ОБЗОР РЕШЕНИЯ

FortiSOAR ускоряет реагирование на инциденты благодаря поддержке операций безопасности

Аннотация

По мере развития угроз и появления инновационных цифровых технологий возникают новые направления сетевых атак. Для противодействия им многие организации внедряют специализированные решения. Это усложняет инфраструктуру безопасности и создает множество проблем: слишком большое количество поставщиков, оповещений и ручных процедур, замедляющих реагирование, наряду с нехваткой персонала для обработки ежедневно возрастающих рабочих нагрузок.

Эти проблемы можно решить за счет интеграции в архитектуру безопасности функций оркестрации, автоматизации и реагирования (SOAR). При помощи FortiSOAR специалисты по безопасности могут настроить автоматизированную инфраструктуру, которая объединит все корпоративные инструменты безопасности, а также позволит сотрудникам реже отвлекаться на оповещения и переключать контекст. Таким образом, это не просто адаптация, но и оптимизация процедур безопасности.

Неинтегрированная система безопасности приводит к усталости персонала от оповещений и порождает риски

Ежедневно специалисты по безопасности вынуждены обрабатывать огромное количество оповещений. Основной причиной этой проблемы является непрерывно растущая сложность и фрагментарность инфраструктур безопасности в результате внедрения множества специализированных продуктов от разных поставщиков. Среднестатистическая современная организация для противодействия новым угрозам и рискам использует 47 разных решений и технологий безопасности[1].

Большое количество оповещений — это существенная составляющая проблемы, однако отслеживание, анализ и попытки вручную устранить оповещения из разных источников также повышают нагрузку на персонал центров операций безопасности (SOC). Неэффективные рабочие процессы замедляют реагирование на инциденты: на выявление и блокировку одного нарушения в среднем уходит 279 дней[2].

Кроме того, организации нередко испытывают нехватку кадров, специализирующихся на операциях безопасности. Почти две трети (65 %) компаний столкнулись с отсутствием квалифицированных специалистов по обеспечению эффективных операций безопасности[3]. Эти пересекающиеся факторы усиливают вероятность того, что нарушение останется незамеченным.

По прошлогодней статистике, нарушения с жизненным циклом менее 200 дней в среднем нанесли на 1,22 миллиона долл. США меньше убытков, чем нарушения, жизненный цикл которых составил более 200 дней (3,34 млн долл. США и 4,56 млн долл. США соответственно). Разница составила 37 %[4].

Согласно прогнозам, за период с 2019 по 2024 г. объем рынка SOAR достигнет около 1,8 млрд долл. США, совокупный среднегодовой темп роста (CAGR) составит 15,6 %[5].

Решение SOAR способствует интеграции инструментов безопасности — оно обеспечивает связь между отдельными компонентами и координирует их работу. Такой подход не только повышает эффективность отслеживания сети, но и снижает количество оповещений: они приобретают более стратегический характер[6]. К примеру, с помощью SOAR сотрудники операционных отделов безопасности могут автоматизировать трудоемкие и повторяющиеся рабочие задачи, не требующие надзора оператора. Лучшие решения SOAR собирают данные об угрозах и увязывают их с контекстом, благодаря чему аналитики могут оперативно сортировать оповещения по степени серьезности риска, конфиденциальности и важности подвергшихся угрозе бизнес-функций[7].

FortiSOAR интегрирует систему безопасности и автоматизирует реагирование

Решение FortiSOAR поддерживает сбор оповещений и данных по ним от широкой линейки продуктов безопасности. Оно упрощает оркестрацию и управление благодаря четко сформулированным стратегиям, а также за счет автоматизации реагирования устраняет необходимость в ручном выполнении времязатратных процедур.

Решение FortiSOAR в составе интегрированной системы безопасности Fortinet Security Fabric объединяет инструменты безопасности в комплексную инфраструктуру. Благодаря этому FortiSOAR автоматизирует многие низкоуровневые процедуры обработки оповещений, что позволяет специалистам SOC сосредоточиться на более важных задачах. Ниже описаны четыре примера использования, которые наглядно демонстрируют преимущества FortiSOAR для испытывающих большую нагрузку сотрудников SOC:

Пример использования 1: единое рабочее место SOC

FortiSOAR упрощает структуру SOC за счет интеграции разрозненных специализированных средств безопасности и создания централизованной системы оркестрации, которую можно развернуть в любой среде. Решение включает более 280 готовых к работе коннекторов. Таким образом, специалисты SOC легко могут объединить решение FortiSOAR с имеющимися средствами безопасности от других поставщиков, а затем воспользоваться функцией централизованного отслеживания и управления, параллельно собирая данные оповещений. Интеграция решает проблему фрагментарности экосистемы, упрощает выполнение операций безопасности и продлевает срок службы существующих инструментов, что способствует максимизации окупаемости (ROI).

Пример использования 2: автоматическая сортировка оповещений

FortiSOAR собирает оповещения в одном месте и дополняет их контекстуальными данными, что ускоряет процесс обработки. Помимо этого, такой подход снижает количество ложных срабатываний и предоставляет доступ к современным функциям управления событиями, которые координируют и убыстряют выполнение анализа. FortiSOAR оптимизирует простые операции SOC, такие как прием оповещений, определение приоритетов в зависимости от уровня рисков и распределение задач. Также решение автоматизирует более сложные задачи exchange-to-exchange (E2E), к числу которых относятся сортировка, сбор дополнительных данных, анализ и устранение угроз. Эти передовые функции интеграции и автоматизации снижают нагрузку на персонал, связанную с необходимостью обработки оповещений, что позволяет специалистам SOC сосредоточиться на выявлении угроз и устранении уязвимостей, которыми могут воспользоваться злоумышленники.

Пример использования 3: ускорение реагирования на инциденты

Выполняемые вручную рабочие процессы замедляют обработку и устранение оповещений, а также повышают риск ошибок и недосмотра в связи с человеческим фактором. Решение FortiSOAR распространяет на всю систему функции автоматизации FortiAnalyzer и управления инцидентами и событиями безопасности (SIEM) FortiSIEM, а также обеспечивает оркестрацию и автоматизацию всех процессов SOC. Специалисты отделов безопасности могут повысить эффективность работы за счет автоматизации всех задач, изменений и обновлений в соответствии с потребностями организации. FortiSOAR не просто автоматизирует корпоративные процедуры, но и повышает результативность работы SOC и системы безопасности в целом.

Кроме того, FortiSOAR обладает уникальной особенностью: это решение поддерживает автоматизацию любых мер реагирования. В случае возникновения критической ситуации специалисты по безопасности могут оперативно перевести объект в автономный режим и применить доступные стратегии и коннекторы.

Пример использования 4: снижение нагрузки на ограниченные ресурсы SOC

Устранение ручных операций облегчает работу загруженного персонала SOC: снижаются затраты времени и трудозатраты, что в свою очередь снижает совокупную стоимость владения (TCO) в сфере безопасности. Решение FortiSOAR обеспечивает интеллектуальную оптимизацию операций и процедур безопасности за счет автоматизации рабочих процессов. Специалисты SOC получают возможность настраивать протоколы и автоматизировать меры реагирования в соответствии с требованиями SOC.

Процесс развертывания FortiSOAR очень прост: решение включает готовые к работе программы быстрой настройки, которые достаточно перетащить в окно. Такой подход позволяет быстро получить результат. Кроме того, благодаря FortiSOAR специалисты SOC могут накапливать коллективные знания. В случае увольнения сотрудника в системе сохранятся данные о рабочих процессах, за выполнение которых он отвечал.

Управление рисками, ресурсами и результатами

В связи с появлением новых направлений атак и нехваткой ресурсов количество рисков, с которыми сталкиваются сотрудники операционных отделов безопасности, будет только расти. Однако при помощи эффективного полнофункционального решения SOAR специалисты SOC могут не только решить эту проблему, но и усилить, оптимизировать и модернизировать корпоративные процедуры безопасности.

FortiSOAR — это гибкое настраиваемое решение, которое повышает эффективность реагирования центров операций безопасности на новые угрозы. Функции автоматизации и оркестрации FortiSOAR способствуют упрощению корпоративных экосистем безопасности, дают сотрудникам возможность реже отвлекаться на оповещения, ускоряют реагирование и снижают нагрузку на ограниченные ресурсы SOC.

Кроме того, решение FortiSOAR поддерживает упрощенное лицензирование при помощи предсказуемой пользовательской модели лицензирования. Эта масштабируемая архитектура отличается высокой доступностью для развивающихся организаций, за счет чего решение обеспечивает охват растущих и/или распределенных корпоративных сетей без ущерба для ресурсов, необходимых для развертывания и администрирования таких структур.

[1] 53% of enterprises have no idea if their security tools are working, Help Net Security, 31 июля 2019 г.

[2] 2019 Cost of a Data Breach Report, Ponemon Institute and IBM Security, 2019 г.

[3] Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)² Cybersecurity Workforce Study, 2019, (ISC)², 2019 г.

[4] 2019 Cost of a Data Breach Report, Ponemon Institute and IBM Security, 2019 г.

[5] Security Orchestration Automation & Response (SOAR) World Markets, Outlook to 2024: The High Number of False Security Alerts Presents Lucrative Market Opportunities, Research and Markets, 15 ноября 2019 г.

[6] Мухаммед Омар Хан (Muhammad Omar Khan), Why SOAR is a Good Bet For Fighting Mega Cyber Security Breaches, Entrepreneur, 23 мая 2019 г.

[7] Сиан Уокер (Cian Walker), SOAR: The Second Arm of Security Operations, Security Intelligence, 9 апреля 2019 г.

FORTINET®

www.fortinet.com/ru

апреля 22, 2020 3:19 PM

587297-0-1-RU

sb-FA-fortisoar-empowers-security-operations-to-accelerate-incident-response-A4_RU