



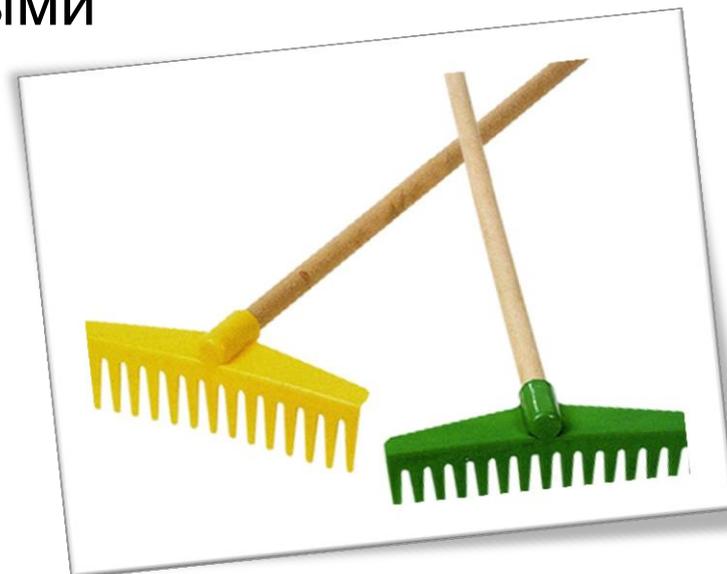
Безопасность в сервисной модели: за и против

Игорь Ляпунов

Директор Центра информационной безопасности

Несколько иллюстраций:

- ❖ 2 года назад построили первый в России коммерческий центр мониторинга и управления ИБ;
- ❖ Реализовали беспрецедентный проект по полному аутсорсингу ИТ-безопасности в Лето-Банке;
- ❖ Конкурируем с международными сервис-провайдерами безопасности (MSSP).



«...тот, кто откажется от аутсорсинга и будет жить в своем натуральном хозяйстве, окажется на обочине цивилизации...»

#ib-bank

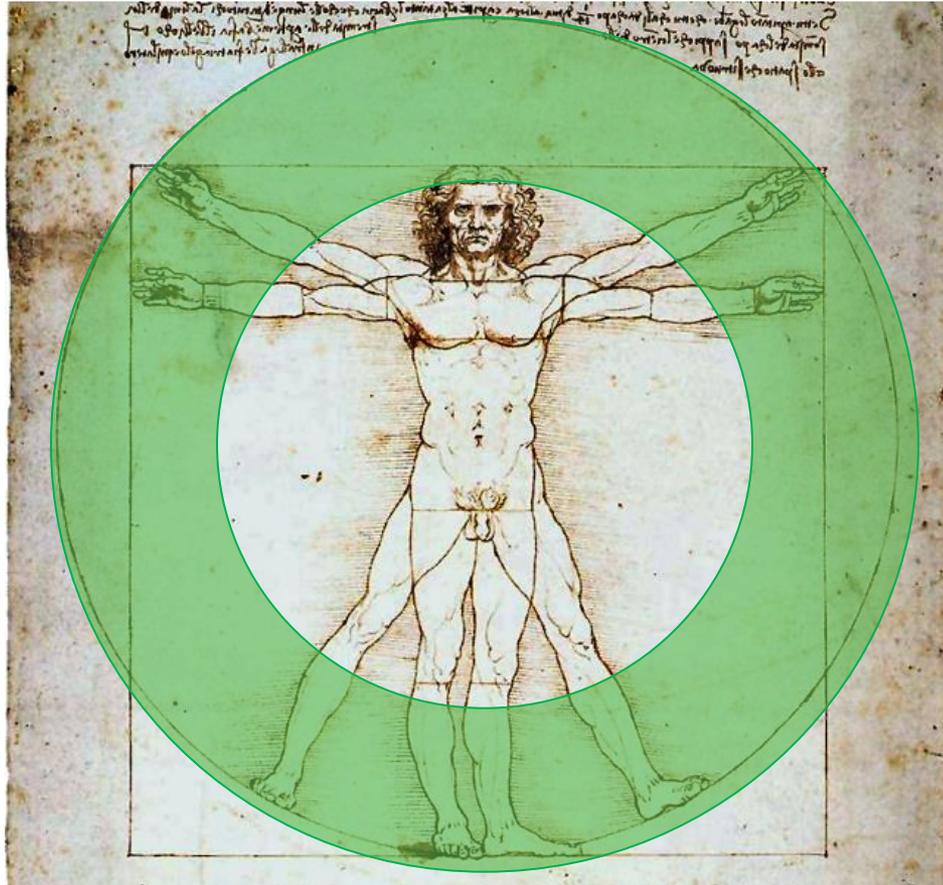
#Емельяников

Что же такое аутсорсинг

«Так вы и есть за меня будете?...»



Что же такое аутсорсинг



Основные кейсы передачи на аутсорсинг:

- ❖ Нужна специфичная точечная квалификация
- ❖ Нужно быстро и круглосуточно
- ❖ Нужны руки, чтобы снять рутину и заняться развитием
- ❖ Нужно прямо сейчас

Основные кейсы передачи на аутсорсинг:

- ❖ Нужна специфичная точечная квалификация
- ❖ Нужно быстро и круглосуточно
- ❖ Нужны руки, чтобы снять рутину и заняться развитием
- ❖ Нужно прямо сейчас

Например, внешний сервис мониторинга может быть единственно возможным способом решить проблему таргетированных атак для онлайн-сервисов

1. Мониторинг безопасности

периметр → внутренняя инфраструктура →
бизнес-приложения

2. Реагирование на инциденты безопасности

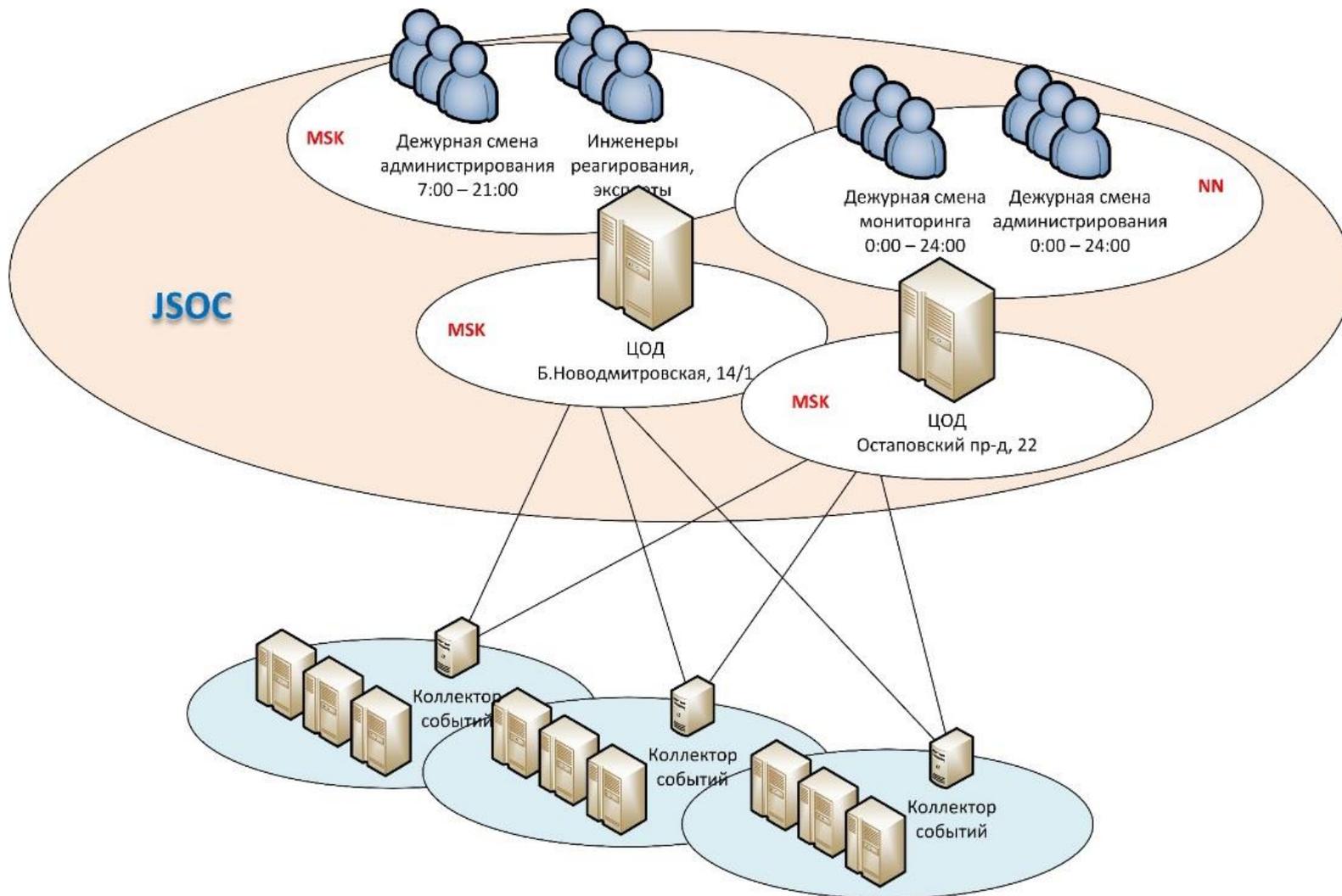
оповещение → план действий →
администрирование

3. Контроль защищенности

контроль уязвимостей → контроль конфигураций
→ план-действий → администрирование

4. Прикладные задачи: контроль безопасности кода,
защита от DDoS, WAF as a service.

Как это работает?



- ❖ А как защищаются мои данные у сервис-провайдера?
- ❖ Не потеряю ли я контроль, если что-то отдам на аутсорсинг?
- ❖ Если есть аутсорсинг, то как я объясню бизнесу зачем нужен я?
- ❖ Аутсорсинг это дорого?

Аутсорсинг позволяет избавиться от чувства тревоги 😊

«...с понедельника начну регулярно смотреть в SIEM и контролировать логи...»

«...наконец-то возьмусь, перелопачу весь отчет сканера и заставлю админов пропатчить сервера...»



Контакты:

Игорь Ляпунов

+7 916 970 9278

«Парус-2» номер 500

Ровно через этаж на «поющим» номером