SCS SBERBANK CYBER SECURITY

Коллаборация, информационное взаимодействия крупных корпоративных, государственных и сервисных SOCов

Исполнительный директор -
Начальник отдела реагирования на киберугрозы
Лесной Василий Геннадьевич

Мировой опыт классификация SOC*

* MITRE

Национальный SOC (mega-SOC) (50,000,000+ users/IPs**)**

Распределенный SOC (500,000 users/IPs)

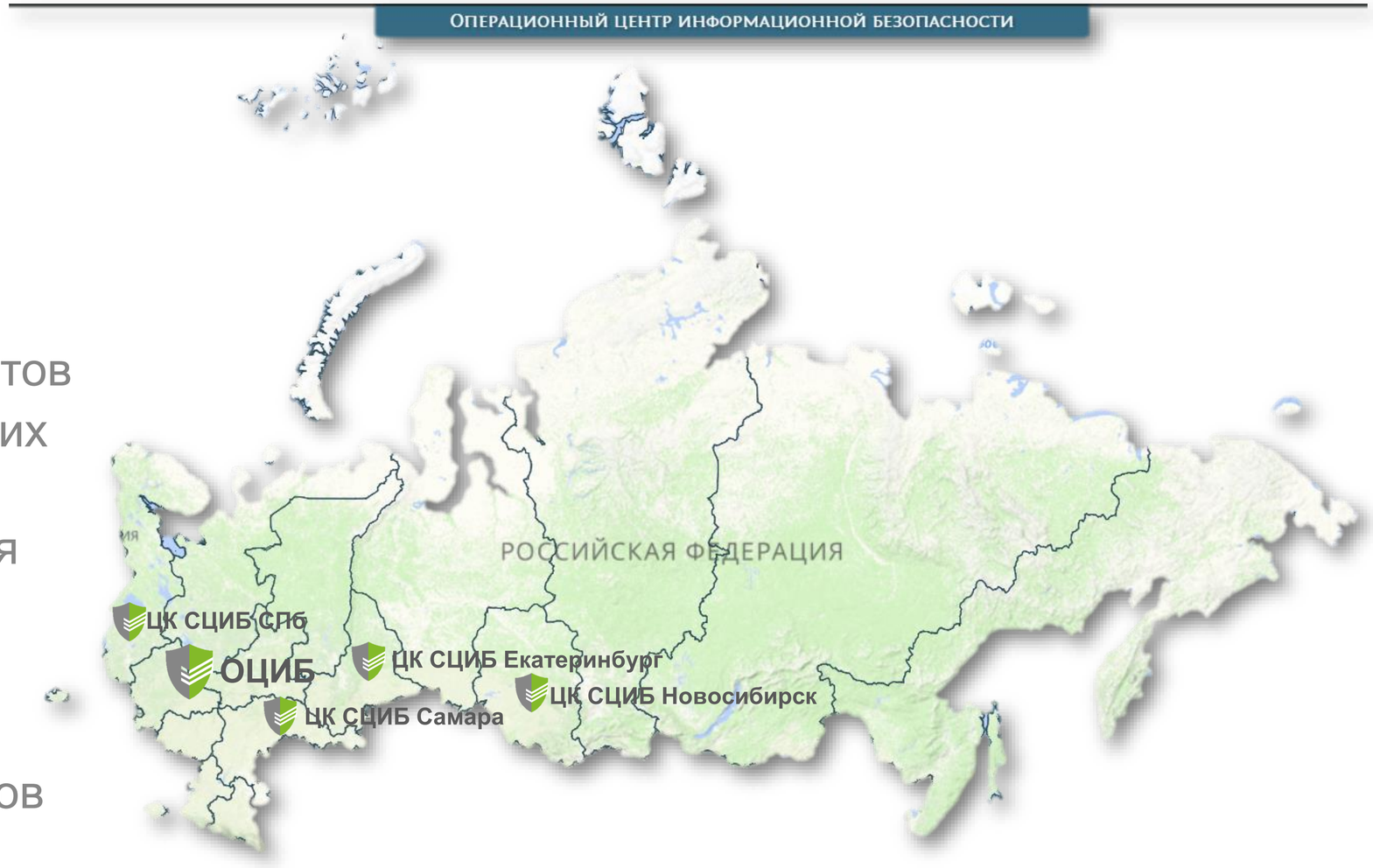
Большой SOC (50,000 users/IPs)

Маленький SOC (10,000 users/IPs)

Виртуальный SOC (1,000 users/IPs)

Распределенный СОК в действии

12 территориальных банков
50+ значимых дочерних зависимых организаций
17 000+ офисов обслуживания клиентов
350 000+ автоматизированных рабочих мест
75 000+ устройств самообслуживания
35 000+ серверов
40 000+ мобильных устройств
1 200+ автоматизированных систем
500 000+ учётных записей сотрудников



Характеристика SOC

Security Operation Center

30+ систем и технологий защиты

100 000+ средств защиты

3 000 000 000+ событий в день

300+ подозрений на инцидент в день

50+ источников данных аналитики

150+ анализируемых угроз в день

500 000+ элементов инф-ры

200 000+ уязвимостей в месяц

70+ мощных DDoS атак в год

2000+ заявок на доступ в день

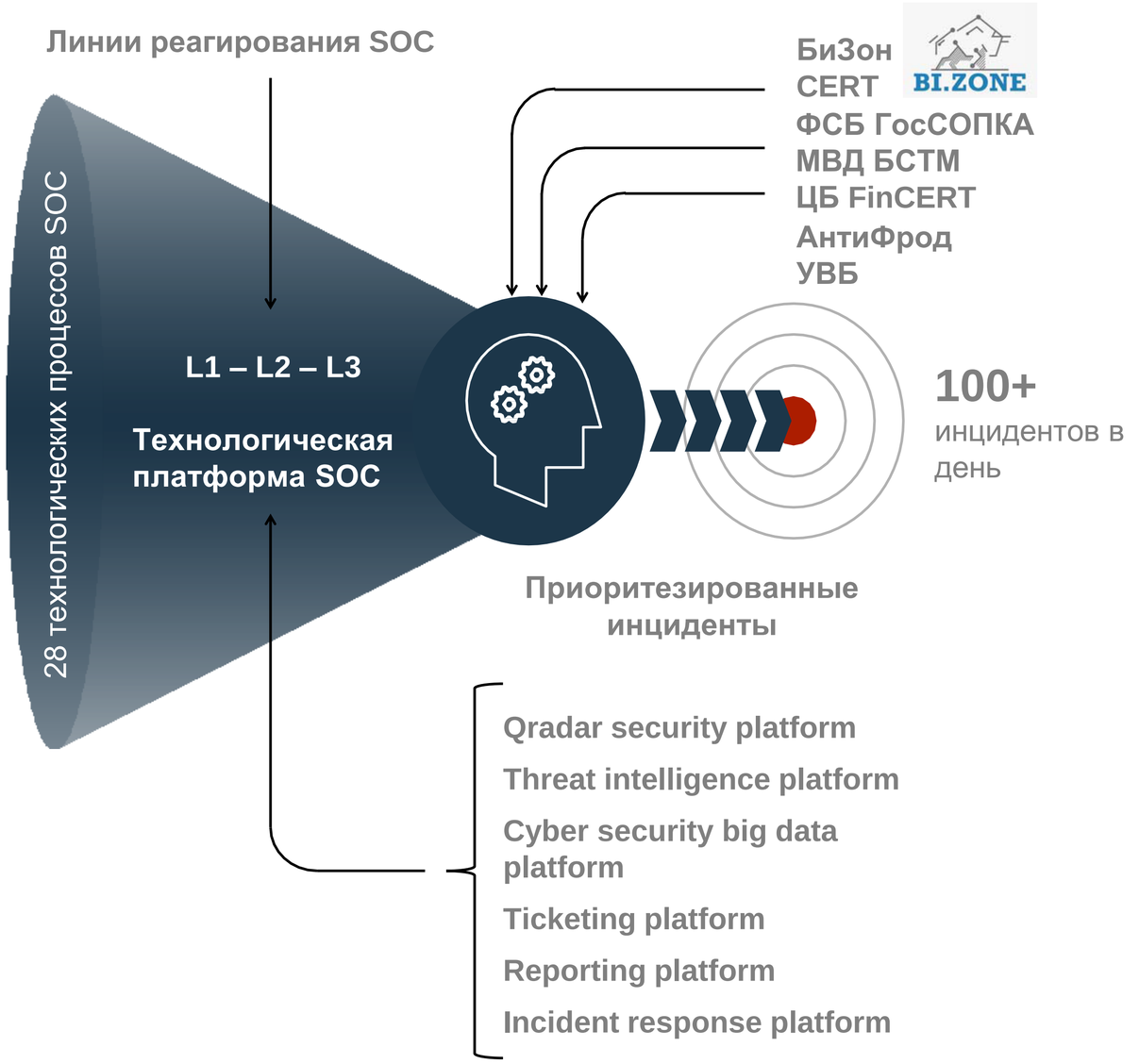
ГРУППА СОПРОВОЖДЕНИЯ СРЕДСТВ ЗАЩИТЫ

ГРУППА РЕАГИРОВАНИЯ НА КИБЕРУГРОЗЫ «CSIRT»

ГРУППА ЭКСПЕРТИЗЫ КИБЕРУГРОЗ «THREAT INTELLIGENCE

ГРУППА ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ «RED TEAM»

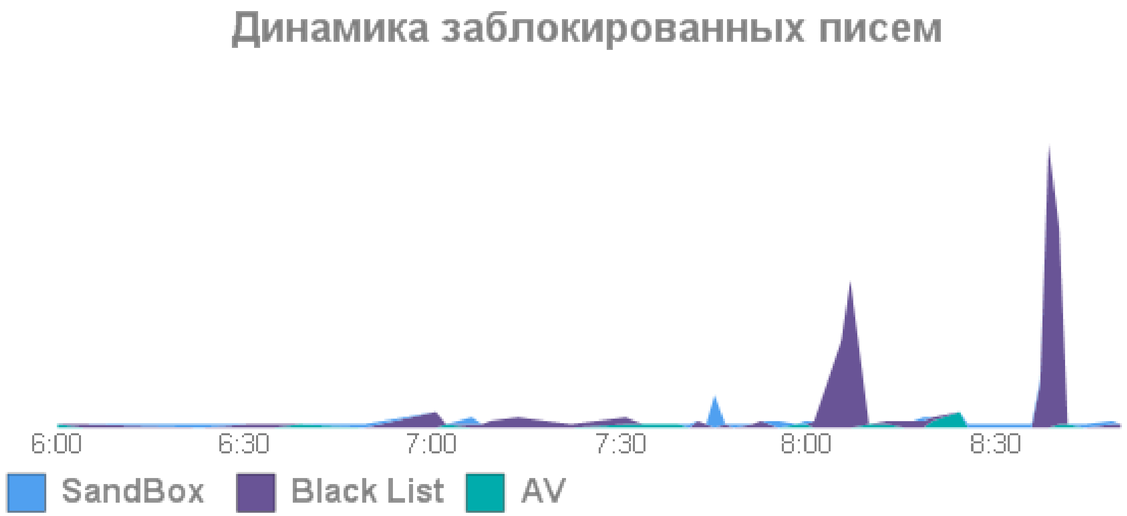
4 РЕГИОНАЛЬНЫХ ЦЕНТРА КОМПЕТЕНЦИЙ



Коллаборация в SOC Сбербанка

В своей деятельности сотрудники взаимодействуют не только между собой, но и другими организациями

Результаты обмена информацией между заинтересованными сторонами хорошо прослеживаются в проактивном реагировании

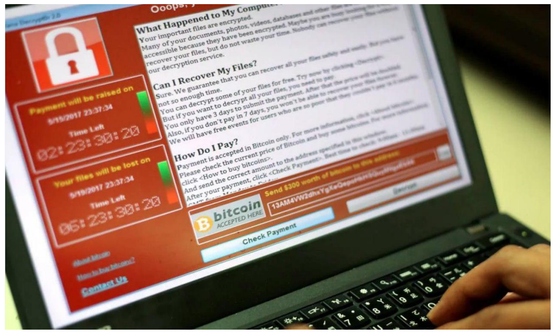


Обмен информацией помогает проактивно реагировать на вредоносные рассылки, что хорошо отслеживается на рабочем дашборде, где большинство рассылок с ВПО отсекаются по black list

Что было?

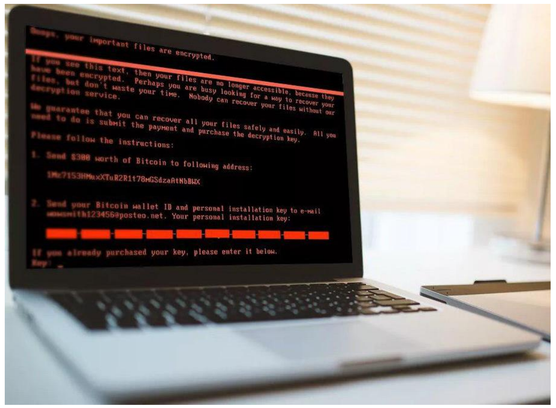
WannaCry в мае 2017

Первое оповещение через 2 дня после начала атаки!



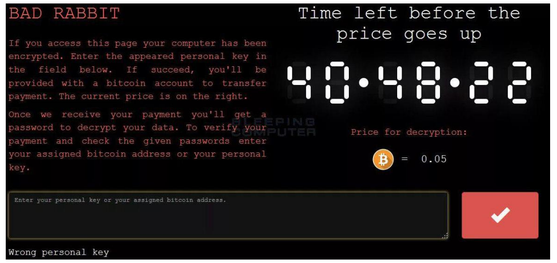
NotPetya в июне 2017

Оповещение через 1 день, с уточнениями еще через день



BadRabbit в октябре 2017

Оповещение через 1 день, с уточнениями еще через день



2018 - Что дальше?

Появление во внешних источниках информации о хакерской атаке на агентство Интерфакс

Threat intell. (TI) Анализ угрозы для Банка

Threat intell. (TI) Идентификация способа осуществления атаки и определение идент. компрометации

Направление дополнительных экземпляров вредоносного ПО

Неофициальные каналы обмена информацией

СМИ

Создание инцидента о потенциальной угрозе

Анализ и категоризация инцидента

Анализ экземпляров вредоносного ПО и определение идент. компрометации

Принятие решения о блокировке ЭДО с Интерфакс

Блокировка ЭДО с Интерфакс

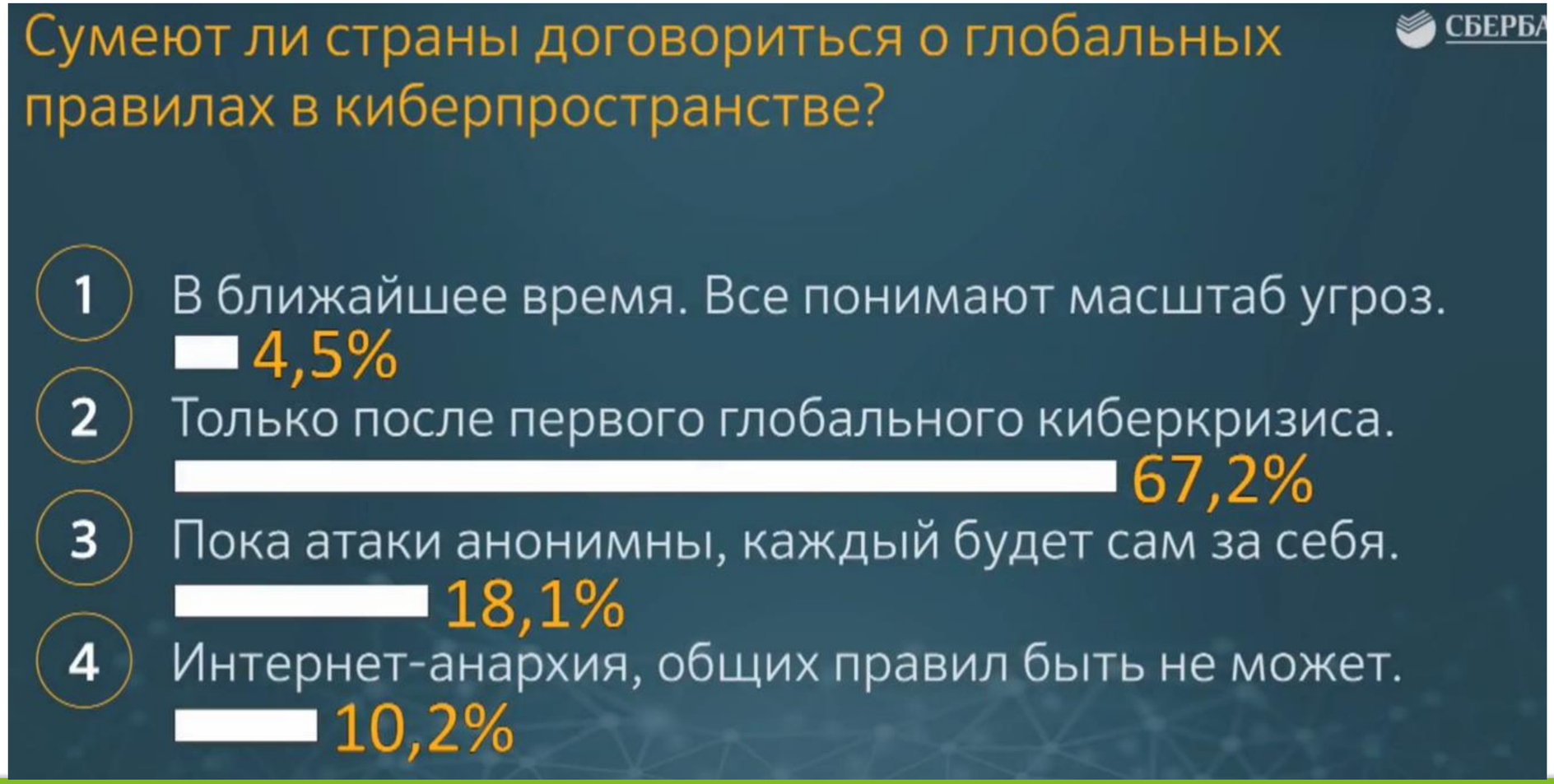
Блокировка идент. компрометации

Передача в региональные центры для блокировки

Ни одного централизованного источника информации

Сможем ли договорится?

Результаты опроса, проведенного на Международном конгрессе по кибербезопасности 5-6 июля показали, что никто не осознает масштабы угрозы.



Единая платформа обмена

Количество инцидентов

10

100

10^3

10^9

ГОСУДАРСТВЕННЫЕ ИНСТИТУТЫ

Обмен информацией

Создание Fusion Centre на уровне ассоциации?

FC FC FC

Промышленность Коммерция

Банки Финансы

ИТ операторы связи

SOC SOC SOC

Sberbank SOC

SOC SOC

SOC SOC SOC

Резюме

- «…Масштабы киберугроз сегодня таковы, что нейтрализовать их можно только вместе…»

  В. В. Путин

- Не важна принадлежность SOC – важен профессионализм!

- Что бы получать информацию нужно делиться своей. Важно доверие! Достижимо ли это? А вы готовы?

СПАСИБО
ЗА ВНИМАНИЕ

SCS SBERBANK CYBER SECURITY