софтлайн РЕШЕНИЯ

Облачные решения для вашей безопасности: Максимум защиты, минимум усилий

Роман Зацепин

Менеджер продукта, Softline Облако

ISOC – Security Operation Center от Infosecurity, ГК Softline

ISOC - сервис круглосуточного мониторинга, выявления и предотвращения киберугроз. Доступен в вариантах стандартного SOC и SOC Mini для гипервизора облака Softline

Центр предназначен для мониторинга, обнаружения, анализа и реагирования на киберинциденты в информационных системах организации

Security Operation Center концептуально состоит из трёх составляющих:

1. Люди – ИБ и ИТ специалисты Infosecurity
2. Программное обеспечение и технологии – SIEM и IRP/SOAR-системы
3. Процессы и регламенты – выстроенные системы оповещения и реагирования

Чем поможет ISOC

Задачи, которые решает SOC:

✓ Снижение рисков ИБ
✓ Сокращение величины ущерба от инцидентов ИБ
✓ Выполнение требований регуляторов
✓ Повышение уровня зрелости ИБ компании
✓ Снижение нагрузки на ИБ и ИТ персонал

Проблемы заказчиков в части ИБ:

- Недостаточная эффективность превентивных средств защиты из СЗИ - нет единого видения инцидента ИБ
- Отсутствие регламентированных и отлаженных процессов реагирования
- Недостаточная численность и квалификация внутренней команды
- Часть оборудования в зоне ответственности ИТ
- Большой поток ложных срабатываний

ISOC 2025

50+ экспертов в команде

10+ лет экспертизы и опыта

Мониторинг и реагирование **24x7**

Расследование сложных инцидентов

Собственный Threat intelligence

Гибкий SLA и условия оплаты

100+ поддерживаемых источников

500+ собственных сценариев детектирования

30+ сценариев автоматического реагирования

Лучшие технологии на рынке РФ

Стоимость владения **в ~4 раза** ниже in-house SOC

Как работает ISOC

События с источников клиента

Автоматический Мониторинг

Создание заявки и email/tg оповещения

Первичный анализ и обработка инцидента

Реагирование L1

(верификация)

Верификация, оповещение

Подключение эксперта к онлайн-анализу

Подробный анализ и обработка инцидента, анализ образцов вредоносного кода

Реагирование L2

(playbooks)

Применение контрмер - активное реагирование на выявляемые инциденты специалистами SOC на KEDR плюс экспертные пошаговые рекомендации

Реагирование L3

(сложные инциденты ИБ)
+расследования

Расширенная поддержка, консультации, сопровождение специалистов заказчика по применению выдаваемых рекомендаций.

Возможные конфигурации сервиса

РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИБ L3

- Реагирование на нетиповые инциденты
- Расследование инцидентов
- Анализ последствий и рекомендации
- Расширенные консультации

РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИБ L2 (24x7)

- Реагирование по плейбукам
- Применение контрмер
- Автоматизация реагирования

РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИБ L1 (24x7)

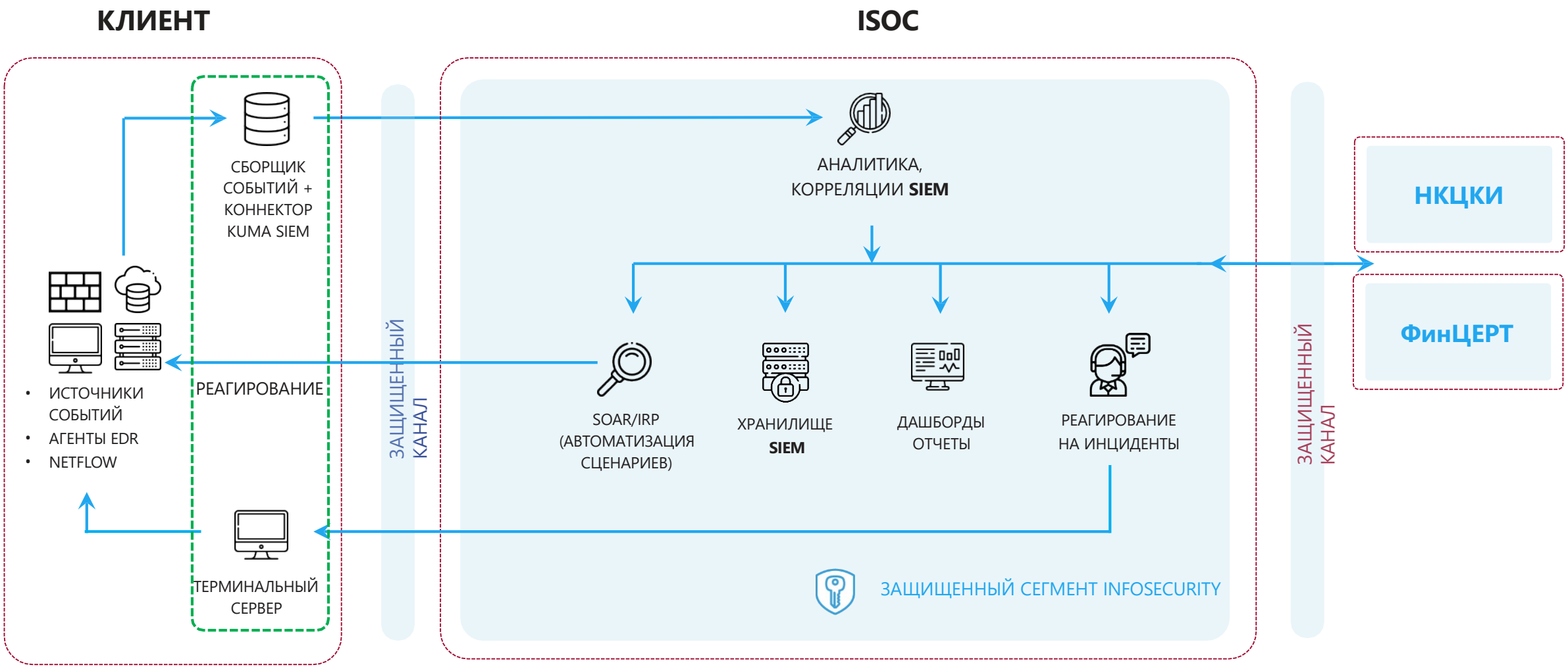
- Верификация инцидентов
- Первичный анализ инцидентов
- Классификация инцидентов
- Фильтрация false positive
- Базовые рекомендации

АВТОМАТИЧЕСКИЙ МОНИТОРИНГ И ВЫЯВЛЕНИЕ ИНЦИДЕНТОВ ИБ (24x7)

- Подключение источников клиента к ISOC
- Использование сценариев детектирования ISOC
- Хранение событий в инфраструктуре ISOC
- Доступ к личному кабинету Платформы ISOC
- Выделенный сервис-менеджер
- Выделенный аналитик (сопровождение контента)

Индивидуальная конфигурация сервиса для каждого клиента!

ISOC – архитектура SOC as a Service



Интерфейсы сервиса ISOC

Автоматические оповещения (telegram/e-mail) о выявленных подозрениях на инциденты ИБ

Личный кабинет для просмотра событий ИБ, алертов, инцидентов, этапов обработки инцидента ИБ (в т.ч. детали и рекомендации)

Рекомендации по самостоятельному разрешению инцидента ИБ и минимизации последствий – по согласованным каналам связи

Телефонные звонки ответственным лицам при верификации особо критичных подозрений на инциденты ИБ

Интеграция с ITSM системами клиента, автоматическое реагирование на инциденты ИБ

Регулярные статистические отчеты по событиям ИБ, детальные отчеты по каждому инциденту ИБ и его разрешению

Автоматизация реагирования на инциденты ИБ

Единое окно контроля за циклом управления и реагирования на инциденты ИБ

Сокращение времени реагирования на типовые инциденты ИБ (снижение MTTR до 20 раз!)

Упрощение процессов и автоматизация рутинных задач

Интеграция с прочими сервисами на уровне плейбуков (в т.ч. Security Awareness)

Защита IT-инфраструктуры от DDoS-атак

Network DDoS Protection – защита IT-инфраструктуры от атак на переполнение каналов, UDP-флуда и прочих типов массовых или сложных атак

Мониторинг атак – 24/7 с покрытием всего трафика через блоки фильтрации и модули сетевой защиты. Есть возможность использования фильтрации во время атак

Превентивно блокирует более 99% сетевых атак на любые корпоративные сервисы по протоколам TCP, UDP, SMTP, FTP, SSH
+ VoIP, VPN

- ✓ Возможность подключения выделенных анализаторов трафика
- ✓ Техническая поддержка 24/7
- ✓ Предоставление личного кабинета с отчётами

Веб-защита от DDoS-атак и ботов

На уровне приложений – защита от прикладных, протокольных и объёмных атак, парсеров и других угроз

Отслеживает, анализирует и фильтрует веб-трафик с последующим определение и блокировкой вредоносного трафика

- Поддерживает настройку белых/черных списков
- Работает с Websocket и IPv6
- Поддерживает балансировку нагрузки и блокировку по сессиям вместо IP-адресов
- Коэффициент ложны срабатываний меньше 0,02%

Q&A

Roman.Zatsepin@softline.com

@ZATSEPIN_CLOUD