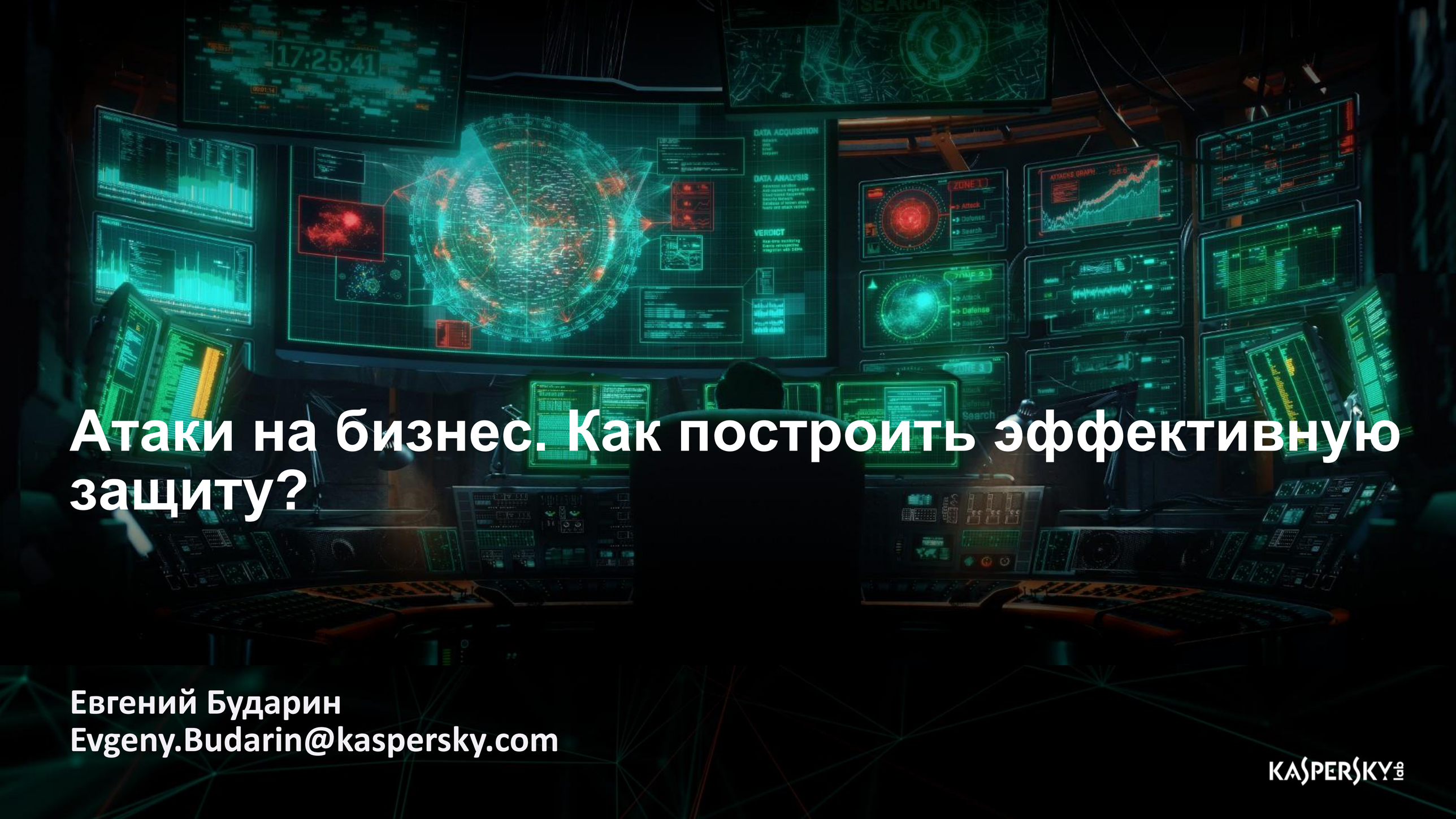


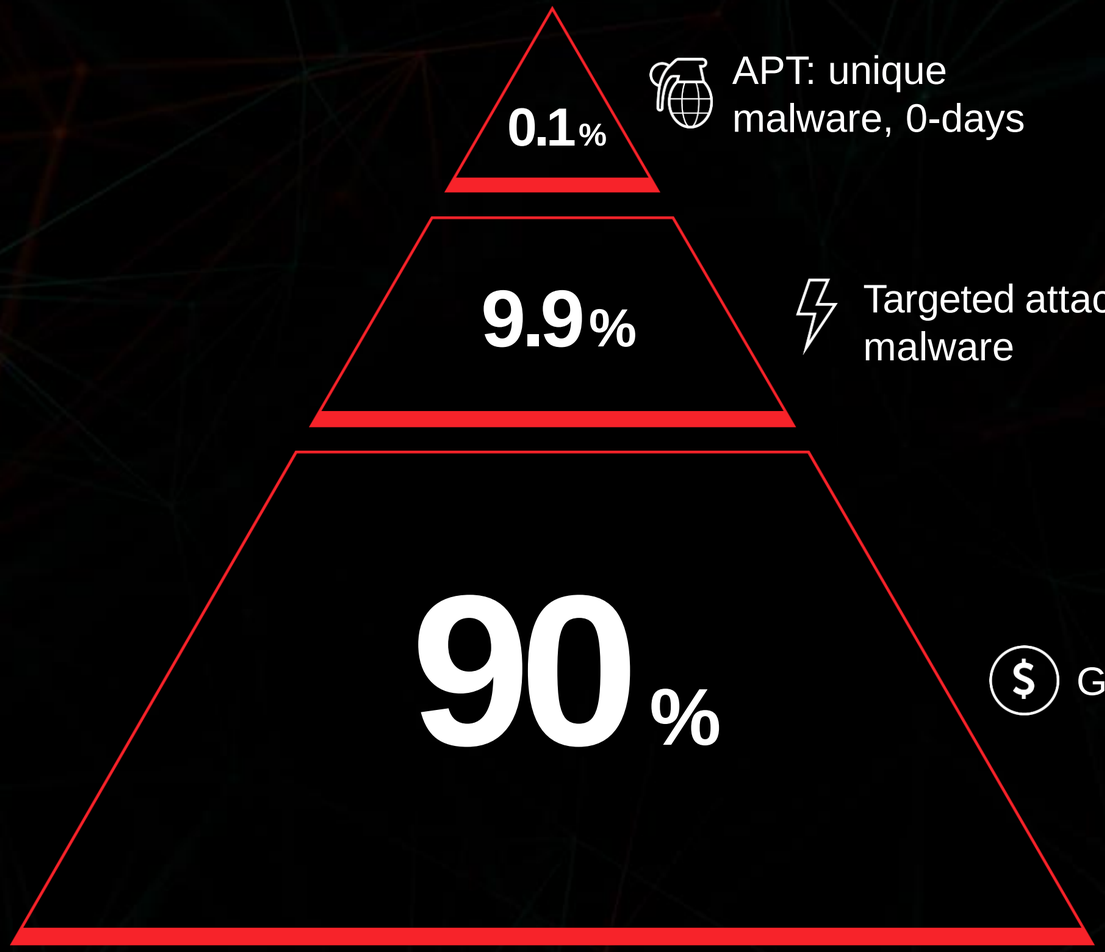
Атаки на бизнес. Как построить эффективную защиту?

Евгений Бударин
Evgeny.Budarin@kaspersky.com

KASPERSKY lab

KASPERSKY lab

УГРОЗЫ СЕГОДНЯ

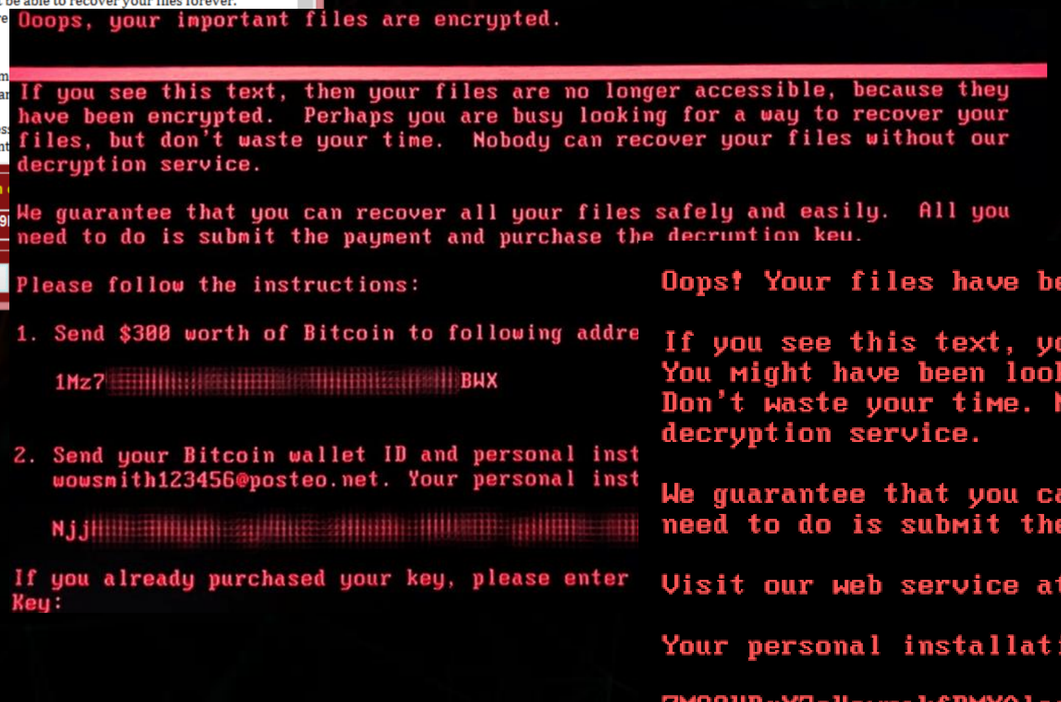


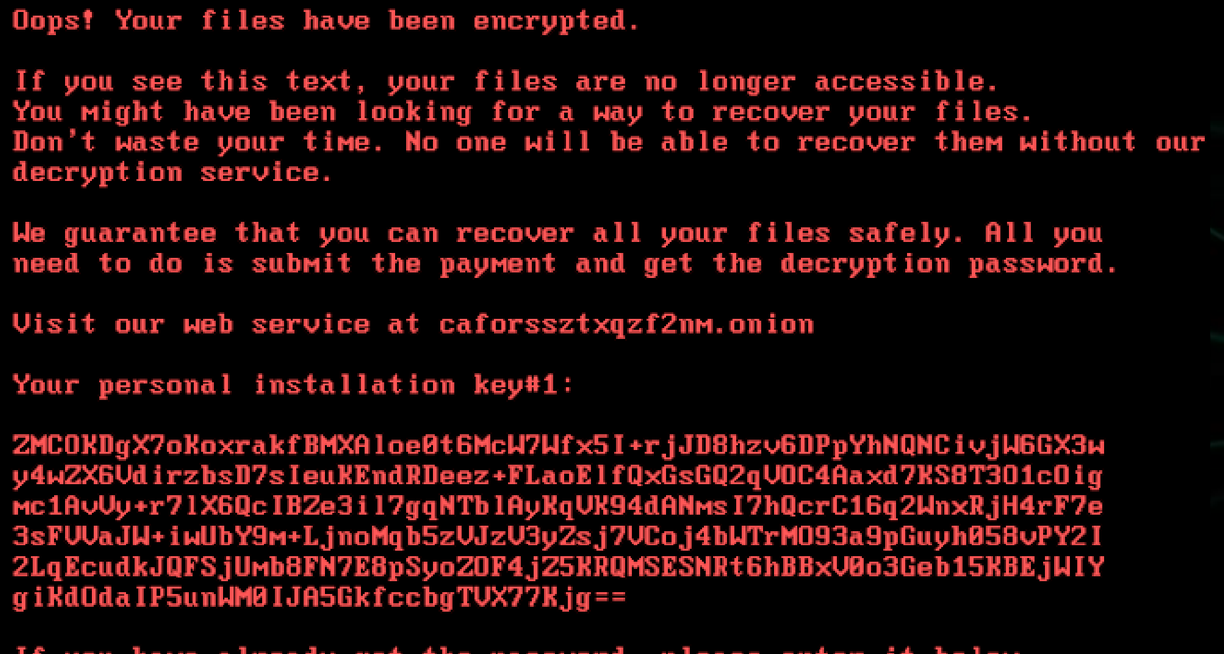
APT: unique malware, 0-days

Targeted attacks: sophisticated malware

Generic malware

ШИФРОВАЛЬЩИКИ





EXPetr: особенности

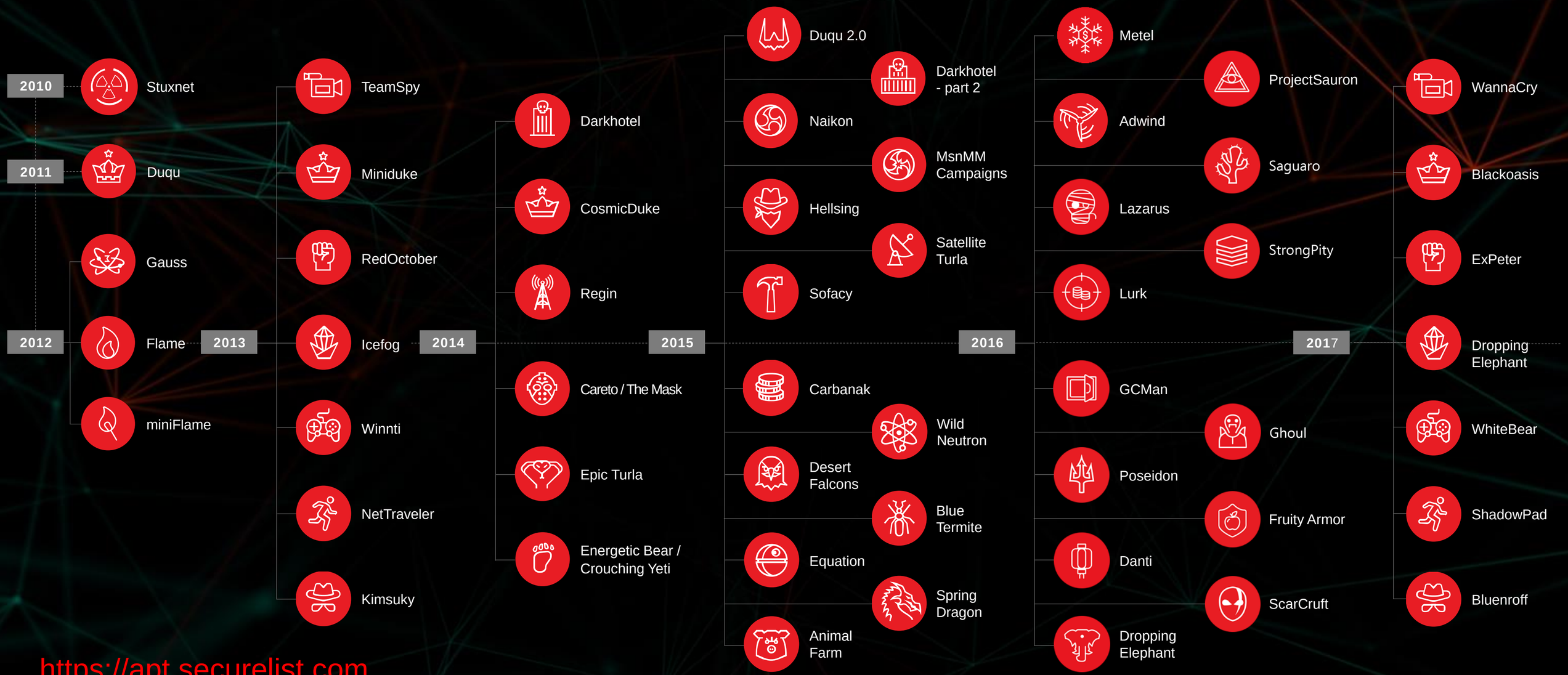
Профессиональные разработчики

- Хорошо продуманная схема заражения через сторонний софт
- Несколько заражённых сайтов, распространяющих угрозу на целевую аудиторию
- Множественные механизмы распространения по корпоративной сети(2 1-day эксплойта, кража учёток, WMIC/PsExec)

Некомпетентные воры(?)

- Один BitCoin кошелёк – легко отследить транзакции
- Один e-mail для связи – легко заблокировать
- Некорректно реализованный механизм шифрования – невозможно расшифровать данные

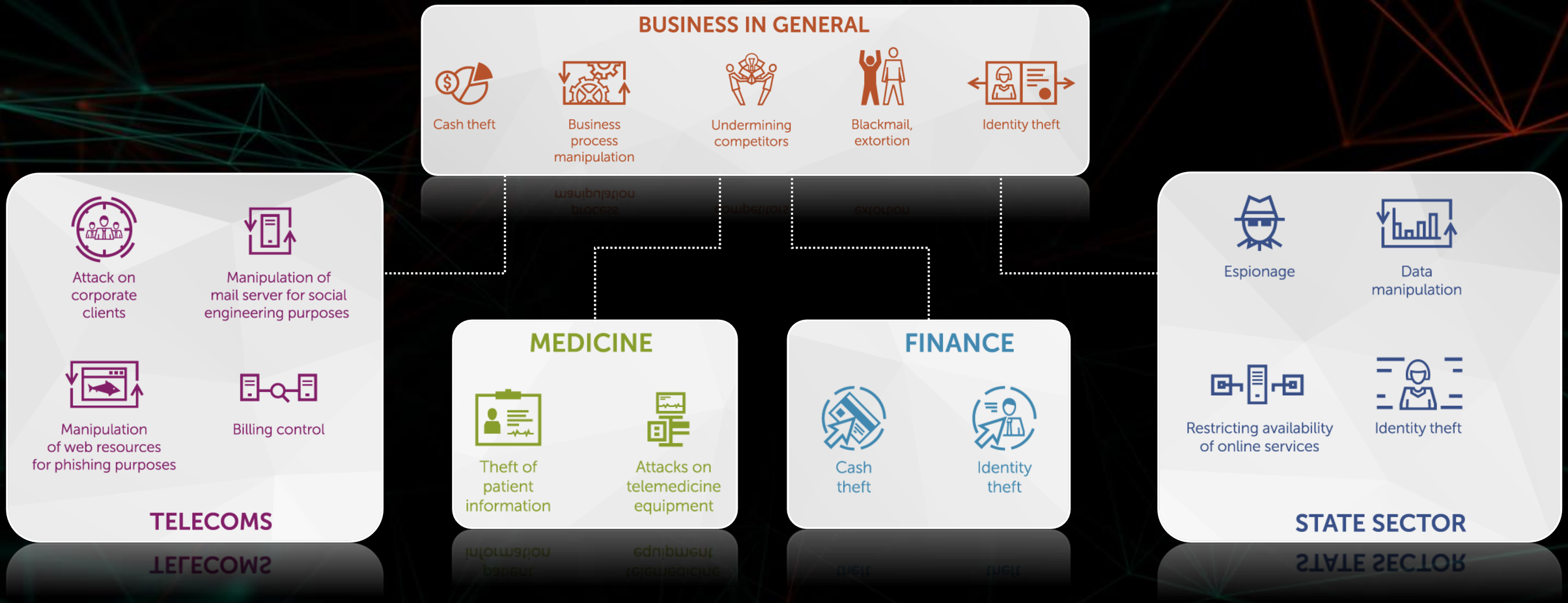
Наши исследования и открытия



https://apt.securelist.com

KASPERSKY lab

Идентичные тактики и методы могут повлечь за собой абсолютно разный результат в зависимости от отрасли

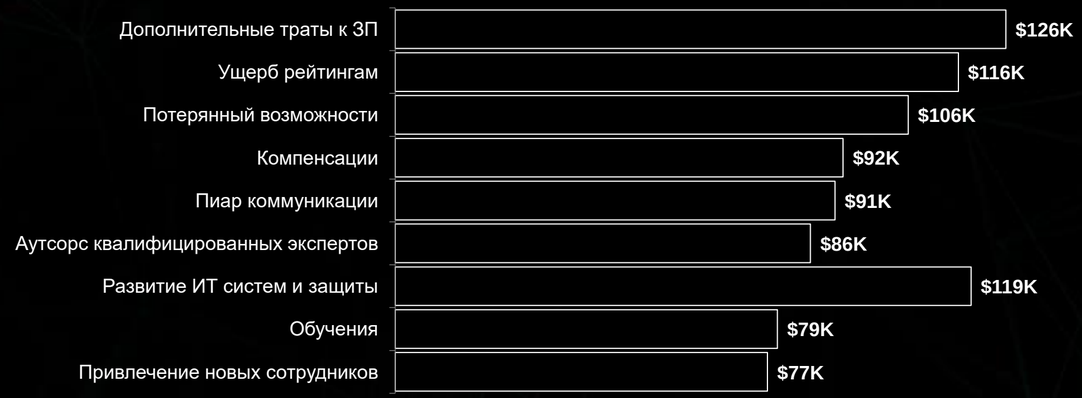


Статистика потерь за 2016 год от инцидентов ИБ

SMB

Средний ущерб:
$86.5k

Крупные компании



Средний ущерб:
$891k

Перераспредленеие трудозатрат ИТ и ИБ служб крупнейшая часть затрат по результату выявленного инцидента

Results from Kaspersky Lab's Corporate IT Security Risks Survey 2016, conducted worldwide by Kaspersky Lab

Base: 926 SMBs/ 590 Enterprises
Suffering At Least One Data Breach

ПРОМЕДЛЕНИЕ И НЕХВАТКА РЕАГИРОВАНИЯ ПРИВОДИТ К УВЕЛИЧЕНИЮ ПОТЕРЬ

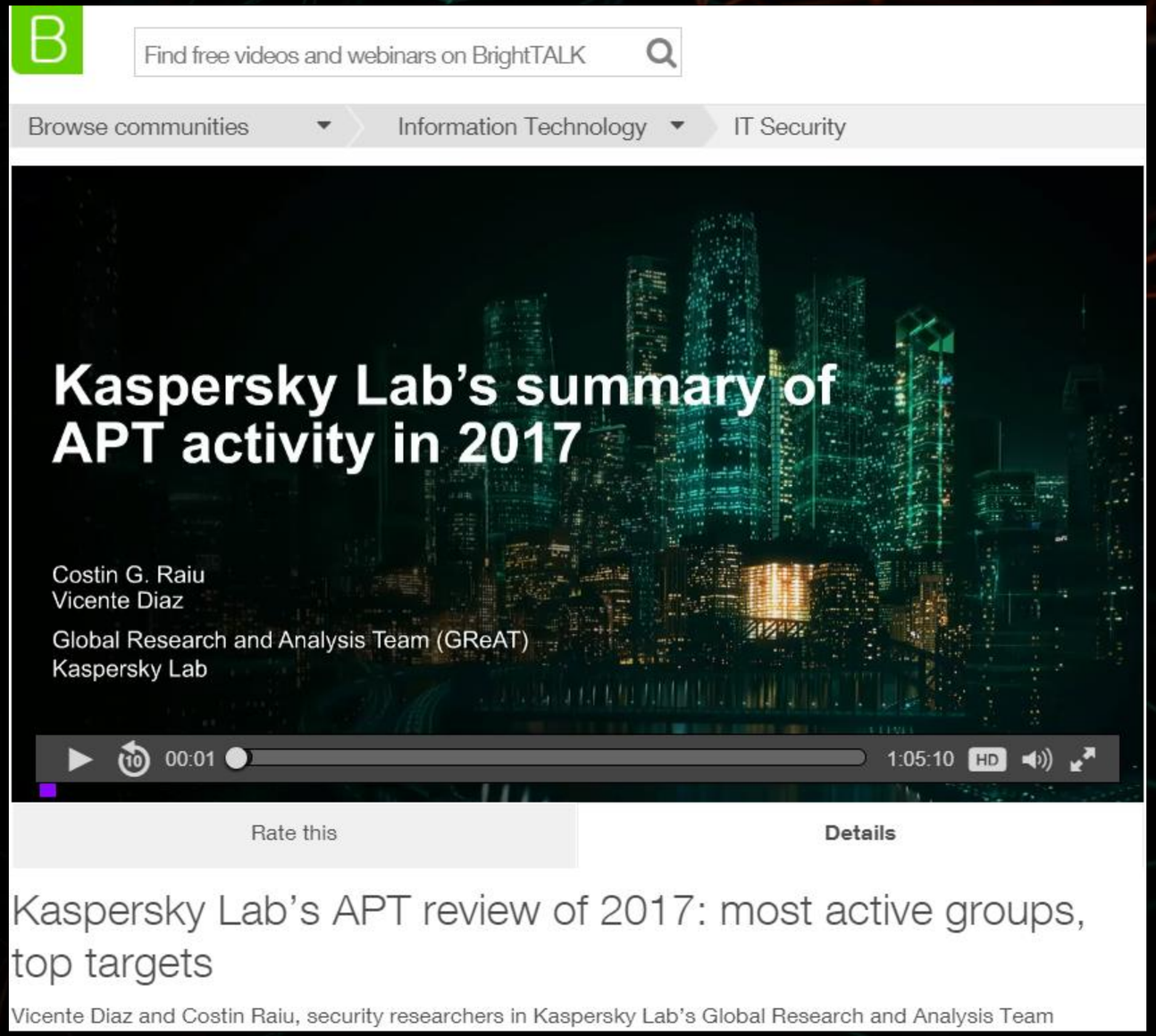
200% рост затрат на восстановление при промедлении с расследованием и реагированием

**Стоимость восстановления в зависимости от времени необходимого для обнаружения и реагирования*

KASPERSKY lab

APT

- Moonlight Maze [Turla]
- WhiteBear [Turla]
- Новый инструментарий [Lamberts]
- [Spring Dragon]
- [Black Oasis]



KASPERSKY lab

УТЕЧКИ ДАННЫХ

UBER

Взлом бюро кредитных историй Equifax

Похищено 209 тыс. кредитных карт и персональные данные 143 млн. человек.

Неизвестные проникли на серверы компании еще в мае 2017 года, но их присутствие оставалось незамеченным вплоть до конца июля 2017 года.

Злоумышленники получили доступ к такой информации, как номера счетов, даты истечения срока действия карт и имена держателей. С помощью этих сведений киберпреступники могут за чужой счет делать покупки в интернет-магазинах и проворачивать другие мошеннические схемы.
Основанная в 1899 году компания Equifax собирает и хранит информацию о более чем 800 миллионах потребителей и более 88 миллионах компаний по всему миру.

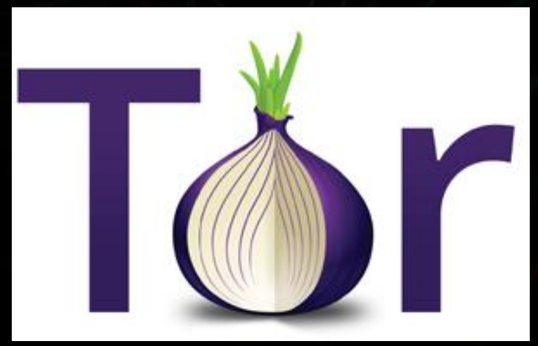
АТАКИ НА ЦЕПОЧКИ ПОСТАВОК ПО

ДРУГОЕ ФИНАНСИРОВАНИЕ

"The ransomware was merely a mechanism to get a large number of people to open a Bitcoin wallet – and that by itself would drive up the value of Bitcoin."

KASPERSKY lab

Абсолютная анонимность



Анонимные платежи + Анонимные коммуникации

Отличные возможности для киберпреступников

KASPERSKY lab

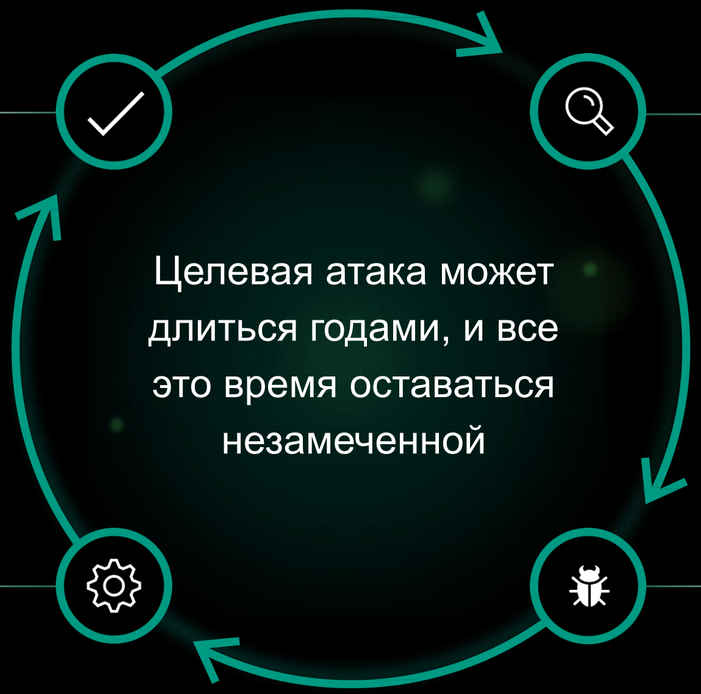
Бизнес-модели преступников

Malware-as-a-Service

Criminal Partnerships

Access-as-a-Service

Целевая атак – 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 корпоративной безопасности

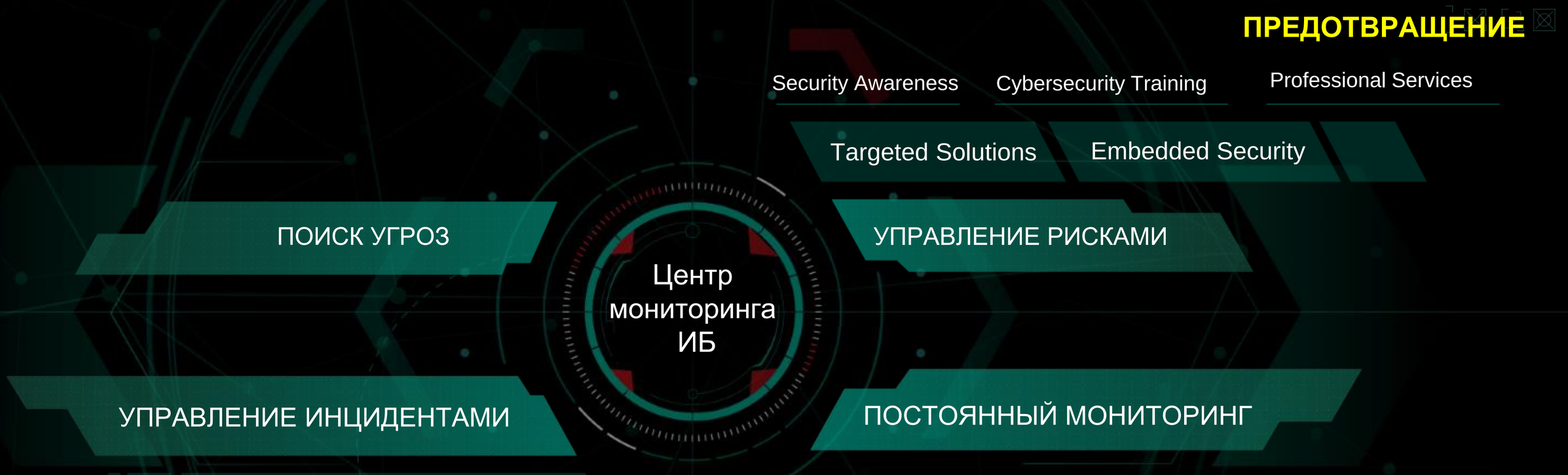
ПРОГНОЗИРОВАНИЕ Глобальная экспертиза

Передовые решения **ПРЕДОТВРАЩЕНИЕ**

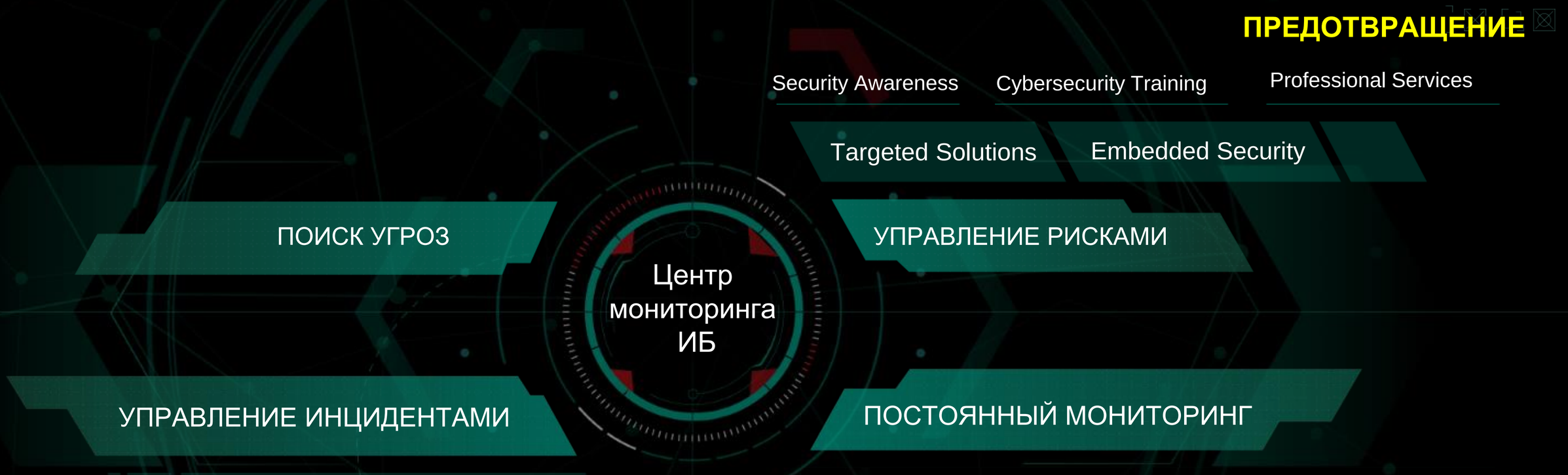
РЕАГИРОВАНИЕ Эффективное реагироание

Многоуровневое обнаружение **ОБНАРУЖЕНИЕ**

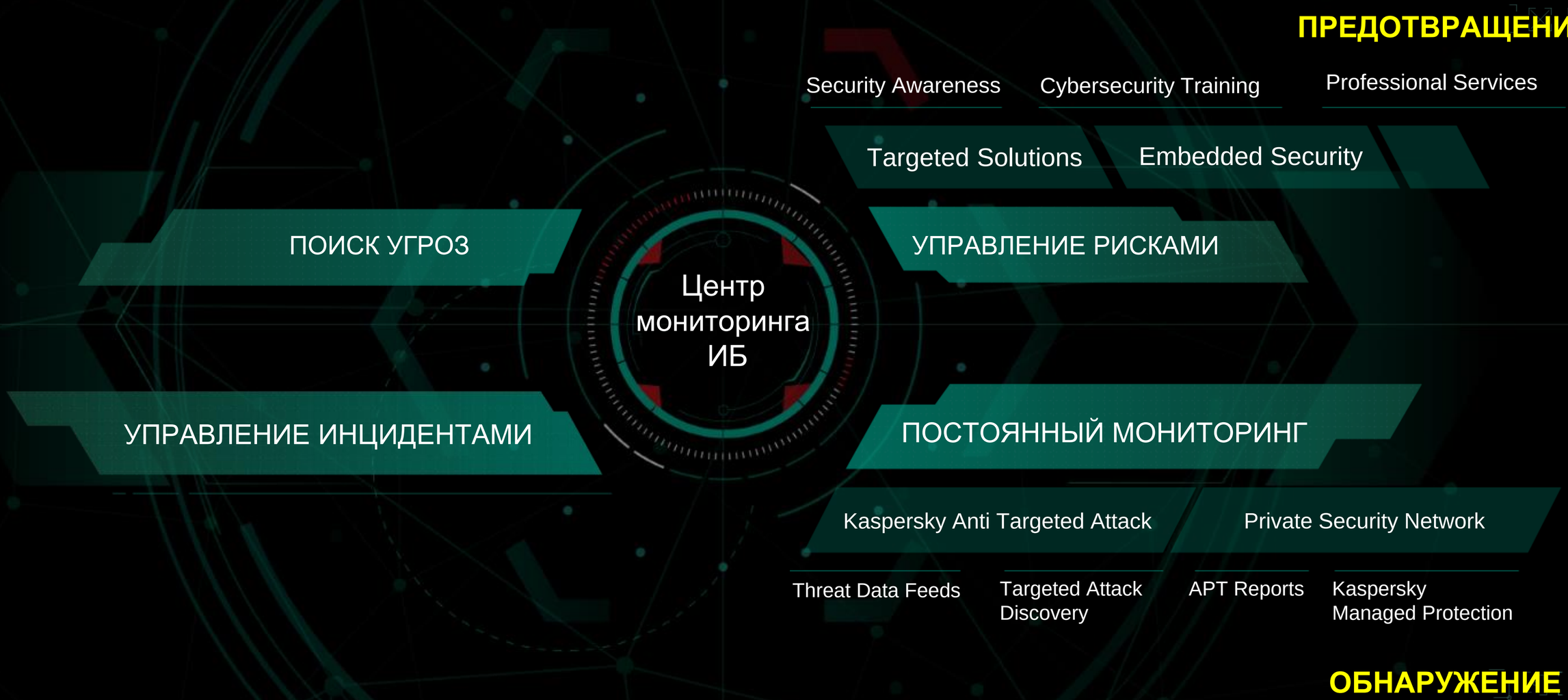
Адаптивная стратегия корпоративной безопасности



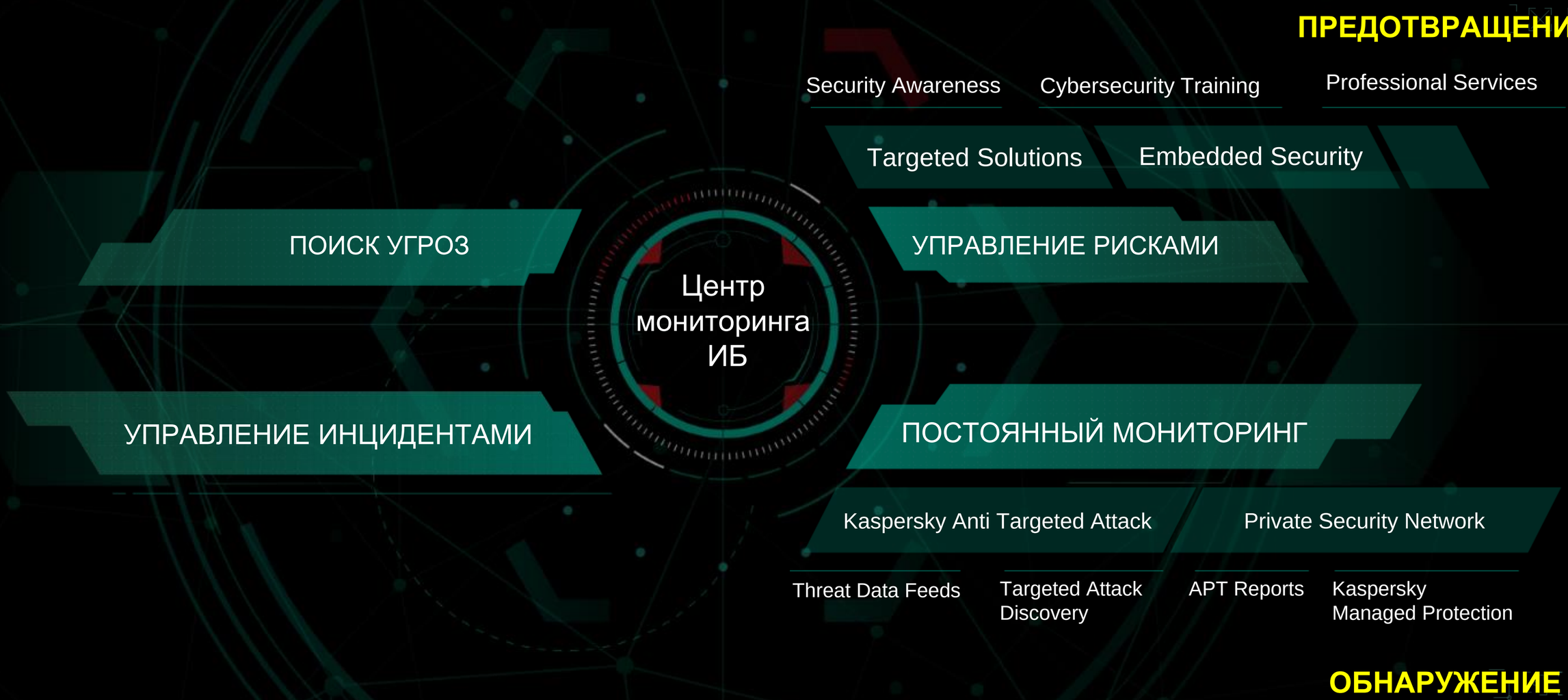
Адаптивная стратегия корпоративной безопасности



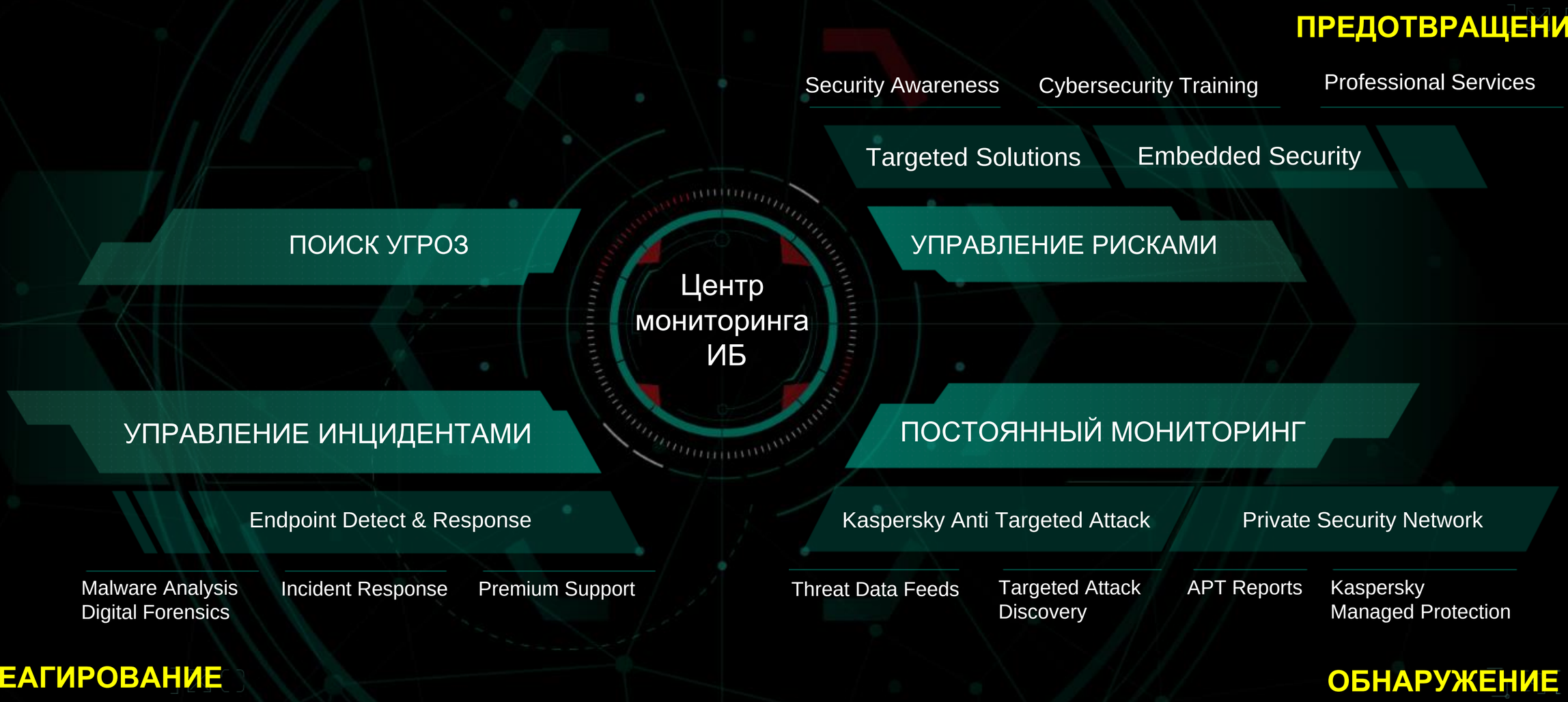
Адаптивная стратегия корпоративной безопасности



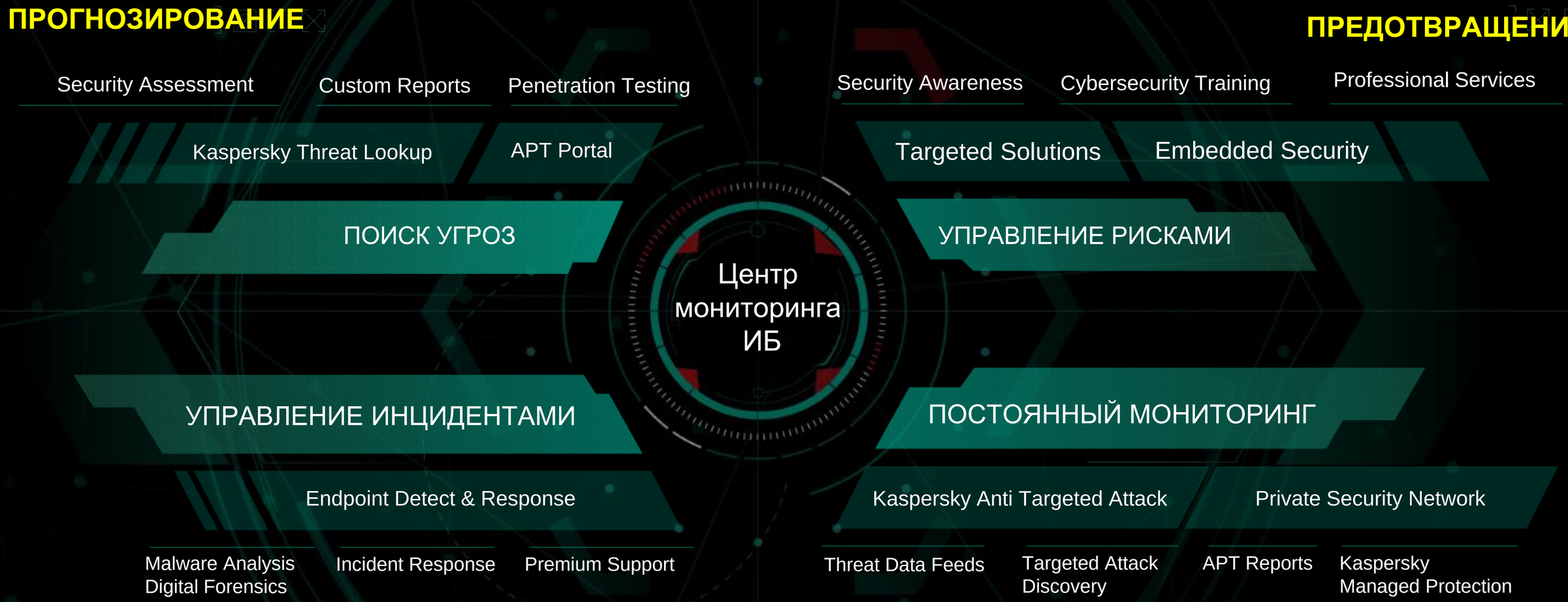
Адаптивная стратегия корпоративной безопасности



Адаптивная стратегия корпоративной безопасности



Адаптивная стратегия корпоративной безопасности



СПАСИБО!

KASPERSKY lab