Место специалиста ИБ в экосистеме технологий противодействия сложным угрозам

Яна Шевченко

Менеджер по развитию направления защиты от передовых угроз

Ключевые слова

СЛОЖНЫЕ УГРОЗЫ

ЛЮДИ

ТЕХНОЛОГИИ

ПРОЦЕССЫ

Что сегодня оказывает наибольшее давление на CISO?

57% Сложность и комплексность IT инфраструктуры

54% Соответствие требованиям регуляторов

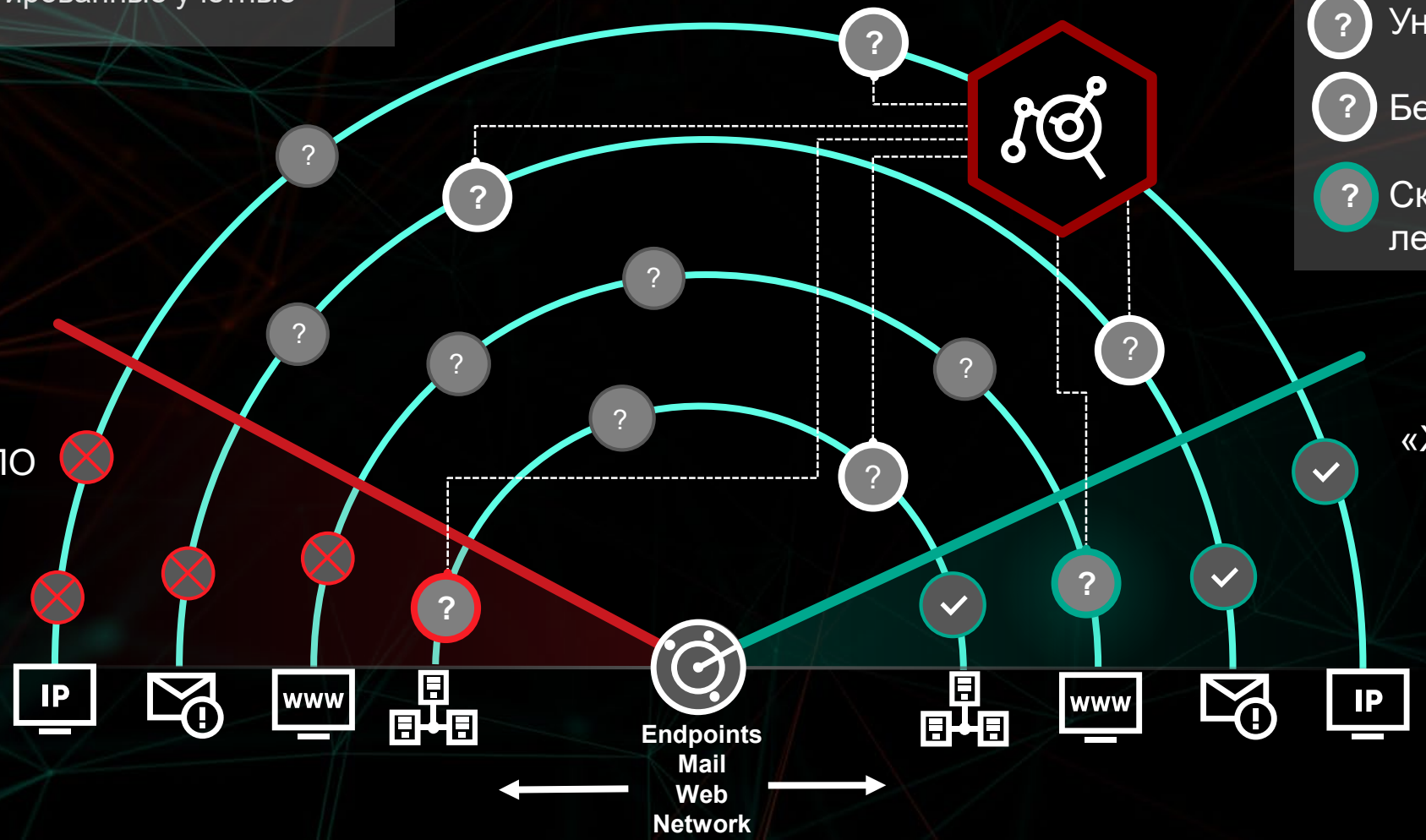
50% Увеличение количества и сложности угроз

Source: What It Takes to Be a CISO: Success and Leadership in Corporate IT Security, Kaspersky Lab, 2018

Тренды сегодняшних атак

- Эксплуатация уязвимостей
- Социальная инженерия и данные от инсайдеров
- Комбинации вредоносного и легитимного ПО
- Скомпрометированные учетные записи

Различные комбинации:

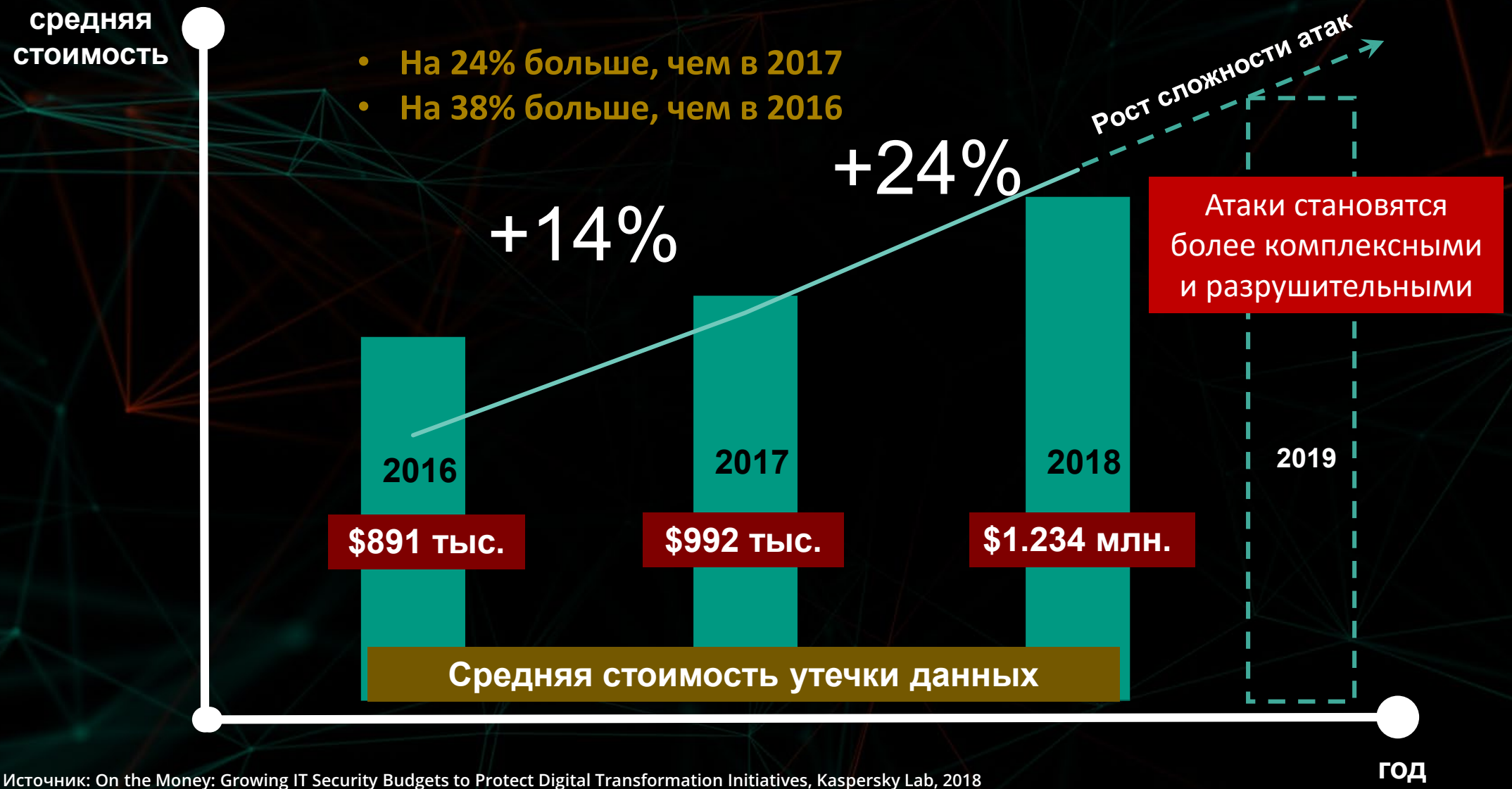


- Известное вред. ПО
- Новое вред. ПО
- Уязвимости нулевого дня
- Уникальное вред. ПО
- Бесфайловые методы
- Скомпрометированное легитимное ПО

KASPERSKY lab

Рост сложности угроз и финансовых последствий от них

Финансовые последствия от кибератак и затраты на последующее действия по восстановлению продолжают расти



Источник: On the Money: Growing IT Security Budgets to Protect Digital Transformation Initiatives, Kaspersky Lab, 2018

Наибольшие финансовые последствия в 2018 г.

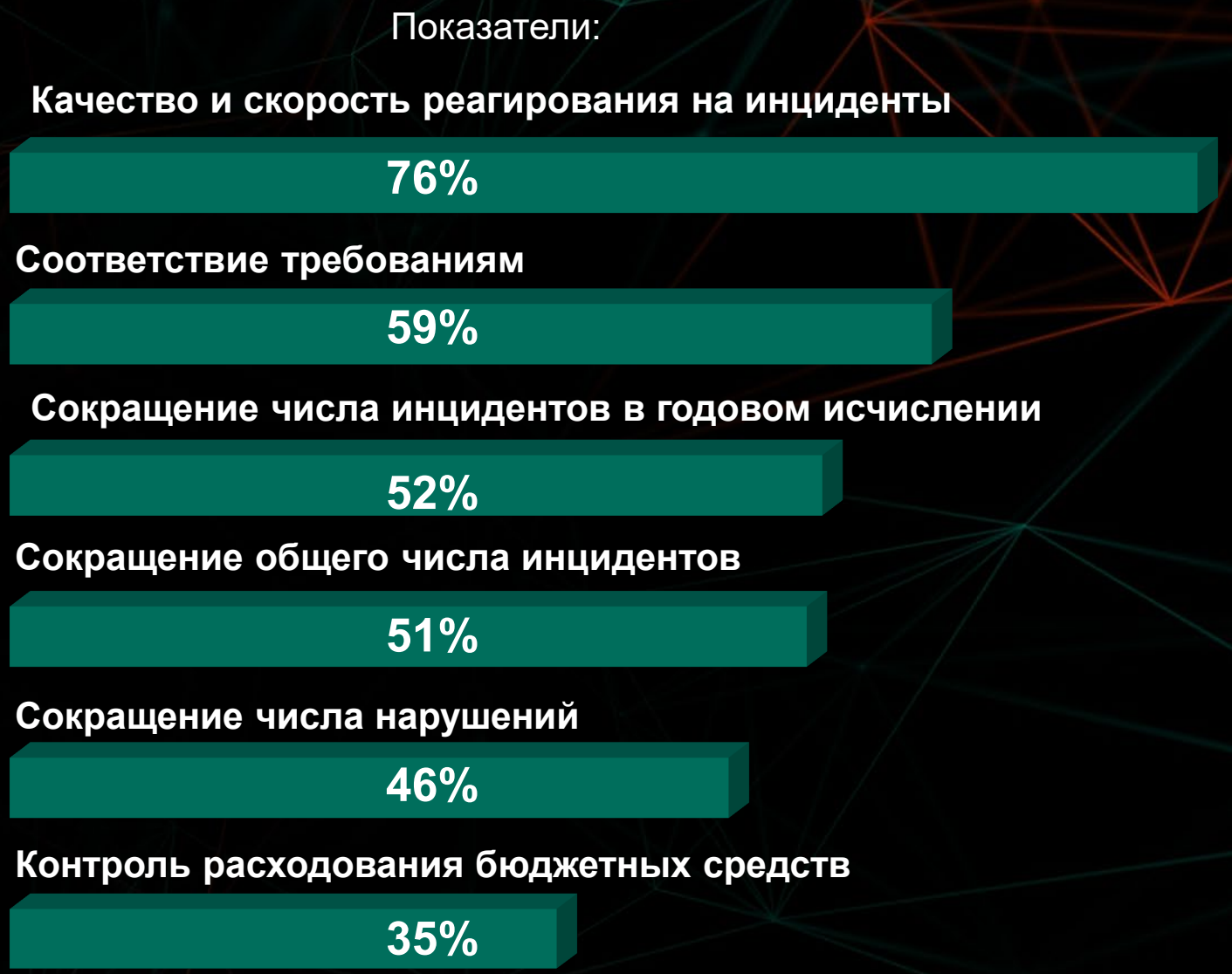
Утечка данных ⟵ **Финансовые последствия** ⟶ **Киберинцидент**

Утечка данных		Киберинцидент	
Целенаправленная атака	$1640k	Целенаправленная атака	$1109k
Инциденты, затрагивающие ИТ-инфраструктуру, которая обсуживается третей стороной	$1474k	Инциденты, затрагивающие ИТ-инфраструктуру, которая обсуживается третей стороной	$1086k
Потеря принадлежащих компании устройств, носителей информации	$1416k	Инциденты, связанные с подключаемыми устройствами / носителями информации	$993k
Инциденты, связанные с подключаемыми устройствами / носителями информации	$1405k	Инциденты, затрагивающие используемые облачные сервисы третьих сторон	$942k
Инциденты, затрагивающие используемые облачные сервисы третьих сторон	$1380k	Утечка данных из внутренних систем	$909k

Source: On the Money: Growing IT Security Budgets to Protect Digital Transformation Initiatives, Kaspersky Lab, 2018

В чем измеряется эффективность работы CISO (KPI)?

- Количество инцидентов растет
- Процесс реагирования на инциденты становится намного сложнее
- Требует от организаций дополнительных ресурсов и затрат



Source: Kaspersky Lab & PAC – a CXP Group Company, 2018

Какие процессы должны быть выстроены в организациях?

Обеспечение процесса обнаружения компьютерных атак

Регистрация инцидентов

Расследование и установление причин инцидентов

Анализ результатов устранения последствий инцидентов

Анализ данных о событиях безопасности

Реагирование на инциденты и ликвидация их последствий

Компаниям придется сосредотачиваться на ресурсоемких, сложных и дорогостоящих задачах по расследованию и реагированию на сложные инциденты

KASPERSKY lab

Выбор организаций

Игнорирование проблемы

- Компании считают, что рассказы о целевых атаках – это история не про них
- Принимают высокий риск столкнуться с разрушительными последствиями сложных угроз

Использование только существующих превентивных технологий или различных несвязанных инструментов

- Перегруженные службы ИТ и ИБ
- Неэффективное использование высококвалифицированных кадров

Высокий риск

Увеличение затрат

Несоответствие

Что получаем на практике

NETWORK TRAFFIC ANALYSIS

SANDBOX

ENDPOINT DETECTION AND RESPONSE

THREAT INTELLIGENCE

THREAT HUNTING TOOLS

SECURITY MONITORING

RESPONSE TOOLS

- Разрозненные интерфейсы
- Разрозненный инциденты
- Ручной труд, чтобы сводить воедино

- Потеря осведомленности
- Нехватка возможностей интеграции
- Нехватка ресурсов и экспертизы

Это всё про оптимизацию затрат, повышение эффективности и KPI

Современная стратегия защиты от передовых угроз и целенаправленных атак

- Уменьшение количества ручных задач
- Оптимизация трудозатрат на процессы расследования и реагирования на инциденты
- Получение результата без привлечения дополнительных ресурсов

СНИЖЕНИЕ РИСКОВ ИБ

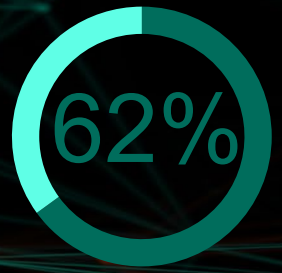
БЫСТРЫЙ РЕЗУЛЬТАТ

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ

KASPERSKY lab

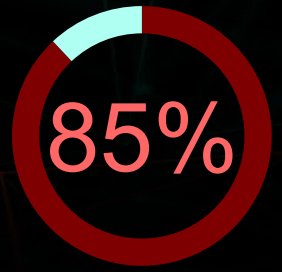
Дефицит кадров в области ИБ

По миру



В ходе опроса, большинство CISO признали, что испытывают трудности в найме ИБ специалистов с нужной квалификацией

СНГ



41% российских компаний признают, что им требуется больше опытных ИБ-экспертов

38% организаций в 2019 году планируют инвестировать в обучение ИБ сотрудников ИБ служб и повышение осведомленности рядовых сотрудников

Вирусный аналитик

 = 43%

Специалист по сетевой безопасности

 = 37%

Специалист по реагированию

 = 20%

Threat hunters & SOC специалисты

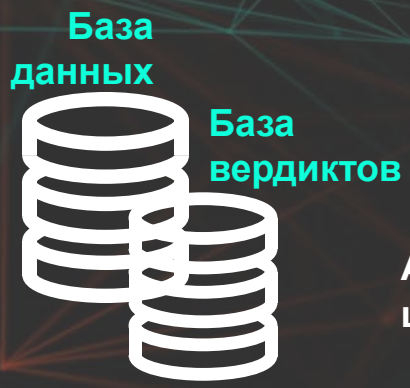
 = 13%

KASPERSKY lab

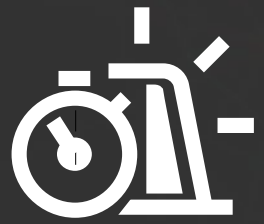
Источник: What It Takes to Be a CISO: Success and Leadership in Corporate IT Security, Kaspersky Lab, 2018; B2B International и IDC, Winning the Cybersecurity Battle

Что может упростить работу ИБ специалиста

Автоматизация рутинных операций в процессе противодействия сложным угрозам

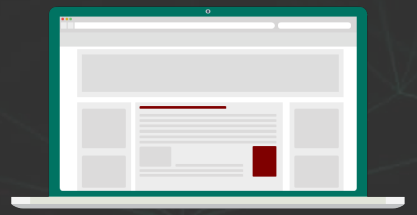


Автоматический сбор и централизованное хранение данных



Централизованный процесс реагирования

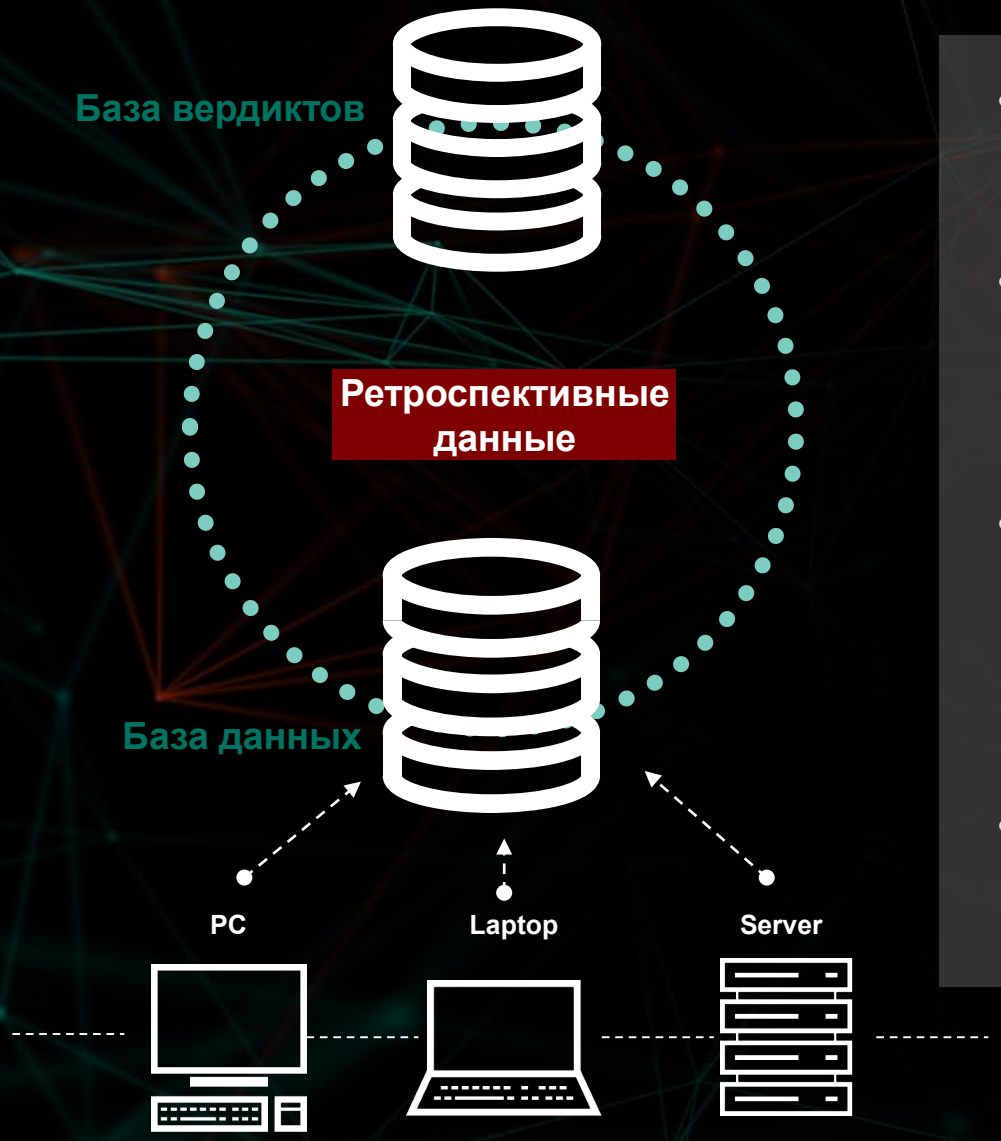
Быстрый поиск индикаторов компрометации (IoC) и возможность самостоятельного проактивного поиска угроз



Один программный продукт с единой консолью

KASPERSKY lab

Централизованное хранение цифровых данных



- Сбор, автоматическая запись и централизованное хранение информации по активностям со всех конечных точек
- Получение доступа к историческим данным, даже в случае недоступности рабочих мест для проведения расследования растянутых во времени атак
- Оказание содействия регулирующим органам (ФСБ России), предоставляя необходимую информацию об обнаруженных угрозах для дальнейшего установления службой причин возникновения компьютерных инцидентов
- Федеральный закон "О безопасности КИИ РФ" N 187-ФЗ и Указ Президента РФ №31с «О создании ГосСОПКА».

ПРОБЛЕМА: Отсутствие возможности у организаций получить доступ к данным для проведения расследования

Быстрый поиск индикаторов компрометации (IoC)

1 ФИНЦЕРТ PC-V-BN-20180404-01-UPD

Предупреждение! Зафиксирована рассылка ВПО!

1. Краткое описание угрозы

Зафиксированы факты распространения ВПО класса Trojan.Downloader, производящего скачивание и установку ВПО, относящегося к классу Trojan.Stealer (кража паролей и личной информации). Предположительно, осуществляется широкомасштабная атака на организации кредитно-финансовой сферы.

2. Основные индикаторы компрометации

№	Тип IOC	Список
1	URL-адреса и IP-адреса, к которым производятся обращения	roordidnsitoft[.]xyz 195.123.225[.]27 195.123.225[.]28 195.123.233[.]132 195.123.233[.]150 195.123.233[.]159 66.70.211[.]246
2	Адреса и домены отправителей писем	getik@fenixrostov[.]ru mnr@lucky-child[.]com olga@lend-tour[.]ru

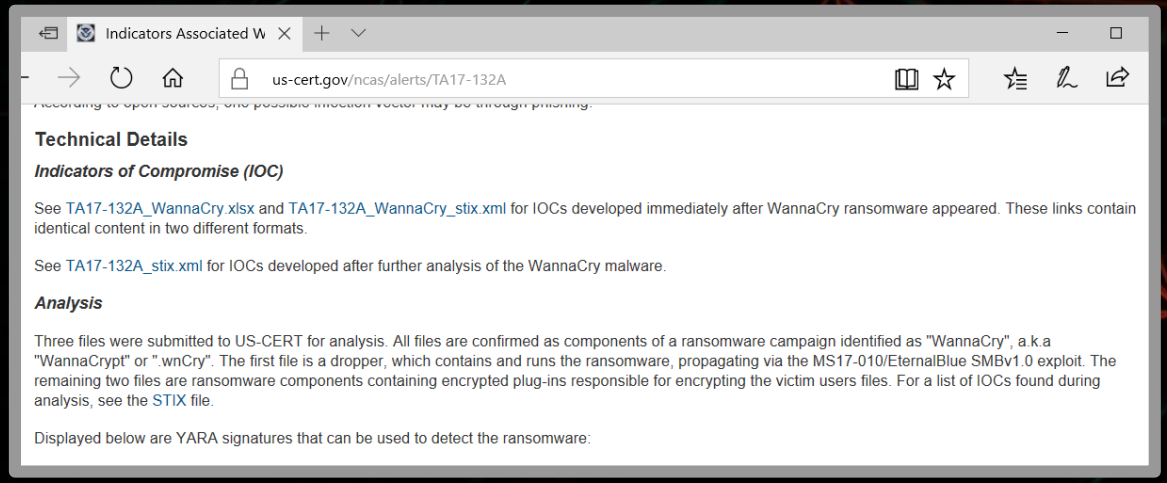
Ниже приведены данные по известным файлам из рассылки.

Информацию об обнаружении файлов антивирусным программным обеспечением различных производителей вы можете получить, например, по данным сайта virustotal.com, введя в поле поиска соответствующие файлам хэш-суммы, либо обратившись в техническую поддержку вендора использующегося в вашей организации антивирусного программного обеспечения.

Обращаем внимание на то, что использование авторами рассылки ВПО иных имён файлов, кроме указанных в настоящем бюллетене, **не исключено**.

1) "Пакет документов на 4 апреля.scr", "Долг 04.04.2018.scr", "Задолженность среда.scr", "Деб.задолженность 04.04.scr".

MD5	85aa01c62c0de3cbe6017219f20b3ce2
SHA1	68becdea8bbe39dc858234a5de17b8ad31327431
SHA256	cd7630673ceacde04adda066150107f3df2698b582df1a89001167e81f0a5854



- Следование рекомендациям ФинЦЕРТ
- Иным источникам данных об угрозах
- Загрузка полученных индикаторов компрометаций (IoC)
- Автоматическое сканирование всей сети конечных точек на наличие и реагирование

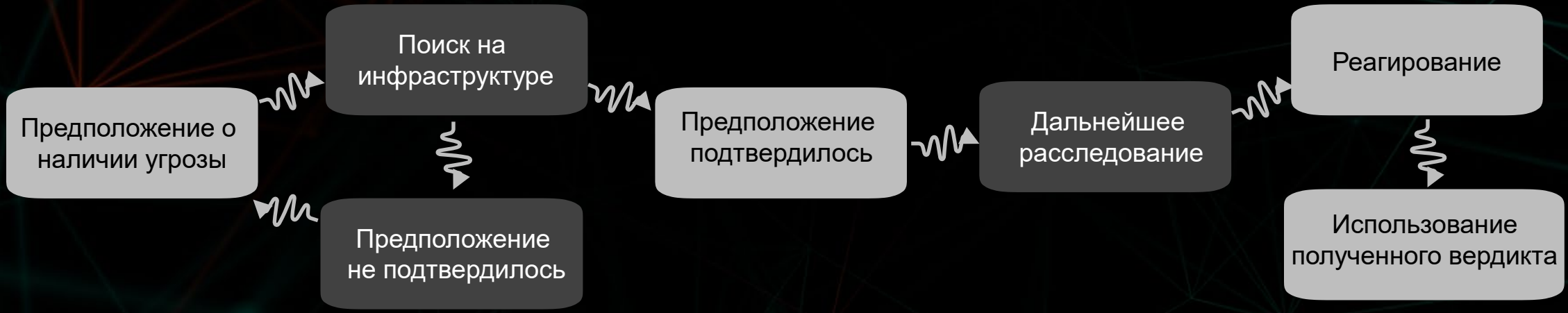
ПРОБЛЕМА: Ручная проверка сети на наличие индикаторов, игнорирование рекомендаций/ предупреждений

Проактивный поиск угроз - Threat Hunting

Процесс поиска новых угроз, не обнаруженных различной автоматической предотвращающей (EPP) и детектирующей логикой (EDR)

Мониторинг и самостоятельный поиск признаков аномальной активности, индикаторов компрометации (IoC) и иных свидетельств взлома по всей сети конечных точек

Охота на угрозы



ПРОБЛЕМА: Не все угрозы можно автоматически заблокировать/обнаружить

Качество и скорость реагирования на сложные инциденты

ПРОБЛЕМА: Долгий и ресурсозатратный процесс реагирования на ИБ инциденты

Типовое рабочее место специалиста по противодействию сложным угрозам

Сеть

Интернет

Рабочие места

Firewall NGFW

Mail Gateway

Web Gateway

Endpoint Protection

Решения по обнаружению, расследованию и реагированию на сложные угрозы

Централизованное хранение данных/ вердиктов

Визуализация обнаруженных угроз

Оповещения, отчетность и управление

API

Сторонние ИБ решения

CEF, SysLog

SOC

SIEM

Преимущества

- Снижение рисков ИБ
- Оптимизация затрат
- Повышение продуктивности
- Сокращение трудозатрат
- Соответствие

СПАСИБО

KASPERSKY lab