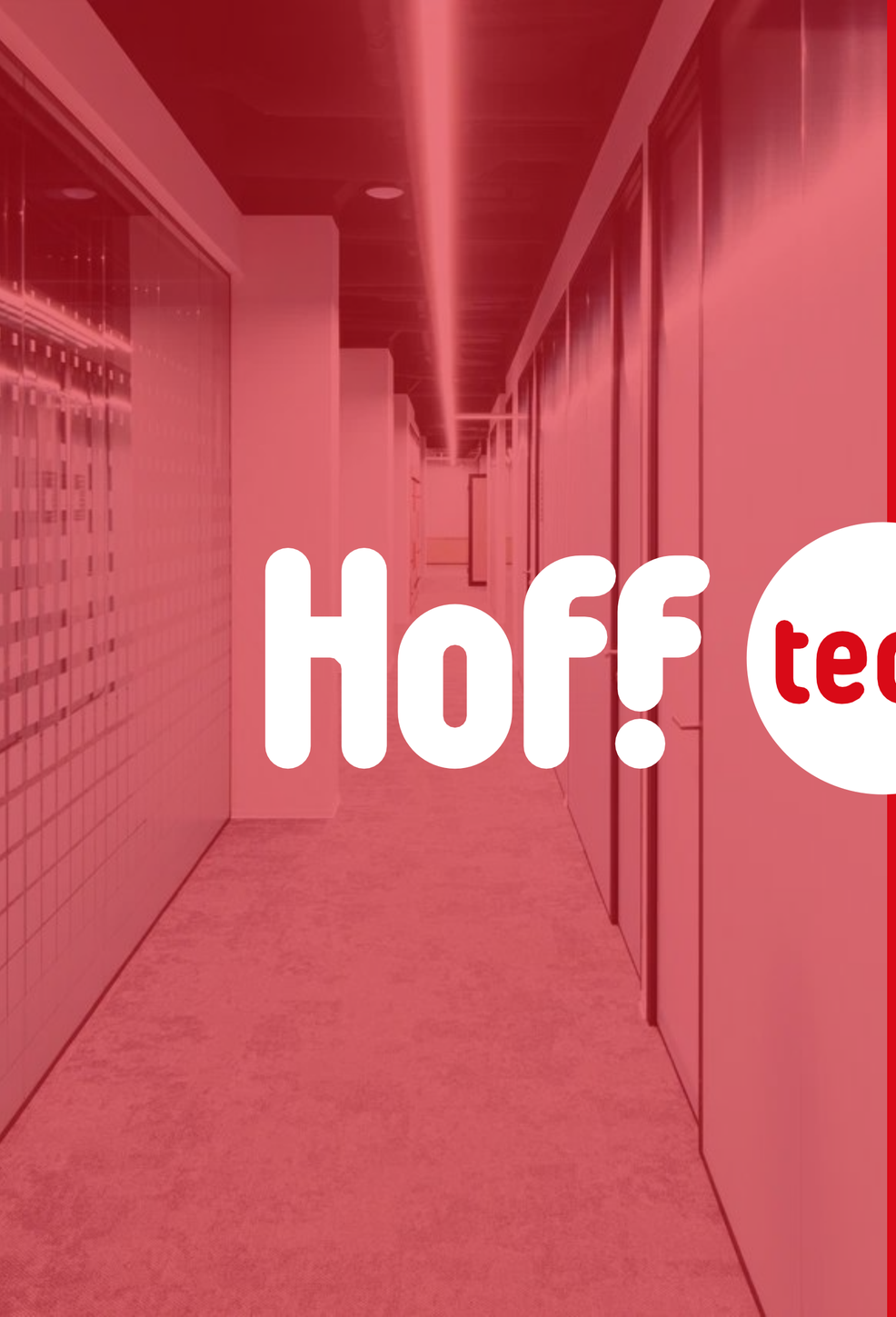


# Собственный SOC или аренда: что выбрать

26 сентября 2024

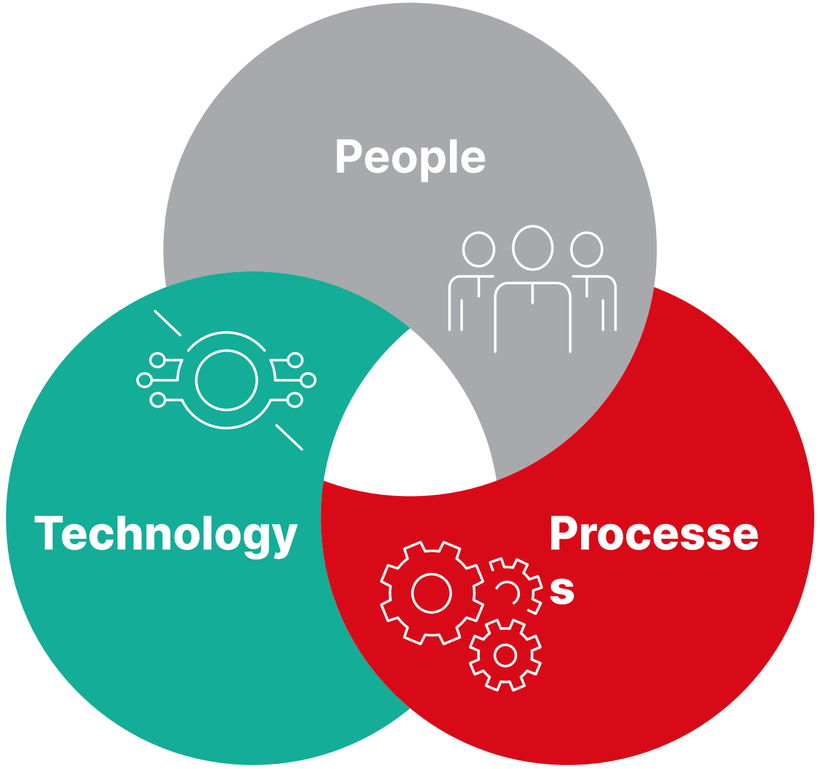
# Содержание

# Что такое SOC?

**SOC** Организационная единица, обеспечивающая решение операционных ИБ-задач с помощью комбинации технологических решений и набора процессов

## Зачем:

- Централизованный и непрерывный мониторинг ИБ
- Сокращение времени выявления и реагирования на инциденты ИБ
- Централизация обеспечения ИБ (security operations)
- База для сервисной модели ИБ (SLA/OLA)
- Соответствие требованиям регуляторов в области ИБ



# Жизнь без SOC

- Отсутствие понимания происходящего в инфраструктуре (нет возможности связать отдельные события ИБ в целостную картину)
- Нет фактуры для фокуса внимания ИБ и реализации как оперативных, так и тактических и стратегических мер по защите
- Невозможность расследовать инциденты оперативно (например, реагирование по журналам СЗИ и систем не будет оперативно)
- Ограниченная экспертиза и ресурсы внутренних специалистов в части выявления, реагирования, предотвращения кибер-атак
- Задержка в реагировании и предотвращении развития инцидентов (в том числе все, что происходит во внерабочее время и выходные)
- Ущерб, которого можно было бы избежать или минимизировать за счет раннего выявления инцидента ИБ

# Жизнь без SOC – примеры инцидентов

## Логистическая компания

Хакеры создали фишинговую страницу, имитирующую портал компании. Собрали в интернете почтовые адреса сотрудников и направили им рассылку с просьбой сменить пароль от учетной записи. Сотрудники переходили на фишинговую страницу и вводили свои логины и пароли. Хакеры, используя эти данные, попали во внутреннюю почту, изучили переписку, нашли бухгалтера, который готовит платежные поручения, подделали их и вывели деньги.

**Ущерб: более 100 млн рублей.**

## Микрофинансовая компания

Компания пользовалась услугами подрядчика для разработки собственного ПО. У подрядчика была учетная запись с правами администратора на хосте, на котором устанавливается ПО.

Хакеры проэксплуатировали уязвимость на периметре у подрядчика, получили доступ во внутренний конфлюенс и обнаружили эту учетную запись. С ее помощью попали в инфраструктуру целевой компании, **повысили привилегии, скомпрометировали домен и запустили шифровальщика. Затем связались с руководством компании с требованием выкупа.**

## Ритейл/Логистическая компания

Скомпрометирован подрядчик и получен первоначальный доступ. Далее эксплуатация уязвимостей Windows и компрометация корпоративного домена. Запуск шифровальщика по всей инфраструктуре (Win, NIX-like, виртуализация).

**Простой бизнес-процессов составил 3 дня.**

**Во всех этих кейсах смог бы помочь SOC и остановить атаку до компрометации домена**

# Как SOC может помочь в борьбе с шифровальщиком

| Тактика MITRE ATT&CK | Описание действий группировки | Варианты выявления и реагирования SOC |
|---|---|---|
| Reconnaissance | Поиск утечек<br>Анализ периметра на предмет уязвимостей | Мониторинг утечек<br>Мониторинг поверхности атаки |
| Initial Access | Доступ с легитимными данными через опубликованные сервисы<br>Эксплуатация уязвимости | Обнаружение нестандартных/нетипичных авторизаций<br>Выявление нелегитимной/потенциально вредоносной активности |
| Execution | Запуск bat-скрипта посредством CMD | Выявление нелегитимных процессов, запуска нелегитимных скриптов |
| Persistence | Создание запланированных задач | Обнаружение создания нелегитимных задач в планировщике |
| Credential Access | Запуск Mimikatz, Impacket | Выявление попыток дампа LSASS, запуска HackTool |
| Discovery | Запуск ADRecon, Rubeus, wmic, nslookup, ping, ipconfig, net, quser, qwinsta, SoftPerfect Network Scanner | Выявление нелегитимной/потенциально вредоносной активности, внутреннего сканирования |
| Lateral Movement | Запуск PsExec посредством CMD/PowerShell | Выявление запуска нелегитимных скриптов<br>Обнаружение вредоносных командлетов |
| Command and Control | Reverse SSH-туннель<br>Отправка POST-запроса через PowerShell на C2-сервер<br>Использование Plink, GOST и SOCKS-прокси | Выявление нелегитимных SSH-соединений<br>Обнаружение вредоносной активности PowerShell<br>Выявление нелегитимных процессов |
| Exfiltration | Запуск Rclone и выгрузка данных в облако | Выявление нелегитимных процессов и попыток выгрузки данных в сеть Интернет |
| Impact | Запуск шифровальщика Cicada3301, PsExec<br>Отключение сервисов ОС, удаление теневых копий, отключение функций восстановления данных, остановка ВМ | Выявление нелегитимных процессов, запуска нелегитимных скриптов, отключения механизмов защиты и ВМ |

**Repellent Scorpius1** — группировка Ransomware-as-a-Service (RaaS), которая распространяет шифровальщик Cicada3301.

На текущий момент группировка запрещает активность в странах СНГ (https://unit42.paloaltonetworks.com/repellent-scorpius-cicada3301-ransomware/)

# Модели SOC

| Параметры | In-house SOC | Hybrid SOC | Outsource SOC |
|---|---|---|---|
| **Архитектура** | Размещение технических платформ SOC в собственной инфраструктуре | | Размещение технических платформ SOC в инфраструктуре провайдера |
| **Процессы** | Самостоятельная реализация процессов SOC | Реализация процессов по установленным SLA (гарантия реализации процессов с высоким уровнем качества) | |
| **Персонал** | Собственный квалифицированный персонал для оказание услуг в режиме 24*7/8*5 | Персонал провайдера + [формирование экспертизы внутри] | Персонал провайдера |
| **Затраты на запуск** | CAPEX на инфраструктуру SOC<br>OPEX на формирование квалифицированной команды | CAPEX на инфраструктуру SOC<br>OPEX на услуги провайдера по реализации сервисов и формирование квалифицированной команды | OPEX на услуги провайдера по реализации сервисов |
| **Скорость запуска** | 24-36 месяцев | 6-12 месяцев | 2 месяца |

# Плюсы гибридной модели для нас


- Экономическая целесообразность (TCO на 5 лет)
- Инвестиции в технологии на нашей стороне
- Контроль за SIEM на нашей стороне
- Оперативное круглосуточное уведомление об инцидентах
- Если провайдер уходит, контент остается
- Относительно быстрый старт
- Четко зафиксированный SLA с провайдером
- Независимая экспертиза и «второе мнение»

# Выбор провайдера

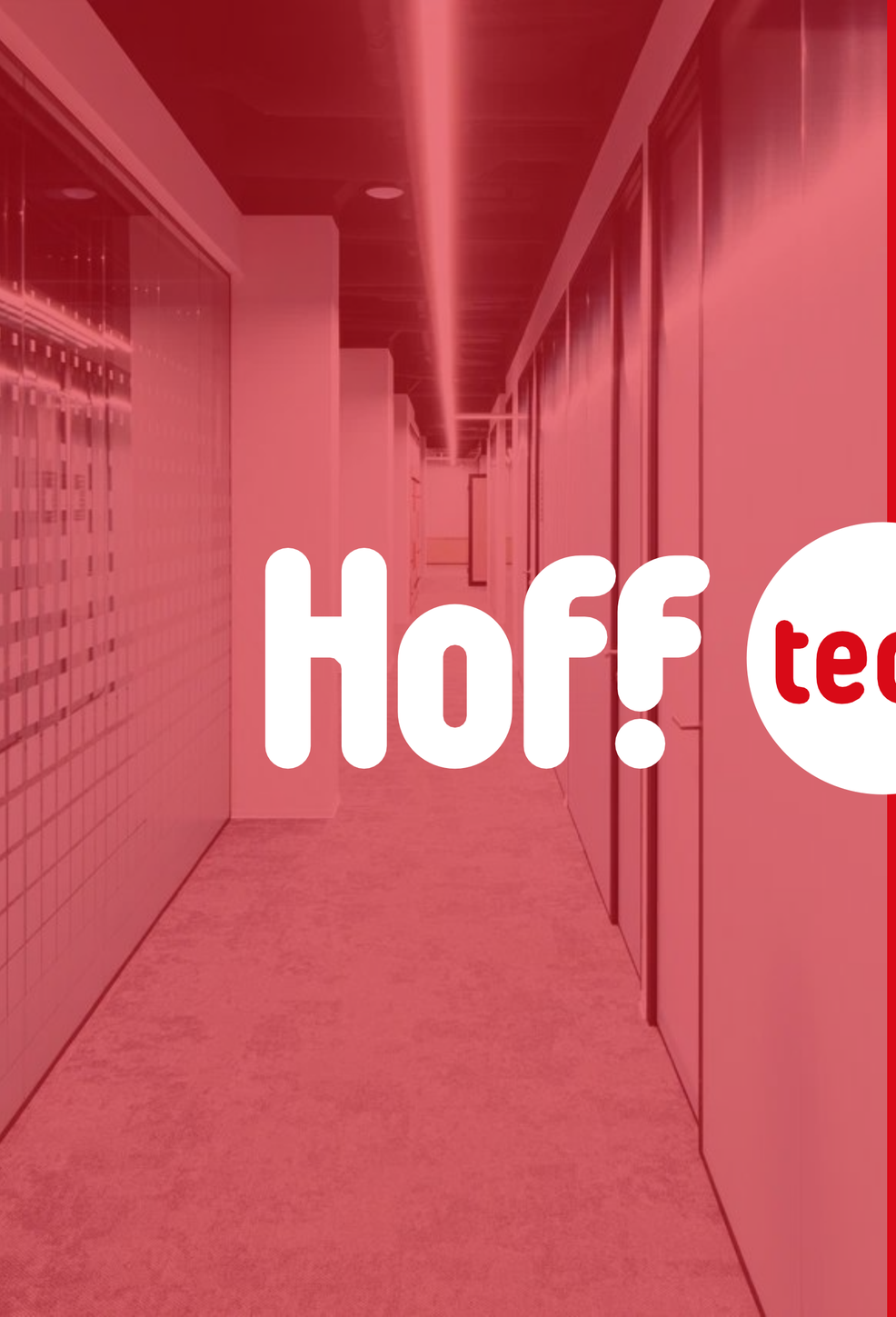
- Экспертиза: опыт оказания аналогичных услуг
- Гибкая настройка объема сервиса
- Четко зафиксированный SLA с провайдером
- Опыт участия и победы в соревнованиях SOC
- Возможность оставить корреляционный контент
- Консалтинг по подключению источников
- Пилот + Тест-кейсы
- Совместимость с SIEM

# Критерии эффективности SOC

1. Количество зарегистрированных инцидентов ИБ:
   - Классификация зарегистрированных инцидентов ИБ
   - Процентное соотношение зарегистрированных ложноположительных срабатываний
   - Классификация ложноположительных срабатываний
2. Количество зарегистрированных событий безопасности
   - Количество событий от подключенных источников за период
   - Средняя скорость поступления событий (EPS) за период
3. Соблюдение параметров SLA
   - доступность системы мониторинга
   - время реакции на потенциальный инцидент ИБ
   - время анализа и информирования о потенциальном инциденте ИБ
   - время реагирования на запросы
4. Распределение и аналитика зарегистрированных событий:
   - по критичности
   - по категориям
   - по классификации
5. Взаимодействие с SOC
   - Количество выполненных профилирований
   - Количество новых корреляционных правил
   - Количество зарегистрированных и обработанных запросов в SOC
6. Время, затраченное заказчиком, на реагирование:
   - % реальных инцидентов от общего числа событий
   - % ошибок от SOC (запрофилированные или технические)
   - % покрытия SOCом «контекста»

# Ожидание vs реальность

- SOC не работает «под ключ» - везде есть люди
- Успешность реализации – совместная работа.
- Заказчик должен выделять внутренний ресурс на обработку события от SOC, реагирование, управление процессом
- Неочевидные области лучше прояснять сразу: допрофилирование, контроль поступления событий и проч.
- Повышение «дисциплины» ИТ
- Правила из коробки / реальная база корреляции



# Спасибо за внимание!

**Шлегель Андрей**
Директор по информационной безопасности
Hoff Tech

26 сентября 2024