

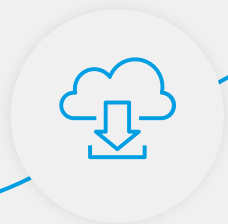
# Облачная ИБ: практический опыт

# NUBES

ОБЛАКА. ИБ. ДАТА-ЦЕНТРЫ



ИБ-сервисы  
по модели подписки



Защищенное облако NGcloud



Дата-центр Tier III

# ОБЛАЧНЫЕ ПРОВАЙДЕРЫ ТОЖЕ ИСПОЛЬЗУЮТ ОБЛАЧНЫЕ СЕРВИСЫ

<b>Провайдер облачного сервиса</b>	ООО “Инновации в управлении кадрами”	АО “ПФ “СКБ Контур”
<b>Используемый нами продукт</b>	КЭДО HR-Link	Экстерн, ДиаДок, Фокус
<b>Реестр операторов ПДн</b>	09-0066830 от 07.09.2009 г.	78-20-007268 от 11.11.2020 г.
<b>Наличие NDA</b>	да	да
<b>Наличие Поручения на обработку ПДн</b>	да	да (в оферте)
<b>Предоставление МУ и МН</b>	Предоставили выписку	Отказали, ком.тайна
<b>Уровень защищенности ПДн</b>	УЗ-3, Акт оценки эффективности	УЗ-3, Заключение

# ИЗ ЧЕГО СКЛАДЫВАЕТСЯ БЕЗОПАСНОСТЬ ОБЛАЧНОГО ПРОВАЙДЕРА?



# А КАК СНАРУЖИ ОЦЕНИТЬ БЕЗОПАСНОСТЬ ОБЛАКА (IAAS, PAAS)?

1.

**Аттестация и сертификация по требованиям регуляторов:**

- PCI DSS
- ГОСТ 57580
- 152-ФЗ + 1119-ПП + Приказ ФСТЭК России № 21
- ISO 27001/27017/27018,
- STAR
- SOC2 и прочее.

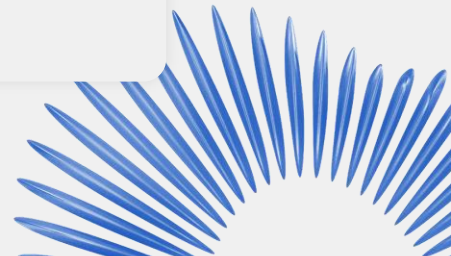
2.

**Практические тесты:** отчеты о проведенных pentest, размещение на площадках bug bounty.

3.

**Самим проверить облако на прочность.**

Но как?



# PRE-IR ASSESSMENT ОБЛАКА: ЗАЧЕМ?

Чтобы быть уверенными, что:

- инцидент не вызывает панику и бесконтрольные действия;
- сотрудники ИТ/ИБ- подразделений могут получить необходимые данные для оперативного расследования и что такие данные собираются/есть;
- процессы по реагированию отлажены, роли распределены;
- журналирование ведется правильно.

## F.A.C.C.T.

подтверждает, что

по результатам оценки готовности к реагированию на инциденты информационной безопасности специалисты NUBES (ООО «НУБЕС», ИНН: 9706005293) способны реагировать и исследовать инциденты информационной безопасности по данным, поступающим в SIEM-систему.

К SIEM-системе NUBES подключено необходимое количество источников данных с различных СЗИ и объектов ИТ-инфраструктуры.

**Валерий Баулин**

Генеральный директор F.A.C.C.T.



19.01.2024 г.

## ДОПОЛНИТЕЛЬНЫЕ «ФИШКИ» ИБ В ОБЛАКЕ

- Защита от DDoS-атак (L3-L4)
- Сканирование на уязвимости клиентских хостов на наших IP-адресах (black box)
- Расширенный сбор логов для реагирования на ИБ-инциденты и их последующего расследования



# ЧТО ОСТАВИТЬ ВНУТРИ, А ЧТО МОЖНО ОТДАТЬ НА АУТСОРС

## СУИБ:

- Политики ИБ;
- Управление рисками
- Планирование и реализация мероприятий по снижению рисков
- Обеспечение соответствия требованиям

## СОИБ:

- Безопасность сети (FW, IPS, NGFW, NTA, WAF, AntiDDoS)
- Работа с уязвимостями (VM, SAST/DAST)
- Защита от вредоносного ПО (AV, SandBox, XDR)
- Security Awareness
- Защита от утечек (DLP)



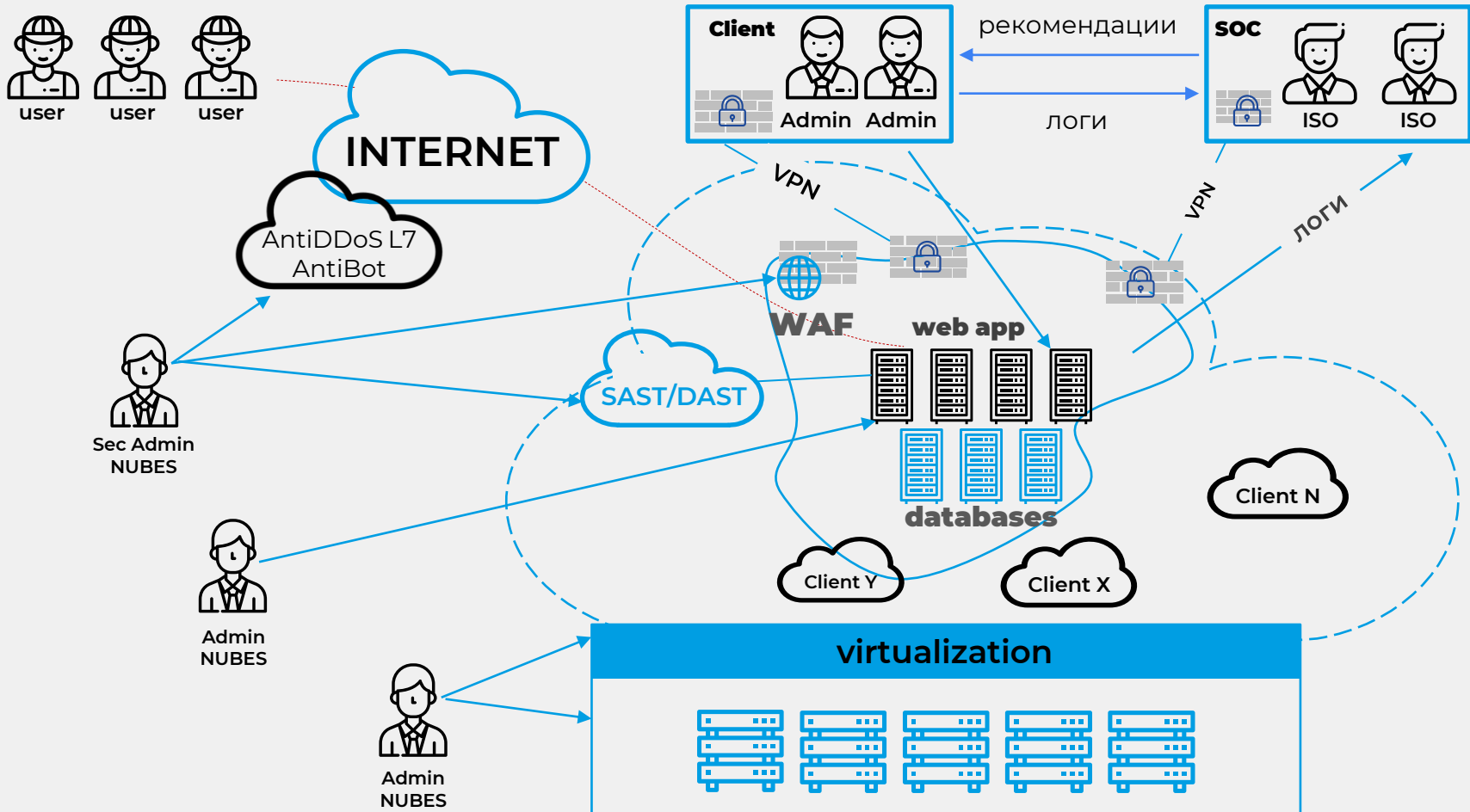
# СРЕДСТВА ЗАЩИТЫ ИЗ ОБЛАКА ПО ПОДПИСКЕ

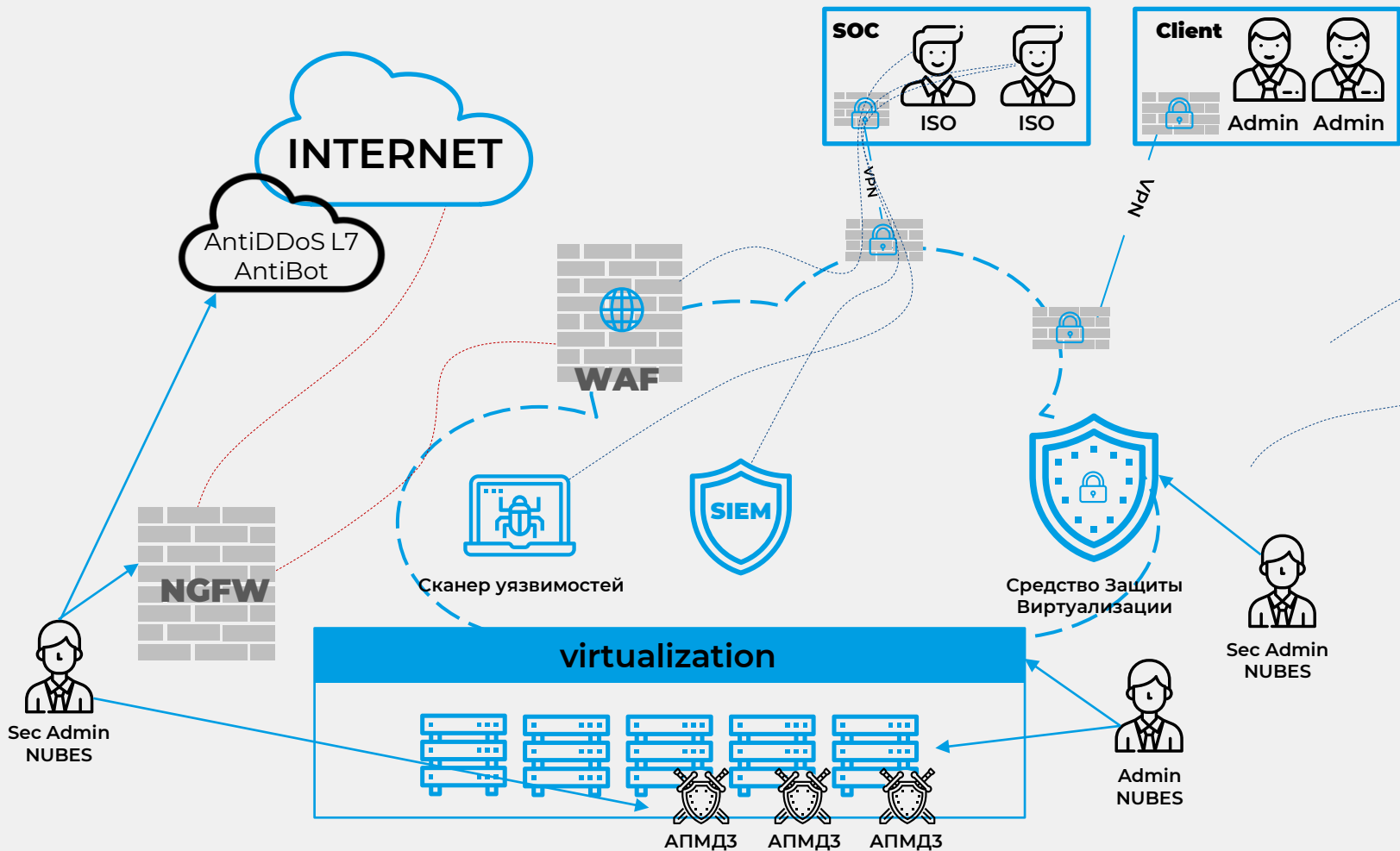
Почему востребовано:

- Необходимость переезжать на новые решения
- Нехватка персонала
- Быстрый пилот и запуск
- Возможность использовать в параллель с уже существующим решением
- CAPEX в OPEX
- Масштабируемость

Все больше вендоров адаптируют свои решения под MSSP:

- Kaspersky
  - UserGate
  - MFASOFT
  - Positive Technologies и другие
- 





# NUBES

ОБЛАКА. ИБ. ДАТА-ЦЕНТРЫ



## ИБ-сервисы по модели подписки:

- WAF
- NGFW
- AntiDDoS
- MFA

## Защищенное облако NGcloud:

- аттестат 152-ФЗ (УЗ-1)
- встроенная защита DDoS
- регулярное сканирование
- поддержка GPU

## Дата-центр Tier III:

собственная площадка  
в Москве

# КОНТАКТЫ



security@nubes.ru



1-я Стекольная улица,  
дом 7, стр. 2, Москва



Telegram



nubes.ru

