

# SECURITY OPERATIONS CENTER

КОНТРОЛЬ БЕЗОПАСНОСТИ ИНФРАСТРУКТУРЫ  
В НАДЕЖНЫХ РУКАХ ЭКСПЕРТОВ

wone IT



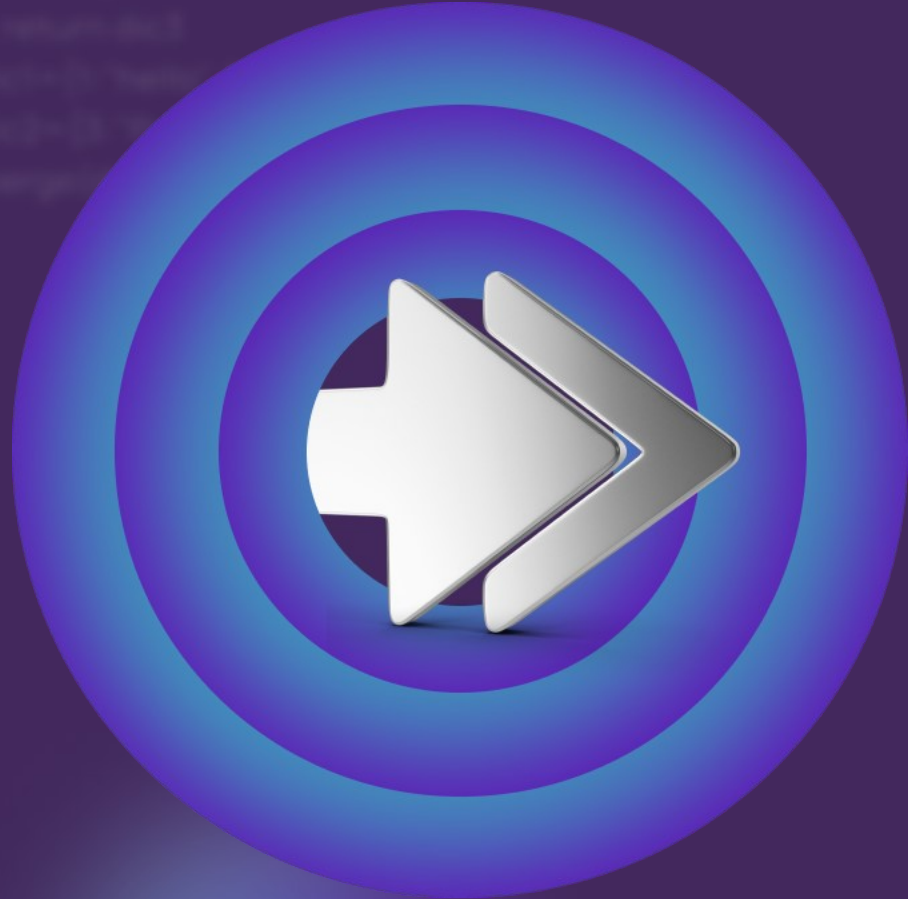
Центр мониторинга информационной безопасности (Security Operations Center) – сервис, оказывающий оперативный мониторинг IT-инфраструктуры и предотвращение киберинцидентов.



Эксперты SOC собирают и анализируют массивы данных с различных объектов инфраструктуры организации и при обнаружении подозрительной активности предоставляют подробный план действий по предотвращению кибератаки.

```
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]
```

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



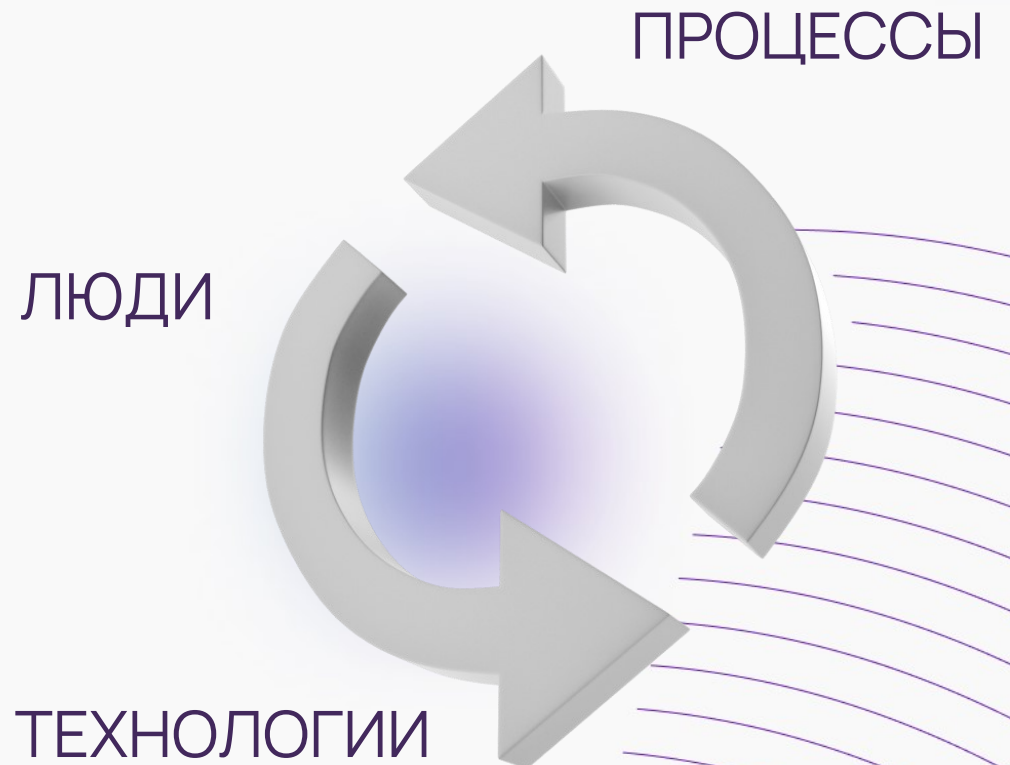
## ОСНОВНОЕ ПРЕИМУЩЕСТВО SOC

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

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

# ИЗ ЧЕГО СОСТОИТ SOC

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.

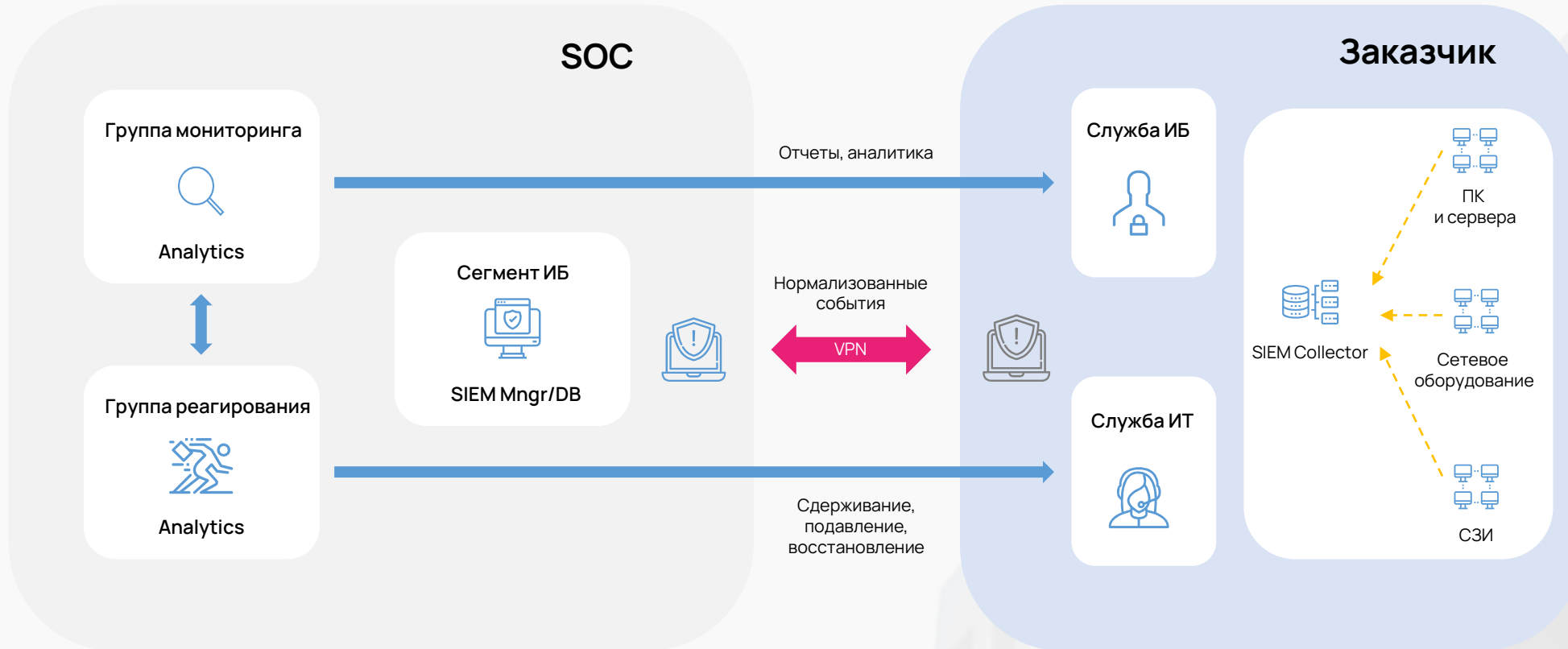


```
def merge(dic1,dic2):  
    dic3=dic1.copy()  
    dic3.update(dic2)  
    return dic3  
dic1={1:"hello", 2:"world"}  
dic2={3:"Python", 4:"Programming"}  
merge(dic1,dic2) # [1: 'hello', 2: 'world', 3: 'Python', 4: 'Programming']
```

# WONE IT MSOC ИЛИ СОБСТВЕННЫЙ SOC?

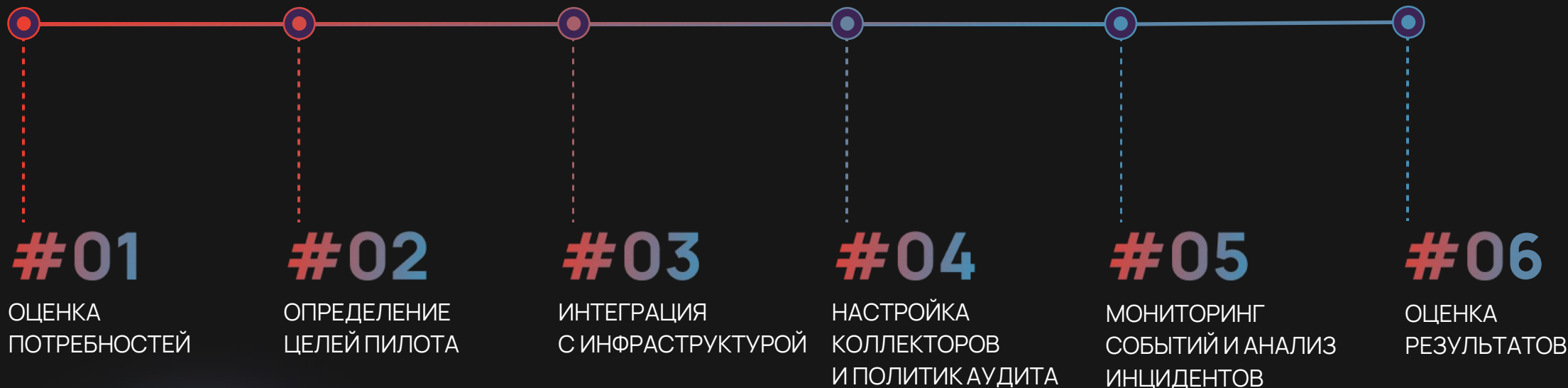
|                       | СОБСТВЕННЫЙ SOC   | WONE IT MSOC   |
|-----------------------|---|--|
| Время запуска         | Непредсказуемо. Первая стадия до 2-х лет  | До 2-х месяцев с учетом пилотирования  |
| Правила корреляции    | Небольшой набор «из-коробки», дополнение требует экспертизы                                     | Индивидуальный готовый набор под инфраструктуру клиента                        |
| Команда SOC           | Сотрудники компании (ФОТ)   | Команда экспертов Wone IT (OPEX)   |
| Ложные срабатывания   | Требуют дополнительных ресурсов L1  | Обрабатываются командой экспертов Wone IT                                      |
| Оперативность реакции | Регламенты потребуется разработать, внедрить, соблюдать и корректировать                        | Строгое соблюдение SLA   |
| Инфраструктура        | Требуются значительные вычислительные ресурсы, закупка, установка и поддержка ПО и оборудования | Требуются только незначительные ресурсы для развертывания серверов-коллекторов |

# СХЕМА ОКАЗАНИЯ УСЛУГИ



# ПЛАН ПИЛОТА

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



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

# ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К КОЛЛЕКТОРАМ

| ПАРАМЕТРЫ СЕРВЕРА     | WEC-СЕРВЕР               | SIEM-КОЛЛЕКТОР                        |
|-----------------------|--------------------------|---------------------------------------|
| Тип сервера           | Виртуальный и физический | Виртуальный и физический              |
| Центральный процессор | 6 CPU                    | 8 CPU                                 |
| Оперативная память    | 16 ГБ                    | 16 ГБ                                 |
| Дисковое пространство | 80 ГБ (RAID 10)          | 500G, смонтированного в разделе /opt. |
| Операционная система  | Windows 2016 и выше      | Oracle Linux версии не ниже 8.6       |

```
def merge(dic1,dic2):  
    dic3=dic1.copy()  
    dic3.update(dic2)  
    return dic3  
dic1={1:"hello",2:"world"}  
dic2={3:"Python",4:"Programming"}  
merge(dic1,dic2) # {1: 'hello', 2: 'world', 3: 'Python', 4: 'Programming'}
```



# ПРЕИМУЩЕСТВА WONE IT MSOC

#01

Международная экспертиза

#02

Возможность написания  
коннекторов

#03

Гибкая тарификация

wone IT



# СПАСИБО ЗА ВНИМАНИЕ!

Андрей Пастухов

Security Presale Generalist

+7 921 858 96 61

Антон Гурьев

Product Manager MSS

+7 985 331 65 05

**wone IT**