kaspersky

Три препятствия на пути «Цифрового Века»

(без пандемии)

Эволюция человечества

Каменный век

3500000 лет

Бронзовый / железный век

5000 лет

Пластиковый век

70 лет

Цифровой век

?

Облако прогнозирует, как вы проведёте утро

Беспилотный автомобиль ждёт вас на выходе из дома

Маршрут оптимизируется облаком во время движения

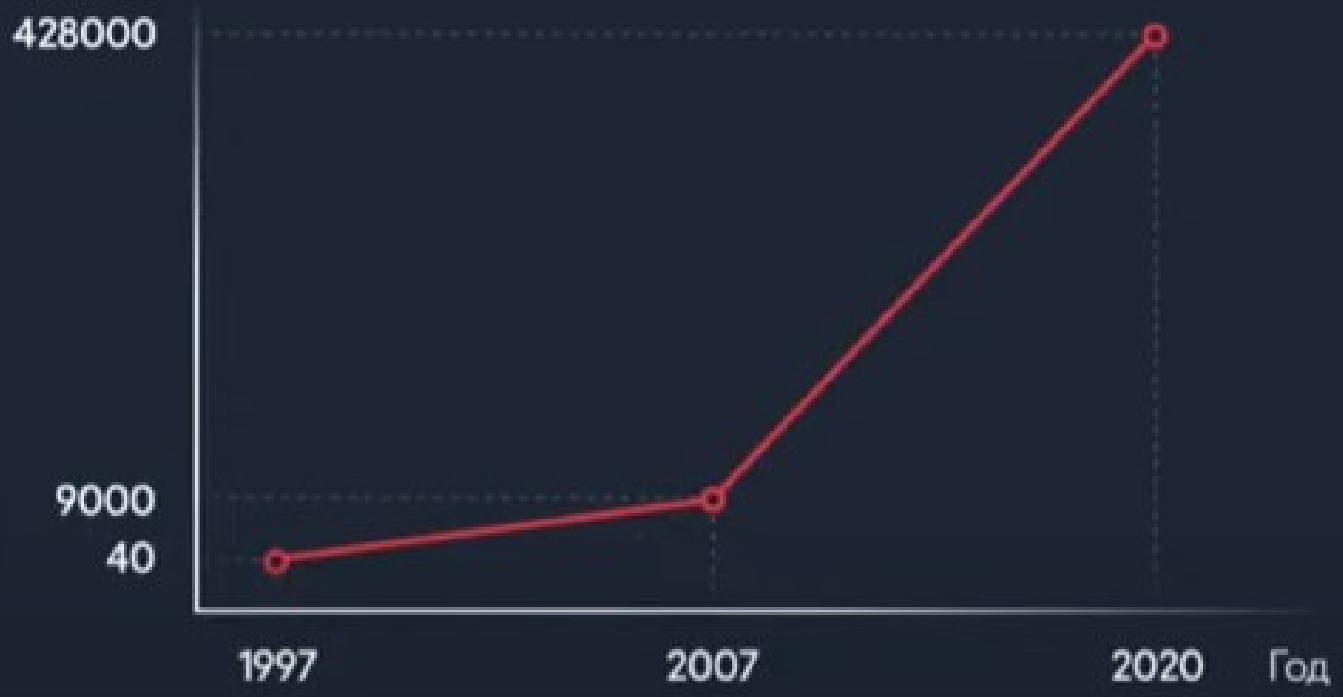
Три препятствия на пути к цифровому веку:

1. **Массовая киберпреступность**
2. **Целевые атаки (APT)**
3. **Атаки на промышленную и критическую инфраструктуру**

1 Киберпреступность

Массовая киберпреступность *

Новые уникальные образцы вредоносного ПО в день



Узнать больше: https://kas.pr/e2xb

Причины

- Люди проводят больше времени online
- Уровень защиты домашней и корпоративной сетей
- Увеличение числа кибератак, направленных на промышленную инфраструктуру (АСУ ТП).

По сравнению с прошлым годом, в 2020 мы обнаруживаем на 25% больше уникальных вредоносных файлов в день.

*данные KSN, июль 2020

Решение:

99.999% автоматизации

- KSN
- Поисковые роботы
- Антивирусные компании
- Партнёры
- Клиенты, волонтёры и т.д.

Дата-центры в

- Москва, Россия
- Цюрих, Швейцария

- KSN (Облако)
- Песочница
- Система похожести
- Машинное обучение
- Тесты и доставка обновлений

2 Таргетированные атаки (APT)

Профессиональные целевые атаки

Масштаб

Более 200 таргетированных вредоносных кампаний

Атрибуция

Язык, часовые пояса, ошибки, утечки, код

Решения

Kaspersky Anti Targeted Attack

Kaspersky Endpoint Detection And Response

Kaspersky Threat Intelligence Portal

Узнать больше: https://kas.pr/3c7k

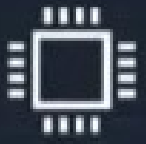
Решение:

Threat intelligence portal

Экспертное расследование угроз

Портал для анализа угроз

- **Источники данных:** KSN, бот-фермы, APT расследования, OSINT, ханипоты, спам ловушки...
- **Инструменты для умного поиска:** Research Sandbox, Threat Attribution Engine, Similarity
- **Экспертиза GReAT**



Реальные данные об угрозах

- Обнаружение угроз
- Валидация и приоритизация
- Автоматизированные расследования и реагирование (CVE, IoC, IoA)
- Активный поиск угроз
- Кастомизированные отчеты

Узнать больше: https://kas.pr/thi

3 Индустриальные атаки

Атаки на промышленную и критическую инфраструктуру, АСУ ТП и интернет вещей

Решения

Kaspersky Industrial CyberSecurity

KasperskyOS®

Решение:

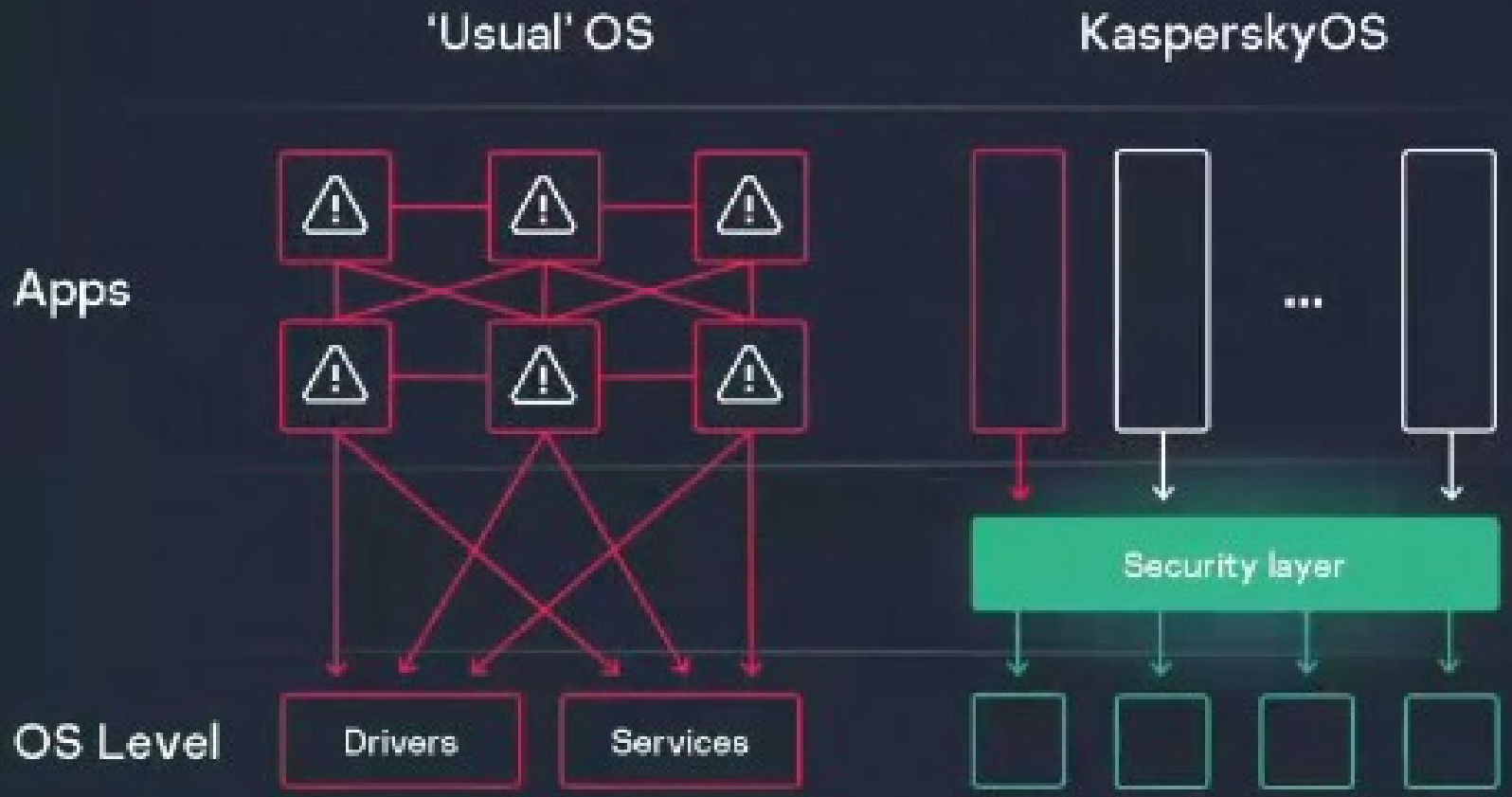
Kaspersky Industrial Cybersecurity

- Инвентаризация АСУ ТП/DCS сети
- Песочница для обнаружения индустриальных угроз
- Обнаружение аномалий в сетевом трафике
- Проверка целостности ПЛК

Узнать больше: https://kas.pr/vgj1

Solution for industrial attacks

Immunity with KasperskyOS



Secure-by-design system

- Microkernel architecture
- Security layer isolating all modules
- Trusted behavior

Learn more: https://kas.pr/y484

+ Что необходимо для защиты

1. Формат международного сотрудничества по трансграничному расследованию киберпреступлений. (киберугрозы – информационные угрозы)
2. Противодействие киберпреступности, цифровые доказательства, готовность судов и следствия
3. Усиление ответственности за преступления против критической инфраструктуры
4. Ответственная фильтрация запрещенного трафика, скорость реакции на нарушения
5. Обучение цифровой гигиене и основам безопасности в сети Интернет (включение в школьную программу)

kaspersky

Спасибо!

Andrey.Yarnikh@kaspersky.com

Энергоменеджмент зданий
Проект «Умный город», г. Оренбург

*β (*Beta-версия*) – *продукт предназначен только для некоммерческого тестирования и пилотирования*

kaspersky