Катрин Кнерлер, Ингрид Паркер,
Карсон Зиммерман

11 СТРАТЕГИЙ ДЛЯ ЦЕНТРА КИБЕРБЕЗОПАСНОСТИ МИРОВОГО КЛАССА

SOC: КИБЕРЩИТ ДЛЯ БИЗНЕСА

Каждый день компании по всему миру подвергаются кибератакам, которые могут привести к утечке данных, остановке бизнес-процессов и многомиллионным убыткам. Хакеры действуют скрытно, используя уязвимости, вредоносные программы и социальную инженерию.

Единственная надежная защита — это хорошо организованный SOC (Security Operations Center), центр мониторинга и реагирования на угрозы. Специалисты SOC собирают и анализируют данные с различных объектов инфраструктуры организации, а при обнаружении подозрительной активности принимают меры для предотвращения кибератак. Такой центр может быть как подразделением крупной компании, так и самостоятельной структурой, оказывающей услуги разным клиентам. Авторы предлагают универсальные стратегии, которые помогут создать и управлять SOC любого размера: от команды из двух человек до крупных международных центров с сотнями сотрудников.

Эти стратегии помогают сделать киберщит компании максимально эффективным в выявлении, анализе и оперативном реагировании на киберугрозы. Опираясь на свой многолетний профессиональный опыт, авторы описывают подходы, которые позволяют успешно решать задачи обеспечения кибербезопасности в контексте приоритетов конкретной компании, максимально эффективно использовать инвестиции в персонал и технологии.

СТРАТЕГИЯ 1. ЗНАТЬ, ЧТО И ПОЧЕМУ ЗАЩИЩАЕТ SOC

Для абсолютного большинства государственных учреждений или частных компаний обеспечение кибербезопасности не основная бизнес-функция. Парадоксально, но даже для компаний, предлагающих услуги в сфере компьютерной безопасности, собственная кибербезопасность не приоритет.

С точки зрения здравого смысла это понятно. Обеспечение кибербезопасности — вспомогательная функция, которая по возможности должна осуществляться незаметно, не оказывая никакого влияния на ведение основного бизнеса. При этом операционный центр по кибербезопасности (SOC) для выполнения своих задач должен оперативно получать необходимые данные для принятия решений, а также полномочия для вмешательства в бизнес для отражения киберугроз. Эта работа требует тонкого и глубокого понимания бизнеса, поэтому вопросы, на которые нужно знать четкий ответ прежде всего, — что и почему защищает конкретный SOC, в каких условиях он это делает и как может реагировать на угрозы.

Оперативный контекст SOC состоит из пяти компонентов:

1) знание основного бизнеса. Как устроен бизнес, что именно нужно защищать, какова связь между миссией компании, основными активами и данными;
2) правовая и нормативная среда: каковы политики компании, а также внешние законы и нормы, влияющие на деятельность SOC;
3) цифровая среда компании: чтобы составить полную картину о техническом окружении SOC и состоянии цифровых активов,

нередко приходится сводить воедино данные из множества разрозненных источников;

4) пользователи: сценарии их профессиональной деятельности, схемы взаимодействия с цифровыми сервисами как внутри компании, так и за ее пределами;
5) угрозы — как внутренние, так и внешние.

Руководство компании, а также юридическая служба и IT-отдел должны оказывать всестороннюю помощь в передаче необходимых данных для SOC.

При этом важно понимать, что определение операционного контекста SOC как на тактическом, так и на стратегическом уровне — это итеративный процесс, который включает наблюдение, ориентацию, принятие решений и действия в киберпространстве.

В первую очередь SOC должен получить представление о критически важных элементах, а затем по мере необходимости получать остальную информацию.

Имея нужные данные, SOC может ответить на самые разные вопросы: от «Чего пытается добиться злоумышленник, атакуя нас?» до «Какие области безопасности вызывают наибольшую тревогу?».

СТРАТЕГИЯ 2. ОБЕСПЕЧИТЬ SOC ПОЛНОМОЧИЯМИ ДЛЯ ВЫПОЛНЕНИЯ ЕГО МИССИИ

SOC — это не просто служба мониторинга атак, а полноценный аналитический центр, который должен быть встроен в стратегию компании. Его эффективность напрямую зависит от грамотного управления ресурсами и полномочиями.

Эффективный SOC должен иметь полный набор полномочий для материального и организационного обеспечения своей миссии. Документы и процедуры, согласованные с руководителями подразделений компании, должны давать центру возможность получать все необходимые материальные ресурсы, а также осуществлять свои рабочие задачи.

Оба варианта расположения SOC имеют свои плюсы и минусы. Важно, чтобы руководство SOC могло их равноправно обсуждать с руководителями компании, имея целью главное: недопущение снижения уровня защиты от кибератак.

Независимо от своего расположения (в основном офисе компании или вдали от него), SOC должен иметь интегрированную бюджетную, материально-техническую и инженерную поддержку для устойчивого обеспечения всех своих операций.

Чтобы поддерживать полноценную работоспособность центра кибербезопасности, SOC нельзя передавать в подчинение IT-отдела. Авторы настаивают, что значимость функций SOC равнозначна значимости других IT-операций, направленных на обеспечение нужд основного бизнеса компании, поэтому эти подразделения должны находиться не в соподчиненных, а в партнерских отношениях.

Роли и полномочия по принятию решений руководителей компании и SOC во время критического киберинцидента должны быть максимально четко определены.

Для обеспечения деятельности SOC нужны:

1) письменная инструкция, наделяющая SOC полномочиями на полноценное функционирование, получение ресурсов, а главное — наличие прав на осуществление изменений в IT-деятельности компании;

2) собственный устав SOC, определяющий все сферы деятельности центра и его право голоса в решении оперативных и стратегических вопросов компании наравне с другими отделами;
3) право активного участия SOC в анализе основного бизнеса компании на предмет кибербезопасности. Также SOC должен иметь право на участие в разработке новых видов деятельности или услуг, производимых компанией;
4) полное финансирование SOC компанией, которую он обслуживает, и прямая подотчетность центра руководству компании;
5) возможность для SOC напрямую получать от руководства компании задачи, связанные с кибербезопасностью, и обсуждать их решение.

СТРАТЕГИЯ 3. ОБЕСПЕЧИТЬ СООТВЕТСТВИЕ СТРУКТУРЫ SOC ПОТРЕБНОСТЯМ КОМПАНИИ

SOC может выполнять множество функций, но выбор того, какие из них действительно необходимы, зависит от уровня рисков и финансовых возможностей компании.

Существует несколько моделей работы SOC:

- аутсорсинг — чаще используется небольшими фирмами, которым выгоднее передать кибербезопасность сторонним специалистам;
- гибридная модель — когда часть задач выполняет внутренний SOC, а часть передается на аутсорс;
- полностью внутренний SOC — чаще встречается в крупных корпорациях с высокими требованиями к безопасности.

Модели сотрудничества компании с SOC могут меняться с течением времени.

Если большинство сотрудников работает удаленно, SOC также может функционировать в распределенном формате. По договоренности с руководством компании принимается и решение о графике работы. Авторы уверены, что в большинстве случаев ежедневное круглосуточное дежурство не требуется. А в экстренных ситуациях SOC может работать в усиленном режиме, подключая специалистов внеурочно.

Основная функция SOC — стратегическое планирование и обеспечение безопасности всех операций компании. Если центр кибербезопасности сосредоточен исключительно на мониторинге атак, это означает, что система уже уязвима. Правильно организованный SOC работает на предупреждение угроз, а не на их пассивную фиксацию.

Чтобы SOC мог эффективно управлять инструментами кибербезопасности компании, ему нужно:

1) обеспечить полноценную IT-поддержку — это позволит оперативно вносить изменения в системы безопасности без дополнительных санкций;
2) дать четкие полномочия и доступ к ресурсам — без этого его работа будет носить формальный характер.
3) действовать в рамках общей стратегии компании — безопасность бизнеса невозможна без координации действий с руководством.

SOC предоставляет аналитику, инструменты и рекомендации для обеспечения кибербезопасности компании, но их практическая реализация зависит

от управленческих решений. Реальная ответственность за кибербезопасность лежит на руководителях бизнес-подразделений, поскольку именно они управляют конкретными рабочими процессами, в которые могут вмешаться киберпреступники.

Поэтому вопрос для бизнеса состоит не в том, нужен ли ему SOC, а в том, как бизнес сможет встроить защиту кибербезопасности в общую стратегию компании. Чтобы не оказаться безоружными перед внезапными угрозами, руководство компании совместно с SOC разрабатывает «План обеспечения непрерывности деятельности» (COOP — Continuity of Operations Plan).

Этот план должен:

- обеспечивать нормальную работу компании при любых сбоях;
- не быть перегруженным маловероятными сценариями.

Нет смысла детально прописывать действия SOC на случай ядерной войны, но важно понимать, что делать, если экскаватор повредит оптоволоконный кабель на соседней улице.

СТРАТЕГИЯ 4. НАНИМАТЬ ЛУЧШИХ И РАЗВИВАТЬ КАДРОВЫЙ ПОТЕНЦИАЛ

Способность SOC выполнить свою работу на отлично больше зависит не от численности, а от уровня квалификации специалистов. Для создания и поддержания качественной команды центра кибербезопасности нужны постоянные усилия и инвестиции, но только так можно добиться долгосрочного успеха.

Принимая на работу специалиста по кибербезопасности, нужно наряду с профессиональными качествами оценивать его готовность к развитию, а также способность играть в команде и помогать развиваться другим сотрудникам. Отдавать предпочтение стоит кандидатам, которые не только демонстрируют умения и навыки в своей узкой профессиональной области, но и обладают широким кругозором и полезными мягкими навыками.

Член команды SOC, который может помочь создать «конвейер талантов», не только многократно повышает собственную эффективность, но и обеспечивает долгосрочный успех всему SOC.

В зависимости от миссии, уровня автоматизации и доступного финансирования конкретный SOC может нуждаться в разном количестве сотрудников. Но общее правило справедливо для всех центров: специалистов в области кибербезопасности не хватает, поэтому каждый SOC должен выращивать таланты внутри компании, а также поддерживать карьерный рост сотрудников.

Чтобы опытные специалисты не стремились покинуть SOC, следует заботиться о других факторах вовлечения персонала: регулярном индексировании заработной платы в соответствии с требованиями рынка, хороших условиях работы, культуре общения, возможностях обучения и обмена опытом внутри команды и др.

В английском языке есть специальный термин для обозначения таких людей — T-shaped (Т-образный) человек: вертикальный элемент буквы Т обозначает экспертность в конкретной области, а горизонтальный — широкий кругозор и личностные качества. Например, руководителю SOC, кроме знаний в области кибербезопасности, полезно иметь хорошие коммуникативные навыки и т. п.

СТРАТЕГИЯ 5. РАССТАВЛЯТЬ ПРИОРИТЕТЫ ПРИ РЕАГИРОВАНИИ НА ИНЦИДЕНТЫ

SOC должен уметь балансировать между быстрым реагированием на кибератаки и сбором информации о противнике с целью предотвращения повторных взломов.

Каждый киберинцидент уникален, поэтому критически важно, чтобы ответные меры соответствовали характеру и масштабу угрозы. На практике большинство атак остаются незамеченными на ранних этапах, что усложняет своевременное реагирование. Кроме того, в системах мониторинга количество ложных срабатываний зачастую превышает число реальных угроз, поэтому эффективная работа SOC невозможна без непрерывной настройки, обогащения контекста и автоматизации процессов выявления атак.

SOC должен обеспечивать системный подход к обработке киберинцидентов, который включает:

1) получение и сортировку сообщений об инцидентах (анализ входящих отчетов, выявление ложных срабатываний);
2) расстановку приоритетов в соответствии с определенной степенью критичности угрозы;
3) реагирование на инцидент (оперативные меры по нейтрализации атаки);
4) анализ инцидента (изучение первопричин и последствий);
5) документирование и подготовку рекомендаций для предотвращения подобных атак в будущем.

Наиболее распространенные инциденты, такие как заражение вредоносным ПО, требуют оперативного реагирования, тогда как более редкие, но опасные целевые атаки требуют заранее продуманной стратегии противодействия.

Эффективное реагирование требует четкого понимания, какие инциденты подпадают под зону ответственности SOC и как именно на них реагировать. Для этого нужно:

- разделить инциденты по категориям (например, заражение вредоносным ПО, фишинговые атаки, DDoS, попытки несанкционированного доступа);
- определить порядок действий в зависимости от типа угрозы и вероятных последствий.

При определении способа и времени реагирования на атаку SOC должен учитывать:

- Уровень знания об угрозе: какие индикаторы компрометации уже выявлены?
- Риски и возможные последствия: как атака повлияет на бизнес-процессы компании?
- Необходимость быстрого ограничения ущерба vs важность сбора информации о противнике: иногда важно не только нейтрализовать угрозу, но и выявить более глубокие аспекты атаки.
- Возможность выявить «нулевого пациента», то есть первый скомпрометированный элемент системы.

В идеале SOC должен устанавливать не только сам инцидент, но и всю цепочку атаки, определяя как первопричину, так и масштаб заражения. Однако на практике это не всегда возможно, и здесь играет роль не только опыт, но и интуиция специалистов.

Работа SOC после ликвидации инцидента продолжается. Крупные киберинциденты требуют не только нейтрализации угрозы, но и детального анализа последствий.

После устранения атаки SOC должен:

- проанализировать первопричину: каким образом атака произошла и почему она не была остановлена на раннем этапе;
- выявить уязвимости в системе: что позволило злоумышленникам проникнуть внутрь;
- разработать обновленные защитные меры (например, изменить политики доступа, усилить мониторинг или обновить систему оповещений);
- обучить персонал на основе опыта инцидента, внедрить новые протоколы реагирования и предотвратить аналогичные атаки в будущем.

СТРАТЕГИЯ 6. ВЫЯВЛЯТЬ ЗЛОУМЫШЛЕННИКОВ С ПОМОЩЬЮ АНАЛИЗА КИБЕРУГРОЗ

В современных киберсредах выявление злоумышленников — сложная задача, поскольку хакеры часто маскируются под законных пользователей. Простого мониторинга активности недостаточно: важно понимать, какие методы используют злоумышленники, как они проникают в системы и как минимизировать эти возможности. В этом помогает анализ киберугроз, или Cyber Threat Intelligence (CTI).

Главная ценность CTI — способность отличить вредоносную активность от легитимных действий пользователей и анализировать угрозу в контексте.

Процесс CTI включает:

- сбор данных о вредоносной активности, тактиках хакеров и их инструментах;
- обогащение контекста — соотнесение угроз с реальной инфраструктурой компании;
- выявление закономерностей в поведении хакеров;
- создание превентивных мер защиты, основанных на полученных данных;
- анализ первопричин инцидентов и разработку стратегии их устранения.

CTI работает на нескольких уровнях:

1) стратегический уровень позволяет прогнозировать глобальные тенденции атак и выявлять долгосрочные риски;
2) оперативный уровень сосредоточен на идентифицировании моделей поведения атакующих и их способов обхода защиты;
3) тактический уровень анализирует технические индикаторы компрометации (IoC) и встраивает их в системы мониторинга.

Аналитики CTI играют ключевую роль в SOC, так как именно они формируют целостное представление о киберугрозах. Их работа включает изучение инфраструктуры атаки, методов проникновения, возможных целей злоумышленников и способов их нейтрализации.

СТРАТЕГИЯ 7. ПРАВИЛЬНО ОТБИРАТЬ И СОХРАНЯТЬ ДАННЫЕ

Эффективный SOC нуждается в большом количестве данных, но их объем должен быть оптимальным. Если информации слишком мало, это делает защиту уязвимой, если слишком много — возникает риск перегрузки, которая мешает анализу и оперативному реагированию на угрозы.

Сбор и хранение данных требуют грамотной селекции, чтобы SOC мог опираться на качественную, актуальную и законную информацию.

При выборе источников данных для SOC нужно учитывать не только их охват и доступность, но и правовые аспекты. Какие данные можно собирать с юридической точки зрения? На каких условиях доступны платные источники информации? Как долго можно хранить данные без нарушения нормативных требований? Эти вопросы критически важны, поскольку

> На практике SOC редко страдает от недостатка данных. Скорее наоборот: обычно центр получает намного больше данных, чем ему нужно, а порой даже больше, чем он может обработать.

хранение данных связано не только с безопасностью, но и с финансовыми ограничениями.

SOC должен регулярно проверять все каналы поступления информации. Даже если источник считался надежным ранее, важно убедиться, что он по-прежнему актуален и его данные соответствуют текущей обстановке.

С развитием облачных технологий мониторинг SOC уже не ограничивается локальными системами. В зону ответственности входят облачные сервисы, хранилища и инфраструктура компании. Это требует переноса подходов к мониторингу, обнаружению вторжений и реагированию на инциденты в облачную среду.

Не каждая компания способна контролировать все узлы своей IT-инфраструктуры, поэтому в SOC должны использоваться разные уровни доступа: доверенные привилегированные пользователи, системный контроль на уровне администраторов и механизмы, позволяющие анализировать информационные потоки внутри организации.

Отдельную сложность представляет контроль за операционными технологиями (OT), то есть программно-аппаратными системами управления промышленным оборудованием. В отличие от классических IT-систем, такие устройства могут работать на нестандартных, закрытых платформах, доступ к которым возможен только через облачные интерфейсы. Это делает их менее прозрачными для SOC и требует специализированных подходов к мониторингу.

СТРАТЕГИЯ 8. ТОЧНО ВЫБИРАТЬ И СОЧЕТАТЬ КЛЮЧЕВЫЕ ИНСТРУМЕНТЫ SOC

Мониторинг киберугроз приносит огромный объем данных, но по отдельности они не дают полной картины. Для эффективного выявления угроз и реагирования на них требуется комплексный подход и интеграция различных инструментов безопасности SOC.

Ключевые инструменты SOC:

- SIEM (Security Information and Event Management) — система управления событиями безопасности, которая собирает, анализирует и хранит данные из различных источников: серверов, сетевых устройств, баз данных и приложений. SIEM позволяет отслеживать подозрительную активность и формировать общую картину состояния кибербезопасности в организации;
- EDR (Endpoint Detection & Response) — решение для обнаружения и реагирования на угрозы на уровне конечных устройств, таких как компьютеры пользователей и серверы. EDR обеспечивает постоянный мониторинг, анализ поведения систем и автоматическое реагирование на потенциальные угрозы.

Для небольших компаний, которые только выстраивают систему защиты, внедрение SIEM может оказаться слишком затратным. В таком случае целесообразно начать с EDR, а при увеличении нагрузки и требований к анализу событий безопасности — добавить SIEM.

Обе технологии играют ключевую роль в стратегии кибербезопасности, но выполняют разные функции. SIEM фокусируется на всей сети в целом, а EDR — на защите конечных точек.

Помимо SIEM и EDR, центр киберзащиты использует дополнительные решения для повышения эффективности работы:

- UEBA (User and Entity Behavior Analytics) анализирует поведение пользователей, устройств и учетных записей, выявляя отклонения от нормы. Эта технология помогает обнаруживать угрозы, которые не фиксируются традиционными инструментами защиты, например подозрительные попытки доступа или аномальную сетевую активность.

- SOAR (Security Orchestration, Automation and Response) отвечает за автоматизацию процессов кибербезопасности, координацию работы систем защиты и обработку данных из различных источников. SOC применяет SOAR, когда стандартные инструменты перестают справляться с нагрузкой и требуется интеграция множества решений в единую платформу.

Универсального алгоритма для объединения всех полученных данных не существует: каждая технология выполняет свою задачу, и их сочетание зависит от потребностей компании.

СТРАТЕГИЯ 9. ОБЩАТЬСЯ, СОТРУДНИЧАТЬ, ДЕЛИТЬСЯ ОПЫТОМ

SOC — это не просто изолированная группа аналитиков, отслеживающих угрозы, а ключевой элемент кибербезопасности компании. Эффективность центра защиты кибербезопасности напрямую зависит от уровня интеграции в бизнес-процессы и качества коммуникации с коллегами, клиентами и партнерами. Чем лучше налажен этот диалог, тем быстрее и точнее SOC может реагировать на инциденты.

Одна из главных задач SOC — донесение информации о рисках и угрозах до всех заинтересованных сторон. Это не должно сводиться к сухим отчетам и техническим терминам — важно, чтобы бизнес понимал, почему те или иные угрозы значимы и как их можно предотвратить. Четкое и понятное объяснение вопросов кибербезопасности позволяет не только повысить уровень осведомленности сотрудников, но и минимизировать человеческий фактор как причину киберинцидентов.

Не менее важно выстроить эффективное взаимодействие внутри самого SOC. Мониторинг угроз требует оперативного обмена информацией между специалистами, иначе критически важные сигналы могут быть упущены. Данные о возможных атаках должны передаваться незамедлительно, а сложные проблемы решаться совместно.

Сотрудничество SOC не ограничивается только внутренними процессами. Современная кибербезопасность — это открытая экосистема, где обмен знаниями и опытом играет ключевую роль. Другие SOC могут столкнуться с атаками, которые еще не дошли до вашей компании, и наоборот. Регулярное взаимодействие с другими центрами безопасности помогает заранее выявлять тренды угроз, анализировать новые тактики хакеров и совершенствовать стратегии защиты.

Чем активнее SOC участвует в информационном обмене, тем эффективнее он работает. Говорить о рисках, сотрудничать с бизнесом, делиться опытом с коллегами — не дополнительные функции, а фундаментальные принципы успешной защиты.

СТРАТЕГИЯ 10. ИЗМЕРЯТЬ ЭФФЕКТИВНОСТЬ ДЛЯ УЛУЧШЕНИЯ РАБОТЫ

SOC работает в двух плоскостях оценки эффективности: с одной стороны, он обеспечивает информированность своих клиентов, с другой — влияет

на общий уровень кибербезопасности организации. Для SOC любого уровня и масштаба нужно внедрить систему оценки своей работы, которая позволит:

- оценить, насколько эффективно SOC предотвращает угрозы;
- выявить слабые места в мониторинге и реагировании на инциденты;
- определить, какие действия SOC приносят реальную ценность клиентам.

Важно, чтобы используемые для оценки эффективности показатели были четкими, прозрачными и независимыми от субъективных оценок.

Однако на сегодняшний момент в сфере кибербезопасности не существует единственного универсального индикатора: оценка строится на системе метрик, KPI и аналитических подходов.

Основные термины, используемые в оценке SOC:

- мера — количественный показатель, фиксирующий конкретное значение (например, число инцидентов за месяц);
- метрика — более сложный показатель, который может включать в себя несколько измерений (например, процентное изменение числа атак за год). В среде специалистов по кибербезопасности термины «мера» и «метрика» часто используются как взаимозаменяемые;
- KPI (ключевые показатели эффективности) — метрики, которые оценивают, насколько SOC помогает компании достигать бизнес-целей в области безопасности;
- оценка — процесс сбора, анализа и интерпретации данных, позволяющий определить текущий уровень защищенности компании.

Результаты измерений можно условно разделить на три группы:

1) внутренние показатели — используются самим SOC для анализа своей работы и поиска точек роста;
2) показатели ценности — демонстрируют клиентам и партнерам SOC, какую реальную пользу он приносит;
3) аналитические данные — не связаны напрямую с клиентами, но помогают оценить, насколько SOC эффективен в предотвращении угроз и управлении рисками.

Кроме того, полезно привлекать внешних аудиторов, которые могут дать объективную независимую оценку работы SOC. Такой подход помогает не только повысить уровень кибербезопасности, но и доказать значимость SOC как стратегического элемента защиты бизнеса.

СТРАТЕГИЯ 11. ПРОАКТИВНО ИСКАТЬ УЯЗВИМОСТИ И РАСШИРЯТЬ ФУНКЦИОНАЛ

Хакеры развиваются, меняют тактики взлома, используют сложные схемы обхода защиты. Это требует от SOC расширения функционала, освоения новых методов работы и интеграции технологий, которые позволяют превентивно выявлять киберугрозы.

Поиск уязвимостей — это непрерывный процесс, включающий мониторинг сети, конечных точек и облачных сервисов. Его цель — обнаружить скрытые угрозы, которые могут оставаться незамеченными стандартными

инструментами защиты. Для этого SOC использует несколько проактивных методов:

- **Red Teaming («красная команда»)** — это комплексная имитация реальных атак с целью оценки кибербезопасности систем. Для этого группа специалистов выполняет тест на проникновение в систему. Специалисты могут быть как нанятыми со стороны, так и сотрудниками SOC, но во всех случаях их роль одинакова: имитировать действия злоумышленников и пытаться проникнуть в систему. Цель Red Teaming — определить, насколько хорошо SOC может противостоять атаке. Типичный процесс комплексной имитации атаки включает тестирование на проникновение во внутреннюю сеть компании.
- **Purple teaming («фиолетовая команда»)** предполагает взаимодействие специалистов «красной команды» и собственной группы специалистов SOC. «Красная команда» имитирует атаку на компанию, используя различные тактики и методы, чтобы обойти защиту. В то же время команда SOC работает над обнаружением и ответом на эту атаку, тесно сотрудничая с «красной командой» для выявления уязвимостей и разработки решений для их устранения. По итогам тестирования Purple Team заказчик получает объективную информацию о состоянии уровня информационной безопасности, вырабатываются практические рекомендации по повышению качества противодействия злоумышленникам, уменьшению времени на обнаружение и реагирование, по настройке и расширению систем защиты информации.
- **Breach and Attack Simulation (BAS)** — автоматизированные симуляции взлома и атаки. Это технология, которая позволяет компаниям тестировать свои средства защиты от имитируемых кибератак. При проведении имитируемых атак на IT-инфраструктуру и активы компании проверяется способность обнаруживать, анализировать атаки и реагировать на них. После запуска симуляций платформы BAS генерируют отчеты, в которых выделяются области, где средства контроля безопасности не смогли остановить имитируемые атаки.
- **Tabletop exercise (TTX) («настольные маневры»)** — имитационный сценарий для проверки готовности к кибератакам. Участники обсуждают и ролевыми играми имитируют действия во время гипотетического инцидента. Цель таких упражнений — оценить готовность компании к конкретной ситуации и определить роль каждого участника в ликвидации реальной угрозы.

Применение проактивных методов меняет саму роль SOC в системе кибербезопасности. SOC учится действовать на шаг впереди злоумышленников и предлагает своим клиентам динамичную и адаптивную кибер-защиту.

10 ЛУЧШИХ МЫСЛЕЙ

1.
Оперативный центр кибербезопасности (SOC) — стратегическая единица бизнеса, которая работает в соответствии с бизнес-целями компании, напрямую взаимодействует с ее руководством и является равноправным партнером IT-отдела.

2.
Для эффективного исполнения своей миссии SOC получает финансирование, доступ к критическим данным, полномочия на быстрые действия в случае киберугроз и возможность участия в стратегических решениях, связанных с развитием бизнеса.

3.
Эффективность деятельности SOC нужно оценивать по заранее определенным, прозрачным и объективным метрикам, KPI, а также с помощью независимого аудита.

4.
В условиях хронического дефицита квалифицированных кадров для SOC нужно стремиться нанимать лучших кандидатов и развивать своих специалистов, особенно тех, кто умеет работать в команде.

5.
Ключ успеха SOC — эффективный обмен информацией в рамках самого SOC, с другими подразделениями компании, а также с коллегами по отрасли.

6.
Стратегическая цель развития SOC — не реагирование на уже существующие киберугрозы, а предотвращение кибератак.

7.
Для выявления уязвимостей до инцидента используются такие инструменты, как анализ угроз (CTI), тестирования (Red Teaming) и имитация кибератак (BAS, TTX).

8.

Избыток данных так же опасен для деятельности SOC, как их нехватка. Центр киберзащиты должен тщательно отбирать информацию из релевантных, законных и актуальных источников и четко расставлять приоритеты при выборе реакции.

9.

В зависимости от потребностей бизнеса и возможности финансирования SOC использует разные инструменты мониторинга, анализа и автоматизации безопасности с целью создания комплексной защиты от киберугроз.

10.

Развитие SOC должно быть гибким и адаптивным, с четким пониманием изменений внешней среды и потребностей бизнеса в области кибербезопасности.