Экосистема ИБ-решений от Лаборатории Касперского

Безопасность как искусство

Александр Тищенко
инженер предпродажной поддержки в ЮФО и СКФО

kaspersky

Физический ущерб

Границы информационной войны выходят на «новый уровень»

Шпионское ПО

Учетные данные

Бизнес и IT-процессы

Финансовая информация

Удаленный доступ

Доступ к системам в будущем – злоумышленники воспользуются им сами или продадут другим

Утечка данных

Персональные данные

Конфиденциальная информация

Коммерческая тайна

Ежегодно

Усложняется ландшафт угроз,
киберпреступники совершенствуют свои методы

Расширяется поверхность атаки
и количество точек входа злоумышленников

Усиливаются требования регуляторов,
особенно в отношении обеспечения защиты КИИ

+ Добавилось

Наступила эра хактивизма
и целевой киберагрессии

Больше лазеек
из-за полного ухода ИБ-вендоров или приостановки обновлений их решений

Началась активная фаза
импортонезависимости

Актуальные ИБ-задачи

Противодействие всем видам угроз в киберагрессив-ной среде

ИБ-замещение ушедших поставщиков в короткие сроки

Соответствие усиливающимся требованиям регуляторов

1

В первую очередь защититься от массовых угроз

2

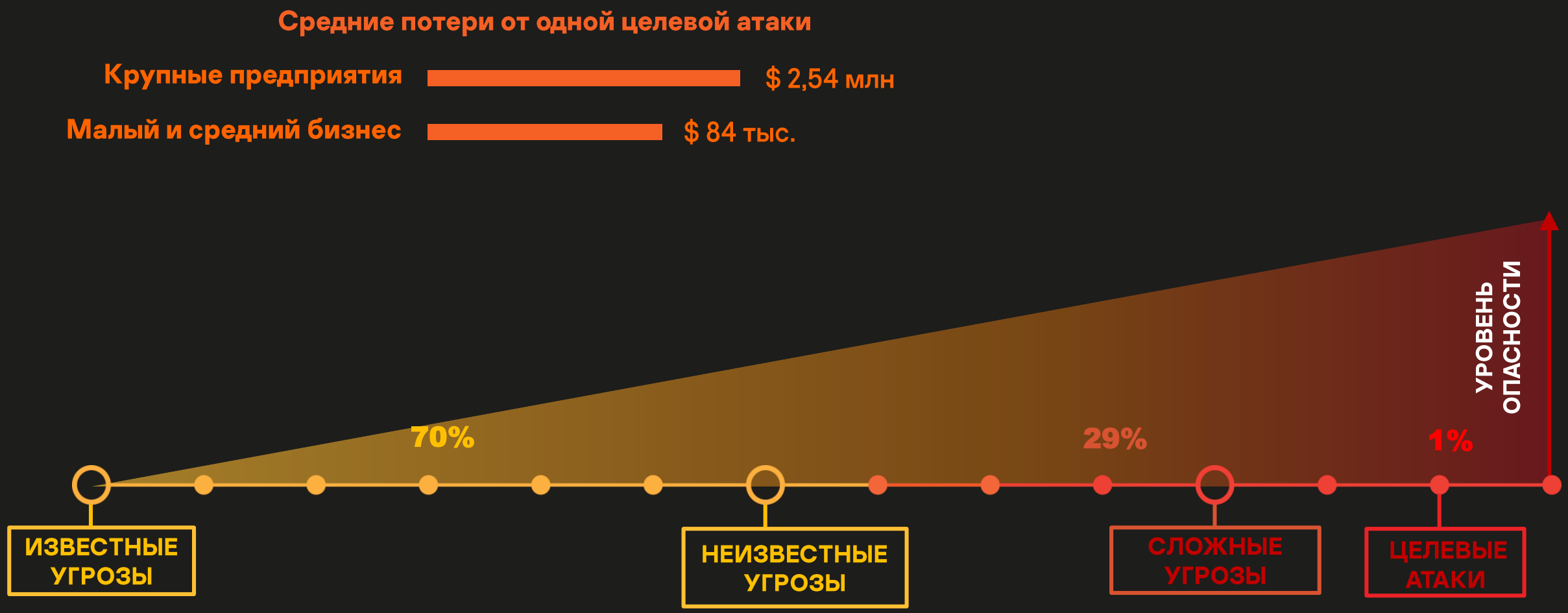
Во-вторых выстроить защиту от сложных угроз

Самостоятельно: постепенно или сразу

Выбрать управляемую защиту

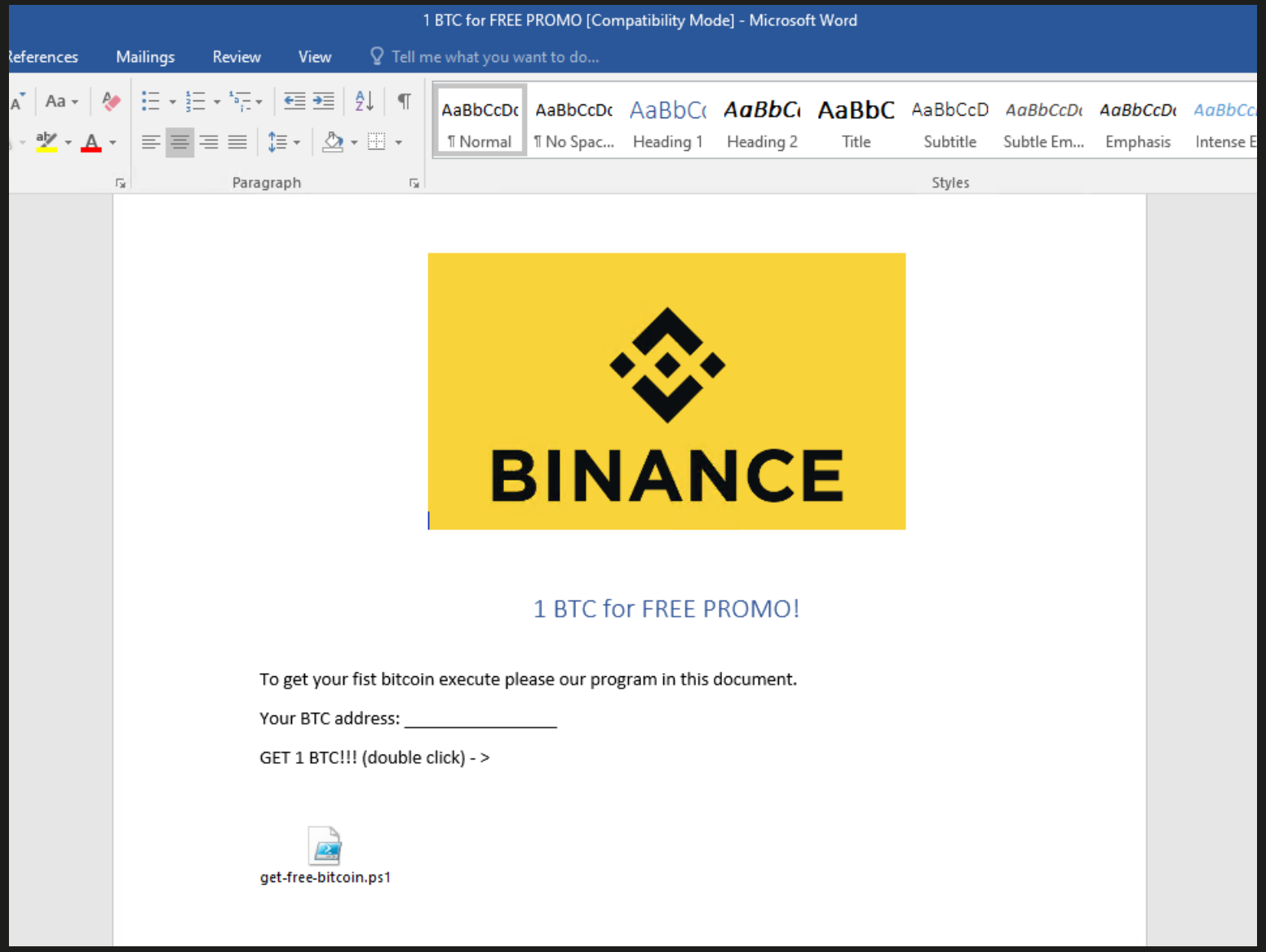
С чем приходится бороться?

1% атак – 90% ущерба

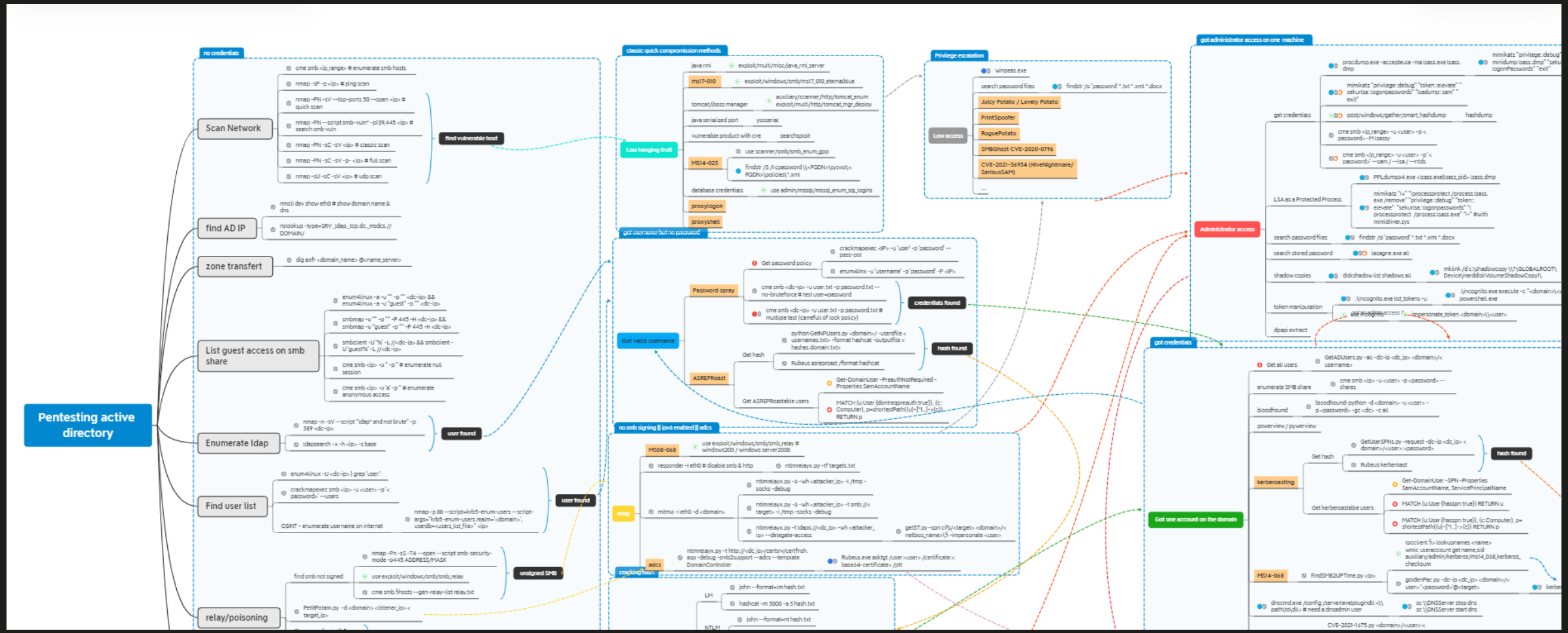


По данным «Лаборатории Касперского» и международного исследования «Информационная безопасность предприятия» (Enterprise information security).
Средний размер ущерба от одной целевой атаки, в том числе прямые убытки, а также косвенные убытки, связанные с восстановлением после атаки.

Биткоин в подарок это круто! Всего лишь запустить скрипт!



Подготовка злоумышленников



Операция “Триангуляция”

- Заражаемое iOS-устройство получает сообщение iMessage со специальным вложением, содержащим эксплойт
- Без какого-либо взаимодействия с пользователем, эксплойт из сообщения вызывает выполнение вредоносного кода
- Указанный код соединяется с сервером управления и приводит к последовательной загрузке нескольких «ступеней» вредоносной программы, включая дополнительные эксплойты для повышения привилегий
- После успешной отработки всех вредоносных компонентов, загружается конечная вредоносная нагрузка – полноценная APT-платформа
- Сообщение и вложение с эксплойтом удаляются в процессе заражения

https://securelist.ru/triangulation-validators-modules/108202/

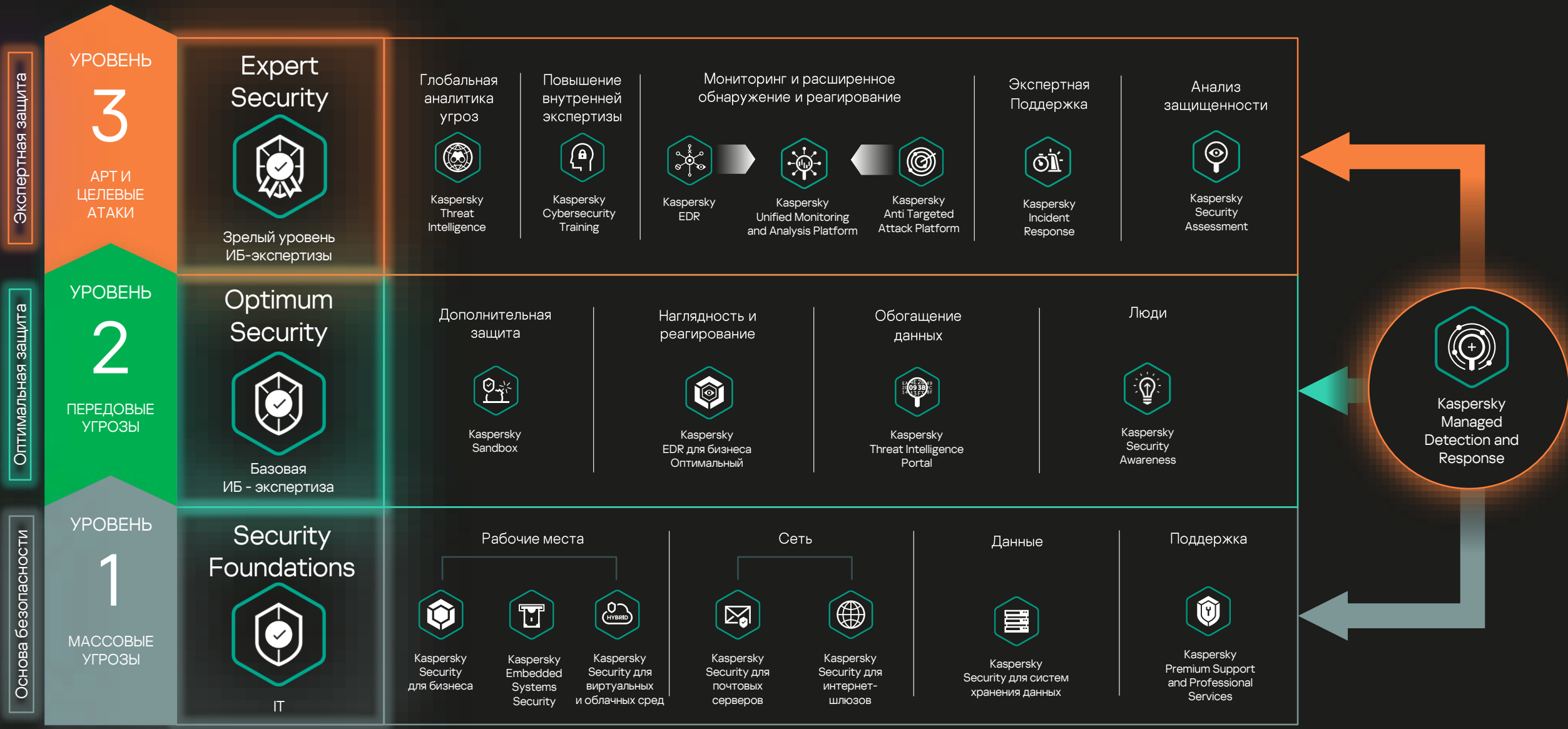
Интересное событие

Производитель поездов решил засудить ИБ экспертов, обнаруживших ошибку в его ПО

Белые хакеры рискуют оказаться в суде, так как им удалось доказать, что поставщик составов Newag встроил в ПО решения, провоцирующие поломки и препятствующие ремонту. Исследовав локомотив Impuls 45WE, белые хакеры обнаружили в прошивке скрытую функцию, с помощью которой Newag блокировала запуск поездов в удалённом режиме. Система отслеживала расположение составов посредством GPS, а после препятствовала запуску двигателя, если поезд не сдвигался с места 10 дней или находился на территории сервисных центров, не являющихся прямыми партнёрами Newag.

https://infobezopasnost.ru/blog/news/proizvoditel-poezdov-reshil-zasudit-ib-ekspertov-obnaruzhivshih-oshibku-v-ego-po/

Чем мы можем помочь?

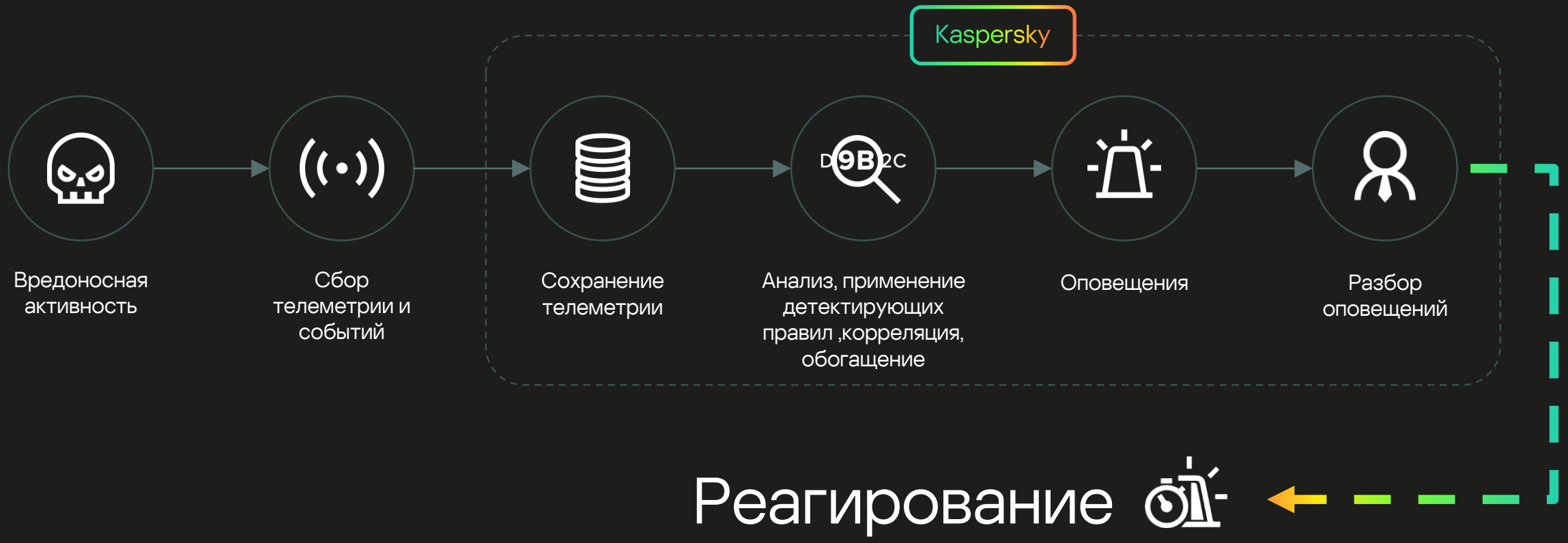


Ну и где же экосистема?

Kaspersky Symphony XDR — Расширенные возможности защиты

- Включена функциональность платформы Threat Intelligence и потоки данных об угрозах
- Включено повышение осведомленности сотрудников
- Включен модуль ГосСОПКА для автоматического взаимодействия с НКЦКИ

Как это работает



Примеры сценариев взаимодействия элементов Kaspersky Symphony XDR

Автоматические

Автоматическая блокировка на уровне почтового шлюза неизвестных вредоносных объектов, обнаруженных детектирующими механизмами KATA (до доставки получателю)

Взаимодействие веб-шлюза и KATA через API для передачи объектов из веб-трафика на проверку в песочницу и последующей их автоматической блокировки в случае выявленной вредоносной нагрузки

Автоматическая блокировка на хостах неизвестных вредоносных объектов при обнаружении песочницей в сетевом и почтовом трафике

Автоматическое отслеживание и реагирование на изменения состояния активов в том числе статусов компонентов защиты, наличия уязвимостей и тд.

Передача релевантных сложных атакам событий с KATA, KES, KEDR, KSMG, KWTS в KUMA для корреляции с данными от сторонних источников

Автоматическое обогащение карточки инцидента в KUMA информацией об уровне осведомленности атакованного пользователя

Реагирование через EDR на найденные угрозы в KUMA:

- Изоляция хоста и снятие с изоляции
- Блокировка хеша по md5 и sha256 на хосте
- Запуск исполняемого файла на хосте по полному пути
- Логирование реагирования в системном журнале

Потоковое обогащение событий в KUMA, предварительно обработанных в CyberTrace:

- Централизованная блокировка доступа пользователей к вредоносному домену
- Запрет скачивания вредоносных файлов из сети Интернет при получении вердикта от KATA Sandbox

Автоматическое создание и обновление карточек активов на основании информации от KSC

Автоматическое реагирование на найденные угрозы в KUMA средствами сторонних решений через запуск различных сценариев

Сбор данных и реагирование на инциденты из KWTS

Передача сырой телеметрии с EDR в KUMA

Полуавтоматические

Доступ в Threat Lookup для получения дополнительного контекста для эффективного расследования

Построение модели активов в KUMA на основании данных из KSC

Принудительный запуск обновления баз и антивирусной проверки через KSC с карточки инцидента в KUMA

Возможность назначить обучение по повышению киберграмотности из карточки инцидента в KUMA

Запуск действий по реагированию через EDR с карточки инцидента в KUMA

Запуск ретроспективной проверки по IoC в CyberTrace через интерфейс KUMA

Ближайший Roadmap

План выпуска новой версий Kaspersky Symphony XDR/SMP

Версия 2.0

Единый интерфейс

Для централизованной работы с комплексными инцидентами

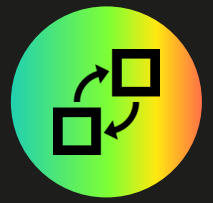
Реагирование и сложные кросс-продуктовые автоматическое сценарии через единую консоль на основе всех доступных интеграций, в том числе со сторонними решениями (AD, UserGate, Континент, CHKP, InfoWatch, PT, RedCheck, ...*)

Граф расследований

С возможностью контекстного обогащения
и запуска сценариев реагирования (playbooks)

* Subject to change

Развитие и совершенствование специализированных продуктов



Импортозамещение

Linux

Android

Платформы виртуализации

Kaspersky SD-WAN

Облачная оркестрация

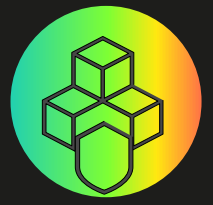
Виртуализация сетевых устройств

Интеграции с облачными провайдерами

KES,KATA/KEDR, KHCS, KSMG

Kaspersky Industrial Cyber Security

KICS for Nodes, Networks, Linux, EDR



Kaspersky Container Security

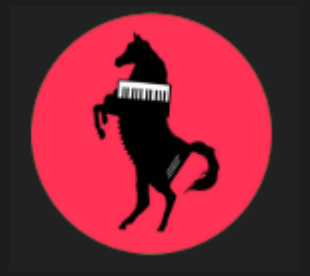
Управление запуском контейнеров и безопасностью среды выполнения

Источники информации

Источники информации в telegram

Kaspersky Daily

Техническая поддержка



Порвали два трояна

Kaspersky Symphony Support

Регуляторный хаб знаний в области ИБ

Регуляторный хаб знаний в области информационной безопасности

Узнайте в несколько кликов все требования регуляторов к вашему бизнесу и получите рекомендации по их выполнению.

- **Автоподбор нормативных документов:** поможем понять, что необходимо именно вашему бизнесу для соответствия законодательству
- **Интерактивная база знаний:** покажем взаимосвязь между документами, подберем необходимую информацию, чтобы вам не пришлось изучать десятки страниц законов, приказов и т. д.
- **Практические ИБ-советы:** подберем решения для обеспечения информационной безопасности с учетом требований законодательства

Вся информация на хабе актуальна и постоянно дополняется.

Получить консультацию

https://regulhub.kaspersky.ru/

Спасибо!

alexander.tishenko@kaspersky.com