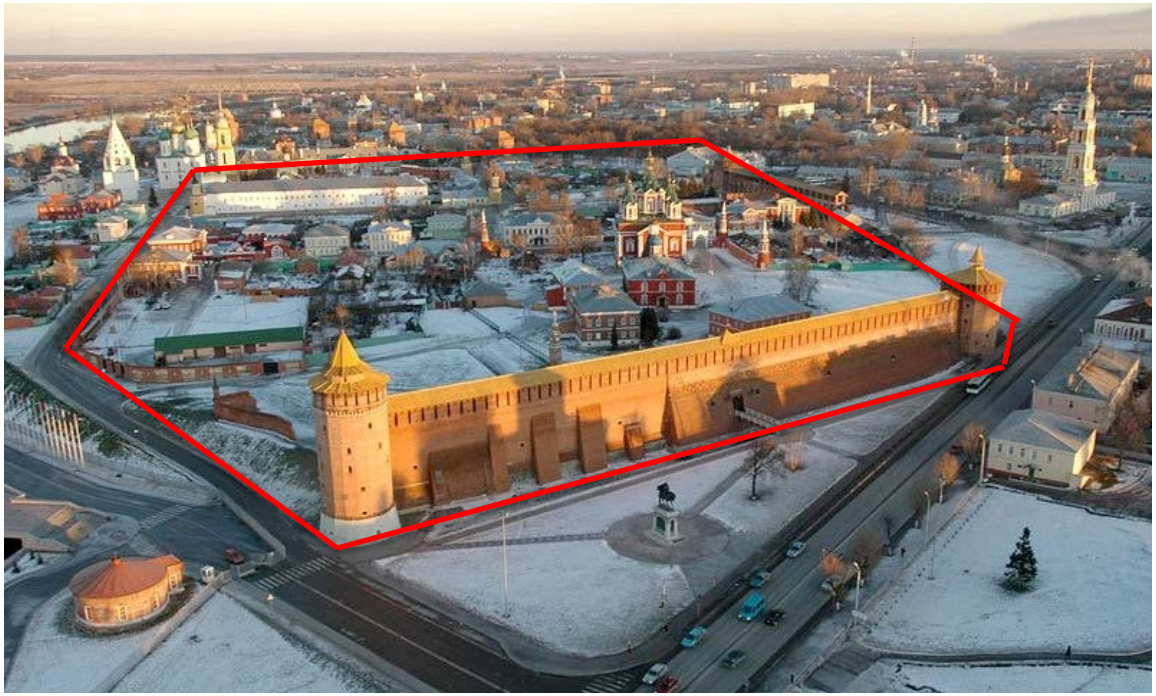
Опыт аутсорсинга SOC

Tinkoff.ru

Июнь, 2017

Много, очень много всего…

- Определяем приоритет того, что для нас важно:
  - Концентрируемся
  - Разбираем на кусочки
  - Создаем границы объекта



Тинькофф

Аудит Бизнес-систем

Tinkoff.ru

Сбор информации

- Собираем встречу с ответственными за систему
  - Документация
  - Ценность и критичность
  - Состав системы (сети, сервера)
  - Интеграции

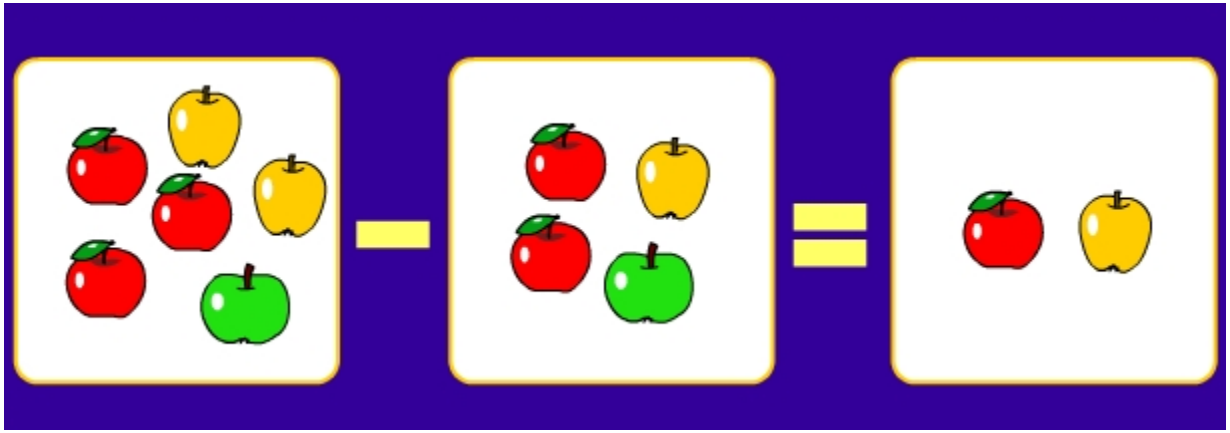
- После встречи изучение:
  - Документации по проекту
  - Бизнес-логики систем
  - Расположение систем и задействованных сегментов

Инвентаризация и поиск уязвимостей

- Сканируем все сети бизнес-системы
  - Составляем список доступных сервисов
    - Ищем уязвимости
    - Делаем классификацию уязвимостей
  - Изучаем доступность найденных сервисов
    - Оцениваем риски (доступность сервисов + уязвимости за ними)
  - Изучаем веб-сервисы
    - Уязвимости веб-приложений
    - Уязвимость взаимодействия с прикладными протоколами
  - Изучение кода (при наличии)
- Оценка архитектуры
  - Отказоустойчивость
  - Разделение системы на прод, предпрод и тест
- Роли пользователей

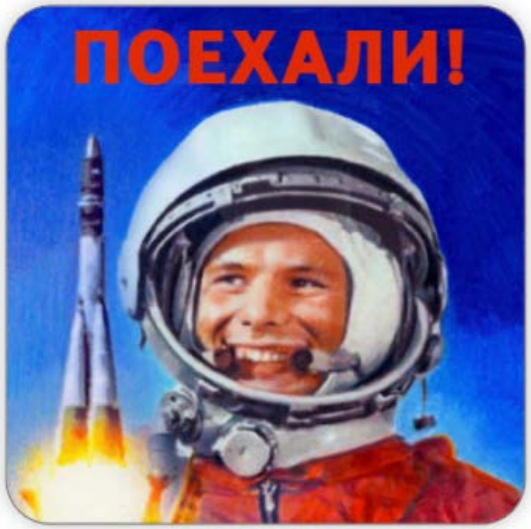
Устранение недостатков

- «Сбор информации» – «Независимая инвентаризация» = Нужно разбираться!
  - Уточняем у владельца системы о разночтении
  - Владелец системы устраняет замечания
- Повторяем процесс инвентаризации



Настройка систем безопасности

- Почти эталонная модель бизнес-системы получена. Но не хватает средств защиты. Расставляем:
  - Антивирусы
  - Настраиваем логи для передачи в SIEM
  - WAF
  - Песочницы
  - и тд
- Оптимизируем профиль средств защиты. Уменьшаем количество false-positive
- Настраиваем передачу данных на SIEM
- Все! К старту готов!



Тинькофф

Передача системы в SOC

Tinkoff.ru

Подготовка к передаче

- Совместно с JSOC определяем правила игры. Определяем:
  - Сценарий (на что реагируем, список источников, кому отправлять оповещение)
  - Критичность события
  - Реакцию на событие
- Подключаем источники к SIEM
- Делаем тестовый прогон сценариев
- Отдаем на реагирование в SOC

Общие итоги совместной работы за 2017 год

Текущие показатели услуги мониторинга JSOC:

	По состоянию на 31.12.17	Динамика за год
1 Контролируемые источники в режиме 24x7	**198 источников** (серверы/АРМ/СЗИ/сетевое оборудование) в мониторинге 24x7	**+ 154 источника**
2 Сценарии мониторинга	Запущено **43 сценария**, из них **4 без участия 1-й линии** (для улучшения оперативности)	**+ 10 сценариев**

3 Результаты мониторинга и расследования

За 2017 год в JSOC зарегистрировано **5888 подозрений на инциденты**, из них:

- **2266 (38%) подозрение слинковано** к ранее регистрируемым
- **742 (13%) подозрений отфильтровано** силами JSOC (как False Positive)
- **2880 (49%) уведомления отправлено** в Тинькофф Банк:
  - **из них 1026 (35,6%) инцидентов подтверждено** со стороны Тинькофф Банка

Основные типы инцидентов за ½ 2017 год

Несанкционированный доступ к ИС и сервисам

- Выявлены **попытки несанкционированного доступа к внешним ресурсам** по протоколам удаленного администрирования (хостинги, ftp-серверы, репозитарии и пр.)
- Регулярное **выявление повышенной активности из сети TOR** к внешним ресурсам Банка.

Использование нелегитимного ПО

- Выявлены **случаи несанкционированного использования средств удаленного управления** типа TeamViewer, VNC, DameWare во внутренних сегментах сети банка
- Зафиксированы **факты обращений к узлам сети TOR** из внутренних подсетей

Сетевые атаки

- Выявление работ по:
  - **пентестам**,
  - **сканирования из VPN-туннеля подрядчика**

Основные типы инцидентов за ½ 2017 год

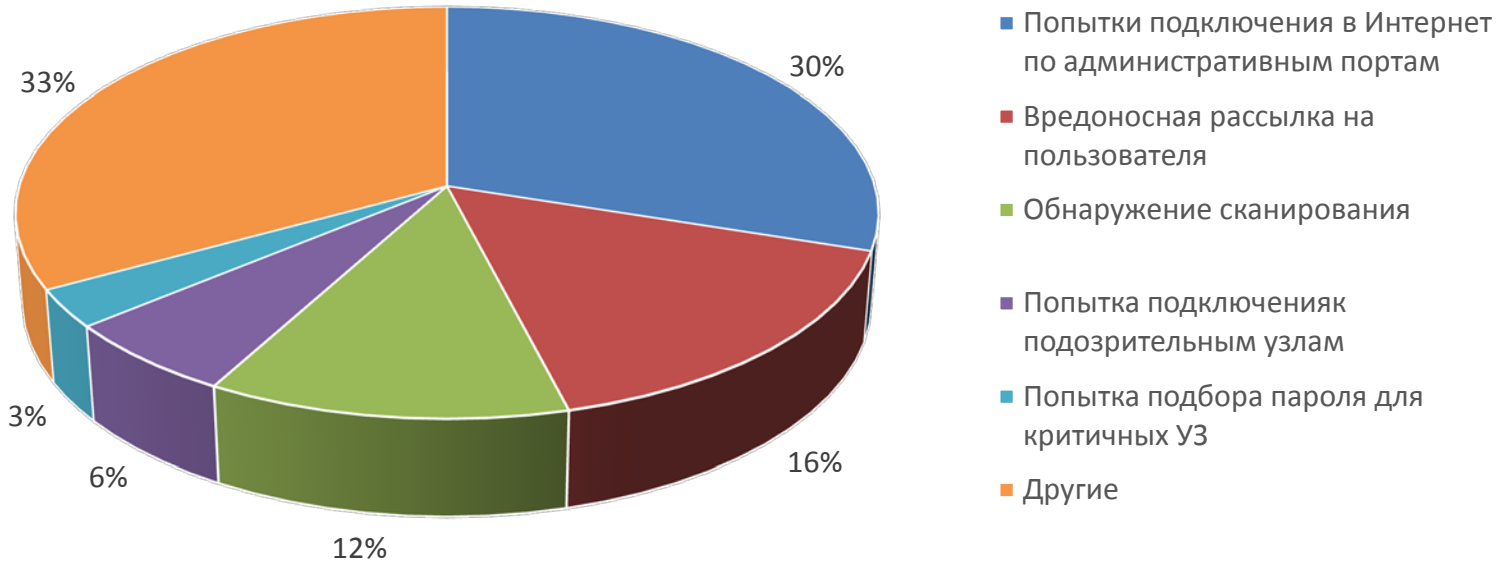
Попытки заражения вредоносным ПО

- Регулярные **оповещения о вредоносных рассылках, которые дошли до пользователей**
- Оперативное **выявление вредоносной почтовой рассылки от имени других банков**)

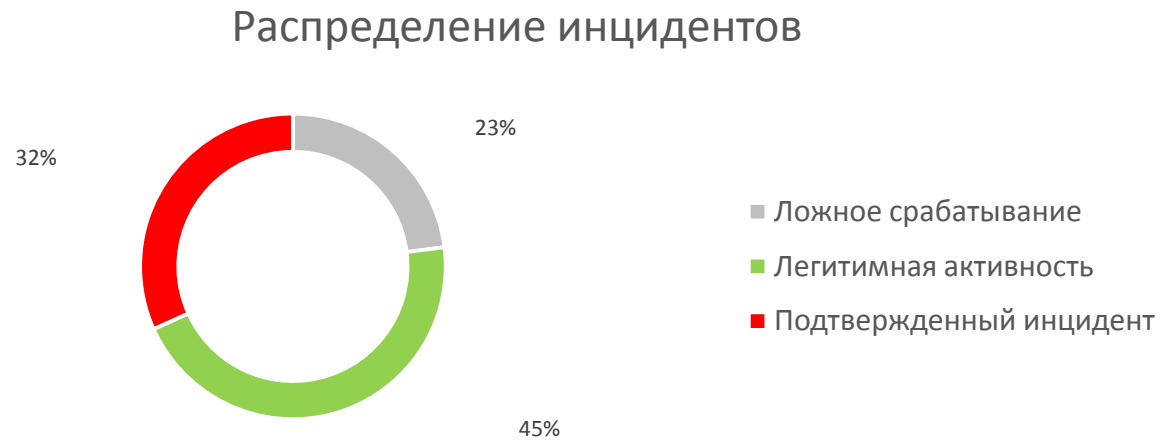
Threat Intelligence

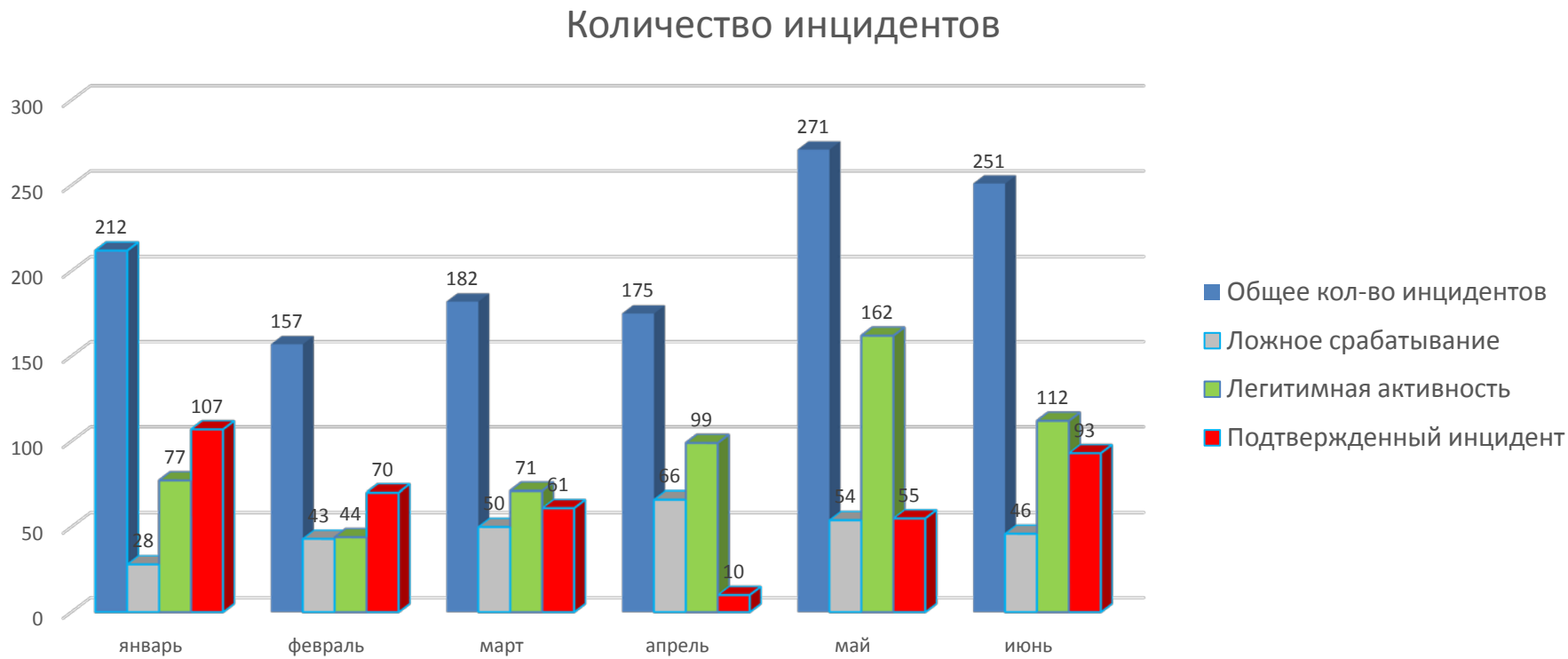
- Несколько **подтвержденных инцидентов по выявленным индикаторам ВПО**
- **Анализ вредоносных сэмплов от Банка** с целью проверки и выявления дополнительных индикаторов компрометации и их блокировки на СЗИ
- **Оповещение по актуальным угрозам** (в т.ч. BadRabbit, Vault8) с результатами ретроспективной проверки индикаторов компрометации в инфраструктуре банка и добавлением их на мониторинг

Распределение подтвержденных инцидентов (½ 2017 год)



Пример статистики по инцидентам за ½ 2017 года





Тинькофф

Руководитель управления информационной безопасности

Сергей Павлов, s.v.pavlov@tinkoff.ru

Tinkoff.ru

Тинькофф

Дальше действовать будем мы!

Tinkoff.ru