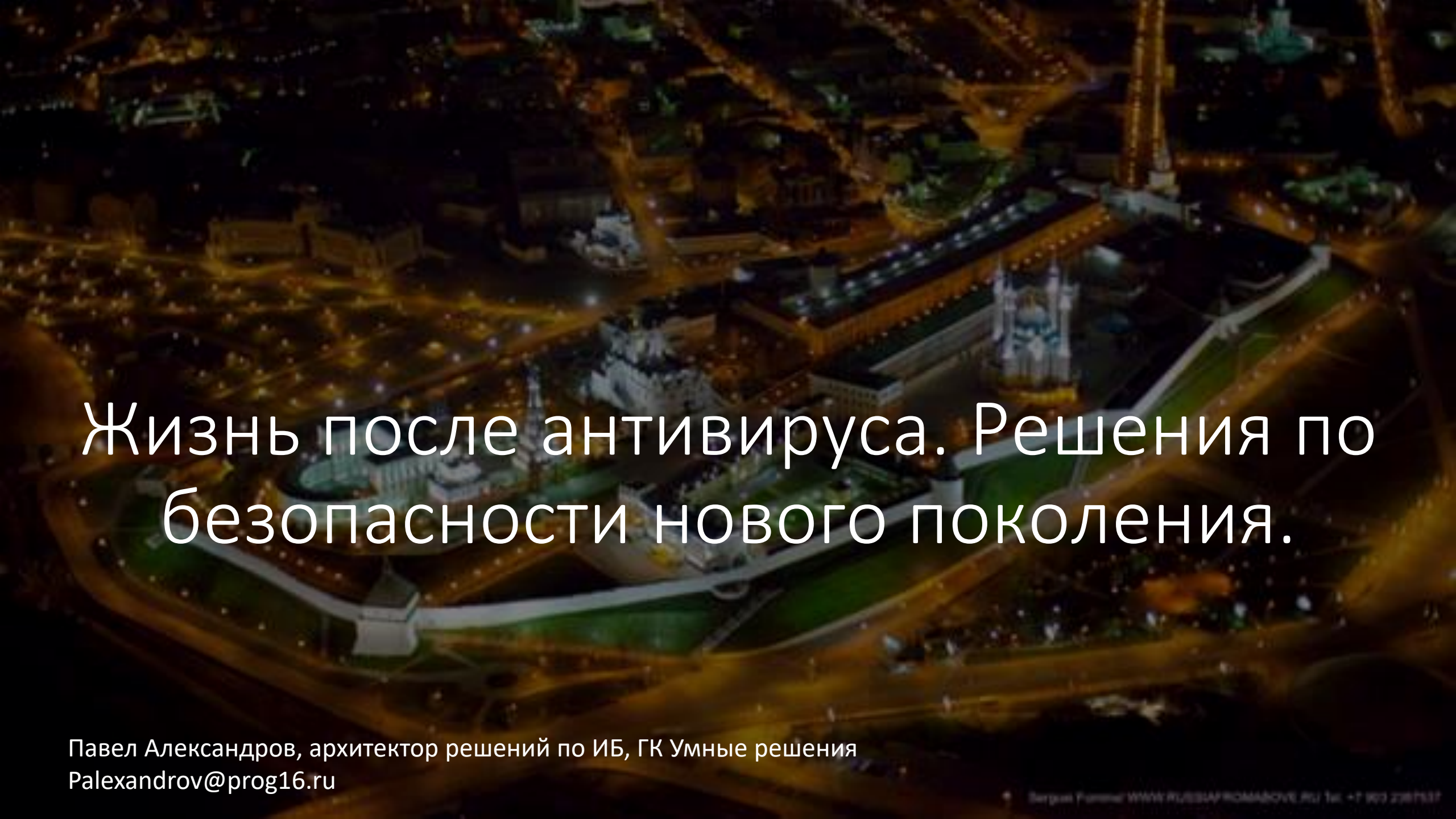
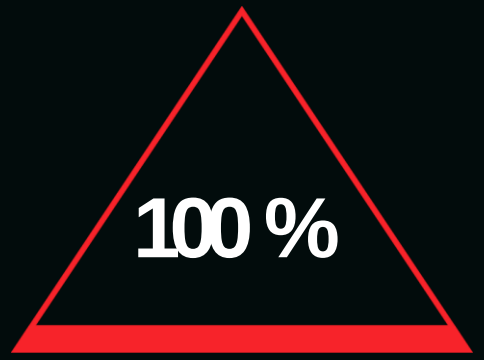


Жизнь после антивируса. Решения по безопасности нового поколения.

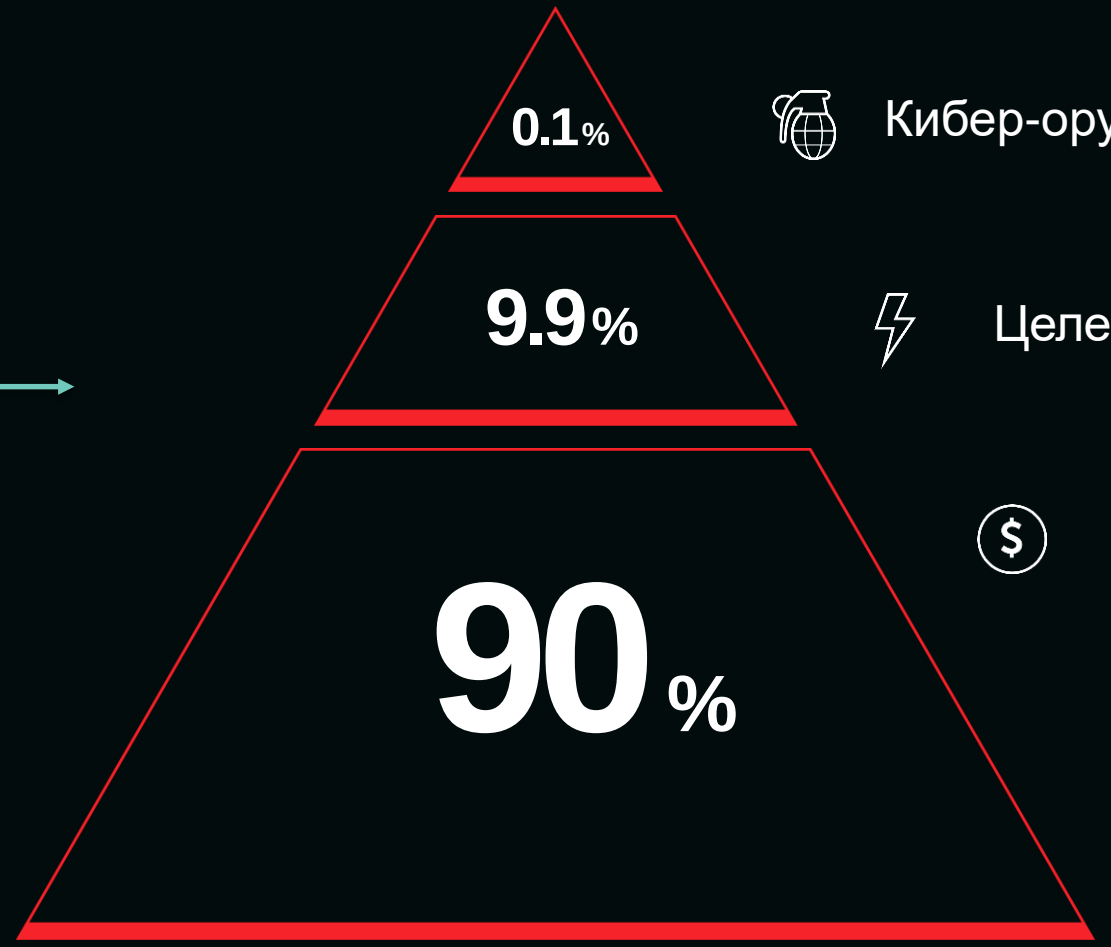
Павел Александров, архитектор решений по ИБ, ГК Умные решения
Palexandrov@prog16.ru

«Таргетированные атаки» vs «Типовое вредоносное ПО»

за 20 лет
1 млн. экземпляров



В 2000-е годы:
10-100 зловредов в месяц



Кибер-оружие

Целевые атаки

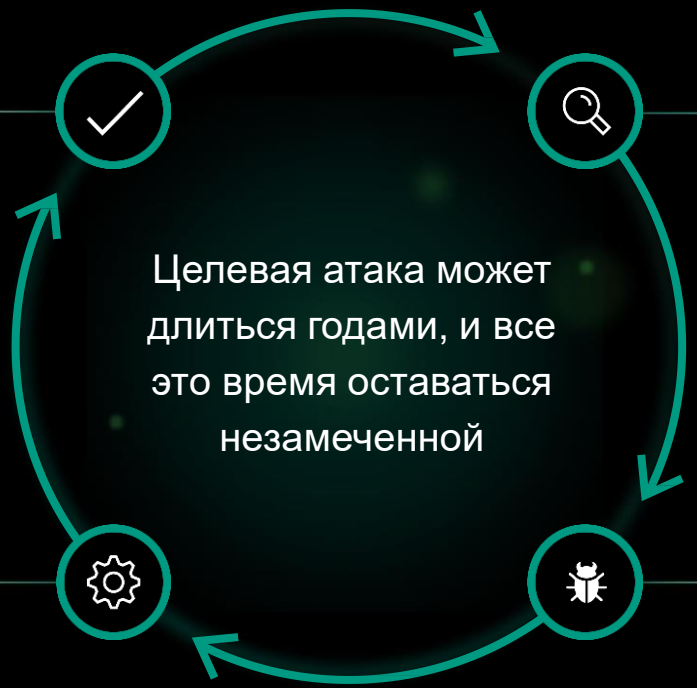
Типовое
вредоносное ПО

Сегодня:
330 000 новых угроз в день
(за 1 неделю больше 2-х млн)

KASPERSKY lab

ЗАЩИТА ОТ ЦЕЛЕВЫХ АТАК

ЦЕЛЕВАЯ АТАКА – ЭТО ПОСТОЯННЫЙ ПРОЦЕСС



ПОДГОТОВКА

— Изучение жертвы
— Подготовка стратегии
— Выбор инструментов

ЗАРАЖЕНИЕ

— Использование уязвимостей
— Проникновение в периметр

РАСПРОСТРАНЕНИЕ

— Получение учетных данных
— Повышение уровня прав
— Establish links
— Move laterally
— Контроль

ИСПОЛНЕНИЕ И УСТРАНЕНИЕ СЛЕДОВ

— Долгое бездействие
— Извлечение данных
— Сокрытие улик и выход

АДАПТИВНАЯ СТРАТЕГИЯ ЗАЩИТЫ ОТ ЦЕЛЕВЫХ АТАК

ПРОГНОЗИРОВАНИЕ

— Оценка уровня защищенности
— Реализация контрмер
— Создание выделенного SOC

РЕАГИРОВАНИЕ

— Реагирование на инциденты
— Действия по снижению возможного ущерба
— Анализ вредоносного ПО

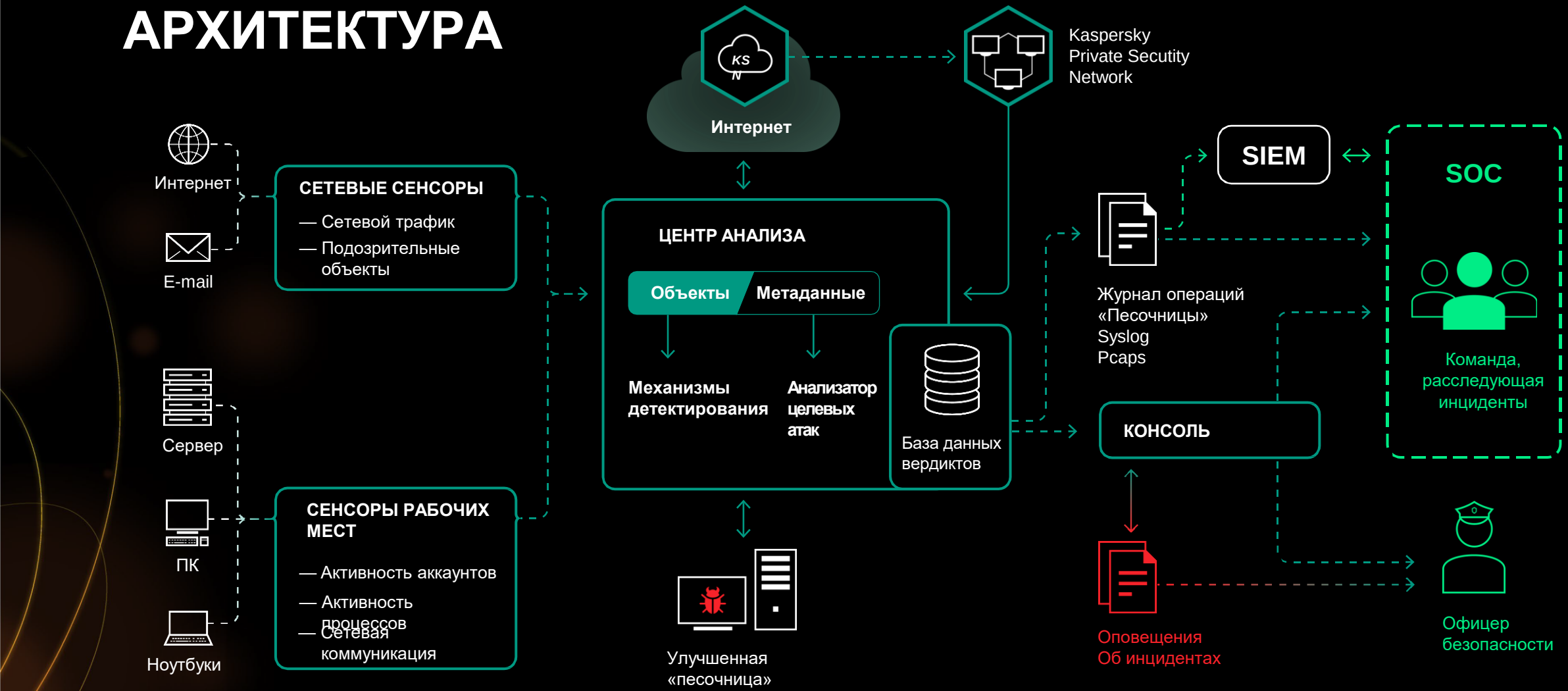
ПРЕДОТВРАЩЕНИЕ

— Уменьшение рисков
— Повышение осведомленности об угрозах
— Применение правильного подхода

ОБНАРУЖЕНИЕ

— Обнаружение инцидента
— Отслеживание источника атаки
— Понимание типа и характера угрозы

АРХИТЕКТУРА



Векторы атаки | Получение данных | Анализ данных | Приоритизация вердиктов | Реагирование

ТЕСТИРОВАНИЕ И ОБОРУДОВАНИЕ

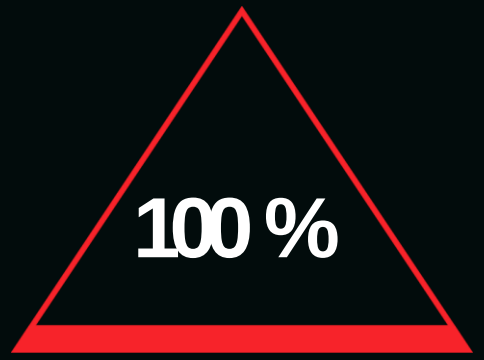
Опросный лист Kaspersky Anti Targeted Attack Platform - Сохранено в: этот компьютер

☐·Да·····☐·Нет·····¶

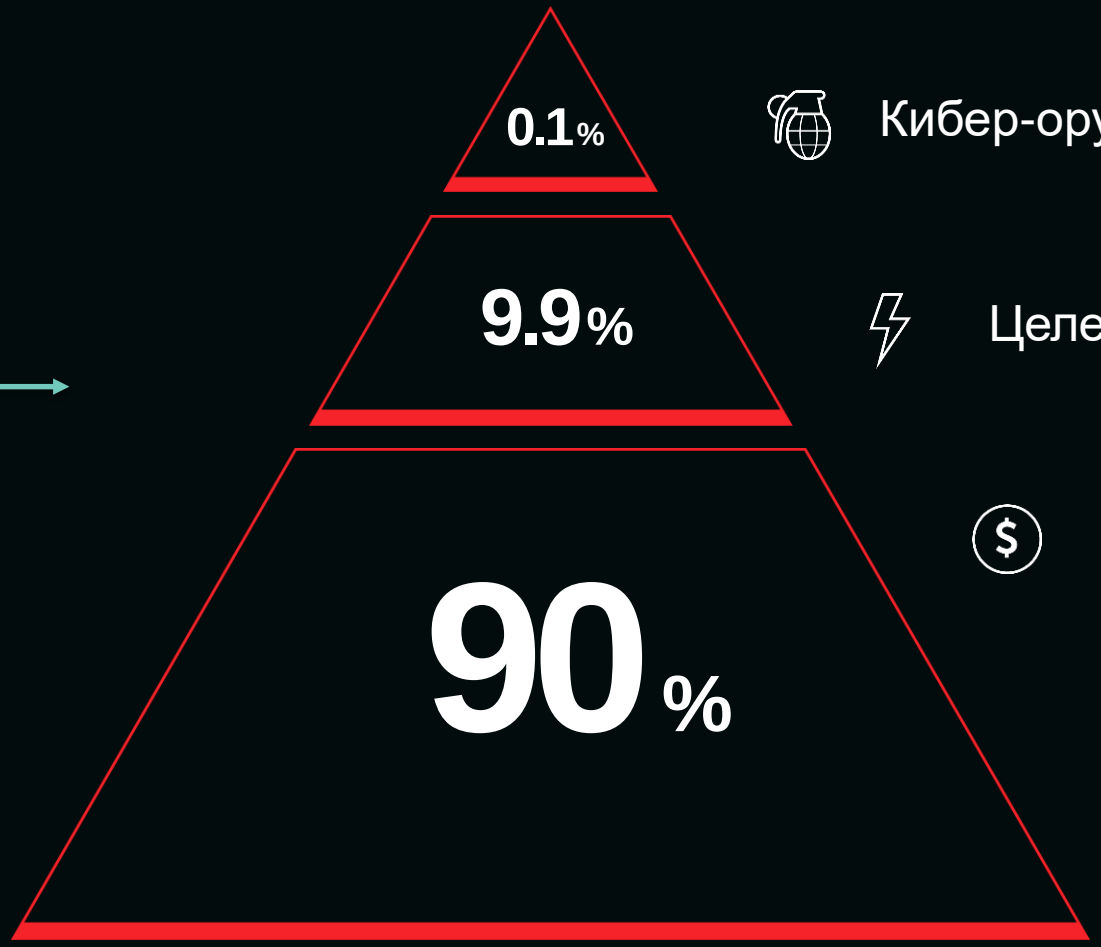
Если·«Да»,·приложите·её·к·опроснику.¶

«Таргетированные атаки» vs «Типовое вредоносное ПО»

за 20 лет
1 млн. экземпляров



В 2000-е годы:
10-100 зловредов в месяц



Кибер-оружие

Целевые атаки

Типовое
вредоносное ПО

Сегодня:
330 000 новых угроз в день
(за 1 неделю больше 2-х млн)

KASPERSKY lab

ЗАЩИТА КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Чем знаменателен 2017 год:

Industroyer/CrashOverride, который называют четверным в истории, созданным специально для промышленных систем (после Stuxnet, BlackEnergy и Havex).

Июнь 2017

digitalsubstation.com/blog/2017/06/28/energetiki-o-win32-industroyer-panikovat-ne-stoit/

A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.

March 15, 2018

https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

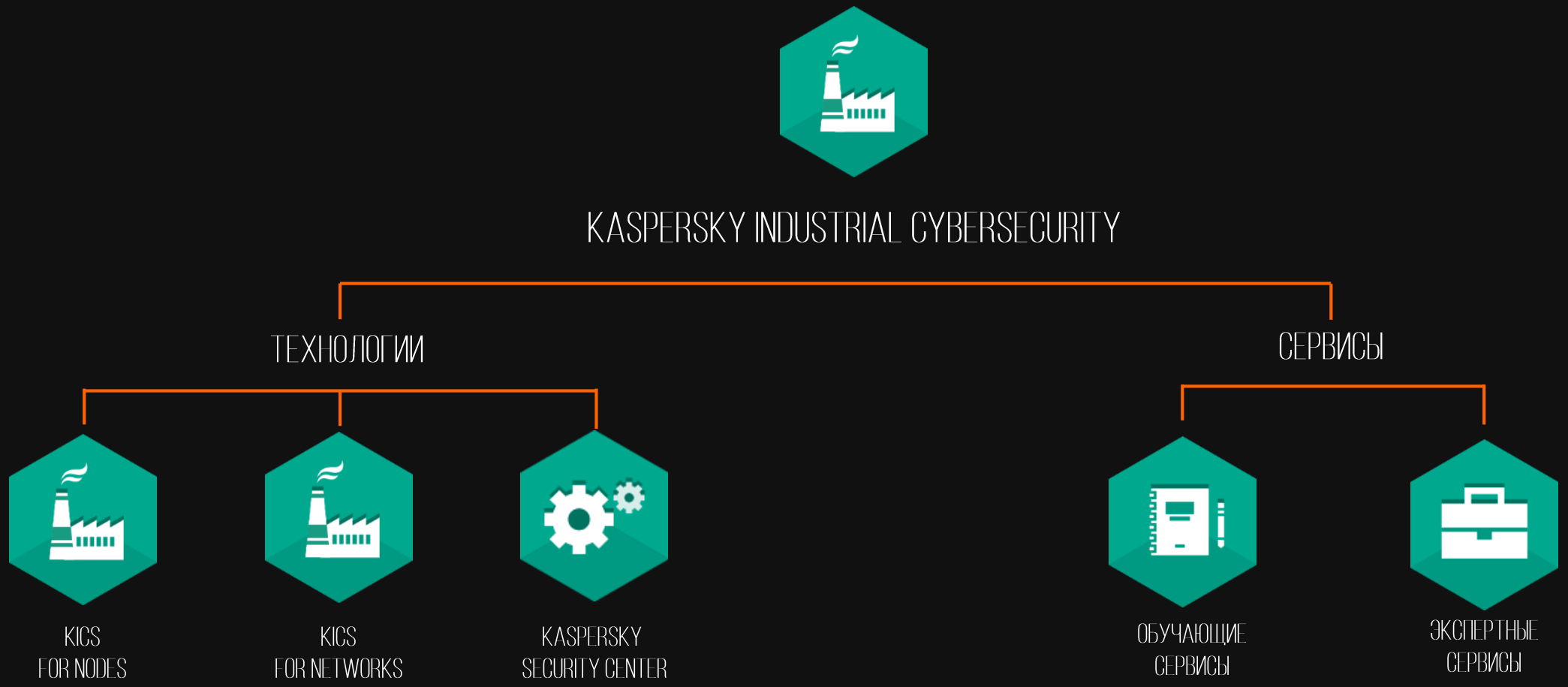
В ЧЕМ ПРИЧИНА «АКТУАЛЬНОСТИ» КИБЕРБЕЗОПАСНОСТИ СИСТЕМ УПРАВЛЕНИЯ ТЕХОЛОГИЧЕСКИМИ ПРОЦЕССАМИ?

1. АСУТП интегрируются с корпоративными ИС;
2. Компоненты АСУТП уязвимы;
3. Последствия киберинцидентов уже не информационные, а физические.

КАК ВРЕДОНОСНОЕ ПО ПРОНИКАЕТ В ИНДУСТРИАЛЬНЫЕ СЕТИ?

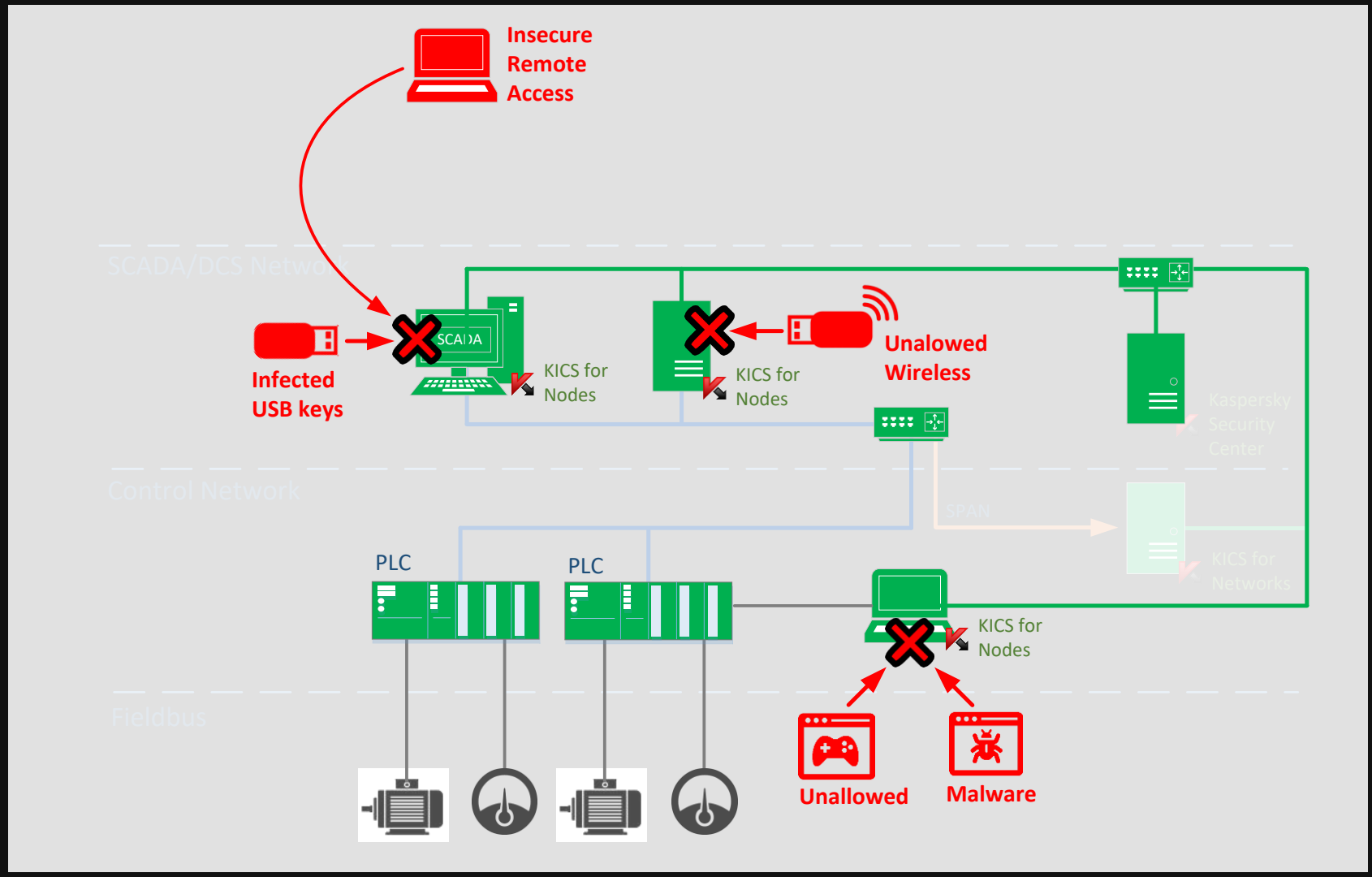
- СТЫКИ ИНДУСТРИАЛЬНЫХ СЕТЕЙ И ЛВС ПРЕДПРИЯТИЯ:
  - Передача данных в систему управления и планирования производства;
  - Маршрутизаторы и сетеобразующее оборудование распределенной сети передачи данных – общее как для корпоративных сервисов, так и для АСУ ТП;
- НЕКОНТРОЛИРУЕМОЕ ИСПОЛЬЗОВАНИЕ СМЕННЫХ НОСИТЕЛЕЙ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПЕРСОНАЛОМ;
- ПОДКЛЮЧЕНИЕ 3 ЛИЦ (ПОДРЯДНЫХ ОРГАНИЗАЦИЙ) К ИНДУСТРИАЛЬНОЙ СЕТИ.

Структура решения
KASPERSKY INDUSTRIAL CYBERSECURITY (KICS)



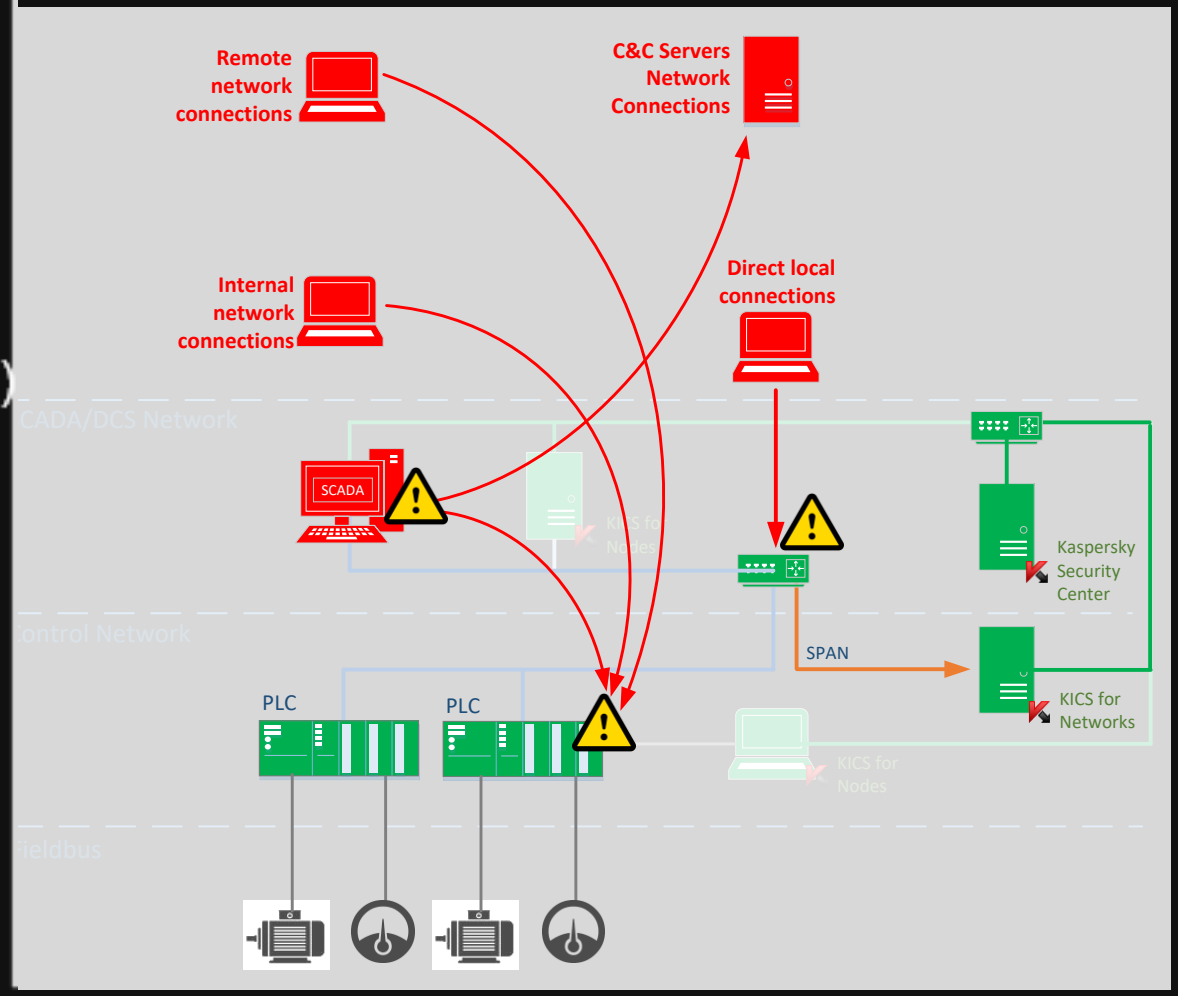
KICS for Nodes: Функционал

- Контроль запуска приложений
- Контроль устройств
- Антивирус
- Пассивный анализ логов ОС
- Защита от шифровальщиков
- Контроль целостности PLC
- Контроль целостности областей диска
- Firewall Менеджмент



KICS for Networks: Сценарии использования

3. Обнаружение критических команд к ПЛК (DPI)
   1. Чтение/запись программы/проекта ПЛК
   2. Попытки аутентификации
   3. Start/stop команды
   4. Чтение/запись конфигураций и прочее…
4. Контроль параметров технологического процесса
   1. Границы конкретных параметров (Min < X < Max)
   2. Связи между параметрами и значениями (if..and/or..if..then)
   3. Попытки фрода
   4. Ошибки конфигурации
5. Сбор и хранение информации для расследования инцидентов
   1. Security logs
   2. Technological events
   3. Raw network dump



Что делать Субъектам КИИ в рамках реализации № 187-ФЗ в период 2018-2021:

1 инвентаризировать объекты КИИ (ИС, ИТС, АСУ субъектов КИИ);

1.1 установить рабочие контакты с ФОИВ;

2 запланировать работы по категорированию и обеспечению информационной безопасности объектов КИИ;

(Постановление Правительства РФ от 8 февраля 2018 г. № 127 "Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений)

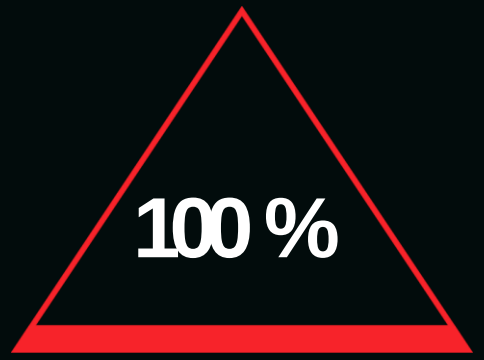
П Е Р Е Ч Е Н Ь показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значения:

- охват количества людей, которым возможно причинение ущерба;
- размер территории на которой нанесен ущерб;
- размер прямого или косвенного ущерба в денежном выражении;
- масштаб и категории нарушения деятельности Государственных органов;
- нарушение условий заключенного международного договора России;
- снижение показателей государственного оборонного заказа.

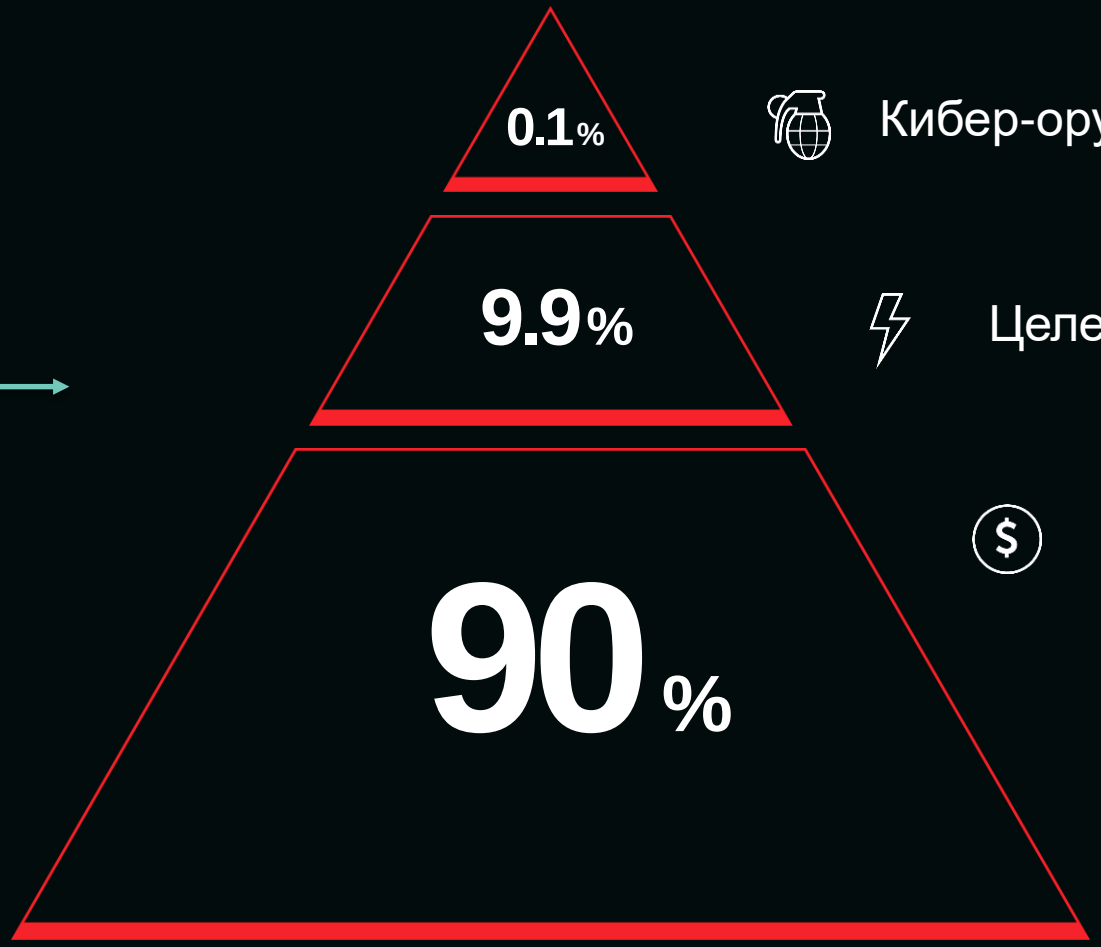
Всего 3 категории….)

«Таргетированные атаки» vs «Типовое вредоносное ПО»

за 20 лет
1 млн. экземпляров



В 2000-е годы:
10-100 зловредов в месяц



Кибер-оружие

Целевые атаки

Типовое
вредоносное ПО

Сегодня:
330 000 новых угроз в день
(за 1 неделю больше 2-х млн)

KASPERSKY lab

УЩЕРБ ОТ ОШИБОК СОТРУДНИКОВ

$861,000

для крупных компаний

прямые расходы на восстановление от киберинцидента *

$86,500

для компаний среднего и малого бизнеса

прямые расходы на восстановление от киберинцидента *

до $400

на сотрудника в год

средний ущерб от фишинговых атак **

ОСНОВНЫЕ ПРИЧИНЫ ОШИБОК СОТРУДНИКОВ

42%	Несоблюдение пользователями ИБ-политик и процедур
42%	Общая беспечность/ халатность
31%	Неосведомленность о новых типах угроз
29%	Недостаточное владение программами и навыками безопасного просмотра вебсайтов
26%	Несоблюдение ИБ-политик и процедур IT-специалистами

ПОЧЕМУ НЕЭФФЕКТИВНЫ СУЩЕСТВУЮЩИЕ ТРЕНИНГИ?

УРОВЕНЬ СОТРУДНИКА

- Занимают много времени
- Мешает исполнять основную работу
- Этим должны заниматься IT
- Кому я интересен?
- С сотрудниками ИБ сложно общаться
- Атаки же редко бывают
- Слишком сложные
- Слишком поверхностные
- Слишком технические
- Сложные и абстрактные
- Быстро забываются
- Оторваны от бизнеса
- С хакерами все равно ничего не сделаешь

- Скучно!

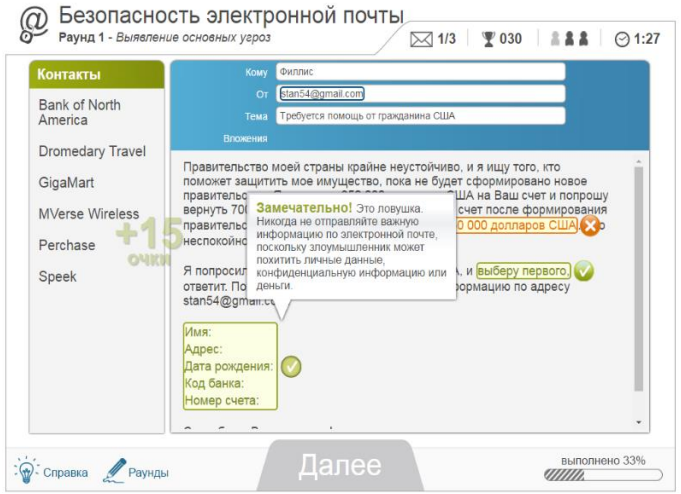
УРОВЕНЬ КОМПАНИИ

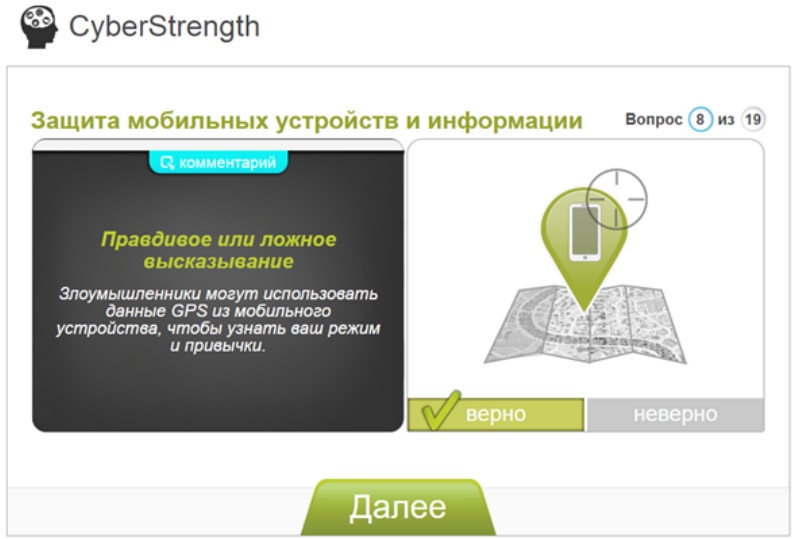
- Таким обучением сложно управлять
- Всех все равно не обучишь
- Это не приоритет
- Нет поддержки сверху
- Плохо поддаются оценке
- Тренинги проводятся формально, многие списывают
- Результаты обучения не проанализировать
- Дорого
- Быстро устаревают
- Начальник требует не тратить время на то, что не приносит прямого результата
- Никак не связаны с реальной работой
- Это разовое обучение (хотя даже им управлять сложно)

- Неэффективно!

ПЛАТФОРМА ОБУЧЕНИЯ НАВЫКАМ – МОДУЛЬНЫЙ ИНТЕРАКТИВНЫЙ ТРЕНИНГ

Для всех сотрудников





العَرَبِية
čeština
Deutsch
English(UK)
English(US)
español
Español
français
français
עִבְרִית
Magyar
Íslenska
italiano
日本語
한국어
Nederlands
Norsk
polski
português
русский
Slovák
svenska
ภาษาไทย
Türkçe
tiếng Việt
简体中文
繁體中文

36 интерактивных модулей

27 языков

Поставка как SaaS-решение или в формате SCORM (on-premise)

Расширенная аналитика

ПЛАТФОРМА ОБУЧЕНИЯ НАВЫКАМ – МОДУЛЬНЫЙ ИНТЕРАКТИВНЫЙ ТРЕНИНГ

Для всех сотрудников

Обучающие модули

Короткие и забавные

Упражнения с немедленным подкреплением

20 модулей на все аспекты ИБ (число модулей растет)

Auto-enrollment: автоматически назначаются после плохого прохождения соответствующего задания

Симулированные фишинговые атаки

3 типа атак разной сложности. Основаны на реальных случаях фишинга

Обучающая страница сразу после совершения пользователем опасных действий

Возможна кастомизация шаблонов

Оценка знаний (assessment)

Позволяет настраивать тематику, продолжительность и сложность оценки

Дает возможность создавать собственные вопросы

Исключает вероятность «списывания» за счет рандомизации вопросов

Аналитика и отчетность

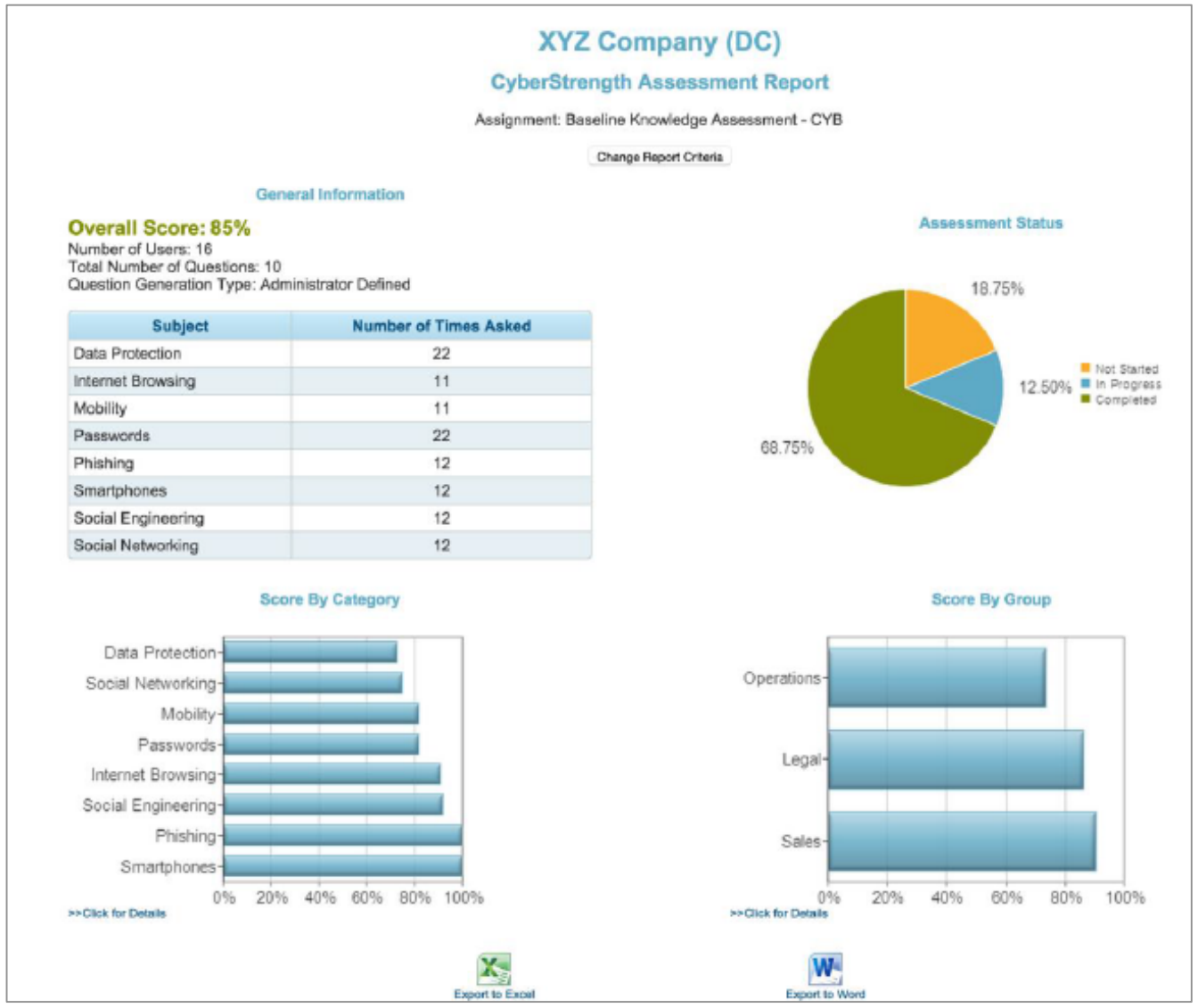
Позволяет отслеживать уровень обучающихся и динамику изменений

Анализ как в целом по организации, так и по подразделениям и на индивидуальном уровне

ПЛАТФОРМА ОБУЧЕНИЯ НАВЫКАМ – МОДУЛЬНЫЙ ИНТЕРАКТИВНЫЙ ТРЕНИНГ

Защита данных	Защита электронной почты	Безопасность мобильных приложений	Безопасность мобильных устройств	Защита персональных данных
Пароли	Физическая безопасность	Охраняемая медицинская информация	Защита от программ-вымогателей	Безопасность платежей в интернете (PCI DSS)
Безопасное использование социальных сетей	Безопасное чтение интернета	Основы информационной безопасности	Основы информа-ционной безопасности для руководителей	Безопасность при работе за пределами офиса
Социальная инженерия	URL Training	Безопасность USB-устройств	Anti-Phishing Phil	Anti-Phishing Phyllis

ОТЧЕТНОСТЬ И АНАЛИТИКА



XYZ Company (DC)

CyberStrength Assessment Report

Assignment: Baseline Knowledge Assessment - CYB

Change Report Criteria

General Information

Overall Score: 85%

Number of Users: 16
Total Number of Questions: 10
Question Generation Type: Administrator Defined

Subject	Number of Times Asked
Data Protection	22
Internet Browsing	11
Mobility	11
Passwords	22
Phishing	12
Smartphones	12
Social Engineering	12
Social Networking	12

Assessment Status

Score By Category

>>Click for Details

Score By Group

>>Click for Details

Export to Excel

Export to Word

Статистика по прохождению

Статистика по модулям

Статистика по пользователям/ группам пользователей

Области наибольшей уязвимости

Соответствие политикам, и пр.

Для симулированных атак:

Отчет по каждой кампании

По группе пользователей

По типу устройства

Повторные провалы (по какому типу атаки)

Годовой тренд

ЭФФЕКТ

- 93% – вероятность применения полученных знаний в повседневной работе
- 90% – сокращение числа инцидентов
- 50-60% – снижение рисков кибербезопасности в денежном эквиваленте
- Более чем 30-кратная окупаемость вложений (ROI)
- Измеримые результаты программы осведомленности

Структура тренингов «Лаборатории Касперского» по повышению осведомленности в области кибербезопасности

* Исследование Aberdeen Group, 2014

Умные решения – Kaspersky Platinum Partner, Сертифицированный Учебный центр «Лаборатории Касперского»

- пилотные проекты
- внедрение и сопровождение
- техническая поддержка

Спасибо за внимание!
Вопросы?