INFOWATCH ATTACK KILLER

ПРАКТИКА ЗАЩИТЫ ОНЛАЙН ГОСУСЛУГ В СОВРЕМЕННЫХ УСЛОВИЯХ

16 ИЮНЯ, ВЛАДИВОСТОК

rustem@khairetdinov.com

РУСТЭМ ХАЙРЕТДИНОВ
CEO ATTACK KILLER

INFOWATCH ATTACK KILLER

ЭВОЛЮЦИЯ ПРИЛОЖЕНИЙ

1990-е

ИНФОРМАЦИЯ

2000-е

ТРАНЗАКЦИИ

2010-е

ПОЛНЫЙ ЦИКЛ

INFOWATCH ATTACK KILLER

ЧТО ПРОИСХОДИТ С УГРОЗАМИ?

1. КИБЕРВОЙНА УЖЕ ЗДЕСЬ. МОЖНО СТАТЬ ЖЕРТВОЙ, НЕ ЯВЛЯЯСЬ ЦЕЛЬЮ
2. ДОСТУП К СИСТЕМАМ У МИЛЛИАРДА ПОЛЬЗОВАТЕЛЕЙ СЕТИ ИНТЕРНЕТ
3. СМЫКАЮТСЯ КИБЕРВОЙНЫ И ИНФОРМАЦИОННЫЕ ВОЙНЫ
4. СМЫКАЮТСЯ ОНЛАЙН И ОФФЛАЙН УГРОЗЫ
5. АТАКУЮЩИЕ АВТОМАТИЗИРУЮТСЯ И ИСПОЛЬЗУЮТ ЭЛЕМЕНТЫ ИИ

INFOWATCH ATTACK KILLER

ЧТО ПРОИСХОДИТ С ПРИЛОЖЕНИЯМИ?

Позавчера – **редкие** изменения в системе
Вчера – **еженедельные** изменения в системе
Сегодня – **ежедневные** изменения в системе
Завтра – **сотни** ежедневных изменений

Что это за изменения?

- Управление учётными записями пользователей
- Управление инфраструктурой
- Обновление стандартных систем
- Изменение функционала систем

INFOWATCH ATTACK KILLER

КТО ОТВЕТИТ ЗА ВСЁ?

- **За функционал** отвечает внутренний заказчик
- **За реализацию** функционала отвечают разработчики и внедренцы (свои или чужие)
- **За инфраструктуру** отвечает ИТ-департамент
- **За поддержку** клиентов - колл-центр
- **За безопасность** – служба информационной безопасности

INFOWATCH ATTACK KILLER

ИБ НЕ МЕНЯЕТСЯ

Осталась такой же, как в XX веке:

- Отдельные «навесные» системы с одной функциональностью

Старые добрые технологии

- «Сигнатуры» (известные угрозы)
- Анализ аномалий (известные и неизвестные угрозы)

INFOWATCH ATTACK KILLER

ПАССИВНАЯ БЕЗОПАСНОСТЬ

1 **МНОГО ЛОЖНЫХ СРАБАТЫВАНИЙ, НЕ БЛОКИРУЕМ, А ДЕЛЕГИРУЕМ ПРИНЯТИЕ РЕШЕНИЯ ЧЕЛОВЕКУ**

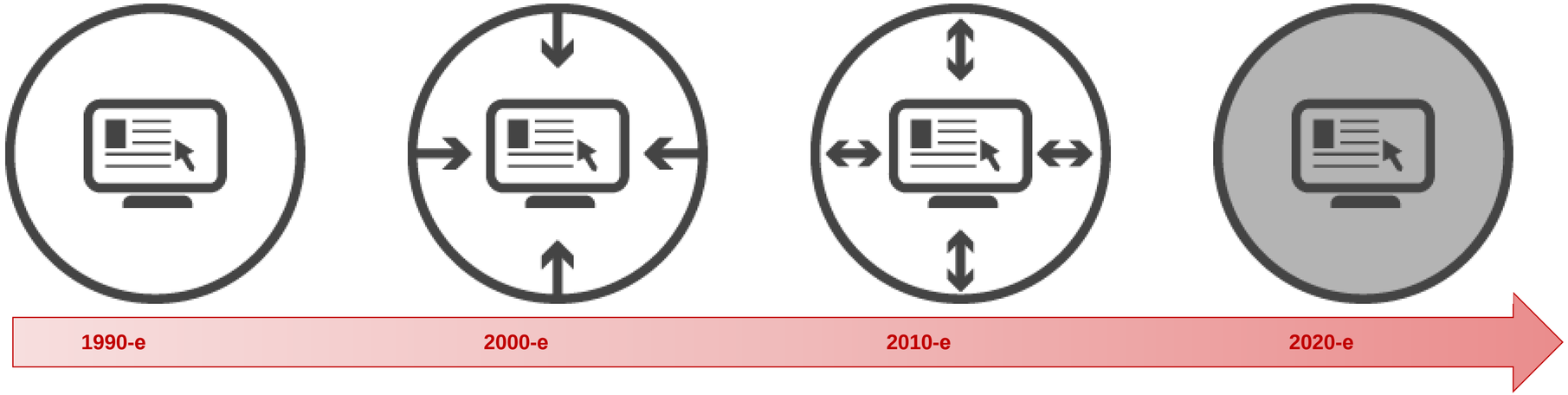
2 **НАЗЫВАЕМ ПАССИВНЫЙ РЕЖИМ КРАСИВО: «РЕЖИМ ФОРЕНЗИКИ», ПО ФАКТУ ВАЛИМ ВСЁ В SIEM**

3 **НАНИМАЕМ АНАЛИТИКОВ И СПЕЦИАЛИСТОВ ПО РАССЛЕДОВАНИЯМ. ВСЁ БОЛЬШЕ И БОЛЬШЕ**

ЭТО ТУПИК

INFOWATCH ATTACK KILLER

ЭВОЛЮЦИЯ ПРИНЦИПОВ ЗАЩИТЫ



1990-е	2000-е	2010-е	2020-е
объект сам по себе, защита сама по себе	защита изучает объект перед защитой	защита влияет на объект	интеграция защиты с объектом

INFOWATCH ATTACK KILLER

КУДА ИДЁМ?

ПОВЫШАЕМ УРОВЕНЬ ОТВЕТСТВЕННОСТИ
КОНЦЕНТРИРУЕМ ОТВЕТСТВЕННОСТЬ В ОДНИХ РУКАХ

Переходим от навесных решений к встроенным, начинаем на этапе проектирования и кодирования

Используем машинное обучение и раннее обнаружение атак

INFOWATCH ATTACK KILLER

БЕЗОПАСНАЯ РАЗРАБОТКА

INFOWATCH ATTACK KILLER

ИЗВЕЧНЫЙ ВОПРОС

INFOWATCH ATTACK KILLER

ВАРИАНТ 1

Дано:

- Свои разработчики в стиле Agile
- Традиционные ИБ
- Конфликт бизнеса, разработки, ИБ и ИТ
- Security-by-design

Решение:

- Переход к тестированию в процессе разработки
- Переход от кейсов к рискам
- Принятие окончательного решения Digital Officer

ВАРИАНТ 2

Дано:

- Разработчики когда какие – госторги решают
- Agile погоняет agil-ом: надо всё, вчера и безопасно
- ИБ нет – один человек на всё

Решение:

- Формулировка требований к ПО с постепенным ужесточением
- Приёмка вместе с тестированием
- «Покорми робота и ничего не трогай»

Спасибо за внимание!

Ваши вопросы?

rustem@khairetdinov.com

РУСТЭМ ХАЙРЕТДИНОВ

CEO ATTACK KILLER