positive technologies

Чек-лист

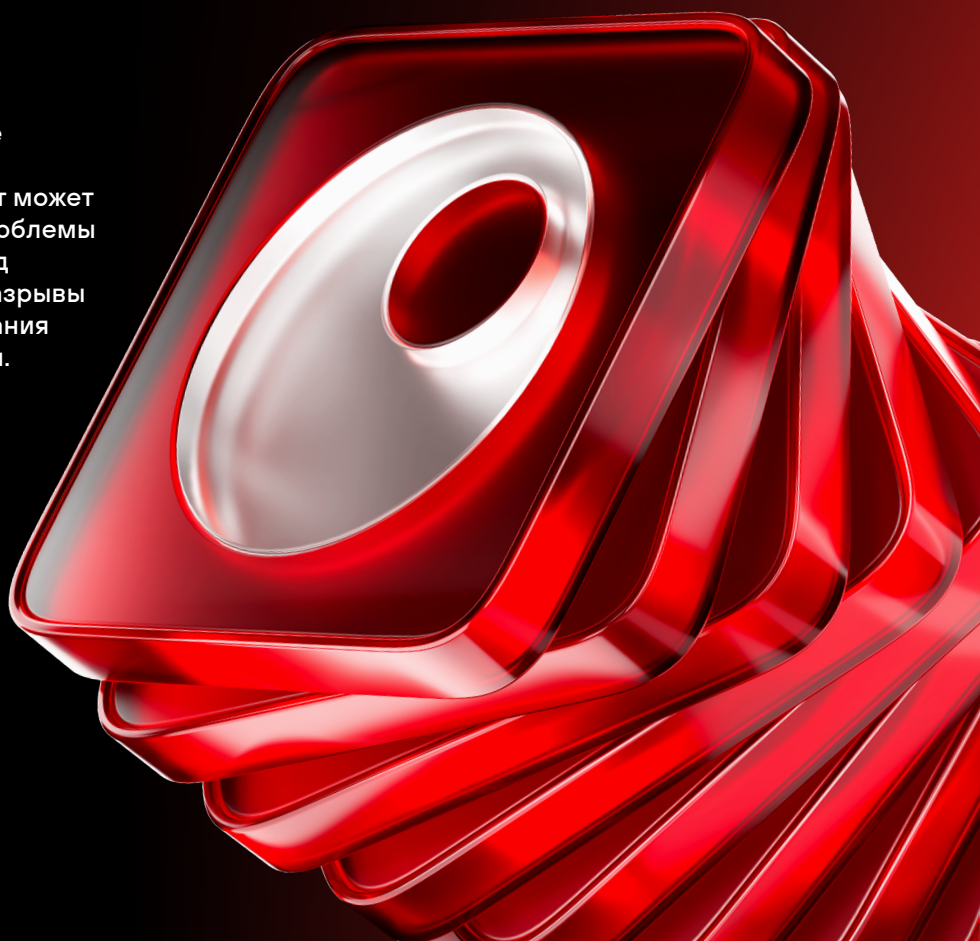
7 ПРИЗНАКОВ ТОГО, ЧТО ВАШ SOC РАБОТАЕТ НА ПРЕДЕЛЕ

Современный SOC может быть оснащен десятками средств защиты: SIEM, EDR, NGFW, NDR, платформами threat intelligence и управления уязвимостями. Но даже большой арсенал инструментов не гарантирует эффективного расследования инцидентов и быстрого реагирования на атаки.

Проблемы часто начинаются не на этапе обнаружения угроз, а во время расследования: аналитики вынуждены переключаться между системами, вручную собирать контекст и координировать действия разных команд.

Мы собрали чек-лист, который поможет найти слабые места в работе вашего SOC.

При ответе на вопросы ориентируйтесь на опыт работы команды за последние 3–6 месяцев или на наиболее значимые инциденты, с которыми сталкивалась организация. Каждый отмеченный пункт может указывать на операционный разрыв: проблемы в процессах, во взаимодействии команд или в работе с инструментами. Такие разрывы замедляют SOC, усложняют расследования и снижают контроль над реагированием.



MaxPatrol 360

01

Расследование превращается в поиск информации

Аналитики тратят время на поиск данных и переключение между инструментами вместо расследования

Признаки

Для расследования одного инцидента приходится работать сразу в нескольких системах

Информация по инциденту хранится в разных инструментах и не собирается в единой карточке

После завершения расследования сложно восстановить историю действий команды

02

SOC тонет в потоке алертов

Вместо управления реальными рисками команда вынуждена разбирать поток уведомлений. В таком режиме легко пропустить по-настоящему опасный инцидент.

Признаки

Аналитики регулярно сталкиваются с большим количеством малозначимых срабатываний

Приоритет инцидента определяется вручную

Много времени уходит на обработку ложноположительных событий

03

Для принятия решений не хватает контекста

Ручной сбор контекста затягивает расследование и повышает риск ошибочных решений.

Признаки

Информация об активах, пользователях, процессах, сетевых связях и уязвимостях собирается вручную

Сложно быстро оценить важность затронутого ресурса, его влияние на бизнес, сложно определить стадию атаки

Нет истории похожих инцидентов и ранее выполненных действий по реагированию

04

Реагирование зависит от конкретных сотрудников

Скорость и качество реагирования зависят от опыта отдельных специалистов, а не от выстроенного процесса.

Признаки

Типовые действия выполняются вручную через разные системы

Нет утвержденных процедур реагирования для распространенных сценариев

В типовых ситуациях сотрудники действуют несогласованно

05

SOC плохо связан с ИТ и бизнес-процессами

Даже качественное расследование может остановиться на этапе взаимодействия с ИТ-службами или владельцами бизнес-сервисов.

Признаки

Задачи по локализации и устранению инцидентов передаются через почту или мессенджеры

Нет прозрачного контроля действий смежных команд

Сложно понять, на каком этапе возникла задержка

06

Нет единой картины для руководителя SOC и CISO

Без прозрачных метрик и контроля процессов невозможно управлять эффективностью SOC и планомерно повышать его зрелость.

Признаки

Руководитель SOC не видит актуальную очередь инцидентов, отсортированных по важности и статусам

Отчеты по инцидентам и метрикам собираются вручную

Нельзя сравнить эффективность смен, команд, филиалов, тенантов или клиентов MSSP

07

SOC не учится на прошлых инцидентах

SOC устраняет последствия инцидентов, но не повышает зрелость процессов. Команда снова и снова решает одни и те же задачи, вместо того чтобы накапливать и масштабировать экспертизу.

Признаки

После инцидента не проводится анализ качества расследования и реагирования

Повторяющиеся инциденты разбираются каждый раз практически с нуля

Накопленный опыт не превращается в инструкции, готовые сценарии и описанные практики

ЕСЛИ ВЫ УЗНАЛИ СВОЙ SOC В НЕСКОЛЬКИХ РАЗДЕЛАХ

Скорее всего, основное ограничение связано не с обнаружением угроз, а с управлением расследованиями и реагированием: когда аналитики вынуждены переключаться между системами, вручную собирать контекст и координировать действия команд, даже зрелый стек средств защиты будет работать неэффективно.

Вернуть управляемость и скорость позволяет MaxPatrol 360. Платформа выступает единым центром управления расследованиями и операционной работой SOC, объединяя процессы, данные и действия команд в едином контуре:

Создает единую рабочую среду для аналитиков без постоянного переключения между инструментами

Централизованно управляет инцидентами на всех этапах жизненного цикла — от триажа до реагирования и последующего анализа

Автоматизирует типовые операции и сценарии реагирования с помощью плейбуков

Предоставляет подробную аналитику ключевых показателей SOC на дашбордах.

Сделать SOC единой системой управления киберустойчивостью