
ISOC: МОНИТОРИНГ
И РАССЛЕДОВАНИЕ
ИНЦИДЕНТОВ ИБ

ЗАЧЕМ НУЖЕН SOC

ЦЕЛИ

Снижение рисков хищения данных и денежных средств

Обеспечение непрерывности бизнеса

Снижение тяжести последствий инцидентов

РЕЗУЛЬТАТ

Выявление кибератак на ранних стадиях

Максимально быстрый разбор инцидентов в большом количестве информационных систем

ВАРИАНТЫ ПОСТРОЕНИЯ SOC

ВНУТРЕННИЙ SOC

Компания сама или с помощью консультантов строит процессы, обучает специалистов, создает и поддерживает SOC

PT MaxPatrol SIEM + Консалтинг

SOC AS SERVICE

Компания заключает договор с провайдером на сервис SOC с установленным SLA (Service Level Agreement)

ISOC

ГИБРИДНЫЙ SOC

Компания делегирует часть функций SOC сервис-провайдеру, остальные функции поддерживает самостоятельно

ISOC + PT MaxPatrol SIEM

ВАРИАНТЫ ПОСТРОЕНИЯ SOC. В ЧЕМ РАЗНИЦА

ВНУТРЕННИЙ SOC	SOC AS SERVICE	ГИБРИДНЫЙ SOC
СТОИМОСТЬ		
$$$ SIEM (Лицензия) $$$ Инфраструктура $$$ Внедрение системы $$$ Сервис 24/7	$ SIEM (Лицензия) $ Инфраструктура $$ Внедрение системы $$ Сервис 24/7	$$$ SIEM (Лицензия) $$$ Инфраструктура $$ Внедрение системы $$ Сервис 24/7
Скорость внедрения		
От 12 месяцев	3-4 месяца	6-12 месяцев
Преимущества		
Обработка и хранение событий на своей стороне	Гибкость в предоставлении сервиса	Обработка и хранение событий на своей стороне Гибкость в предоставлении сервиса

ПРЕИМУЩЕСТВА СЕРВИС-ПРОВАЙДЕРА

Экономия ресурсов

Снижаются затраты (оборудование, персонал) на инфраструктуру для управления инцидентами*

Решение проблемы кадров

Не нужно искать дорогих специалистов и обучать своих: сервис сопровождают профильные эксперты

Ожидаемый результат

Затраты и сроки внедрения сервиса заранее определены договором с провайдером

Фиксированные SLA

Клиент понимает, как быстро будет обработан инцидент или решен определенный вопрос

Оперативная реакция

Сервис предоставляется в режиме 24/7, поэтому вся информация об угрозах и уязвимостях поступает своевременно

Дополнительные сервисы

Сервис-провайдер может взять на сопровождение СЗИ и IT-инфраструктуру клиента

ТЕХНОЛОГИЧЕСКАЯ ПЛАТФОРМА

ОБЛАЧНЫЙ SOC: ISOC SIEM

Система мониторинга событий ИБ и выявления инцидентов в реальном времени, разработанная компанией Infosecurity

Ключевые преимущества:

1. Высокая надежность, отказоустойчивость и горизонтальное масштабирование до требуемой производительности
2. Разработка сценариев любой сложности благодаря использованию полноценного языка программирования (Scala)
3. Высокая производительность обработки потоков данных и скорость выполнения ретроспективных запросов
4. Поддержка основных типов источников событий
5. Постоянно обновляемая база правил выявления инцидентов

ISOC SIEM

2 Тб/сутки

Поток данных

1:30

Сжатие данных

2 мин поиск по IP-адресу

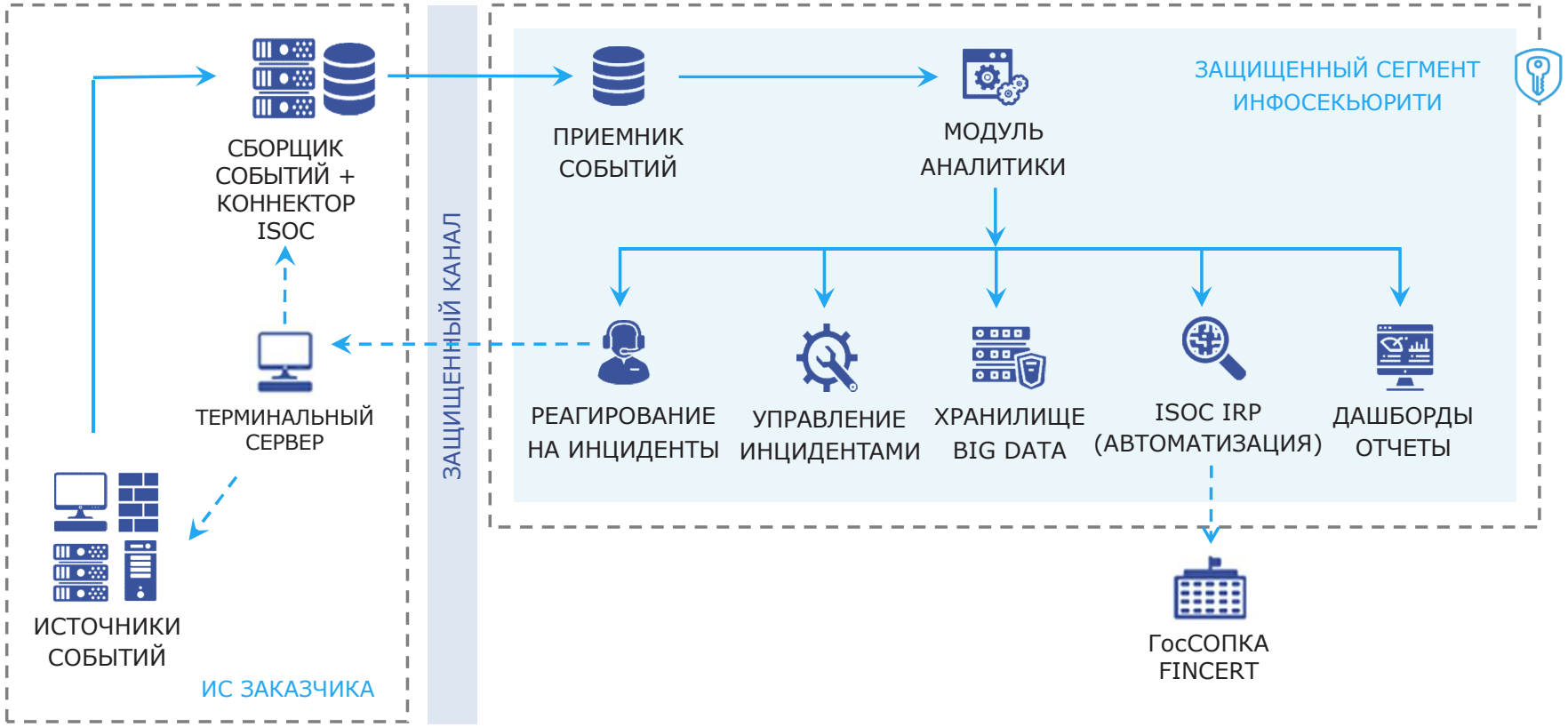
8 мин GroupBy + Sort

Скорость и надежность BigData*

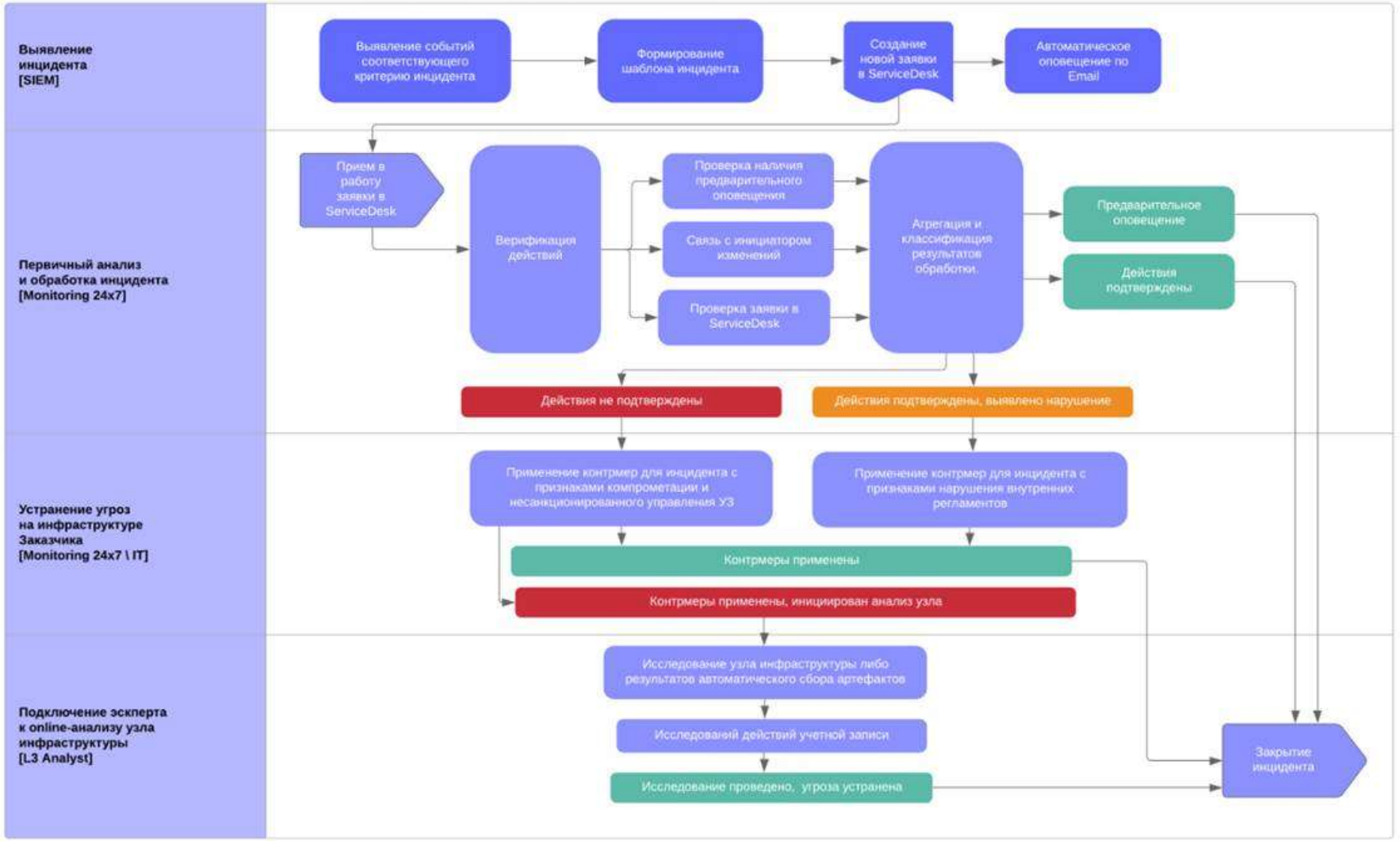
** На тестовой выборка 3 мес. Netfow: 17 млрд. событий, 24 Тб данных*

АРХИТЕКТУРА ВЗАИМОДЕЙСТВИЯ

ОБЛАЧНЫЙ SOC: ISOC SIEM



КАК РАБОТАЕТ СЕРВИС ISOC



ЭКСПЕРТИЗА И ПРОЦЕССЫ ISOC

Эффективность работы SOC обуславливается рядом уникальных характеристик компании «Инфосекьюрити»

8 лет управления инцидентами ИБ

Участник FIRST, статус CERT

Соглашение НЦКИ позволяющее выступать в роли корпоративного центра ГосСОПКА класса «А»

База знаний и use case по обработке инцидентов

Использование актуальных данных Threat Intelligence

Опыт предоставления сервиса компании с количеством сотрудников 30.000

Более 30 сотрудников участвующих в мониторинге и реагировании и более 60 профильных экспертов

КОМАНДА ISOC

В команде более 30 экспертов, занимающихся непосредственно мониторингом и расследованиями инцидентов.

Кроме того, с ними в непрерывном режиме взаимодействуют более 60 профильных инженеров по различным направлениям информационной безопасности.

ПЕРВАЯ ЛИНИЯ
Мониторинг и оповещение 24/7

ВТОРАЯ ЛИНИЯ
Анализ инцидентов 24/7

ТРЕТЬЯ ЛИНИЯ
Расследования 8/5

СЕРВИСЫ ИБ
Реагирование на инциденты 24/7

АНАЛИТИКА
Правила реагирования

РАЗРАБОТКА
Платформа и автоматизация

ЭКСПЛУАТАЦИЯ ISOC
Сопровождение инфраструктуры ISOC

ЭТАПЫ ПОДКЛЮЧЕНИЯ

1

Аналитика и консалтинг

- Анализ инфраструктуры (ОС, СУБД, ПО, СЗИ, сетевое оборудование)
- Анализ текущих процессов сбора событий и реагирования на инциденты

2

Организация каналов связи

- Получение доступов
- Настройка защищенного сетевого канала
- Настройка защищенного почтового канала

3

Подготовка инфраструктуры

- Настройка систем сбора и передачи событий
- Подключение источников
- Настройка оповещений и доступа к дашбордам

4

Согласование взаимодействия

- Определение схемы подключения новых источников
- Определение схем оповещения об инцидентах и эскалации

5

Согласование SLA

- Установление режима работы
- Определение приоритета и скорости реагирования на инциденты
- Определение параметров и сроков отчетности
- Выбор срока хранения данных

6

Введение в эксплуатацию

- Тестирование
- Запуск мониторинга событий и реагирования на инциденты

ЦЕНООБРАЗОВАНИЕ

Стоимость сервиса ISOC рассчитывается, исходя из нескольких параметров

in4security.com