софтлайн решения SOFL

Безопасность в облаке: как за каменной стеной: ISOC, WAF, ADDoS

Роман Зацепин

Менеджер по развитию продуктовой экспертизы

Цифры и факты за 2023 год*

- 2 500+ атак на компании РФ в 2023 году
- 74% атак носят целенаправленный характер
- 96% компаний не защищены от проникновения внешнего злоумышленника
- 53% компаний не защищены от векторов атак низкой сложности
- до 80% инцидентов могут быть обнаружены на основании всего лишь одного события ИБ
- 37 дней медианное время обнаружения факта компрометации инфраструктуры

***По данным компаний Positive Technologies и Лаборатория Касперского**

ISOC. На страже вашей облачной инфраструктуры

Инфраструктура. Надёжная. Защищённая.

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

ИБ в облачной инфраструктуре

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

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)

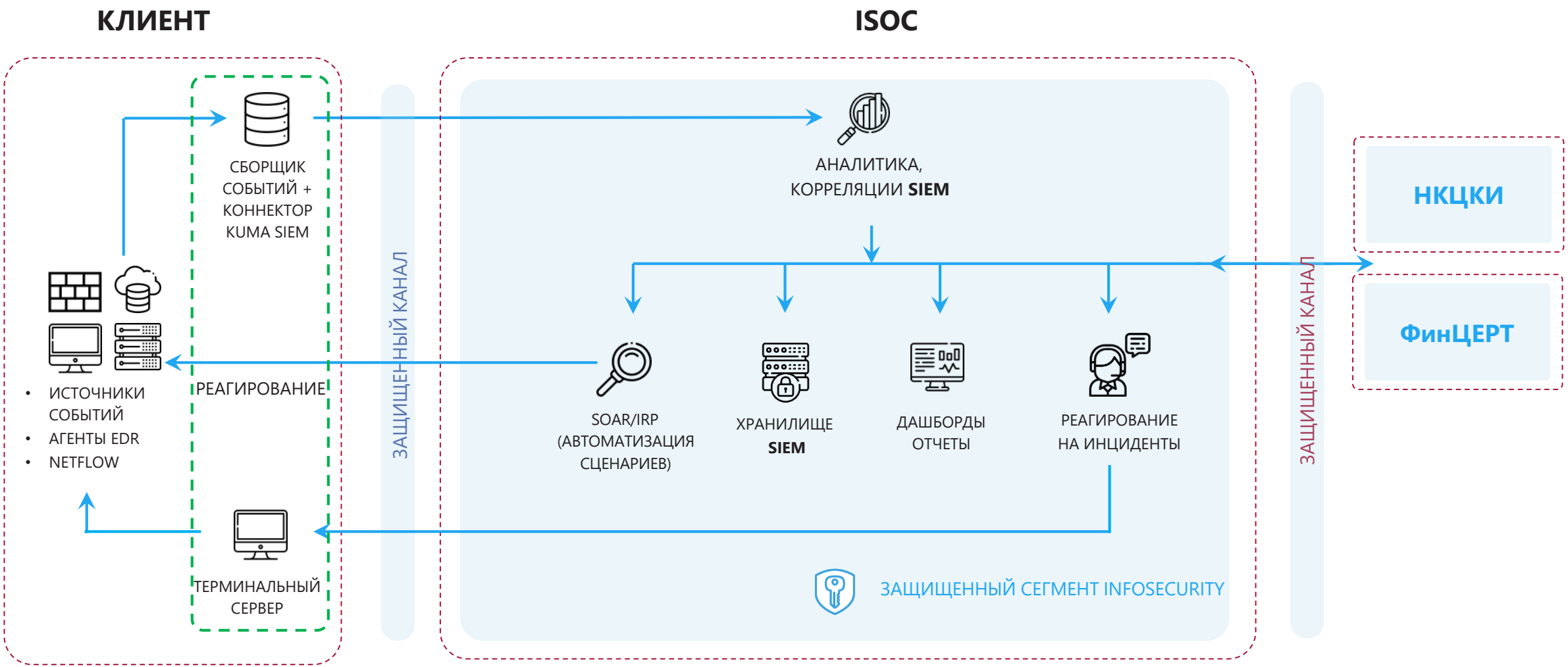
- Верификация инцидентов
- Первичный анализ инцидентов
- Классификация инцидентов
- Фильтрация false positive
- Базовые рекомендации

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

WAF + ADDoS/Анти-Бот L7: предотвратить и обезвредить

Вебмониторэкс - WAF как сервис

Вебмониторэкс – комплексная система для защиты веб-приложений и API

Сервис решает задачи:

- Защиты от угроз OWASP Top-10 и 0-day уязвимостей
- Защиты конфиденциальной информации от утечек
- Сокращения репутационных рисков, вызванных взломами
- Защиты личных кабинетов партнеров и клиентов компании
- Сокращения затрат на защиту веб-приложений, микросервисов и API
- Соответствия требованиям стандартов безопасности

Продукт внесён в Единый реестр российских программ для электронных вычислительных машин и баз данных

Проходит испытания ФСТЭК, ожидается получение сертификата в течение 2024 года

Фильтрующая нода

Фильтрующая нода разворачивается в инфраструктуре облака Софтлайн в виде виртуальных машин

Под конкретное приложение* разворачивается отдельная VM, в целом, количество VM зависит от прогнозируемой нагрузки

Фильтрующий узел выполняет следующие действия:

- Блокирует вредоносные запросы и пропускает легитимные
- Анализирует http-запросы компании
- Собирает и выгружает их в Вычислительный кластер Вебмониторэкс
- Загружает индивидуальные правила для сетевых ресурсов из Вычислительного кластера Вебмониторэкс

**под приложением подразумевается некоторое к-во доменов, использующих один SSL-сертификат; доступность по одному или нескольким однородным эндпоинтам; расположение на уникальных портах)*

Вычислительный кластер

Вычислительный кластер находится в инфраструктуре Вебмониторэкс в ЦОД на территории РФ

Вычислительный узел выполняет следующие действия:

- Обрабатывает полученные от фильтрующей ноды метрики трафика
- Формирует индивидуальные правила для сетевых ресурсов
- Сканирует защищаемые ресурсы компании на наличие уязвимостей

ADDoS L3-L7 + анти-бот

Network DDoS Protection – защита IT-инфраструктуры от сетевых атак на базе технологии DosGate

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

Для защиты веб-приложений от DDoS-атак и ботов используется решение Cybert

Cybert использует многофакторные методы анализа, включая машинное обучение, для анализа трафика и активностей ботов

Обеспечивает защиту от любых объёмных, протокольных и прикладных DDoS-атак без ограничений по объёму и типу атак

Резюмируя

Комплекс решений обеспечивает защиту Облака Софтлайн:

- на уровне сети – надёжная ADDoS-защита
- на уровне приложений – ADDoS L7, WAF и анти-бот
- мониторинг инфраструктуры и реагирование на инциденты – ISOC

Данные решения доступны в формате SaaS для защиты ваших IT-инфраструктур: облачных и локальных

Q&A

Roman.Zatsepin@softline.com

@ZATSEPIN_CLOUD

Инфраструктура. Надёжная. Защищённая.

софтлайн РЕШЕНИЯ