Ростелеком

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Сервисная модель в действии

C-CLOUD@RT.RU

CNEWS: «ИБ в финансовом секторе»

07 июня 2017 г.

ПРОБЛЕМЫ ДАЛЬНЕЙШЕГО РАЗВИТИЯ ИБ

Ростелеком

Постоянный рост числа эксплуатируемых СЗИ
Новая проблема/ИТ-система – новое СЗИ (новый контракт/проект). Высокие сроки поставки. Зависимость от производителя СЗИ. Необходимость прогноза на 3-5 лет. CAPEX.

Необходимость автоматизации ИБ
Реальное управление «зоопарком» СЗИ и документирование ИБ возможно только с существенной автоматизацией процессов

Нехватка квалифицированного персонала
Универсальных специалистов мало, стоят они дорого, постоянная текучка

ИБ не успевает за ИТ
Постоянно меняющаяся инфраструктура. ИТ уходят в облако. Новые угрозы, вектора атак.

Возрастающее реальное влияние кибер-рисков на бизнес (см. слайд 4)
Нужна реальная безопасность, а не только на бумаге.

Enemy Inside. Первый рубеж ~~с~~создан. Необходимо ловить «врага» внутри своей сети
Высокая стоимость собственной 24/7/365 службы мониторинга и расследования инцидентов

КИБЕРУГРОЗЫ В РОССИИ

КОЛИЧЕСТВО АТАК 70+ МЛН В 2016 ГОДУ (ФСБ РОССИИ)

ПРЯМОЙ УЩЕРБ 200+ МЛРД. РУБ.

РОССИЯ В ТОП-3 АТАКУЕМЫХ СТРАН. ОСНОВНЫЕ ВИДЫ ВНЕШНИХ УГРОЗ: DDoS - 30%, FISHING - 50%.

ОСНОВНЫЕ ИНДУСТРИИ В ЗОНЕ РИСКА:

- ФИНАНСОВО-КРЕДИТНАЯ СФЕРА
- ОПЕРАТОРЫ ИТ-СЕРВИСОВ
- ЭНЕРГЕТИКА
- ГОСУДАРСТВЕННЫЙ СЕКТОР
- РИТЕЙЛ
- ПРОМЫШЛЕННОСТЬ

WannaCry

САМОСТОЯТЕЛЬНАЯ ЗАЩИТА

- Стоимость решения **20+ МЛН. РУБ.**
- Актуализация защиты **РАЗ В ГОД**
- **НЕПРОГНОЗИРУЕМЫЕ** ресурсы поддержки
- Безопасность компании в руках **ОДНОГО ЧЕЛОВЕКА**
- **НЕУВЕРЕННОСТЬ** в актуальности киберзащиты

ИБ - КАК СЕРВИС ОПЕРАТОРА СВЯЗИ

КОМПЛЕМЕНТАРНОСТЬ С ДРУГИМИ СЕРВИСАМИ ОПЕРАТОРА

ПРОФЕССИОНАЛЬНЫЕ ГАРАНТИИ В РАМКАХ SLA

ЭКОНОМИЯ И ЭФФЕКТИВНОЕ УПРАВЛЕНИЕ ЗАТРАТАМИ

MSSP: ЕДИНЫЙ КОМПЛЕКСНЫЙ ПОСТАВЩИК КИБЕРБЕЗОПАСНОСТИ

СЕРВИСЫ ИБ ОТ РОСТЕЛЕКОМ

Ростелеком

TelcoCloud

Виртуальная сетевая инфраструктура СЗИ

АнтиDDOS

до 160ГБит/сек

SOC - Центр кибербезопасности

Security Awareness

Повышение осведомленности в ИБ

Compliance

Соответствие требованиям (ПДн, ГИС, СТО БР ИББС…)

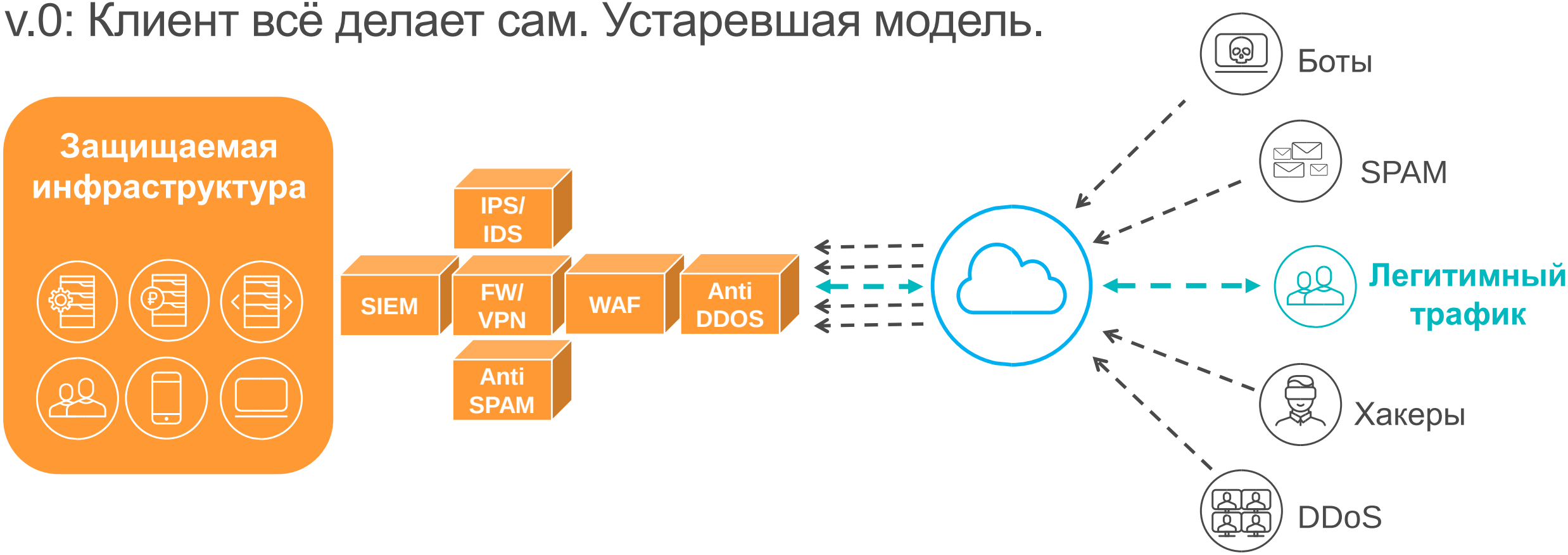
Ростелеком

ПРЕДОСТАВЛЕНИЕ СЕРВИСОВ ИБ ИЗ ОБЛАКА (РТК MSSP)

Managed Security Services Provider/
Провайдер управляемых сервисов безопасности

ТРАДИЦИОННЫЙ ПОДХОД К ИБ

v.0: Клиент всё делает сам. Устаревшая модель.



Сегмент ИС Клиента | Сеть провайдера | Интернет

MSSP: TELCOCLOUD+SOC

v.1: Дата-центр остается у клиента.

Защитой инфраструктуры занимается оператор.

Сегмент ИС Клиента | Сеть провайдера | Интернет

MSSP: ВЦОД+TELCOCLOUD+SOC

v.2: Дата-центр переезжает в ВЦОД оператора.

Оператор предоставляет инфраструктуру и её защиту

Сегмент ИС Клиента | Сеть провайдера | Интернет

Ростелеком

МОНИТОРИНГ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИБ (РТК SOC)

Security Operation Center/
Оперативный центр мониторинга информационной безопасности

ПОДРОБНЕЕ ПРО SOC

СБОР СОБЫТИЙ

- SIEM
- FW
- IPS/IDS
- WAF
- VPN
- AV
- Anti DDoS
- Vulnerability scanners/management
- SandBox
- Сканеры кода

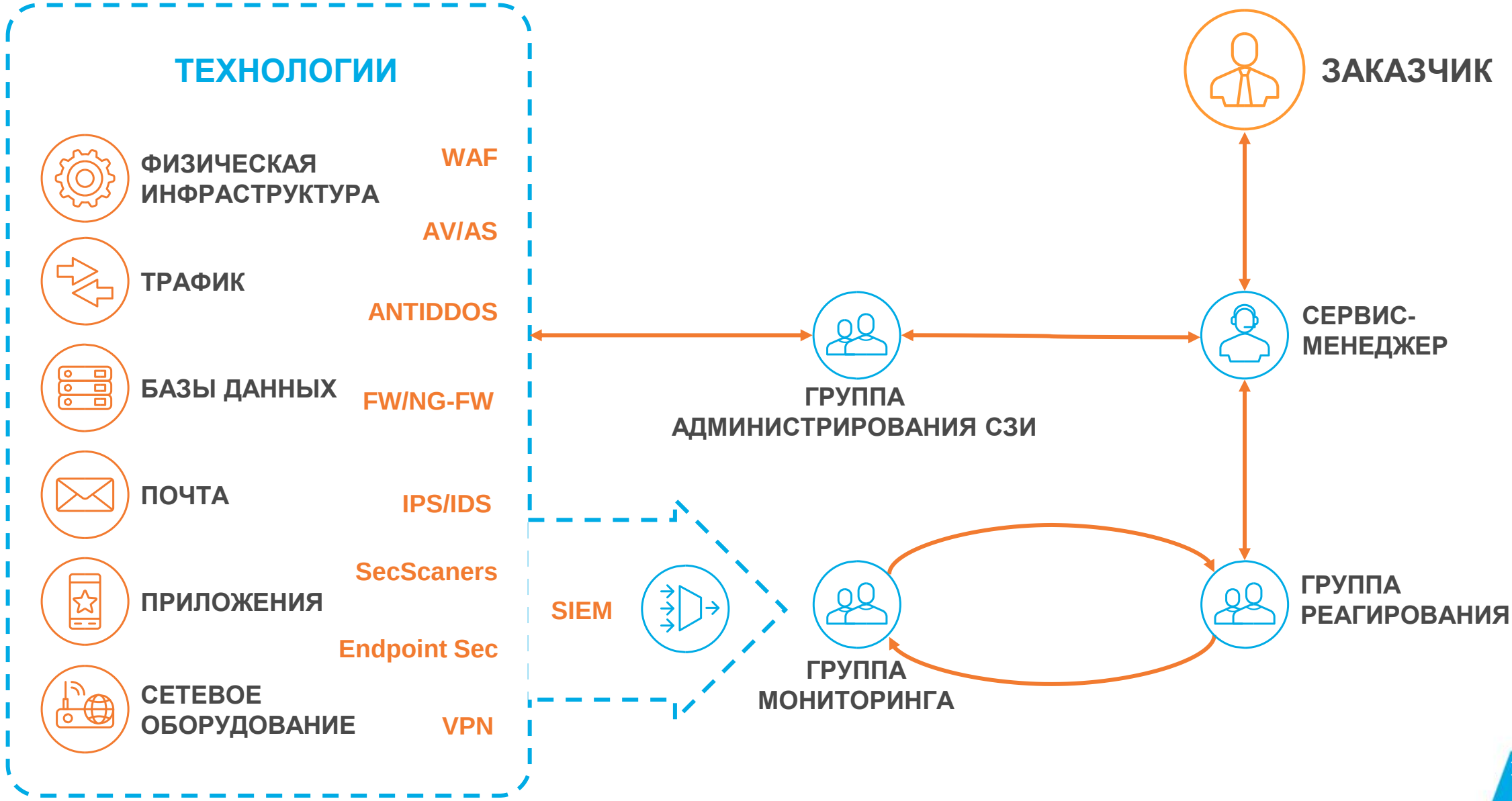
АНАЛИЗ СОБЫТИЙ

- мониторинг поступающих событий безопасности в режиме 24x7x365;
- обработка входящих данных и выделение инцидентов;
- мониторинг работоспособности подключенных услуг по обеспечению информационной безопасности;
- сбор необходимых данных для обработки инцидента;
- уведомление Заказчика об инциденте.

РЕАКЦИЯ НА ОБНАРУЖЕННЫЕ ИНЦИДЕНТЫ

- анализ инцидентов на основании информации, поступившей из разных источников
- определение информационных активов, пострадавших в результате инцидентов ИБ
- координация устранения инцидента в рамках всех оказываемых услуг
- принятие необходимых мер для устранения инцидента

SOC: ТЕХНОЛОГИИ-ПРОЦЕССЫ-ЛЮДИ



Ростелеком

Мониторинг трафика и защита от DDOS-атак

Distributed Denial Of Service Protection /
Защита от распределенных атак типа
«отказ в обслуживании»

http://moscow.rt.ru/b2b/internet/protection

АНТИ-DDOS: КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА

Масштаб
Крупнейшая в Восточной Европе инсталляция защитного комплекса Arbor Peakflow дает возможность отразить атаки различной мощности, продолжительности и типов.

Эффективность
Атаки до 160 Гбит/с
Услуга защиты от DDoS-атак позволяет отражать атаки мощностью до 5 Тбит/с на границе сети и до 160 Гбит/с на уровне приложений — мощнее любой из зарегистрированных атак.

Гибкие тарифы
Тарифы на услугу основаны только на пропускной способности защищаемого канала. Стоимость услуги не зависит от количества и мощности атак.

Ресурсы
Ростелеком располагает самой большой в СНГ командой профессиональных сертифицированных инженеров, которые оперативно выявляют DDoS-атаки и противодействуют им.

Квалификация
Инженеры Ростелеком имеют колоссальный опыт отражения атак мощностью более 200 Гбит/с. Нашу защиту используют крупнейшие государственные и коммерческие ресурсы.

Портал статистики
Предоставляет доступ к информации о текущем состоянии трафика, возникновении атак, их параметрах; позволяет выгружать итоговый отчет для дальнейшего расследования.

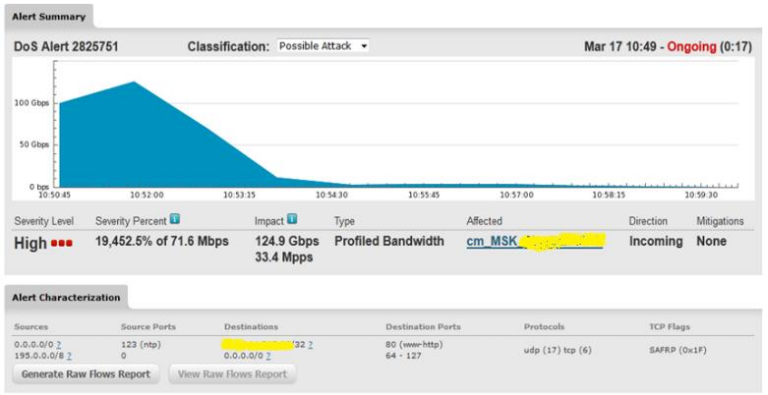
Предоставление статистики (порты, протоколы), DDOS-on-Demand*

Уже используют: банки, страховые организации, госкорпорации, государственные учреждения

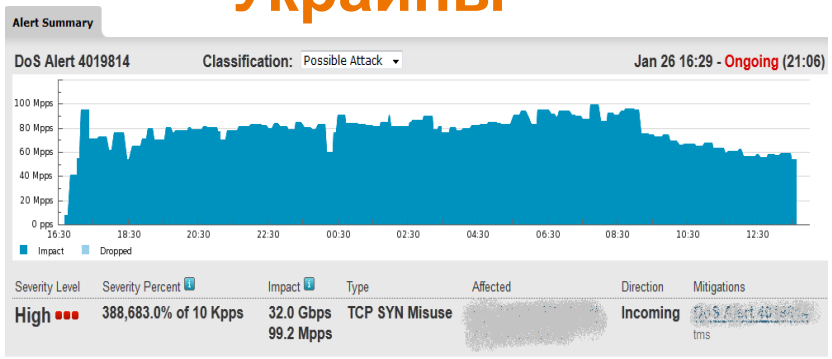
* - будут доступны в ближайшем будущем

ОТРАЖЕННЫЕ АТАКИ (PUBLIC REFERENCE)

33,4 Mpps
124,9 Gbps
олимпиада в Сочи



99,2 Mpps
32 Gbps
активизация военных действий на востоке Украины



3,2 Mpps
атака на 5 крупнейших банков РФ, декабрь 2016

2014 | 2015 | 2016

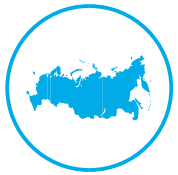
ПОЧЕМУ СЕРВИСЫ ИБ ОТ РОСТЕЛЕКОМ

Аттестованная Национальная облачная платформа

Размещение ГИС (до К1), ИСПДН (до УЗ-1) и 1Г по РД ГТК

Защищенный канал передачи (в т.ч. ГОСТ VPN)

С-Терра (в т.ч. виртуальный шлюз), ViPNet, Континент



Инфраструктура от Калининграда до Владивостока

Возможность сбора собственных FEED и наполнение базы индикаторов компрометации (IOC).

Группы мониторинга, расследования и реагирования, администрирования СЗИ (24/7/365) (*InHouse*)

35 человек в SOC. Более 100 в ИБ. Постоянное развитие и рост.

Успешные реализованные проекты

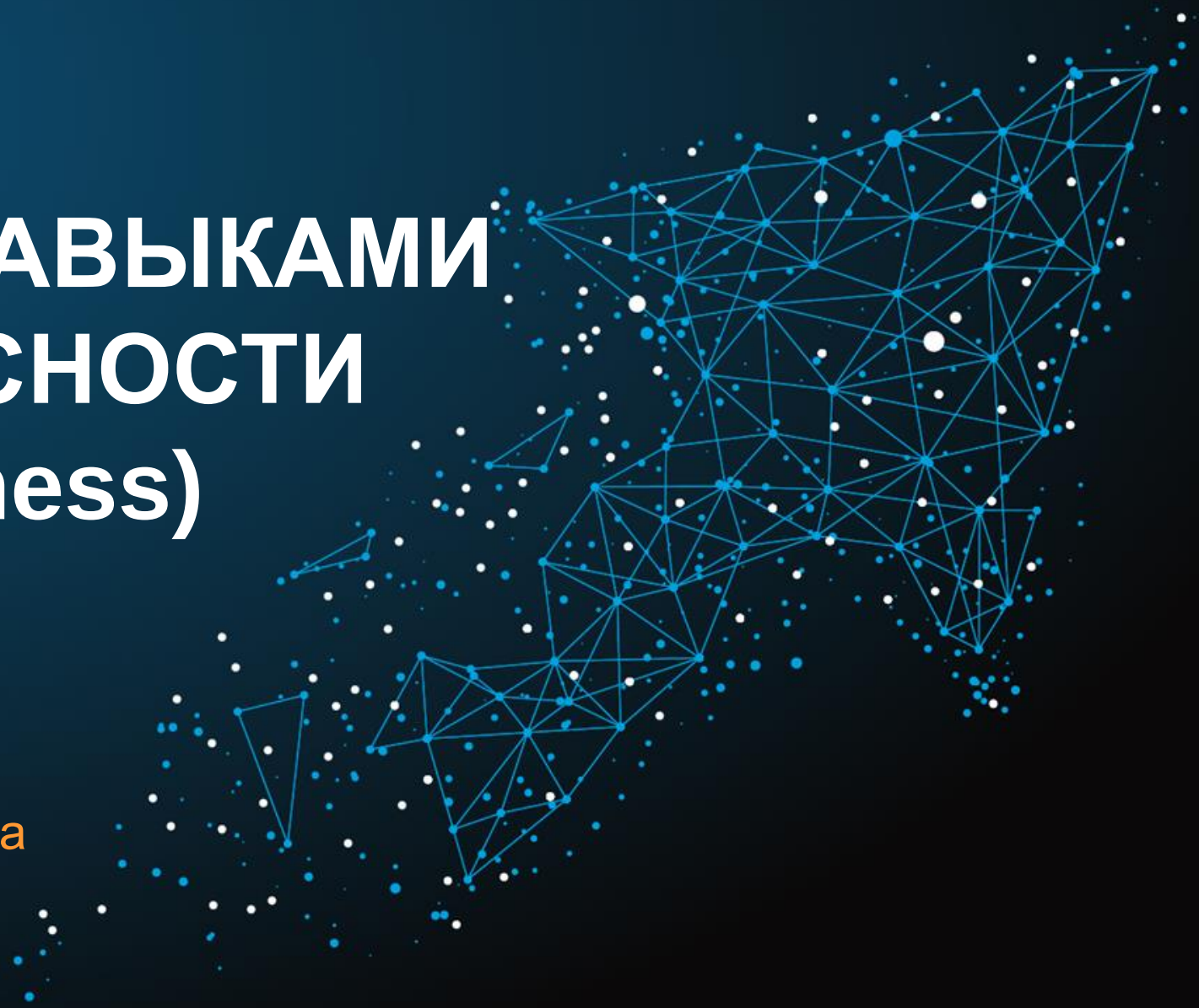
Более 5 лет на страже ЭП, Госуслуги, Клиенты НОП, SOC, антиDDOS

Переложите ответственность за обеспечение безопасности на Ростелеком

Поручение обеспечения безопасности ПДн, ГИС Ростелекому.

Ростелеком

УПРАВЛЕНИЕ НАВЫКАМИ КИБЕРБЕЗОПАСНОСТИ (Security Awareness)



Повышение осведомленности персонала в области ИБ.
Постоянный контроль, фокусировка и актуализация.

СОСТАВ ПРЕДЛАГАЕМОГО СЕРВИСА

ПЕРВИЧНОЕ ТЕСТИРОВАНИЕ И СТАТИСТИКА

Предоставление отчёта по уязвимостям пользовательского программного обеспечения, которые идентифицируются в результате действий персонала во время тестирования и могут эксплуатироваться злоумышленником для развития атаки

ПЛАНИРОВАНИЕ И ОБУЧЕНИЕ

Согласование значимых действий с выделенными сотрудниками заказчика, обучение навыкам работы с платформой повышения осведомленности

АКТУАЛИЗАЦИЯ

Ежемесячная разработка четырех шаблонов имитации атак на пользователей с учётом особенностей и должностных обязанностей каждой группы тестируемых пользователей

ПОДДЕРЖКА

Автоматизация и поддержка процесса дистанционного обучения и тестирования навыков выбранных групп пользователей с учётом изменений, происходящих в организации

ОТЧЕТНОСТЬ

Предоставление ежемесячной отчётности по текущему уровню навыков персонала и их изменениям с учётом предыдущих периодов

Ростелеком

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ (Compliance)

Платформа оценки, контроля и управления соответствием требованиям регуляторов в области ИБ (ПДн, ГИС, СТО БР, ОТИ)


Ростелеком
С НАМИ НАДЁЖНО!
C-CLOUD@RT.RU