

Wone IT

```
def get_vowels(String s)
  return [each for each in s if each in "aeiou"]
get_vowels("animal") # [a, i, u, a]
get_vowels("sky") # []
get_vowels("football") # [o, o, u, a]
```

# Информационная безопасность от Wone IT

Контроль безопасности инфраструктуры  
в надежных руках экспертов

```
def get_vowels(s)
  return [each for each in s if each in "aeiou"]
end

get_vowels("animal")
# => ["a", "i", "u", "a"]

get_vowels("sky")
# => []

get_vowels("football")
# => ["o", "o", "u", "a"]
```

# Что мы предлагаем?

01

Проводим аудит контура безопасности

02

Демонстрируем подходящие продукты ключевых партнеров

03

Подбираем и внедряем нужный класс решений

04

Предоставляем услугу «Центр мониторинга информационной безопасности» (Security Operation Center)

05

Сопровождаем и поддерживаем

```
def get_vowels(String s)
  return [each for each in s if each in "aeiou"]
get_vowels("animal") # ["a", "i", "u", "o"]
get_vowels("ay") # []
get_vowels("football") # ["o", "o", "u", "o"]
```

# Проводим аудит контура безопасности

**Пентест** — это имитация проникновения в систему по всем возможным сценариям, чтобы выявить слабые места инфраструктуры. Тестируем инфраструктуру компании дешевле, чем платить хакерам выкуп, нести денежные и репутационные потери

**Внешнее тестирование** — имитация атаки от лица, у которого нет никаких сведений о компании. Определяем можно ли получить доступ к системе дистанционно и насколько глубоко можно проникнуть

В результате вы получите перечень рекомендаций по защите инфраструктуры



# Подбираем и внедряем нужный класс решений

## **MXDR**

Обнаружение угроз и реагирование на них за счет использования многочисленных источников телеметрии и передовых технологий машинного обучения

## **SIEM**

Мониторинг событий безопасности в реальном времени

## **EDR**

Выявление и изучение вредоносной активности на конечных точках: подключенных к сети рабочих станциях, серверах, устройствах Интернета вещей и так далее

## **NGFW**

Сетевой экран для контроля трафика, управления доступом пользователей и приложений, предотвращения атак

## **Sandbox (Песочница)**

Заставляет потенциально опасную программу проявить себя в контролируемой среде, где она не сможет нанести вреда

## **WAF**

Обнаруживает и блокирует сетевые атаки на веб-приложение

## **NTA**

Изучает сетевые события, обнаруживает и расследует операции злоумышленников в информационной инфраструктуре предприятия

## **EPP**

Комплексная защита рабочей станции, включающая классический антивирус, расширенные технологии безопасности

**А также:** сессионный антифрод, защита бренда и интеллектуальной собственности, решения класса IRM (контроль над документами)

# Демонстрируем подходящие продукты ключевых партнеров

**kaspersky**

## KSC + KES

- Демонстрация возможностей антивируса

## KSMG

- Контроль почтового трафика для выявления вредоносной активности
- Защиты организации от фишинга, спама, вредоносных ссылок

## KEDR Optimum + Kaspersky Sandbox

- Решение строит цепочку активностей выявленного ВПО, тем самым облегчает расследования инцидентов ИБ, а с помощью Kaspersky Sandbox реализуется автоматическое реагирование на угрозы

## KUMA (SIEM система)

- Анализ и корреляция событий безопасности из различных источников данных

## KATA/KEDR + KATA Sandbox

- Позволяет выявить аномалии в трафике и на хостах, выявлять и расследовать АРТ-атаки, расследовать выявленные инциденты ИБ, построенные по матрице MITRE. В связке с Sandbox анализировать неизвестное ВПО в изолированной среде

**F.A.C.C.T.**

## MXDR

- Защита конечных станций пользователей и реагирование (EDR)
- Защита корпоративной почты (модуль NTA)
- Детонация ВПО (Sandbox)
- Анализ сетевого трафика (NTA)
- Threat Intelligence
- Управление поверхностью атаки — контроль защищенности периметра

## ASM

- Индексация ресурсов
- Выявление угроз
- Управление рисками и устранение недостатков

А также совсем скоро станут доступны стенды от партнеров:

 **positive technologies**

 **UserGate**

 **ideco**

 **MULTIFACTOR**

 **КОМПАНИЯ ИНДИД**

# Предоставляем сервис от Wone IT по аналитике и предотвращению кибератак «**Центр мониторинга информационной безопасности**» Security Operation Center (SOC)

Эксперты SOC от WONE IT в режиме реального времени анализируют вашу IT-инфраструктуру, собирая массивы данных событий безопасности с различных объектов организации

И при обнаружении подозрительной активности предоставляют подробный план действий по предотвращению кибератаки

Возможность распознать возникновение **киберинцидента на ранней стадии** и предотвратить его развитие до того, как он сможет нанести существенный ущерб IT-системам организации

Услуга предоставляется по подписке



SOC базируется на платформах и технологиях мониторинга угроз (SIEM, SOAR, TI и др.), поддерживается экспертами SOC и выполняет все этапы обработки киберинцидентов в рамках четко выстроенных процессов: от обнаружения угрозы до предоставления финального отчета после предотвращения атаки



# Сопровождаем и поддерживаем

Мы можем обеспечить техническую поддержку выбранных вами решений в формате 24x7

В нашем штате – квалифицированные специалисты по информационной безопасности, которые имеют широкую экспертизу по работе с ведущими вендорами

Как правило, наши услуги обходятся дешевле, чем работа штатных специалистов

Кроме того, к нам можно обращаться за помощью в сложных ситуациях. При необходимости мы приедем к вам и разберемся с проблемой на месте или передадим запрос производителю решения

WONE IT



Специальное предложение

## kaspersky

Продукты:

- Kaspersky Security Center (KSC, KSCL)
- Kaspersky Endpoint Security (KES, KESL, KESMac, KESC)
- Kaspersky Security для Windows Server (KSWs)
- Kaspersky Security for Virtualization Light Agent (KSVLA)
- KEDRO + Sandbox
- KATA/KEDR
- KUMA

## Wone IT в цифрах

**16** ЛЕТ

Опыта работы  
на рынке РФ

**50+**

Официальных  
партнеров

**200+**

Технических  
экспертов

**500+**

Заказчиков

**wone IT**

## Сертификаты соответствия



ГОСТ Р ИСО/МЭК 27001-2021



ГОСТ Р ИСО 9001-2015

Platinum partner

kaspersky

Platinum  
Partner

Advanced partner

■ positive technologies

Authorized Partner

ASM & MXDR

**F.A.C.C.T.**

# Спасибо!

Оставляйте заявку сегодня, и уже завтра мы приступим к защите вашей компании!

**8 499 322 05 45**

[info@wone-it.ru](mailto:info@wone-it.ru)

[www.wone-it.ru](http://www.wone-it.ru)

Группа компаний WONE IT

- 📍 Москва, ул. Барклая, д. 6, стр. 3, этаж 3, офис XXVII
- 📍 Санкт-Петербург, Волховский переулок, д. 4, лит. А
- 📍 Новосибирск, ул. Кропоткина, 271, оф. 805

**wone IT**