Ключевые угрозы безопасности МФО. Мировые тренды и ситуация в России. Работа Комитета по безопасности СРО «МиР» в 2018-2019 г.г.

Грунтов Антон, директор по безопасности ГК Eqvanta

Председатель комитета по безопасности СРО «МиР»

Москва, 23 мая 2019

Eqvanta — группа компаний, работающих в сфере альтернативных финансов и финансовых технологий

- 3,7 млн клиентов
- 66 млрд руб. выданных займов
- 1,1 млн выпущенных карт
- 3,5 тыс. сотрудников
- №1 на онлайн-рынке

Быстроденьги
на пути к лучшему

РЕШКА
деньги здесь

крупная сеть офисов по выдаче займов наличными

ТУРБОЗАЙМ

онлайн-сервис мгновенных займов на банковские карты

ФИН ПРОТЕКТ

профессиональная служба взыскания

scortech

оценка кредитоспособности клиентов для МФО

Быстрокарта

дистанционные займы на карту компании

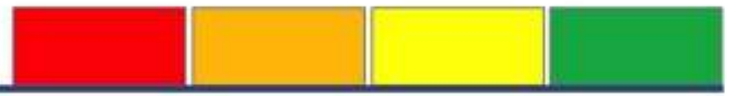
eqvanta

ИБ	Информационная безопасность
ЭБ	Экономическая безопасность
МА	Защита материальных активов

ПРОФИЛЬ РИСКА ПОДНАДЗОРНОЙ ОРГАНИЗАЦИИ

R (ПНО, ПОН, ПОС, ИФ, ККУ)

формирование зон



Дистанционный надзор

- **Показатель уровня несанкционированных операций** — **ПНО**
- **Показатель операционной надежности** — **ПОН**
- **Показатель уровня информационного фона** — **ИФ**

Внешний аудит

- **Показатель оценки соответствия требованиям ГОСТ** — **ПОС**

Инспекционные проверки

- **Показатель качества корпоративного управления** — **ККУ**

Источники

Сейчас

Формы отчетности

Информационный обмен с ФинЦЕРТ (для субъектов НПС)

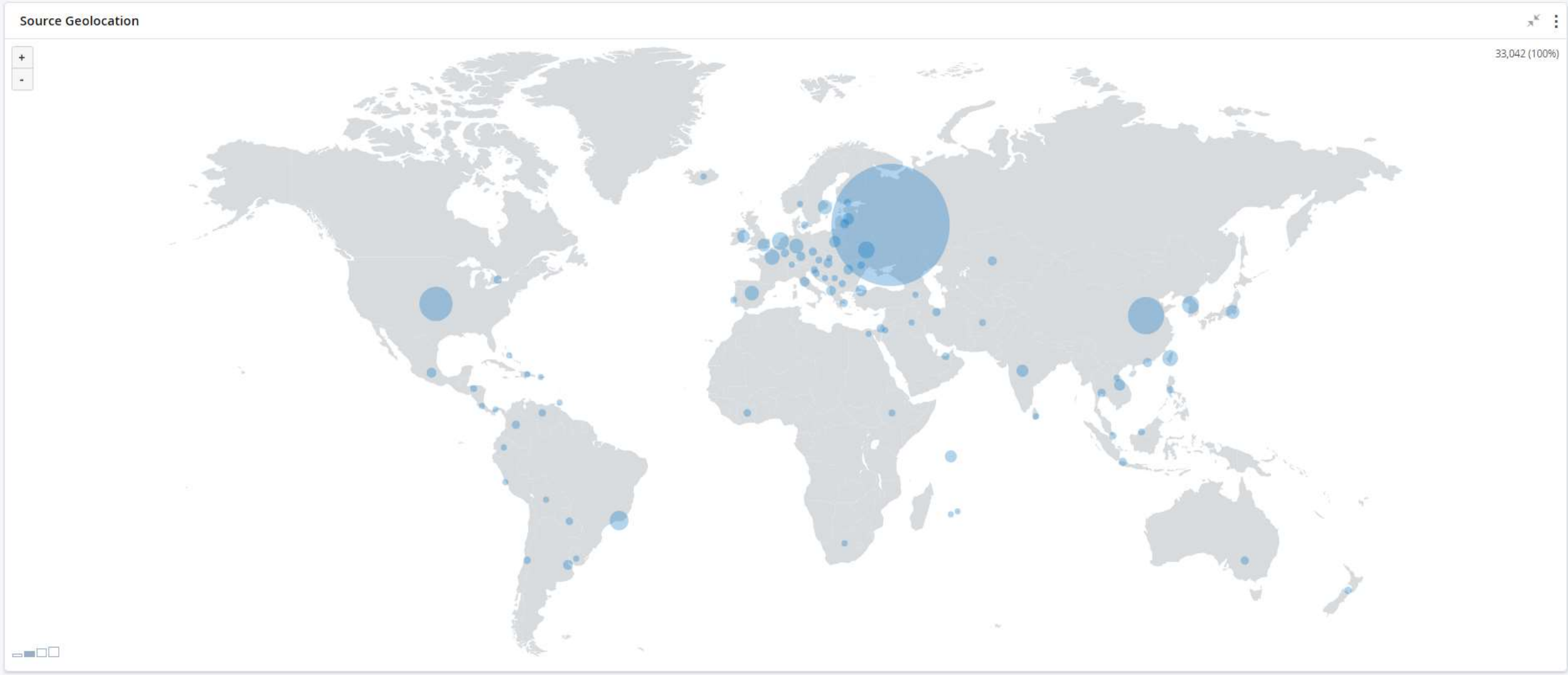
Целевая модель

Сбор исходных данных

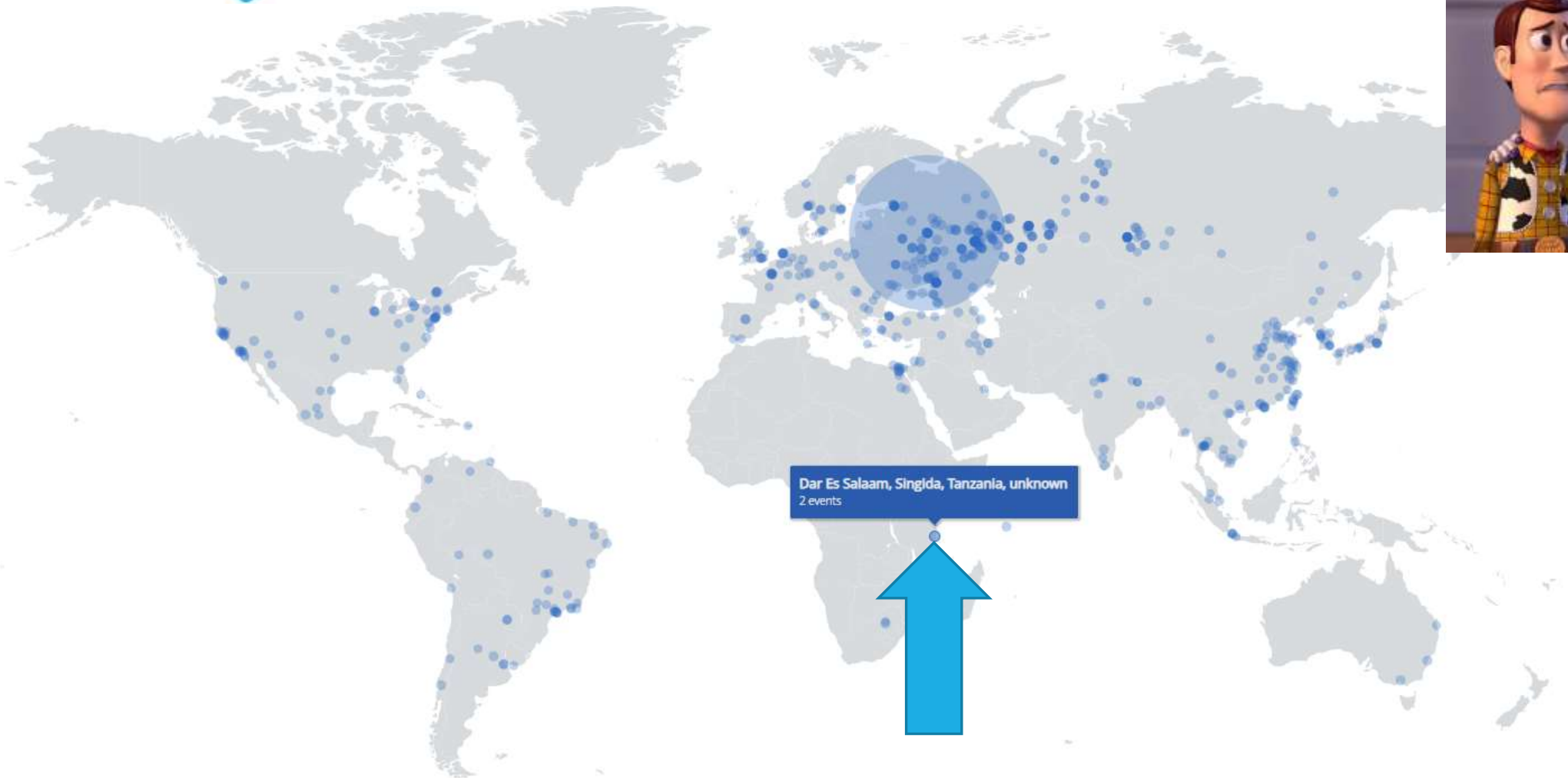
Участие всех субъектов надзора в информационном обмене с ФинЦЕРТ

Применение технологий BigData

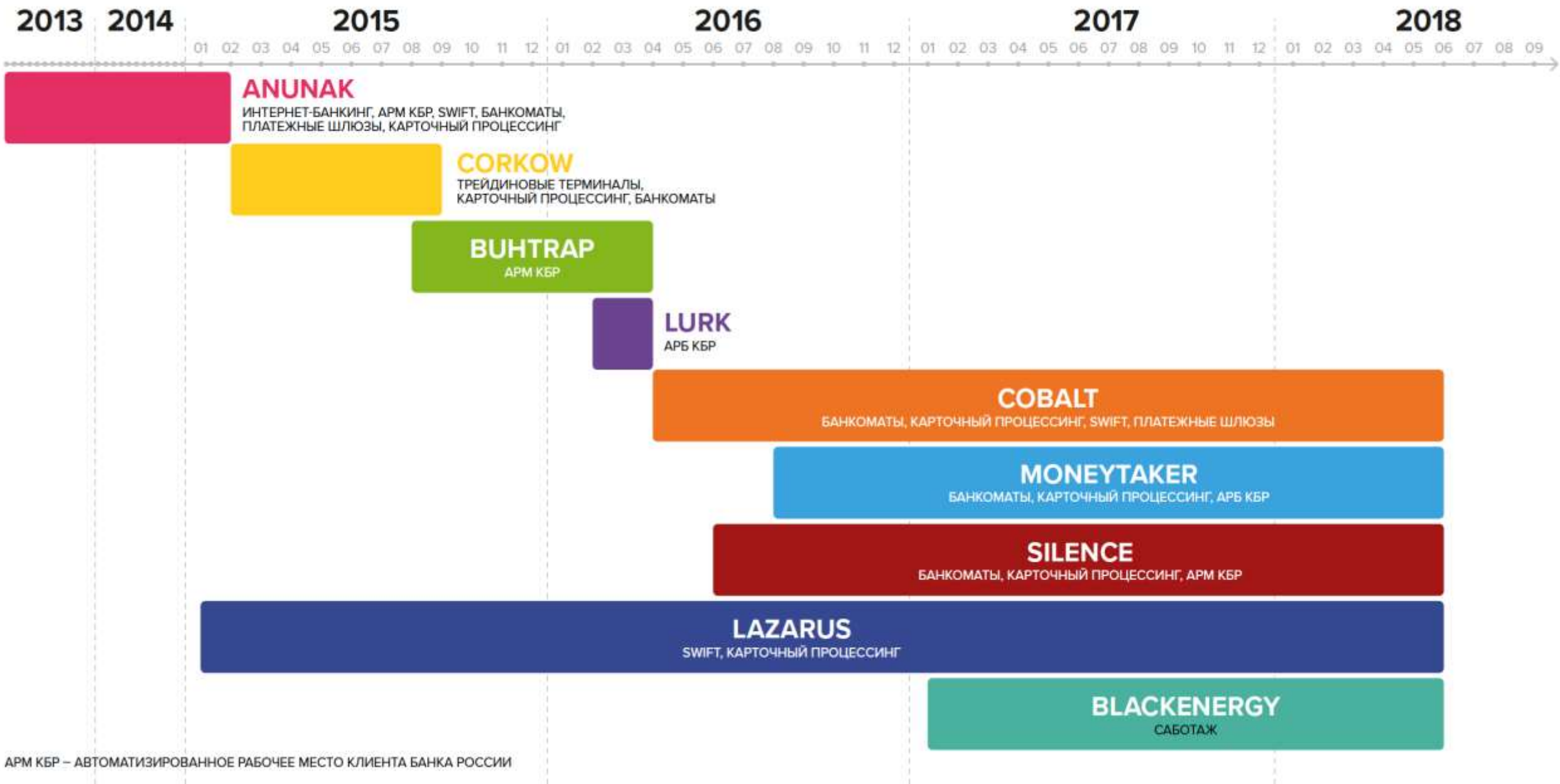
SOC: география источников угроз



Сканирование нашего периметра… повсюду



Зачем из Танзании обращаться в «Быстроденьги»?



АРМ КБР – АВТОМАТИЗИРОВАННОЕ РАБОЧЕЕ МЕСТО КЛИЕНТА БАНКА РОССИИ

США и Латинская Америка	Европа	Юго-Восточная Азия	Ближний Восток и Африка	Россия
APT28 — Russia	Lazarus — North Korea	DarkHotel — North Korea	OilRig — Iran	Equation — USA
Turla — Russia	APT28 — Russia	Lazarus — North Korea	APT37 — North Korea	APT10 — China
Lazarus — North Korea	APT15 — China	Thrip — China	Slingshot — USA	APT17 — China
APT15 — China	Tick — China	APT32 — Vietnam	Newscaster	PlugX — China
Thrip — China	BlackEnergy — Russia	Andariel — North Korea	Team — Iran	Prikormka — Ukraine
Charming Kitten — Iran	Dragonfly — Russia	Mustang Panda — China	APT34 — Iran	APT28 — Russia
Mustang Panda — China	TEMP.Periscope — China	APT37 — North Korea	APT33 — Iran	BlackEnergy — Russia
Dragonfly — Russia	Gorgon Group — Pakistan	Slingshot — USA		PowerPool
Gorgon Group — Pakistan	Orangeworm	Kimsuky — North Korea		
TEMP.Periscope — China	PowerPool	Tick — China		
Newscaster		BlackEnergy — Russia		
Team — Iran		Charming Kitten — Iran		
Orangeworm		APT28 — Russia		
		MuddyWater — Iran		
		Sidewinder — India		
		Chafer — Iran		
		TEMP.Periscope — China		
		APT17 — China		
		Orangeworm		
		Rancor		

Проблемы взаимодействия по линии киберзащиты с МВД в рамках УК РФ

- Слабая компетенция большинства подразделений МВД
- Отставание защитных мер полиции от уровня роста киберугроз
- Отсутствие системы предупредительной работы МВД

Пример с атакой на автодилера

Проблемы взаимодействия с ФССП РФ в рамках 230-ФЗ от 03.07.2016

- Отсутствие легальной возможности проверки персонала коллекторских подразделений на наличие судимостей

Привлечение к взаимодействию с должником лиц, имеющих неснятую или непогашенную судимость за преступления против личности, преступления в сфере экономики или преступления против государственной власти и общественной безопасности, не допускается.

Проблемы противодействия мошенничеству в сфере кредитования с МВД в рамках УК РФ

- Отсутствие возможности **проверки регистрации телефонных номеров** заемщиков (Минкомсвязь и ЦБ)
- **Слабый уровень сервиса** ГУ МВД РФ по вопросам миграции по проверке паспортов
- **Непонимание**, как работать по блокировке мошеннических сайтов, мобильных приложений

Пример с черным майнингом

Противодействие мошенничеству. Заявления по конкретным фактам

- Возбуждение МВД лишь **до 30% уголовных дел** от всех заявлений (Москва и Санкт-Петербург — не более 5%)
- Привлечение к уголовной ответственности **10% преступников**
- Не исполнение приказа МВД России № 196 от 03.04.2018
- Регистрация **заявлений как «Обращение»**, а не в КУСП
- Списание заявлений в **номенклатурное дело**

Проблемы противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма ФС по ФМ в рамках 115 – ФЗ от 07.08.2001

- Сложная интеграция для проверок ЕСИА

Проблемы взаимодействия с Роскомнадзором в рамках 152-ФЗ от 27.07.2006

- Контроль персональных данных происходит **формально**
- По выявленным нарушениям **не принимается действенных мер**
- Это способствует **развитию мошенничества**

Пример с утечкой данных в банке

Проблемы взаимодействия с ЦБ

- **Сложные процедуры** электронного взаимодействия
- **Растущий серый рынок** (уход в тень легальных игроков рынка)
- **Рост технологичного мошенничества** (сайты двойники, мобильные приложения и пр.)

Проблемы взаимодействия со всеми госорганами

- **Несовершенность** российских криптографических средств
- Они требуют **индивидуальных настроек каждого рабочего места**, которые конфликтуют и часто допускают сбои
- Используется **зоопарк софта**
- Проблема там, где российские криптографические средства **интегрируются с американскими браузерами**
- Российская криптография часто бывает **несовместима**. Ключи от КриптоПРО не подходят к ViPNet

Комитет по безопасности СРО «Микрофинансирование и развитие». Итоги:

- Онлайн взаимодействие СБ МФО;
- Информирование через СМИ населения об особенностях работы «серых кредиторов»;
- Создание рабочей группы по борьбе с «серыми кредиторами»;
- Проведение вебинаров для членов СРО;
- Выявление киберуязвимостей и информирование членов СРО;

САМОРЕГУЛИРУЕМАЯ ОРГАНИЗАЦИЯ МИР

Комитет по безопасности СРО «Микрофинансирование и развитие». Итоги:

- Доведение до ЦБ информации о готовности к совместному противодействию «серому» рынку кредитования;
- Участие в конференциях СРО, проведение сессий по безопасности;
- Направление в ГД РФ резолюции о необходимости совершенствования работы правоохранительных органов.

САМОРЕГУЛИРУЕМАЯ ОРГАНИЗАЦИЯ МИР

Ваши вопросы?

Грунтов Антон,
Head of security Eqvanta
agruntov@eqvanta.com