SOC: ГАРАНТИЯ РЕАЛЬНОЙ БЕЗОПАСНОСТИ ДЛЯ БИЗНЕСА

Современные центры мониторинга и противодействия кибератакам (Security Operations Center, SOC) становятся ключевыми игроками в обеспечении информационной безопасности бизнеса. Сегодня SOC — это не просто защита от киберугроз, а целый спектр услуг, от мониторинга до защиты бренда и первых лиц компаний. Поговорим о том, как SOC может изменить подход к обеспечению безопасности и почему компании уже сегодня выбирают эту услугу, с командой Центра мониторинга и противодействия кибератакам IZ:SOC («Информзащита»).

— Какие киберугрозы сегодня актуальны для ваших заказчиков?

Александр Матвеев (А.М.), *директор Центра мониторинга и противодействия кибератакам IZ:SOC:*

Кибератаки растут в геометрической прогрессии. Наша компания работает в сфере ИБ почти 30 лет, мы выросли вместе со всей отраслью, прожили все ключевые изменения и набрались колоссального опыта. Однако на этом пути есть и константы, например, увеличение числа атак. Сегодня они растут в геометрической прогрессии.За девять месяцев 2024 года их количество на российские компании выросло на 35%, деструктивные атаки увеоичились на 45%, а частота DDoS-атак выросла более чем на 50%.

Сегодня нет организаций, которые могут считать себя вне

Александр Матвеев

зоны риска. Атаки касаются не только крупного бизнеса, но и среднего и даже малого. В 2024 году мы видим четкий тренд: злоумышленники нацеливаются на всех без исключения, используя сложные методы, инновационные технологии и широкий спектр мотивов — от финансового вымогательства до деструктивных атак, инициированных государственными структурами. Компаниям уже не актуально задаваться вопросом: «А взломают ли нас?», более актуально спрашивать себя: «А когда нас взломают?» и «Не взломали ли нас уже?»

— Почему атак становится всё больше?

Сергей Сидорин, *руководитель третьей линии аналитиков:*

Рост количества атак связан с несколькими ключевыми аспектами: усложнением технологий, человеческим фактором и эволюцией самих киберпреступников. Хакеры используют инновации, такие как искусственный интеллект, для автоматизации атак, поиска уязвимостей и проведения фишинговых рассылок. Киберпреступность давно стала высокоорганизованным бизнесом, где преступные группы масштабируют свои операции, создают новые

Сергей Сидорин

инструменты и используют модели монетизации, схожие с легальным рынком.

Финансовая мотивация остается основным драйвером их активности, но при этом часть злоумышленников движима исключительно вредоносными целями — они стремятся нарушить работу систем, нанести ущерб или просто создать хаос. В 2024 году 60% компаний столкнулись с атаками на цепочку поставок — вектор атак через поставщика ПО или провайдера услуг.

Не стоит забывать о человеческом факторе: 60% утечек данных происходят из-за ошибок сотрудников. Решение — системное обучение работников правилам информационной безопасности, что может значительно сократить риск успешной атаки.

— Какое влияние оказывает на безопасность импортозамещение?

Артём Цалпанов, *эксперт третьей линии аналитиков:*

С 2022 года процесс импортозамещения сопровождается рядом проблем. Во-первых, не для всех западных решений есть отечественные аналоги. Российские вендоры активно работают над созданием новых продуктов, и многие из них уже демонстрируют отличные результаты. По ряду функций они даже превосходят зарубежные аналоги и лучше интегрируются в ИТ-инфраструктуру отечественных организаций.

Тем не менее некоторые российские решения пока не могут полноценно заменить западные продукты. Часть продуктов сталкивается с проблемами при высоких нагрузках, имеет ограничения по масштабированию или совместимости с уже существующей инфраструктурой. Однако работа по устранению этих

Артём Цалпанов

недостатков ведется активно, и мы видим, что многие отечественные решения постепенно становятся более устойчивыми и гибкими, предлагая конкурентоспособные альтернативы зарубежным продуктам.

Указ Президента РФ от 01.05.2022 № 250 обязывает объекты критической информационной инфраструктуры прекратить использование западных решений к 1 января 2025 года. При этом частные компании, не подпадающие под действие указа, часто откладывают замену технологий, надеясь на возвращение западных вендоров. Однако они игнорируют реальность: оборудование и ПО устаревают, что значительно снижает их эффективность в противодействии современным киберугрозам.

— Как можно охарактеризовать рынок коммерческих SOC в России?

А.М.: Рынок растет стремительными темпами. Коммерческие SOC становятся ключевыми центрами компетенций по защите бизнеса. В 2023 году при общем увеличении объема рынка ИБ на 20–30% рынок SOC вырос на 50–60%, и в 2024 году мы ожидаем сохранения этих показателей. В денежном эквиваленте он оценивается примерно в 23–24 млрд рублей. Развитие рынка стимулируют три ключевых фактора:

1) строгое законодательство, которое требует высокого уровня защиты;

2) цифровизация, открывающая новые векторы для атак;

3) расширение целей для хакеров, которые охватывают всё больше отраслей.

Однако сдерживающими факторами остаются нехватка квалифицированных специалистов и высокая сложность подготовки аналитиков экспертного уровня. Даже самая передовая технология бесполезна без опытной команды, которая сможет ее грамотно применить.

> Настоящая защищенность достигается только через комплексный подход и профессиональную экспертизу

— Как компании понять, что настало время строить свой SOC или воспользоваться услугой коммерческого? Какой вариант выбрать?

Кирилл Дёмин (К.Д.), *руководитель отдела систем мониторинга:*

Выбор между собственным SOC и коммерческим центром мониторинга зависит от множества факторов, включая размер компании, бюджет, доступные ресурсы, цели и уровень зрелости информационной безопасности. Существующие модели мониторинга ИБ можно рассматривать через призму трех основных подходов:

- *Собственный SOC* — это решение для крупных компаний с высокими требованиями безопасности, которые готовы к крупным и долгосрочным инвестициям на создание и содержание собственного центра. Такой in-house SOC позволяет интегрировать процессы мониторинга и обеспечения безопасности во все бизнес-аспекты, при этом предоставляет высокий уровень контроля, так как вся команда работает исключительно на одну организацию. Однако это требует значительных финансовых и временных затрат на поиск, развитие и удержание специалистов, закупку оборудования и технологий, а также их постоянную модернизацию.
- *Коммерческий SOC* — идеальный выбор для большинства компаний, которые хотят быстро и эффективно обеспечить защиту без значительных капитальных

Кирилл Дёмин

затрат на создание собственного центра. Коммерческие SOC предлагают проверенные решения, современную инфраструктуру и экспертизу высокого уровня, что позволяет оперативно реагировать на угрозы. Этот вариант подходит для бизнеса, которому важна реальная безопасность под ключ уже сегодня без значительных денежных и временных вложений в построение собственного SOC, а также для тех компаний, которые предпочитают аутсорсинг вместо создания внутренней команды безопасности. Важно отметить, что коммерческий SOC может предложить более широкий спектр услуг, таких как киберкриминалистика, пентест, защита периметра, защита бренда и другие специализированные сервисы по подписке.

- *Гибридный SOC* — это модель, в которой сочетаются лучшие черты коммерческого и собственного SOC. Классический пример, когда решения из технологического стека SOC (SIEM, SOAR и др.) расположены на стороне организации, тем самым позволяя сохранить контроль над основными процессами ИБ, при этом их непосредственный мониторинг осуществляется командой внешних экспертов, что помогает эффективно защитить вашу ИТ-инфраструктуру, оптимизировать затраты. Гибридный SOC всё чаще становится выбором для компаний, которые по тем или иным причинам не готовы полностью перейти на классический in-house SOC или полностью передать все составляющие защиты коммерческому SOC-провайдеру.

Ключ к выбору SOC — стратегический подход. Коммерческий SOC может стать оптимальным выбором для быстрого запуска эффективной защиты. Крупным корпорациям, которые хотят максимальной кастомизации и контроля, имеет смысл развивать собственный SOC. Гибридные модели — это золотая середина для бизнеса, который ищет баланс между эффективностью и затратами. Выбор SOC — это не только решение о безопасности, но и стратегическое инвестирование в стабильность бизнеса.

ГЛОССАРИЙ

SIEM
(Security Information and Event Management)
Система управления ИБ и событиями безопасности. Позволяет обнаруживать, анализировать и устранять угрозы безопасности раньше, чем они нанесут ущерб бизнес-операциям.

SOAR
(Security Orchestration, Automation and Response)
Система, которая помогает автоматизировать и ускорить процессы обнаружения и реагирования на кибератаки. Объединяет разрозненные инструменты и данные безопасности в единое целое, позволяя командам реагировать на угрозы быстрее и эффективнее.

— Что такое киберкриминалистика и почему она важна?

Шамиль Чич, *эксперт третьей линии аналитиков:*

Киберкриминалистика — это комплексное расследование инцидентов ИБ, включающее сбор и анализ цифровых доказательств, установление источника атаки, методов ее реализации и выявление виновных.

Эта услуга важна не только при крупных инцидентах или судебных разбирательствах. Киберкриминалистика помогает компаниям понять причины и последствия любых кибератак, выявить уязвимости в системе и предотвратить повторение подобных инцидентов в будущем.

Специалисты по форензике обладают уникальными компетенциями, объединяя знания в области ИБ и криминалистики, а также понимание технических, юридических и бизнес-аспектов инцидентов. Поскольку киберпреступления могут произойти в любой момент и затронуть организации любого размера, компаниям нет необходимости держать таких

Шамиль Чич

экспертов в штате постоянно. Поэтому бизнес обращается за помощью к специализированным организациям, таким как наша.

— Допустим, в компании уже выстроен процесс мониторинга ИБ. Какие еще услуги безопасности может предложить коммерческий SOC?

Станислав Кузнецов, *руководитель направления развития MSSP-сервисов:*

Дополнительные сервисы безопасности по подписке, которые помогут усилить защиту и закрыть специфические задачи. Такие услуги позволяют компаниям гибко адаптироваться к изменениям угроз без необходимости масштабных инвестиций в собственную инфраструктуру и штат.

Популярные сервисы безопасности по подписке:

- *непрерывный анализ защищенности* (Attack Surface Management, ASM) — мониторинг внешнего периметра для выявления потенциальных уязвимостей и рисков;
- *комплексная симуляция атак* (Breach and Attack Simulation, BAS) — автоматизированная симуляция реальных кибератак на ИТ-инфраструктуру с целью выявления слабых мест и проверки эффективности существующих мер безопасности;
- *защита бренда* (Digital Risk Protection, DRP) — защита цифровой репутации и активов организации, включающая обнаружение и предотвращение угроз, связанных с компрометацией бренда, утечкой данных и кибершпионажем;
- *поставка потоков данных об угрозах* (Malicious Feed Information, MFI) — предоставление доступа к актуальной и точной информации о киберугрозах в реальном времени для повышения эффективности систем обнаружения и реагирования на кибератаки;

Станислав Кузнецов

- *реверс-инжиниринг вредоносного ПО* — глубокий анализ и исследование вредоносных программ с целью определения механизмов их работы и функционального назначения с последующим использованием полученных данных для улучшения защиты.

Эти услуги позволяют компаниям сосредоточиться на ключевых задачах бизнеса, доверив сложные и узкоспециализированные аспекты защиты профессионалам.

— А если говорить именно о технологических решениях, что сегодня нужнее всего?

К.Д.: Технологический стек любого SOC крутится вокруг одних и тех же решений: SIEM, SOAR, TIP, VM, EDR. Данные классы продуктов при правильном внедрении и настройке позволяют обеспечить достаточный уровень защиты. Дополнительно данный стек может быть расширен решениями для анализа сетевого трафика (NTA), тестирования и наступательной безопасности (BAS, автопентест), средствами поведенческой аналитики (UEBA) и базовыми средствами защиты: NGFW, WAF, PAM и др. Помимо этого, выделенные команды SOC, например форензики, используют свои специфические инструменты для более узкоспециализированных задач.

Технологии SOC постоянно совершенствуются, искусственный интеллект и машинное обучение всё активнее внедряются в работу линий аналитиков SOC и другие процессы. Сейчас на пике всеобщая автоматизация процессов SOC, которая позволяет значительно повысить эффективность, ускорить ряд задач и оптимизировать ресурсы команды.

При этом двух одинаковых SOC не существует — каждая реализация уникальна благодаря сочетанию технологий, инструментов, процессов и уровня компетенций команды. Даже SOC, построенные на одних и тех же платформах, могут кардинально различаться по качеству работы, уровню предоставляемого сервиса и удобству для клиентов. Это зависит от того, как внедрены и настроены технологии, организованы процессы и обучен персонал. Ключевую роль играет наличие единого клиентского портала и единого окна взаимодействия, которые обеспечивают удобство, прозрачность и оперативность работы с SOC.

— Как компании эффективно проверить свой уровень защищенности?

Анатолий Песковский, *руководитель отдела анализа защищенности:*

Выбор подхода к проверке защищенности напрямую зависит от уровня зрелости вашей системы ИБ. Компании с базовым уровнем защиты и высокими рисками могут начать с простых решений, тогда как организации с развитой ИБ-инфраструктурой и собственной командой экспертов требуют более сложных методов оценки.

Для начала стоит обратить внимание на системы имитации атак, известные как BAS (Breach and Attack Simulation). Эти решения содержат готовую экспертизу по безопасной имитации сотен атак и методов злоумышленников, что дает компаниям возможность оперативно и недорого оценить уровень своей защищенности. BAS-системы работают автоматически, предоставляя дорожную карту для улучшения безопасности без необходимости привлекать дорогостоящих специалистов. Более того, существуют BAS-сервисы, которые могут быть использованы для проверки работы вашего действующего SOC-провайдера, выявляя, насколько эффективно он реагирует на имитацию реальных атак, давая объективное подтверждение уровня предоставляемой защиты.

Анатолий Песковский

Следующим этапом может быть проведение пентестов. Базовый пентест — это анализ безопасности, при котором команда экспертов вручную проверяет системы на наличие уязвимостей, оценивает потенциальные векторы атак и проводит ограниченное моделирование действий злоумышленников. Он обеспечивает глубокое понимание слабых мест инфраструктуры, но ограничен по времени. Чтобы сделать пентест быстрее и доступнее, компании могут дополнить его автоматизированными решениями класса «автопентест». Эти инструменты помогают пентестерам ускорять проверку векторов атак и эффективно закрывать основные риски.

Для компаний с высокой зрелостью в ИБ подойдут более сложные подходы, такие как Red Team (комплексное моделирование атак злоумышленников), Purple Team (синергия атакующих и защитных команд) и полноценные киберучения. Эти методы не только проверяют защиту, но и помогают оттачивать навыки внутренних команд, адаптируя их к реальным угрозам и повышая общий уровень киберустойчивости.

— Вы говорите о том, что на рынке есть запрос на реальную безопасность. Что же это все-таки такое?

А.М.: Реальная безопасность — это не просто набор модных технологий, а стратегический подход, где решения и процессы информационной безопасности строятся вокруг конкретных рисков и потребностей бизнеса. Такой подход позволяет не только эффективно реагировать на изменения в ландшафте угроз, но и сохранять оптимальный баланс между защитой и затратами. Попытка создать систему защиты исключительно силами внутренней команды, даже с использованием самых известных продуктов, редко обеспечивает желаемый уровень безопасности. Настоящая защищенность достигается только через комплексный подход и профессиональную экспертизу. Мы помогаем бизнесу делать безопасность не просто опцией, а конкурентным преимуществом. Обратившись к нам, вы получаете поддержку, которая превращает угрозы в возможности для роста и стабильности вашего бизнеса.