RTM GROUP

Обучение и учет

Мало просит и много дает

Эксперт

RTM Group — ведущая консалтинговая компания в области информационной безопасности, судебной экспертизы и ИТ-права.

Евгений Царев

Управляющий RTM Group

Эксперт в области информационной безопасности и

ИТ-права (более 15 лет профессионального опыта)

RTM GROUP

О компании RTM Group

Работаем на всей территории России, Беларуси и Казахстана.

Головной офис: г. Москва.

Производственный департамент: г. Воронеж.

RTM Group ежегодно выполняет сотни проектов, делая свой вклад в стабильность и безопасность киберпространства, а также помогает провести анализ цифровых доказательств для судов и следственных органов.

250+

Проектов по построению комплексной системы ИБ

3

Компании в группе компаний

50+

видов аудитов ИБ, включая пентесты и анализ кода

100+

вариантов компьютерных экспертиз

4-й

каждый российский банк наш клиент

1-я

экспертно-юридическая компания в области ИТ в России

RTM GROUP

О чем пойдет речь

01 Что требует нормативка

02 Как есть

03 Как надо

04 Что делать

05 Дополнительные плюсы от реализации

Требования – обучение

21 приказ ФСТЭК
п.18.6

31 приказ ФСТЭК
п.16

239 приказ ФСТЭК
п.13.7

235 приказ ФСТЭК
п.15

282 приказ ФСБ
п.10

ГОСТ 57580.1
РЗИ.15-16

Реализация неправильная

Обучение с тренерами
• Много денег, много времени, не очень много результата

Как надо – обучение

LMS:

Назначение курсов

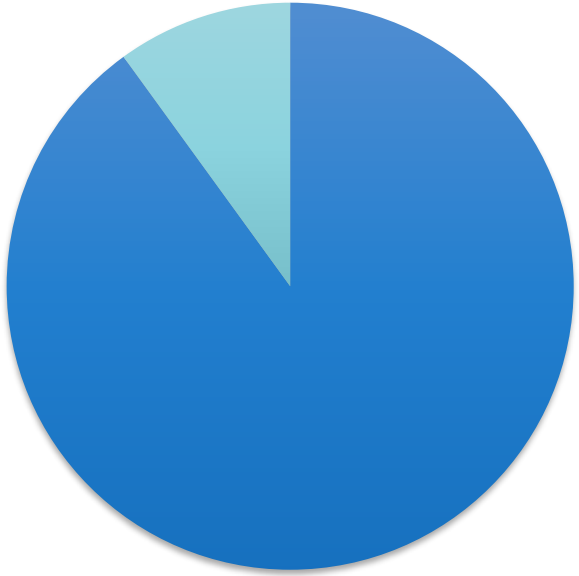
Контроль прохождения

Тестирование

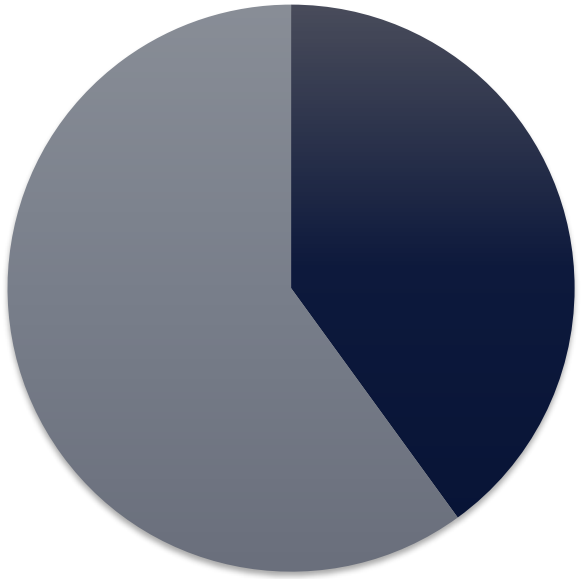
Выборочный контроль с привлечением тренера

Что дает?

Прерывание **90%** цепочек атак, с участием социнженерии



Без автообучения это только **40%**



Требования – учет инфраструктуры

21(аналогично 17) приказы ФСТЭК

АН3.4

239 приказ ФСТЭК

АУД.1

ГОСТ 57580.1

ИУ.1-3, РЗИ.1

Реализация неправильная

Инвентаризация в руках IT
• Не зря ИБ разделяют от IT по полномочиям

Как надо – учет активов

Учитываем:

Информационная система

Программное обеспечение

Оборудование

RTM GROUP

Учет текущего состояния

bush/shell

ITSM/SAM

Иные инструменты, но только автоматические (возможно, кроме ИС)

Что важно?

- Текущее состояние
- Прошедшее состояние
- Изменения за период

RTM GROUP

Что это дает?

1. Имеем представление об инфраструктуре
2. Получаем козырь против недобросовестных IT
3. Контролируем наличие средств защиты на всех хостах
4. Экономим на лицензиях
5. Выполняем требования регуляторов

Что это дает? Самое важное

Прерывание цепочек атак, связанных с:

Удалением средств защиты

Установкой вредоносного ПО

Установкой оборудования (в том числе VPN адаптеров)

RTM GROUP

Платформа MEDOED
для автоматизации ИБ
(UEBA, ITSM, SAM, LMS, VS, VM)

Телеграм-канал
ИТ. Право. Безопасность
Экспертный контент и срочные новости из мира ИБ

You Tube RTM Group
Подкаст «Утечка»
Технологии в современном мире, кибербезопасность, IT-право

Спасибо за внимание!

Готовы ответить на Ваши вопросы


+7 (495) 197-64-95


info@rtmtech.ru


https://rtmtech.ru


@RTM_Group


rtm.group


it_law_security