IZ:SOC

Информзащита
Системный интегратор

Актуально о SOCе

www.izsoc.ru

На протяжении последних лет мы можем наблюдать уверенный тренд по смещению интереса в области информационной безопасности с так называемой «бумажной» к «практической».

Одним из существенных компонентов обеспечения реальной безопасности является процесс выявления и реагирования на инциденты. Наиболее часто этот комплекс мер, а также многое другое, обозначается словосочетанием **Security Operation Center (SOC).**

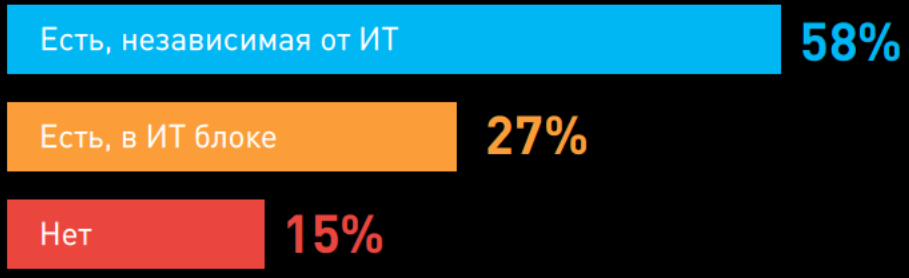
SOC уже не первый год является рыночным трендом, и по нашим оценкам спрос на него ежегодно увеличивается примерно в два раза.

В первом полугодии 2019 года мы провели опрос среди организаций различных отраслей и масштаба.

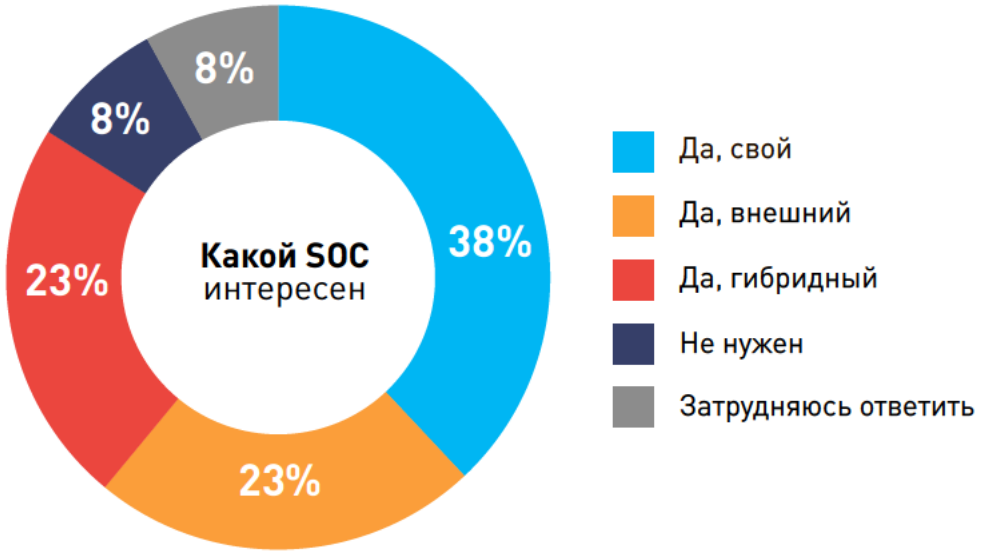
Среди ответивших на опрос - **66%** относятся непосредственно к информационной безопасности, являясь CISO или ключевыми сотрудниками службы ИБ.

Основная часть участников опроса - **54%** относятся к крупным компаниям. Размер компании, как показал наш опрос, не влияет на наличии выделенной службы ИБ и далеко не у всех компаний она есть.

Наличие службы ИБ



Стоит отметить, что подавляющее большинство участников опроса считают необходимым наличие SOC в организации. При этом наметилась тенденция отхода от обязательного построения своего SOC. На графике ниже мы видим, что предпочтения в части построения своего SOCа или использования внешнего разделились примерно поровну.



Актуальность функций SOC

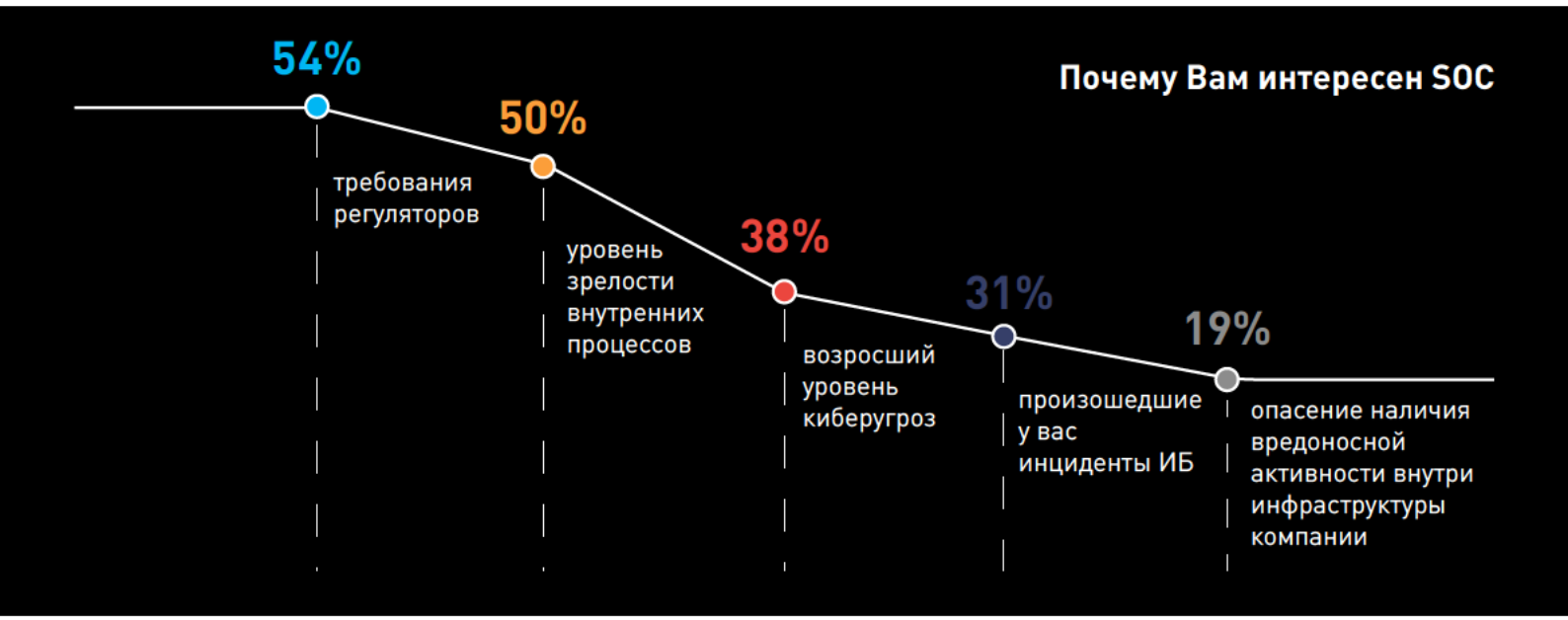
Одним из самых актуальных вопросов является вопрос о том, какой собственно функционал должен включать в себя современный SOC.

Под термином SOC на рынке представлены различные сервисы, некоторые включают в себя исключительно мониторинг событий ИБ, другие – наоборот, делают упор на реагирование, а ряд на Threat Intelligence.

Исходя из полученных ответов, мы видим, что заказчики скорее видят в SOC универсальное подразделение, которое может закрыть большую часть функций по обеспечению ИБ и стать центром компетенций по кибербезопасности.

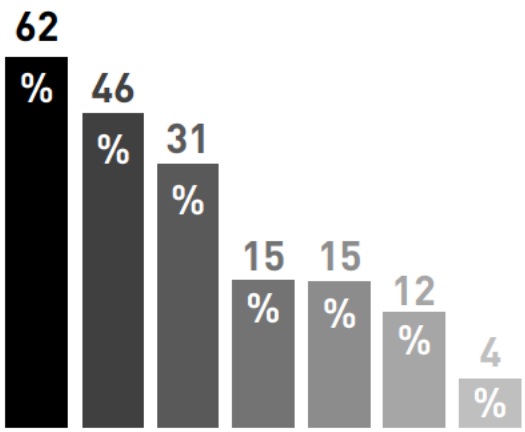
Вполне ожидаемо опрошенные ответили на вопрос о технологической платформе, на которой должен быть построен SOC. **42%** респондентов указывают необходимость использовать сертифицированное ПО, **31%** использование отечественно ПО. Это реакция на действия регуляторов в части использования отечественных продуктов и требования по защите КИИ. При этом, **19%** ответивших на опрос, готовы рассматривать open-source решения. Скорее всего это продиктовано желанием быть защищенными с более скромными затратами.

Требования регуляторов повлияли и на фактор спроса SOC, сместив киберугорзы на позицию ниже. Большая половина респондентов – **54%** заявили о необходимости SOC из-за требований регуляторов, **50%** и **38%** соответственно среди решающих факторов назвали высокий уровень зрелости внутренних процессов и возросший уровень угроз.



С точки зрения ожиданий в части отчетности, предоставляемой SOC, заказчики хотят видеть всю доступную информацию, начиная от доступа в консоль SIEM платформы **(58%)**, заканчивая аналитическими отчетами **(50%)** и данными Service Desk **(46%)**.

Понимая основные параметры по потребностям SOC у бизнеса, мы не могли обойти стороной вопрос мотивации, что влияет при принятии решения о внедрении технологии, и чем может оперировать интегратор/оператор SOC.



Какие факторы влияют при принятии решения о внедрение SOC

- Цена
- Функционал
- Технологическая платформа
- Простота подключения
- Наличие тестового периода
- Известность на рынке
- Количество подключенных клиентов

Подводя итоги

Как мы видим из опроса, подавляющее большинство участников считают необходимым реализовать функции SOC в своих организациях, при этом половина из них готова отдать этот функционал внешнему поставщику сервиса.

При выборе такого поставщика основополагающим фактором будет цена, предоставляемый функционал и технологическая платформа.

Обязательный функционал SOC - это сбор, хранение и обработка логов и событий ИБ; детектирование, реагирование и расследование инцидентов; выявление уязвимостей.

Хорошим дополнением будет являться управление СЗИ и реализация проактивной защиты. Потребители сервисов SOC хотят иметь доступ к отчетности различных технологических компонентов платформы от SIEM систем до Service Desk и предпочитают отечественное сертифицированное ПО.

Информзащита
Системный интегратор

Системный интегратор
+7 495 980 23 45
market@infosec.ru
www.infosec.ru

Центр противодействия кибератакам IZ SOC
+7 495 980 23 45
izsoc@infosec.ru
www.izsoc.ru

Сервисный центр
+7 495 981 92 22
+7 495 980 23 45 доб.06
support@itsoc.ru
www.itsoc.ru

Центр противодействия мошенничеству
antifraud@infosec.ru

Пресс-служба
pr@infosec.ru