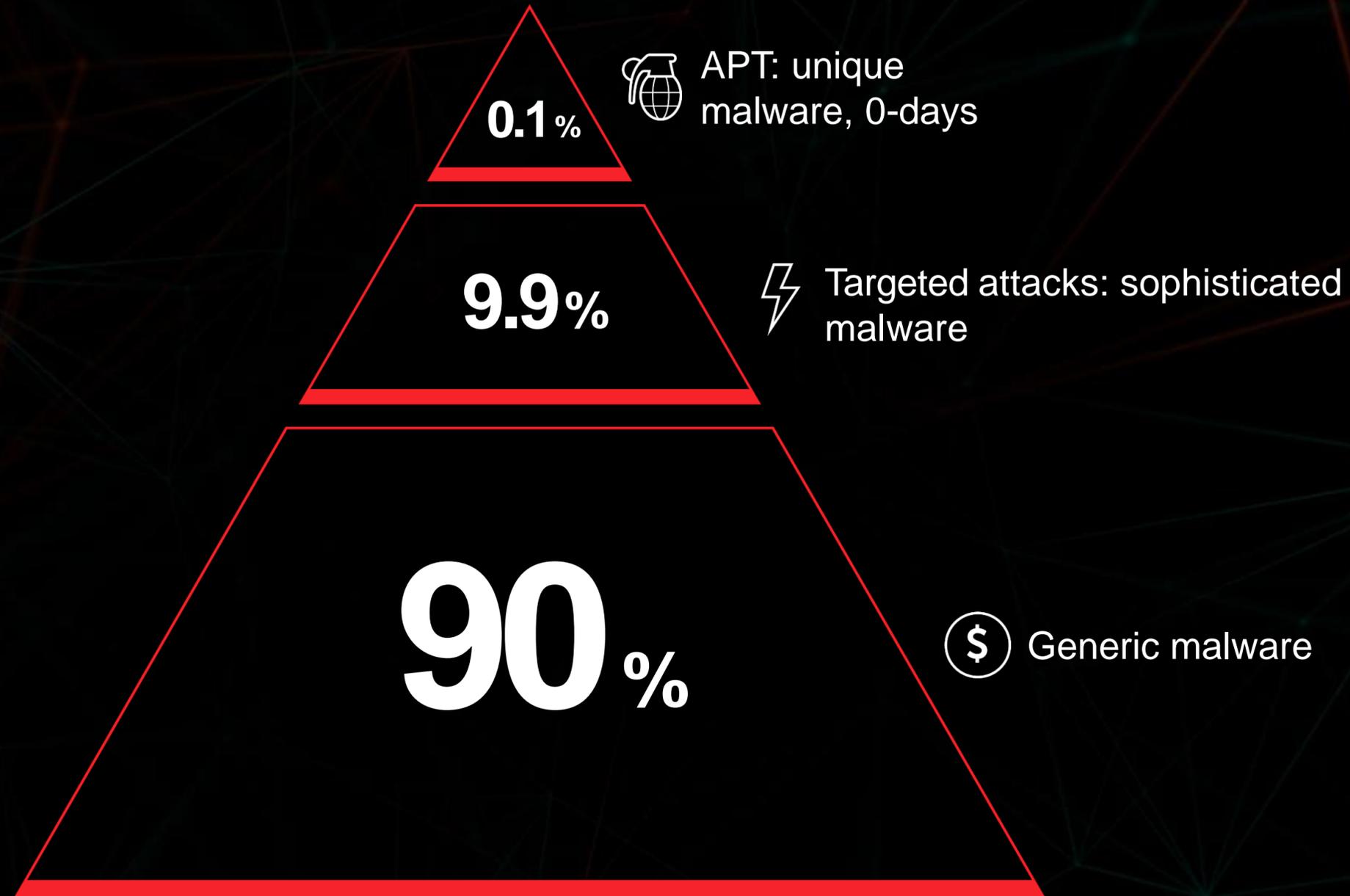


Атаки на бизнес. Как построить эффективную защиту?

Евгений Бударин
Evgeny.Budarin@kaspersky.com



УГРОЗЫ СЕГОДНЯ



ШИФРОВАЛЬЩИКИ

Wana Decrypt0r 2.0

Ooops, your files have been encrypted! English

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, please check the current price of Bitcoin at [Bitcoin.com](#) and click <How to buy bitcoins>. And send the correct amount to the address: [12t9YDPgwueZ9](#). After your payment, click <Check Payment>.

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

Send \$300 worth
12t9YDPgwueZ9

Check Payment

Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:
[1Mz7](#)  [BMX](#)
2. Send your Bitcoin wallet ID and personal installation key:
[wowsmith123456@posteo.net](#). Your personal installation key:
[Njj](#) 

If you already purchased your key, please enter Key:

Oops! Your files have been encrypted.

If you see this text, your files are no longer accessible. You might have been looking for a way to recover your files. Don't waste your time. No one will be able to recover them without our decryption service.

We guarantee that you can recover all your files safely. All you need to do is submit the payment and get the decryption password.

Visit our web service at caforssztxqzf2nm.onion

Your personal installation key#1:

```
ZMCOKDgX7oKoxrakfBMXAloe8t6McW7WfX5I+rjJD8hzv6DPpYhNQNCivjW6GX3w  
y4wZX6UdirzbsD7sIeukEndRDeez+FLaoEIfQxGsGQ2qUOC4Aaxd7KS8T301c0ig  
mc1A0Uy+r7lX6QcIBZe3i17gqNTb1AyKqUX94dANmsI7hQcrC16q2WnxRjH4rF7e  
3sFUUaJW+iwUby9m+LjnoMqb5zUJzU3yZsj7UCoj4bWTrM093a9pGuyh058vPY2I  
2LqEcudkJQFSjUmb8FN7E8pSyoZ0F4jZ5KRQMSESNRt6hBBxU0o3Geb15KBEjWIY  
gikdOdaIP5unWM0IJA5GkfccbgTVX77Kjg==
```

If you have already got the password, please enter it below.
Password#1: _

EXRetr: особенности

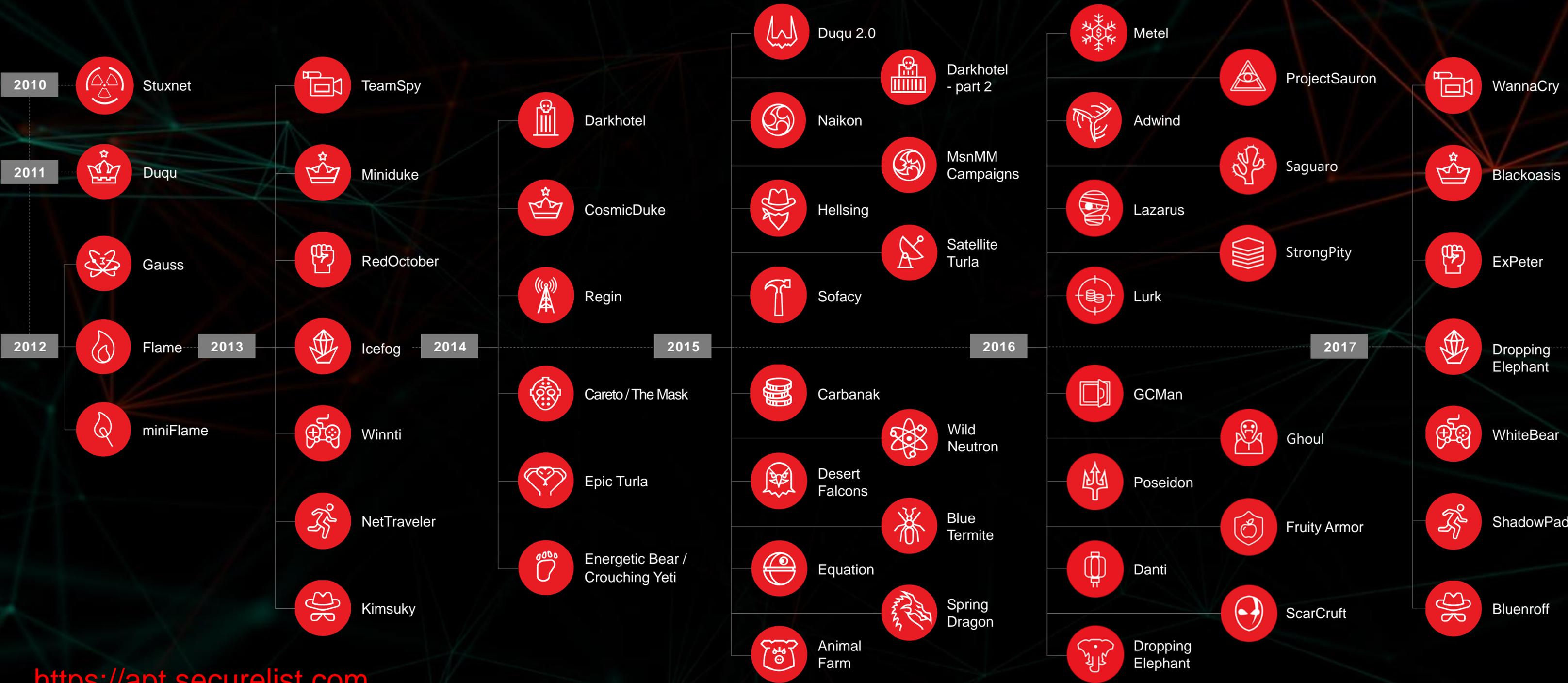
Профессиональные разработчики

- 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 учётки, WMIC/PsExec)

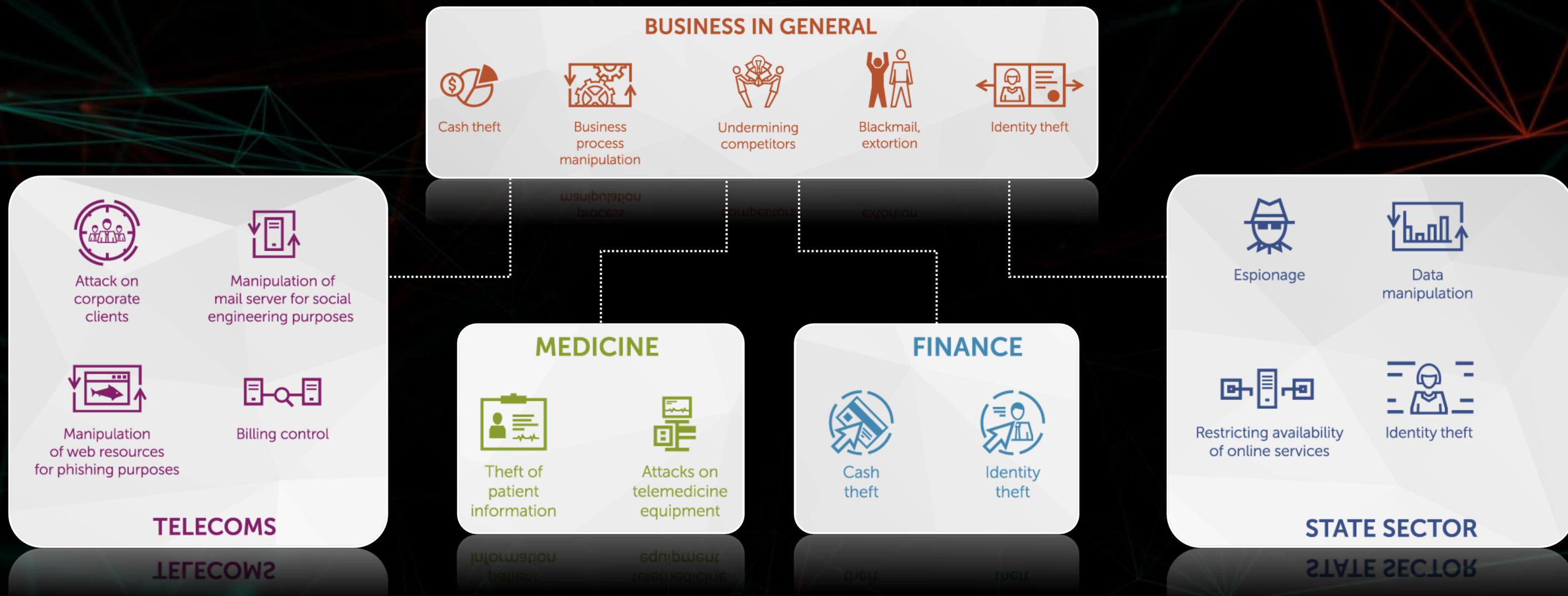
Некомпетентные воры(?)

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

Наши исследования и открытия



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

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

ПРОМЕДЛЕНИЕ И НЕХВАТКА РЕАГИРОВАНИЯ ПРИВОДИТ К УВЕЛИЧЕНИЮ ПОТЕРЬ

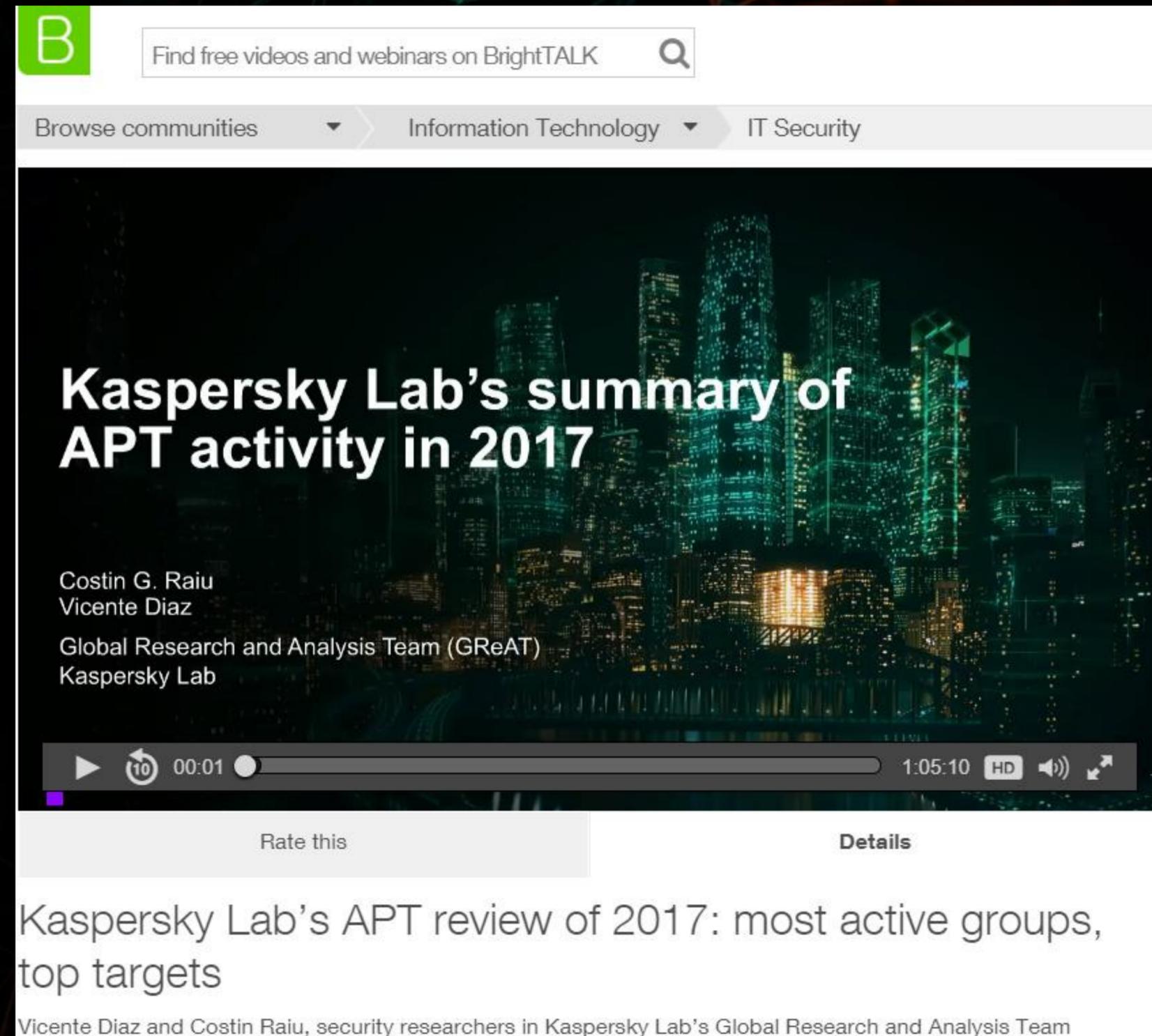
200% рост затрат на восстановление при промедлении с расследованием и реагированием



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

APT

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



The screenshot shows a video player interface on the BrightTALK website. The video title is "Kaspersky Lab's summary of APT activity in 2017". The presenters are listed as Costin G. Raiu and Vicente Diaz, from the Global Research and Analysis Team (GReAT) at Kaspersky Lab. The video player includes a search bar at the top, navigation tabs for "Information Technology" and "IT Security", and a progress bar at the bottom of the video frame. Below the video player, there are buttons for "Rate this" and "Details", followed by a text description of the video content.

B

Find free videos and webinars on BrightTALK

Browse communities

Information Technology

IT Security

Kaspersky Lab's summary of APT activity in 2017

Costin G. Raiu
Vicente Diaz

Global Research and Analysis Team (GReAT)
Kaspersky Lab

00:01 1:05:10 HD

Rate this

Details

Kaspersky Lab's APT review of 2017: most active groups, top targets

Vicente Diaz and Costin Raiu, security researchers in Kaspersky Lab's Global Research and Analysis Team

УТЕЧКИ ДАННЫХ



UBER



Взлом бюро кредитных историй Equifax

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

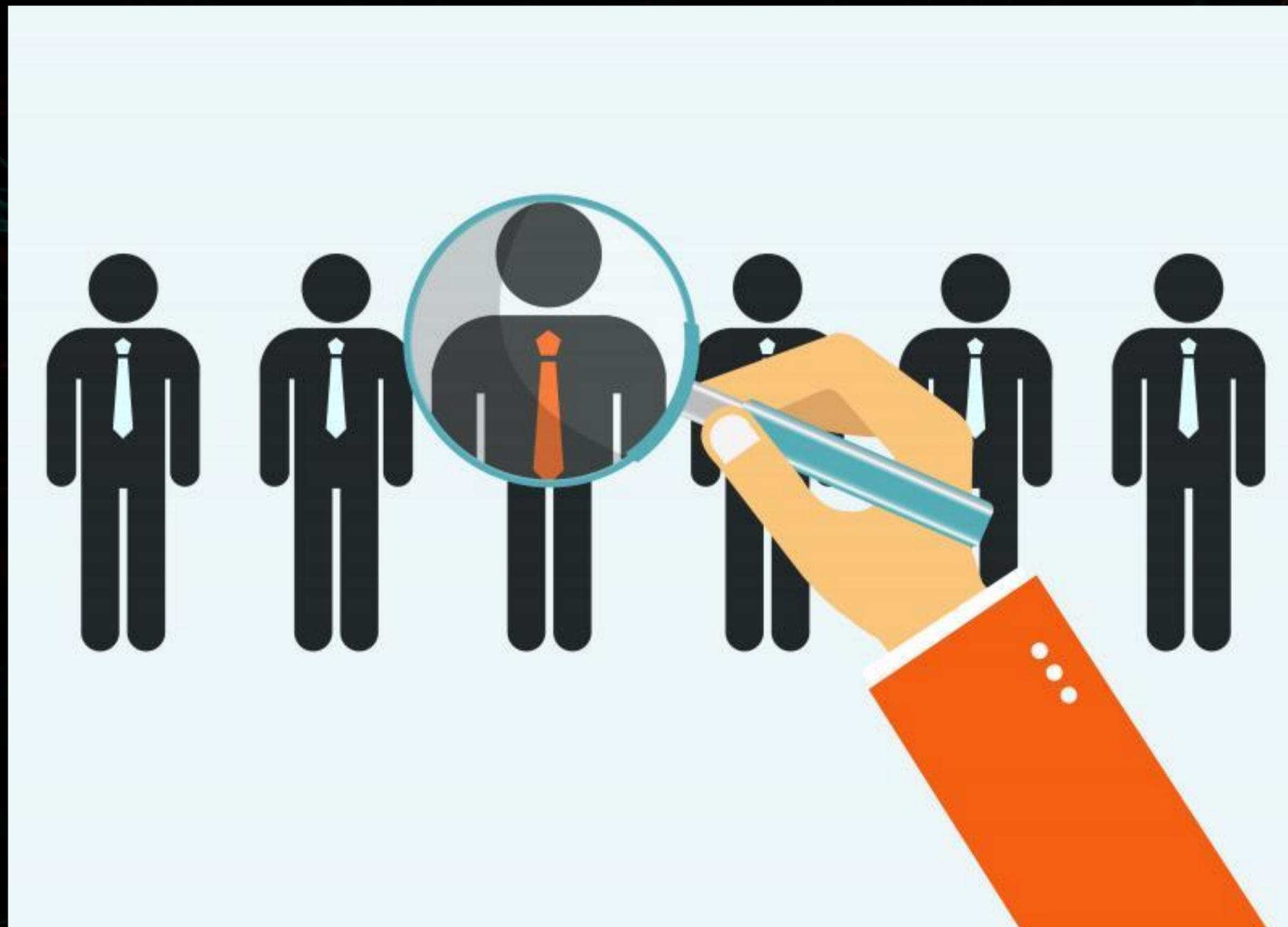
Неизвестные проникли на серверы компании еще в мае 2017 года, но их присутствие оставалось незамеченным вплоть до конца июля 2017 года.

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

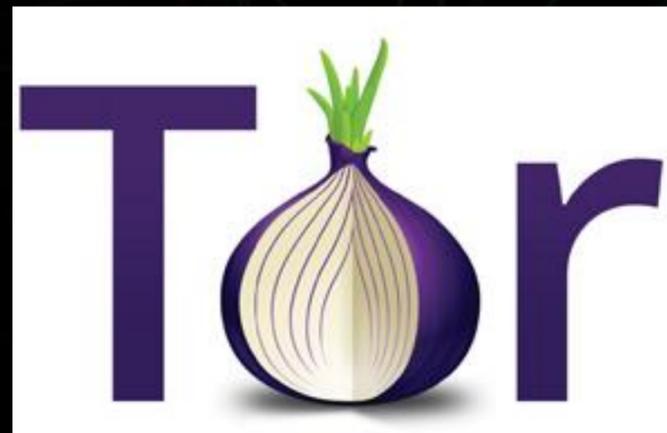
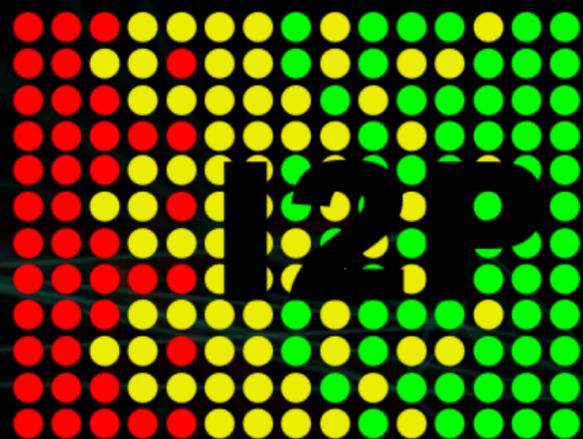


ДРУГОЕ ФИНАНСИРОВАНИЕ

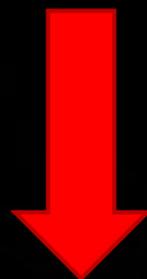
"The ransomware was merely a mechanism to get a large number of people to open a Bitcoin wallet – and that by itself would drive up the value of Bitcoin."



Абсолютная анонимность

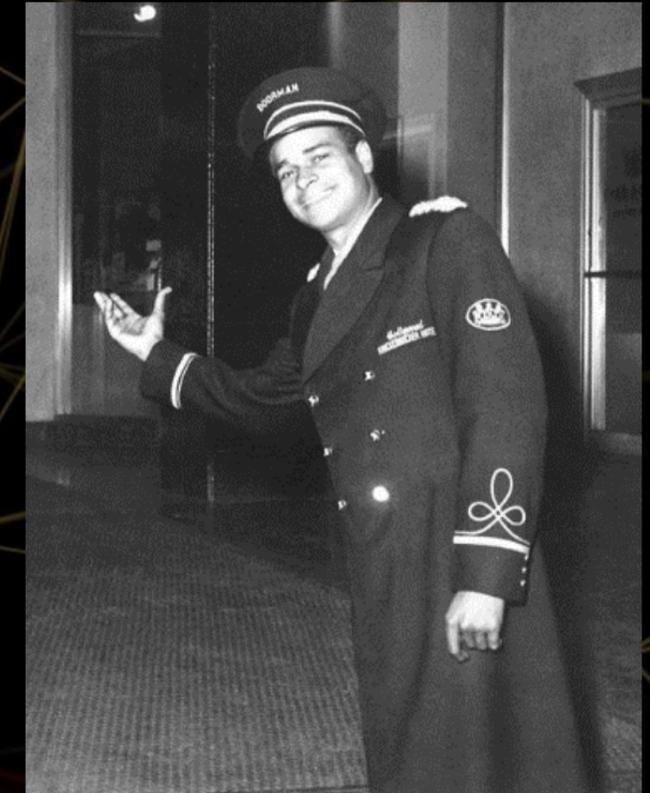


Анонимные платежи + Анонимные коммуникации



Отличные возможности для
киберпреступников

Бизнес-модели преступников

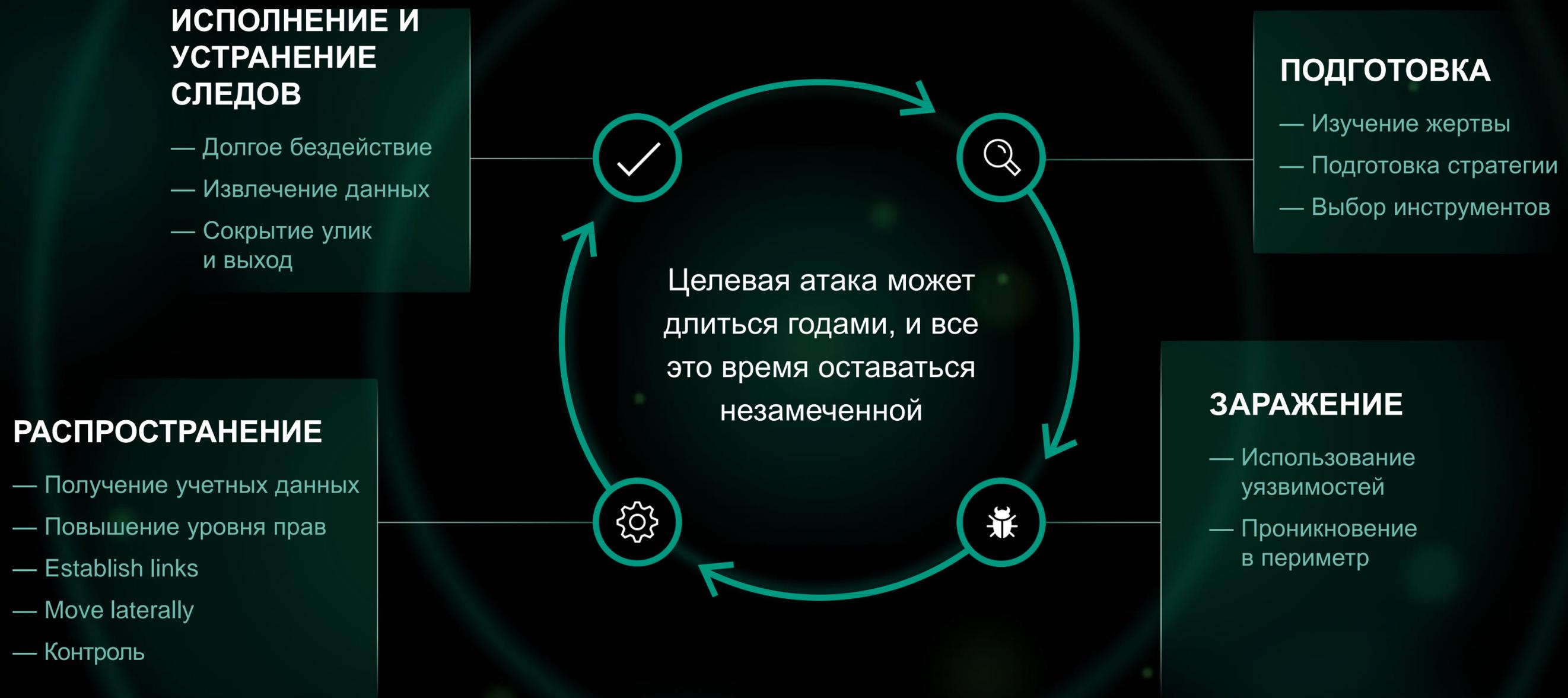


Criminal Partnerships

Malware-as-a-Service

Access-as-a-Service

Целевая атак – это постоянный процесс



Адаптивная стратегия корпоративной безопасности

ПРОГНОЗИРОВАНИЕ

Глобальная экспертиза

Передовые решения

ПРЕДОТВРАЩЕНИЕ

ПОИСК УГРОЗ

УПРАВЛЕНИЕ РИСКАМИ

Центр
мониторинга
ИБ

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

ПОСТОЯННЫЙ МОНИТОРИНГ

РЕАГИРОВАНИЕ

Эффективное реагироание

Многоуровневое обнаружение

ОБНАРУЖЕНИЕ

Адаптивная стратегия корпоративной безопасности

ПРЕДОТВРАЩЕНИЕ 

Security Awareness

Cybersecurity Training

Professional Services

Targeted Solutions

Embedded Security

ПОИСК УГРОЗ

УПРАВЛЕНИЕ РИСКАМИ

Центр
мониторинга
ИБ

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

ПОСТОЯННЫЙ МОНИТОРИНГ

Адаптивная стратегия корпоративной безопасности

ПРЕДОТВРАЩЕНИЕ 

Security Awareness

Cybersecurity Training

Professional Services

Targeted Solutions

Embedded Security

ПОИСК УГРОЗ

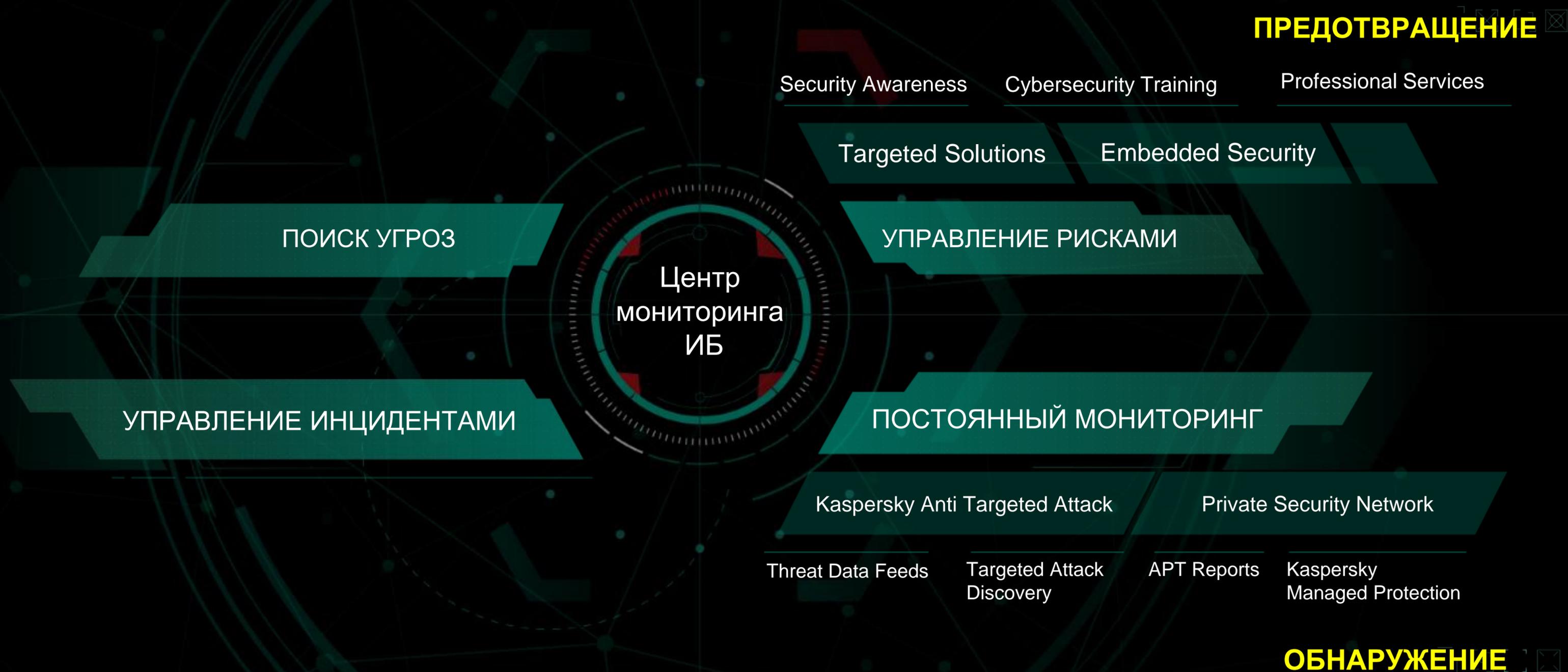
УПРАВЛЕНИЕ РИСКАМИ

Центр
мониторинга
ИБ

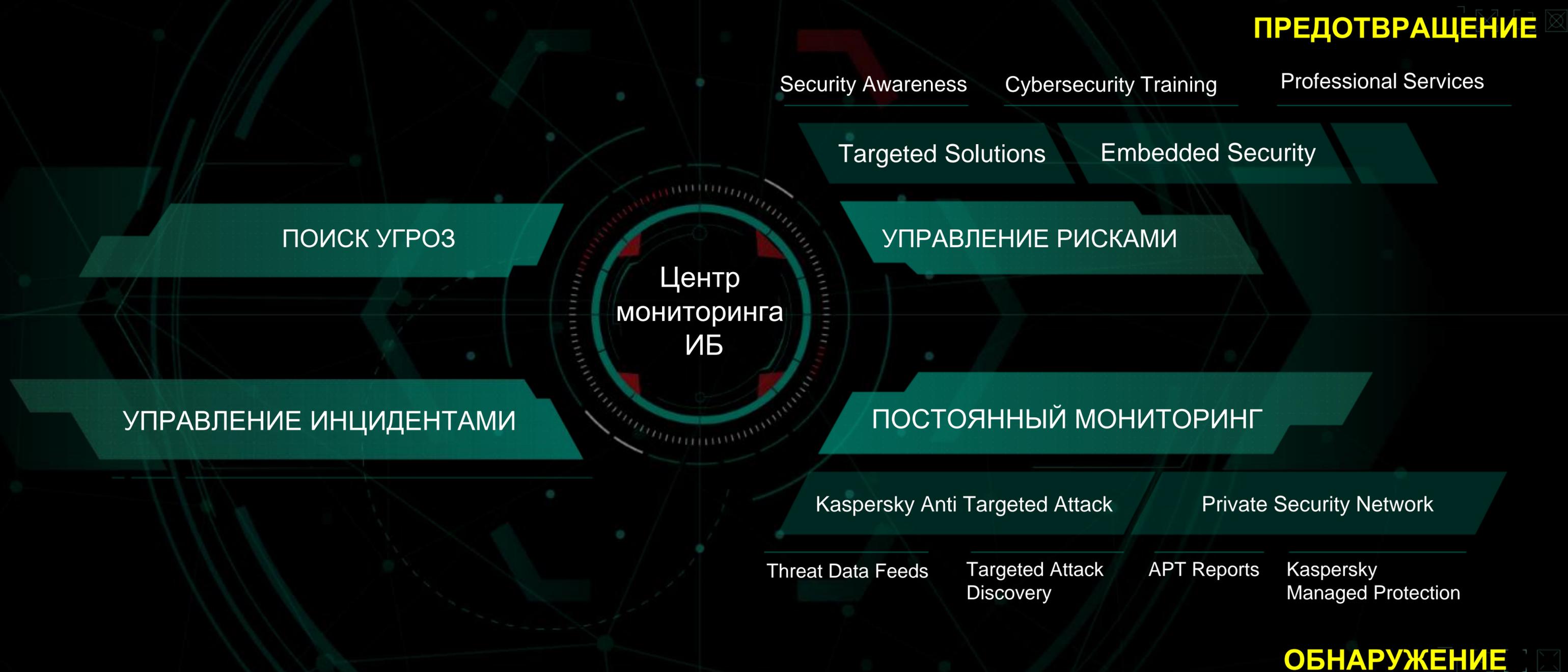
УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

ПОСТОЯННЫЙ МОНИТОРИНГ

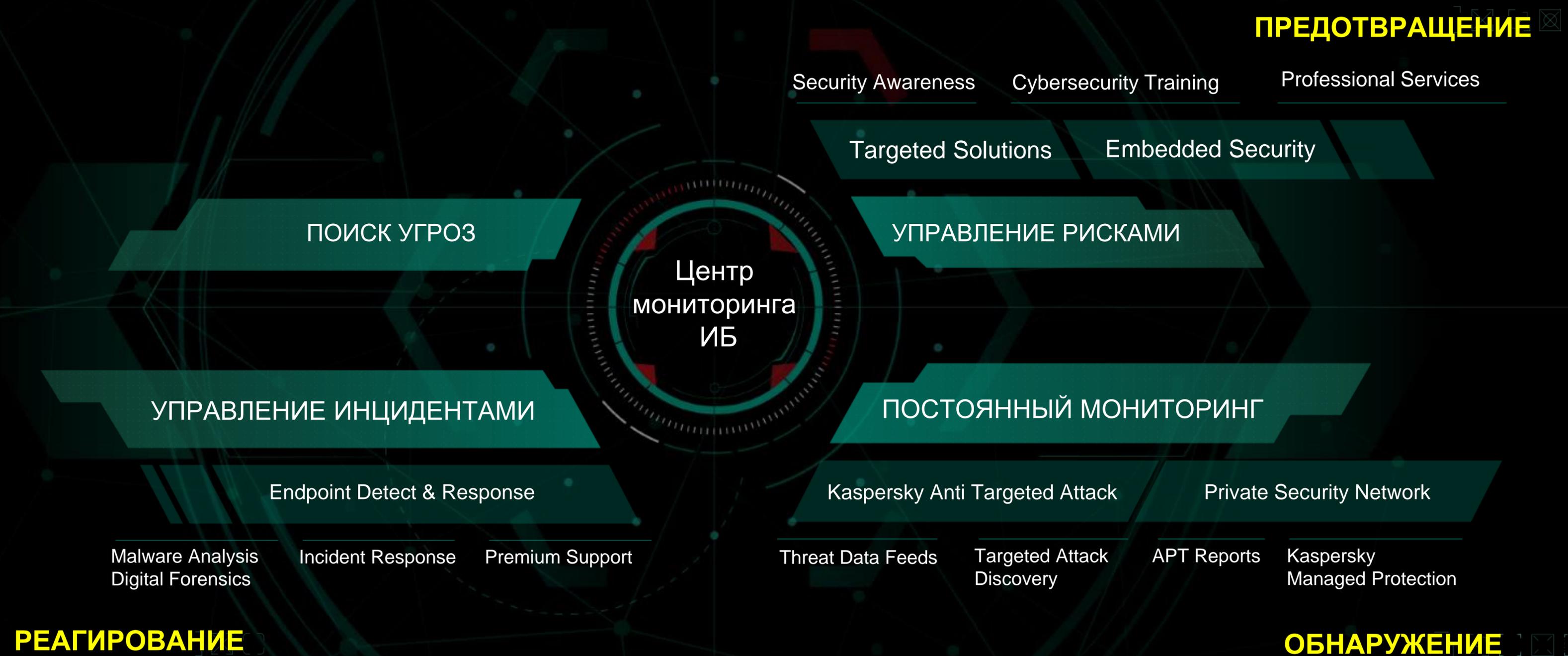
Адаптивная стратегия корпоративной безопасности



Адаптивная стратегия корпоративной безопасности



Адаптивная стратегия корпоративной безопасности



Адаптивная стратегия корпоративной безопасности

ПРОГНОЗИРОВАНИЕ

Security Assessment

Custom Reports

Penetration Testing

Kaspersky Threat Lookup

APT Portal

ПОИСК УГРОЗ

ПРЕДОТВРАЩЕНИЕ

Security Awareness

Cybersecurity Training

Professional Services

Targeted Solutions

Embedded Security

УПРАВЛЕНИЕ РИСКАМИ

Центр
мониторинга
ИБ

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

ПОСТОЯННЫЙ МОНИТОРИНГ

Endpoint Detect & Response

Kaspersky Anti Targeted Attack

Private Security Network

Malware Analysis
Digital Forensics

Incident Response

Premium Support

Threat Data Feeds

Targeted Attack
Discovery

APT Reports

Kaspersky
Managed Protection

РЕАГИРОВАНИЕ

ОБНАРУЖЕНИЕ

СПАСИБО!

KASPERSKY lab