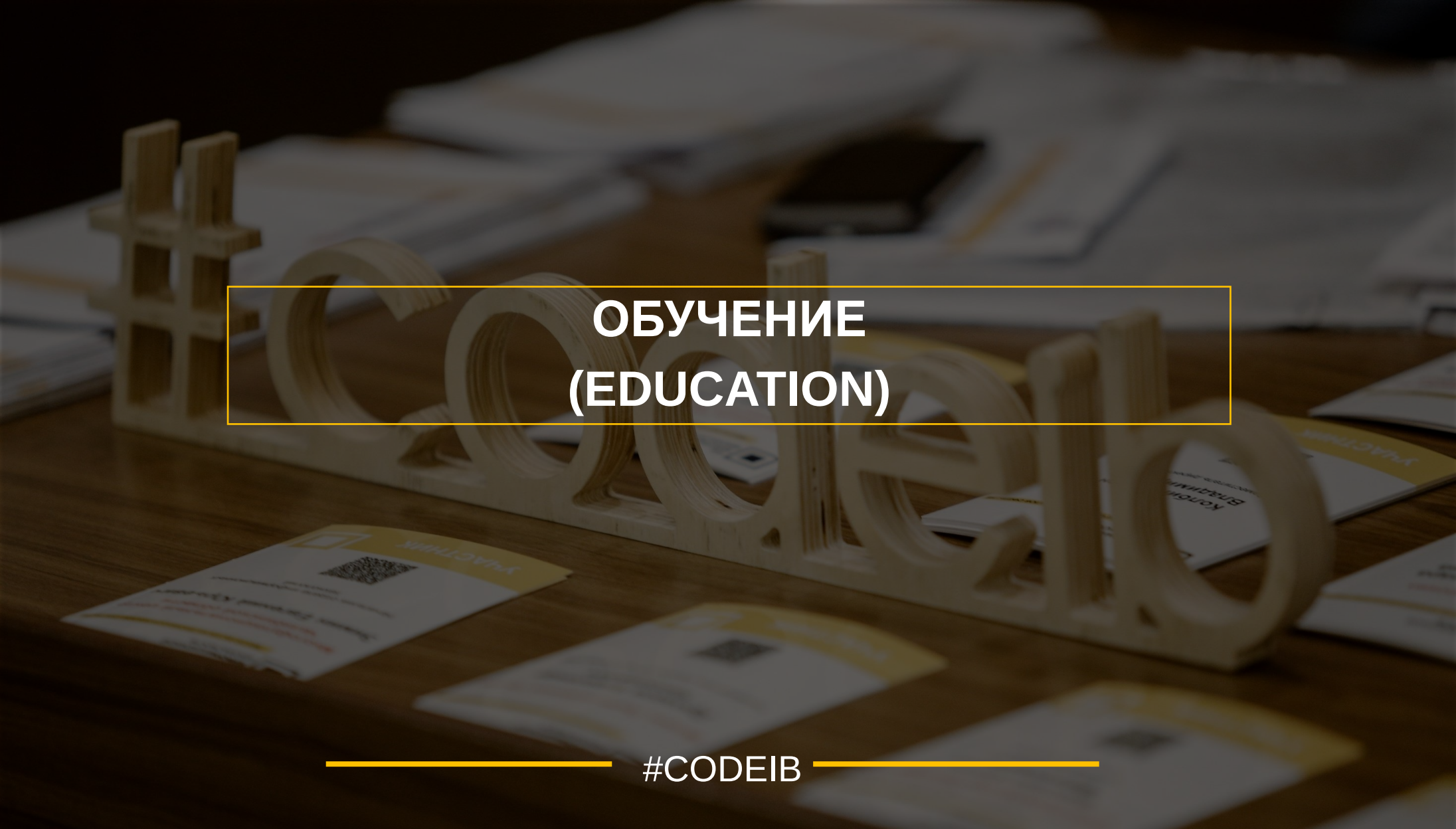


РАССКАЗЫВАЙТЕ ВСЕМ ПРО ИБ

- ✓ Запустите регулярную рассылку, публикацию. Рассказывайте об интересных новостях ИБ в каких-нибудь командах, новых инструментах ИБ, что у коллег/конкурентов
- ✓ Обязательные отчеты не только для CEO, но и для руководителей всех команд – важно отслеживать метрики и слушать обратную связь.
- ✓ Расставляйте приоритеты отдельных задач по уровню риска. Помогайте руководителям принимать решения, основанные на данных.
- ✓ Полагайтесь на Security Champions и людей внутри команд – это работает эффективнее.







ОБУЧЕНИЕ
(EDUCATION)

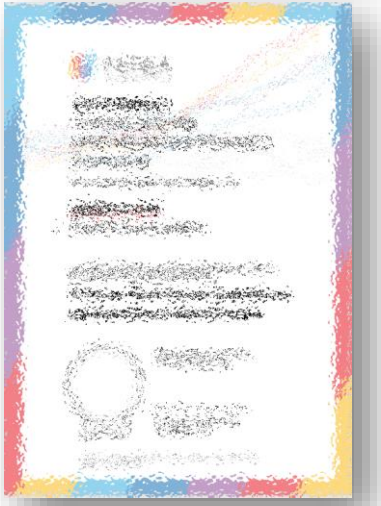
#CODEIB

ВЫ ДОЛЖНЫ «ПРОДАТЬ» ИБ КАЖДОМУ

- ✓ Безопасность - это не “еще одна галочка”, а скорее поведение и мышление, которые имеют смысл только при вовлечении каждого.
- ✓ Безопасность - это наш стандарт надежности и уверенности, что делает ее обязательной.
- ✓ Спросите инженера: мы здесь для того, чтобы выпустить лучший продукт, использующий лучшие практики, не так ли?
- ✓ Безопасность может быть инновационной (как и ИТ в целом) и должна быть нативна и автоматизирована – это хороший вызов.

БАЗОВЫЕ И ПРОСТЫЕ ЗНАНИЯ ПО ИБ

- ✓ Должен быть курс для всех (не более 30 мин.) и отдельные классы для каждой роли и нового сервиса.
- ✓ Используйте «записки на манжетах» сотрудников и распространяйте практики ИБ и примеры по всей компании.
- ✓ Не обязательно сходу тратиться на внешних тренеров. Возможно – для отдельных ролей.
- ✓ Не забудьте про правила общения про ИБ с внешними клиентами, партнерами, даже если подразделения на первый взгляд не вовлечены. Это важно для имиджа и доверия.



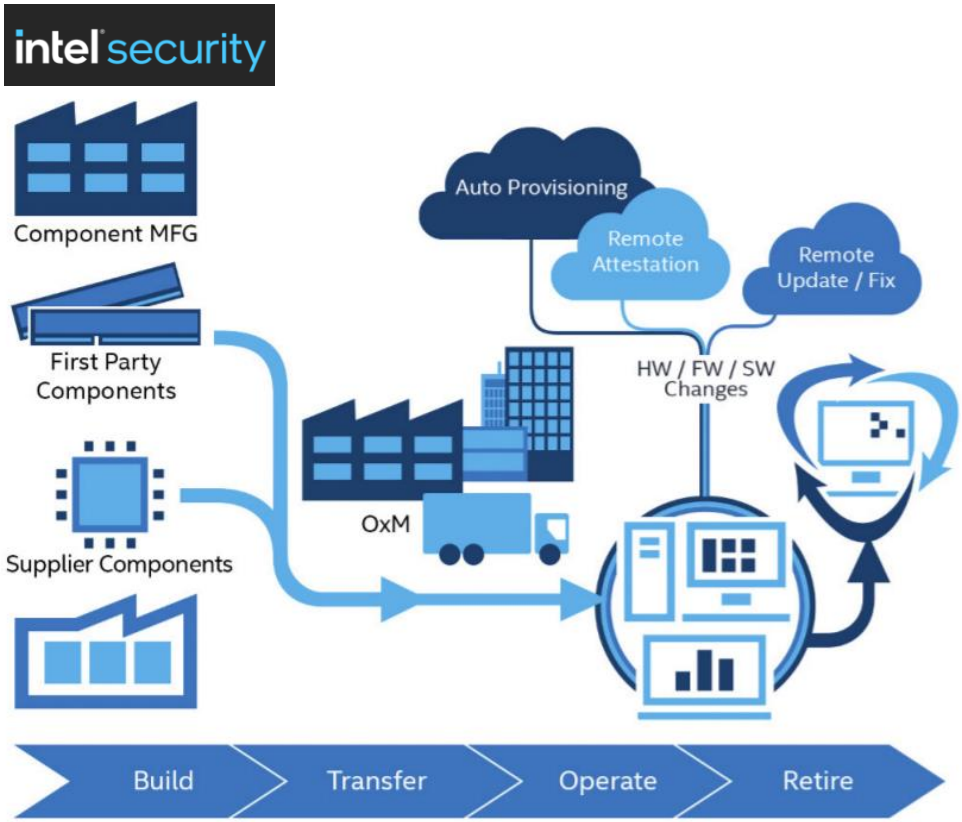
ПРИЗНАНИЕ (RECOGNITION)

#CODEIB

ИБ ДОЛЖНЫ СТАТЬ ЦЕННОСТЬЮ

- ✓ Об ИБ должны открыто говорить лидеры и руководители.
- ✓ Нужно рассказывать о карьерных возможностях для сотрудников, которые больше думают об ИБ.
- ✓ Все лучше, когда не скучно: игры, соревнования, пояса, внутренний bug bounty.
- ✓ Для ИБ должна быть отдельная Recognition программа, включенная в риторику руководителей всех уровней. Начните с простого: есть много интересного, кроме денег.

ПРИМЕР. PRODUCT SECURITY AT INTEL



Безопасность внедрена и автоматизируется на всем цикле производства, поставки и поддержки.

Когда безопасность – не просто выделенная «навешенная» функция:

1. Эффективное распределение ресурсов
2. Лучшее планирование и запуск продуктов
3. Контролируемость изменений
4. Открытость перед партнерами и рынком
5. Ускорение TTM и гибкость процессов

*Иллюстрация из отчета Intel Product Security Report, 2020

ПРИМЕР. ТРАНСФОРМАЦИЯ БЕЗОПАСНОСТИ SCHNEIDER

Вызовы

- IT&Security трансформация: от R&D до сервисов supply chain
- Интеграция IT & OT: новые сущности, данные, уязвимости
- Растущая экосистема партнеров и вендоров

> “I didn’t want to grow bigger teams because you give the impression that it will be fixed by someone else. Here, security is everyone’s responsibility. ”
>
> — *Christophe Blassiau*

Результаты

- ✓ Вместо жестко централизованной «тяжелой» команды создана «Практика кибербезопасности»
- ✓ Лидеры [«security & risk champions»] интегрированы в каждый регион/BU
- ✓ Они сфокусированы на специфичных рисках и ориентированы на бизнес-результаты BU
- ✓ Это принесло “the sense of control in digital space”

Schneider Electric

*www.csoonline.com

ЧЕК-ЛИСТ: ИНДИКАТОРЫ КУЛЬТУРНЫХ ИЗМЕНЕНИЙ В ИБ

1. ИБ практически не отвечает на базовые вопросы
2. ИБ тратит меньше времени на «докажи».
3. Рядовые сотрудники сами приносят проблемы ИБ.
4. Вам реально есть за что поощрять сотрудников каждый квартал.
5. Почти все изменения ИБ за последний год – не от службы ИБ.

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ

Connect me:

FACEBOOK.COM/R.O.ZHUKOV

ROZHUKOV.BLOGSPOT.COM

LINKEDIN.COM/IN/ROZHUKOV