"Информационная безопасность 2025"

Собственный SOC или сервис-провайдер: что бы выбрать. На основе реального кейса.

20 февраля 2025 г.
Москва

О чем поговорим

1. Вызовы современного ландшафта киберугроз, необходимость непрерывного мониторинга корпоративной инфраструктуры
2. Что представляет собой современный центр мониторинга: функции, технологии, процессы
3. Варианты реализации мониторинга инцидентов кибербезопасности и реагирования на них
4. Некоторые сложности при построения внутреннего SOC
5. Особенности SOC от провайдера
6. Ключевые выводы

Коротко: Почему превентивных средств защиты недостаточно

Атаки на цепочку поставок и взлом подрядчиков

По данным исследования Threat Zone 2024 такие атаки явились одним из трендов

Уязвимости нулевого дня

Пример: за один месяц обнаружено 7 уязвимостей в CMS «1С-Битрикс» (CVE-2023-1713 — CVE-2023-1720)

Зачем нужен мониторинг событий кибербезопасности?

- Множество разрозненных средств защиты **не дают** целостной картины происходящего в инфраструктуре
- Для того чтобы выполнять ретроспективный анализ и выявлять **атаки активные в прошлом**
- (При необходимости) Для удовлетворения требований законодательства (ФЗ-187, 152)
- (При необходимости) Чтобы пройти сертификацию (PCI DSS, ISO 27001)

Что такое SOC

SOC (Security Operations Center) — это центр безопасности, отвечающий за мониторинг, анализ и реагирование на инциденты кибербезопасности в реальном времени.
Его команда специалистов круглосуточно следит за инфраструктурой компании, выявляет угрозы и предотвращает (сообщает Заказчику) кибератаки.

Технологии

Люди

Процессы

Основные функции SOC

1. **Мониторинг безопасности:** круглосуточное наблюдение за сетями, системами и приложениями для выявления аномалий и подозрительной активности.

2. **Анализ инцидентов:** оценка и исследование выявленных инцидентов для понимания их природы и возможного воздействия.

3. **Реагирование на инциденты:** разработка и выполнение плана действий для устранения угрозы, минимизации ущерба и восстановления нормальной работы.

4. **Проактивный поиск угроз:** исследование данных и поведения систем, поиск подозрительной активности, для выявления угроз до нанесения ущерба

5. **Управление уязвимостями:** поиск и устранение слабых мест в инфраструктуре, которые могут быть использованы злоумышленниками.

6. **Отчетность и аналитика:** составление отчетов по инцидентам, анализ трендов и предоставление рекомендаций для улучшения безопасности бизнеса.

Security Operation Center (SOC): варианты организации

Способ реализации зависит от различных факторов: размера компании, ее информационной инфраструктуры и финансовых возможностей

On-premise

Построение функции SOC полностью внутри организации

Гибридная модель

Частичная реализация функций во внутреннем SOC, а на «аутсорс» отдаются отдельные задачи

Аутсорсинг

Полная передача функции SOC MSS-провайдеру*

*Managed Security Services (MSS) - это внешняя компания (провайдер), которой делегировано управление средствами защиты информации.

Сравнение SOC

	Внешний SOC	Гибридный SOC	Внутренний SOC
Режим работы	24/7	24/7	24/7 (8/5)
Скорость развертывания	2–3 недели	3–9 месяцев	3–9 месяцев + 1 год обучения команды заказчика
Уровень компетенций	Высокий	Высокий/средний	Высокий/средний
Форма наибольших затрат	OPEX	CAPEX + OPEX	CAPEX + ФОТ + OPEX
Масштабирование	Высокое	Среднее	Среднее
Уровень нагрузки на заказчика	Низкий	Средний	Высокий
Необходимый размер команды (min)	2	5	12
Гибкость в настройке под свои нужды	Средняя (стандартные сервисы и SLA)	Средняя (стандартные сервисы и SLA)	Высокая
Возможности по реагированию	Средние (MDR*)	Средние (MDR)	Высокие
Зависимость от каналов связи	Высокая	Высокая	Средняя\минимальная
Ответственность за результат	На провайдере	Смешанная	На клиенте

* Managed Detection and Response (MDR) — это сервис для бизнеса по обнаружению киберугроз и реагированию на них. Службы MDR включают сочетание технологий и опыта человека для выполнения охоты на киберугрозы, мониторинга и реагирования.

Сложности при запуске SOC in-house: нехватка экспертизы

- Независимой оценки финансово-экономического обоснования на создание и развитие SOC
- Методологической базы для обследования, проектирования, обучения персонала
- Понимания в силу нехватки опыта необходимого образа SOC in-house и его границ
- Знаний о ландшафте киберугроз и профилях злоумышленников, нацеленных на компанию
- Привязки пакетов экспертизы в коробочных решениях (SIEM, SOAR, EDR и т. д.)* к рабочим процессам SOC и инфраструктуре компании
- Времени и опыта для разработки релевантного контента SOC

*SIEM (Security information and event management), SOAR (Security Orchestration, Automation and Response), Endpoint Detection and Response (EDR)

Сложности при запуске SOC in-house: развертывание технологической платформы SOC

Компоненты технологической платформы

Система реагирования на инциденты – Incident response platform (IRP) – единый инструмент для работы аналитиков всех линий SOC

Security information and event management (SIEM) – система сбора событий безопасности из разнородных источников и управления ими

Брокер событий – компонент SIEM для сбора событий информационной безопасности, осуществляет предварительную фильтрацию и обработку поступающих событий.

Система управления контентом – централизованная база знаний и оркестратор правил корреляции

Endpoint detection and response (EDR) – система защиты конечных точек

Система управления информацией о киберугрозах – Threat intelligence platform (TIP) – инструмент сбора, агрегации и поиска информации об угрозах кибербезопасности

Типовая орг.структура in-house SOC

* (Digital Forensics and Incident Response, DFIR)

Сложности при запуске SOC in-house: дефицит кадров в ИБ

Число вакансий стремительно растет и специалистов не хватает

48%

Составил рост числа вакансий в кибербезопасности за последние два года по данным hh.ru

Мифы о сервисной модели в кибербезе

Компания будет зависеть от провайдера, если перейдет на сервисную модель безопасности

Реальность

1. Гибкий и простой переход возможен
2. Локальное внедрение больше сковывает компанию
3. Провайдеров больше, чем продуктов

Мифы о сервисной модели в кибербезе

Опасно передавать данные организации стороннему подрядчику

Реальность

1. Подрядчик отвечает за безопасность данных и защищаемой инфраструктуры
2. Требования регуляторов к провайдерам сервисов выше, чем к клиентам
3. Для провайдера сохранность данных — вопрос существования бизнеса

Мифы о сервисной модели в кибербезе

Свои сотрудники лучше знают инфраструктуру и бизнес-процессы компании, поэтому эффективнее решают задачи

Реальность

1. Сотрудникам провайдера помогают высокая квалификация и система личных менеджеров
2. Своя инфраструктура изначально может быть с проблемными местами, а аутсорсинг поможет ее оптимизировать

SOC от сервис-провайдера: ключевые особенности и преимущества

- Экономия ресурсов
- Доступ к экспертизе сервис-провайдера
- Быстрая масштабируемость
- Оперативное реагирование на возникающие инциденты
- Решение кадрового вопроса
- Возможность сосредоточиться на стратегических задачах

Ключевые выводы

1. Актуальный ландшафт киберугроз требует непрерывного мониторинга инфраструктуры
2. Существуют несколько вариантов реализации центра мониторинга и реагирования на киберинциденты
3. Аутсорсинг функции SOC помогает компаниям сэкономить ресурсы и выстроить надежную защиту от актуальных угроз с использованием современных технологий