Максим ПЯТАКОВ
заместитель генерального директора, CtrlHack

Владимир СОЛОВЬЁВ
руководитель направления внедрения средств защиты АО «ДиалогНаука»

РУССКИЙ ХАКЕР. БЕЛЫЙ ХАКЕР. РОБОТ-ХАКЕР

АВТОМАТИЧЕСКАЯ СИМУЛЯЦИЯ КИБЕРАТАК КАК ЧАСТЬ ЭФФЕКТИВНОЙ СИСТЕМЫ ЗАЩИТЫ

Сейчас большинство компаний, государственных предприятий и органов власти обеспокоены проблемой защиты от кибератак. В зависимости от текущего уровня защиты и понимания возможных последствий кибератак принимаются различные меры, направленные на повышение уровня защищённости до приемлемого уровня. При этом средства защиты компаний включают в себя большое количество различных продуктов, причём очень часто от разных вендоров. Для реагирования на более сложные атаки компании выстраивают свой SOC или подключают соответствующую услугу от сервис-провайдера. Расширяется штат сотрудников, отвечающих за настройку средств защиты, мониторинг и реагирование на инциденты. Но насколько эффективно работает вся эта система в целом и каждый из её компонентов? Действительно ли вероятность проведения успешной кибератаки снизилась или злоумышленник всё так же легко может проникнуть в сеть компании? Это общие вопросы, с которыми сталкиваются каждый день специалисты по информационной безопасности. Вопросов много, а возможностей получить ответ, подтверждённый фактами, не так много.

СПОСОБЫ ПРОВЕРКИ КИБЕРЗАЩИТЫ

Ответить на вопросы об эффективности системы киберзащиты можно, реализуя у себя в инфраструктуре симуляцию действий злоумышленников. Фактически это единственный способ определить, насколько вы реально защищены от кибератак. Много лет такие активности проводились в рамках выполнения тестов на проникновение (pentest). В последние годы в дополнение к тестированию на проникновение ряд компаний стал пользоваться услугами red team. В основе этих услуг лежит работа «белых» хакеров, которые используют различные техники и средства, полностью повторяющие действия реальных злоумышленников. Однако обе эти услуги имеют ряд недостатков. За время выполнения работ у команд нет возможности покрыть всю инфраструктуру, особенно если мы говорим об инфраструктурах из десятков тысяч узлов в сети. Команды могут отработать только часть векторов атак и хакерских техник. При этом такие работы практически никогда не выполняются на постоянной основе без перерывов. И результат сильно зависит от квалификации команды, которую не всегда возможно точно определить — человеческий фактор. Ко всему прочему, результаты проведённых тестирований на проникновение попадают в «чужие» руки, за пределы компании.

Таким образом, тестирование на проникновение и работа команд red team позволяют в некотором объёме оценить уровень реальной защищённости компании. Но этот результат не является полной оценкой, и в большинстве случаев компании могут позволить себе тестирование на проникновение раз в полгода или год. А в ситуации постоянного развития технологий и изменений в инфраструктуре нужно иметь возможность получать такую оценку на постоянной основе с максимальным покрытием различных атакующих техник и для всей инфраструктуры.

АВТОМАТИЧЕСКАЯ СИМУЛЯЦИЯ КИБЕРАТАК

Для решения таких задач на мировом рынке появились продукты, позволяющие в автоматическом режиме проводить симуляции кибератак во всей инфраструктуре. Позднее Gartner выделил такие решения в отдельный класс Breach and attack Simulation (BAS). Сейчас продукты данного класса представлены и на российском рынке. Решения класса BAS позволяют проводить проверки работы средств защиты, эффективности работы SOC, качества работы выстроенных процессов, а также работу персонала. То есть автоматически можно проверить все составляющие комплексной системы киберзащиты и при этом делать это на постоянной основе и не зависеть от внешних команд и уровня их компетенций.

Основным вектором проверки в рамках симуляций кибератак традиционно для продуктов класса BAS были периметровые средства защиты, средства защиты электронной почты и средства защиты конечных точек. Все из представленных на рынке решений позволяют проводить такие проверки. Однако каждый продукт выполняет такие проверки по-своему.

В последнее время продукты класса BAS стали также предлагать возможности по проверке работы правил обнаружения в решениях класса SIEM и SOC в целом. В рамках проведения таких проверок разработчики продуктов активно используют методологию и соответствующую базу знаний о тактиках, техниках и их реализациях, например матрицу MITRE ATT&CK.

Также проведение симуляций действий злоумышленника позволяет проверить и работу персонала в части мониторинга и реагирования на эти инциденты.

Таким образом, применение BAS позволяет:

- CISO получать в любой момент времени реальную оценку защищённости инфраструктуры и в зависимости от этого более эффективно и обоснованно планировать развитие системы киберзащиты;
- подразделениям, отвечающим за эксплуатацию и развитие средств защиты, определять, как средства защиты в реальности реагируют на различные хакерские действия, корректны ли настройки этих средств защиты и нет ли отличий в настройках средств защиты в разных сегментах сети;
- сотрудникам SOC проверять работу правил обнаружения подозрительных действий злоумышленников, реализацию процессов реагирования на инциденты и корректность playbook'ов в системах класса SOAR.

Для получения полной информации о реальном уровне защищённости вашей компании применение решений класса BAS нужно выстроить в отдельный процесс, который позволял бы проводить симуляции по всей инфраструктуре по заранее заданному и согласованному расписанию с использованием различных сценариев.

ПОВЫСИТЬ ЭФФЕКТИВНОСТЬ SOC

Проблема повышения эффективности работы SOC намного сложнее, чем проблема выбора эффективных настроек средств защиты. Основа SOC — корреляционные правила обнаружения различных техник злоумышленников (в большинстве случаев реализованных на базе решений класса SIEM) как на этапе первичного проникновения, так и на последующих этапах кибератаки. При этом, по оценкам независимых экспертов, корреляционные правила обнаружений, которые поставляются вендорами решений класса SIEM, позволяют детектировать не более 20% техник из матрицы MITRE ATT&CK. До 15% из этих правил работают некорректно в реальной инфраструктуре. То есть нельзя поставить SIEM-систему с набором правил детектирования от вендора и работать с этим набором. Для того чтобы эффективно обнаруживать техники злоумышленников, необходимо постоянно развивать набор правил корреляции. Для этого, во-первых, нужно постоянно анализировать новые и постоянно развивающиеся техники злоумышленников. Во-вторых, разрабатывать средства для проверки того, как эти техники работают в конкретной инфраструктуре и достаточно ли событий поступает в SIEM-систему для обнаружения злоумышленника. И уже на основе анализа этих данных разрабатывать правила корреляции. На последнем этапе нужно проверить, как это правило работает во всей инфраструктуре. Руками выполнять все эти действия, даже используя необходимые техники, что используют настоящие злоумышленники, дорого и требует огромного количества ресурсов.

Продукты класса BAS позволяют решить эти проблемы. Во-первых, они несут с собой необходимую экспертизу и знания по новым атакующим техникам злоумышленников. Во-вторых, позволяют провести автоматическую симуляцию этих техник. На основе полученных результатов аналитики SOC смогут разработать необходимые правила корреляции и далее автоматически перезапустить симуляции для проверки корректности их работы.

Фактически BAS на данный момент — это единственное средство, которое позволяет проводить автоматический аудит всех изменений в инфраструктуре и помогает более эффективно разрабатывать новые правила корреляции для эффективного обнаружения злоумышленников.

СИМУЛЯЦИЯ АТАК И РОССИЙСКИЙ CTRLHACK

Единственным на данный момент российским продуктом класса BAS является платформа CtrlHack. CtrlHack позволяет проводить симуляции различных техник злоумышленников непосредственно в инфраструктуре организации. Симуляции выполняются на узлах, где установлены агенты CtrlHack. При этом вся система может быть полностью развёрнута внутри инфраструктуры организации.

CtrlHack позволяет проводить симуляции, направленные на проверку работы периметровых средств защиты (IPS, NGFW), средств защиты электронной почты («песочница», почтовые антивирусы), средств защиты конечных точек (антивирусы, EDR). Но основным вектором для CtrlHack является симуляция различных техник злоумышленников, направленных на проверку работы правил корреляции в решениях класса SIEM, а также на повышение эффективности разработки данных правил.

В базе знаний CtrlHack есть симуляции техник для всех стадий выполнения атаки, и этот набор постоянно обновляется и расширяется. Решение также позволяет добавлять собственные объекты во внутреннюю базу знаний для последующего использования при запуске симуляций. Это могут быть вредоносные ссылки, файлы, скрипты.

По результатам симуляции станет понятно, насколько полно собираются все необходимые события, как работают правила корреляции в решениях класса SIEM и насколько полно обнаруживаются разные стадии выполнения атак. А детальная техническая информация о выполненных в рамках симуляций действиях позволит аналитикам SOC легко разрабатывать новые правила корреляции (или модифицировать имеющиеся) и в дальнейшем тестировать работу этих правил.