

wone IT

Практика информационной безопасности

```
def get_vowels(string):  
    return [each for each in string if each in "aeiou"]  
get_vowels("winner") # ['a', 'i', 'e']  
get_vowels("sky") # []  
get_vowels("football") # ['o', 'o', 'a']
```

```
def merge_sort(arr):  
    if len(arr) < 2:  
        return arr  
    mid = len(arr) // 2  
    left = arr[:mid]  
    right = arr[mid:]  
    merge_sort(left)  
    merge_sort(right)  
    return merge(left, right)  
def merge(left, right):  
    result = []  
    i = j = 0  
    while i < len(left) and j < len(right):  
        if left[i] < right[j]:  
            result.append(left[i])  
            i += 1  
        else:  
            result.append(right[j])  
            j += 1  
    result.extend(left[i:])  
    result.extend(right[j:])  
    return result
```

Что мы предлагаем?

- 01 Проводим аудит контура безопасности
- 02 Демонстрируем подходящие продукты ключевых партнеров
- 03 Подбираем и внедряем нужные классы решений
- 04 Развиваем направление Managed Security Services
- 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, e]
get_vowels("sky") # []
get_vowels("football") # [o, o, u, e]
```

Демонстрируем подходящие продукты ключевого партнера

kaspersky

```
return [each_for_each(:string if each in "hello")
get_vowels("hello") # ["a", "e", "o"]
get_vowels("ay") # []
get_vowels("football") # ["o", "o", "u"]]
```

KSC + KES

- Современный корпоративный антивирус

KSMG

- Контроль почтового трафика для защиты организации от фишинга, спама, вредоносных ссылок

KEDR Optimum + Kaspersky Sandbox

- Решение строит цепочку активностей выявленного ВПО, тем самым облегчает расследования инцидентов ИБ

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 можно анализировать неизвестное ВПО в изолированной среде

Готовим стенды от партнеров:



Подбираем и внедряем нужные классы решений

NTA

Изучает сетевые события, обнаруживает и расследует действия злоумышленников в ИТ инфраструктуре предприятия.

EDR

Выявляет и изучает вредоносную активность на конечных точках: подключенных к сети рабочих станциях, серверах, устройствах Интернета вещей и т.д.

NGFW

Комплексный сетевой экран для контроля трафика, управления доступом пользователей и приложений, предотвращения атак на информационные системы.

WAF

Специальный сетевой экран, который обнаруживает и блокирует сетевые атаки на веб-приложения и API.

Sandbox

Заставляет потенциально опасную программу проявить себя в контролируемой среде, где она не сможет нанести вреда с целью дальнейшей блокировки.

Security Awareness

Позволяет повысить знания пользователей компании о кибербезопасности за счет проведения учебных атак и назначений обучающих курсов.

SIEM

Позволяет производить мониторинг и корреляцию событий безопасности в реальном времени, а также вести управление инцидентами ИБ.

VM

Отслеживает наличие уязвимостей в инфраструктуре организации и позволяет организовать процесс по их устранению.

Подбираем и внедряем нужные классы решений

MDM (Безопасность мобильных решений)

Защита корпоративных данных на устройствах пользователей, контроль использования приложений, удаление данных и т.д.

DCAP

Категорирование информационных массивов организации – файловых хранилищ, аудит прав доступа к файлам, а также регистрация и управление обращений пользователей к ним.

VPN

Защита межфилиальных взаимодействий по недоверенным каналам и организация удаленного доступа к ресурсам предприятия.

DLP

Предотвращение утечек конфиденциальной информации по различным каналам – почта, веб, мессенджеры и т.д.

Безопасность контейнеров

Защита на всем жизненном цикле контейнерных приложений и средств оркестрации на базе Kubernetes.

Безопасность облачных и виртуальных сред

Антивирусная система, предназначенная для использования в средах виртуализации.

Защита от DDoS

Комплекс мер, направленных на снижение влияния вредоносного трафика и минимизацию его негативных последствий для цели атаки.

РАМ

Контроль и управление действиями привилегированных пользователей в т.ч., защита цепочек поставки.

MFA (Двухфакторная аутентификация)

Решение усиливает защиту учетных записей в различных информационных системах, добавляя второй фактор (SMS, одноразовый пароль, push-уведомление).

IDM

Централизованное автоматизированное управление учетными записями и правами на доступ к различным информационным системам предприятия.

Развиваем направление **Managed Security Services**

Для того чтобы помочь вам повысить эффективность защиты и сэкономить ресурсы на ИБ, мы развиваем модель «безопасность по подписке». Выберите набор услуг исходя из своих возможностей и потребностей.

Основным преимуществом MSSP-модели является доступ к передовым технологиям защиты по подписке, которые поддерживаются квалифицированными экспертами.

Экспертное знание

У нас работают квалифицированные специалисты по кибербезопасности, которые помогут быстро реагировать на угрозы.

Экономия времени и ресурсов

Вам не нужно приобретать дорогостоящие технологии и заботиться о лицензиях. Пока наши специалисты работают над вашей безопасностью, вы можете сосредоточиться на основной деятельности.

Снижение рисков

Managed Security Services помогают предотвращать атаки и минимизировать потенциальные убытки.

Managed Security Operation Center (SOC)

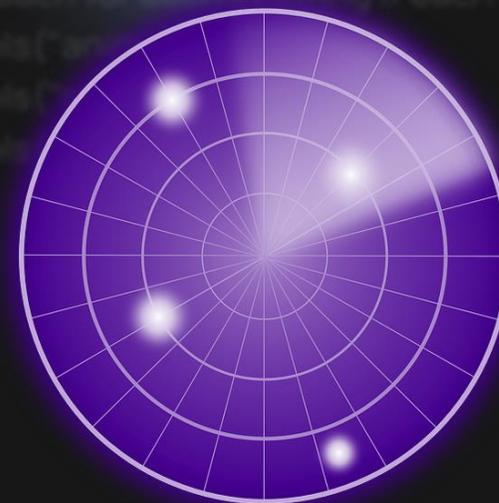
«Центр мониторинга информационной безопасности»

Эксперты SOC от WONE IT анализируют вашу IT-инфраструктуру, собирая массивы данных событий безопасности с различных объектов организации.

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

При обнаружении подозрительной активности проводится проверка на ложное срабатывание и предоставляется подробный план действий по предотвращению кибератаки.

Услуга предоставляется по подписке.



SOC базируется на платформах и технологиях мониторинга и реагирования на угрозы, поддерживается экспертами SOC и выполняет все этапы обработки кибер-инцидентов в рамках четко выстроенных процессов.



Managed Security Awareness

Сервис повышения осведомленности пользователей о кибер-рисках

Managed Security Awareness — это сервис, который помогает организациям повысить уровень осведомленности своих сотрудников по вопросам кибербезопасности. Он включает в себя регулярное обучение сотрудников, тестирование их знаний, а также предоставление отчетности по результатам.

Результатом использования сервиса является снижение риска возникновения кибератак, связанных с человеческим фактором.

ОСНОВНЫЕ ПРЕИМУЩЕСТВА SECURITY AWARENESS

- ✓ Подключение, настройка и сопровождение от опытного сервис-провайдера с соблюдением всех SLA.
- ✓ Полнофункциональное решение от российского вендора.
- ✓ Возможна разработка курсов под заказ.



Сопровождаем и поддерживаем

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

В нашем штате квалифицированные специалисты, 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 нестандартных 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!

+7 499 322 05 45
info@wone-it.ru
www.wone-it.ru

Группа компаний WONE IT

- 📍 Москва, ул. Нижняя Красносельская, д. 40/12, корпус 2, офис № 323
- 📍 Санкт-Петербург, Волховский переулок, д. 4, лит. А
- 📍 Новосибирск, ул. Кропоткина, 271, оф. 805

wone IT

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



**Подписывайтесь на наш
telegram-канал!**