Антон Башарин (Swordfish Security): Большинство типовых проблем решается на этапе аудита

Антон Башарин, технический директор Swordfish Security, рассказал «Б.О» о том, почему практики DevSecOps получили такую популярность и как сделать процесс разработки действительно безопасным

Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**

— Антон, на ваш взгляд, насколько остра проблема импортозамещения стека автоматизированного DevSecOps? Какие тенденции здесь можно выделить? Может ли помочь ИИ?

— После ухода иностранных вендоров в 2022 году российским разработчикам потребовалось срочно создавать новые решения в сегменте DevSecOps. Сегодня в этом направлении есть успехи, но многие продукты еще далеки от идеала.

В сегменте статического анализа кода хорошая конкуренция — представлено четыре неплохих коммерческих решения. В то же время на рынке всего один коммерческий инструмент для динамического анализа. Самый бурный рост был и остается в сегменте анализа компонентов с открытым кодом, из которых на 80–90% стоит современное ПО.

В последнее время с ними возникает много проблем: отказ работать на территории нашей страны, показываются баннеры с политическими высказываниями (protestware), а также заметен рост атак на цепочки поставок (supply chain attack).

Традиционно ИИ (нейросети и машинное обучение) используется при поиске аномалий в SIEM-инструментах и в поведенческом анализе. Уже есть решения, которые помогают ИБ-инженерам разбирать результаты срабатываний. Другие предлагают исправлять уязвимости в автоматическом режиме.

— Почему так много внимания сегодня уделяется вопросам разработки стратегии внедрения DevSecOps, часто по модели As a Service?

— Большинство IT-организаций использует Agile-подход к внедрению любых изменений, и здесь как раз модель As-a-Service (SaaS) вполне уместна. Она как нельзя лучше соответствует условиям, в которых находится сегодня рынок: нехватка квалифицированных специалистов, необходимость соответствия требованиям регуляторов, а также потребность в оперативном запуске процессов безопасной разработки продуктов.

Модель As-a-Service позволяет использовать все существующие практики и инструменты безопасной разработки «из коробки», то есть не внедряя их во внутренние процессы заказчика. Вся инфраструктура и анализ защищенности продуктов при этом остаются на стороне сервисной компании, а это означает колоссальную экономию ресурсов для заказчика.

— В целом, в IT и ИБ виден всплеск интереса к консалтингу. Наблюдаете ли вы эту потребность в DevSecOps? Что нужно сегодня вашим клиентам?

— Всплеск интереса нередко связан с требованиями регуляторов. В то же время многие осознают, что выстраивание процесса безо-

пасной разработки (DevSecOps) необходимо, а иногда может обеспечить конкурентные преимущества. Если у продукта есть проблемы с безопасностью, злоумышленники могут взломать как обычных пользователей, так и внутренние системы больших организаций. Где-то хакеры задействуют уязвимости самих систем, а где-то идут более длинным путем — через атаку на поставщика.

Итог всегда один — потеря финансов и репутации заказчиков. Внедрение DevSecOps позволяет существенно снизить вероятность успеха подобных атак. Важно понимать, кто из IT- и ИБ-сообществ максимально качественно и эффективно сможет спроектировать процессы, подобрать необходимый инструментарий, провести внедрение и обучение. Экспертиза и эффективно работающие процессы безопасной разработки — это то, что сегодня необходимо нашим клиентам.

— С чего начинается ваш типовой проект у клиента? Насколько сложно разобраться со спецификой?

— Специфики не так много. Чаще всего работа с клиентом начинается с обследования или экспресс-аудита. Здесь определяется текущий уровень готовности компании к внедрению новых процессов. Формируются стратегия развития, бюджет на внедрение и разрабатывается дорожная карта. Затем происходят реализация и внедрение. Да, тут есть ряд типовых проблем, включая, например, сетевой доступ или порядок обновления инструментов, но большинство из них решается еще на этапе аудита. Многие «грабли» видны еще на первых встречах с клиентом, и их часто удается обойти заблаговременно.

— Нужны ли центры компетенций в этой сфере и какие именно лучшие практики могли бы войти в них? Где их находить? Есть ли у нас уже свой опыт?

— Центры компетенций нужны, и они уже появляются у интеграторов, специализирующихся на внедрении процессов безопасной разработки. Они аккумулируют наиболее известные и эффективные практики на рынке. К примеру, SAST (статический анализ исходного кода) знаком уже почти каждому разработчику, но продукты пока грешат большим количеством ложных срабатываний. Безопасность контейнеров (CS, Container Security) — хайповая тема, но на рынке нет полноценных решений, а у имеющихся — свои особенности.

Зачастую проще начать с анализа компонентов с открытым кодом, как с наименее ресурсоемкой практики, которая может быстро дать ощутимые результаты: внедрить ASOC-инструменты и вокруг них выстраивать полноценную DevSecOps-платформу. Все эти знания накапливаются в центре компетенций, где есть специалисты, способные разобраться в запросе каждого клиента и подсказать оптимальный путь решения. Такой опыт (и немалый) есть и у нас, и у других компаний на рынке.

— Компания Swordfish Security развивает собственную платформу для внедрения, измерения и автоматизации процесса безопасной разработки — AppSec.Hub. Расскажите немного о ней.

— AppSec.Hub, по сути, является ответом на ожидания наших клиентов, которые мы увидели в рамках прошлых консалтинговых проектов. Прежде всего рынку было необходимо встроить ИБ в DevOps, не теряя в скорости time to market, то есть в скорости вывода решения на рынок. Это значит, что обнаруживаемые ИБ-проблемы необходимо решать как можно быстрее, реагировать на них, передавать рекомендации разработчикам. По терминологии Gartner, подобные задачи относятся к ASOC-инструментам, а AppSec.Hub является первым и пока единственным коммерческим решением такого класса на территории нашей страны.

Перечислю его преимущества: скорость развертывания полнофункциональной платформы DevSecOps, которая включает в себя все необходимые сканеры и интеграции; автоматическая обработка результатов сканирования с помощью машинного обучения и модуля корреляции; оценка эффективности процесса на базе данных и метрик, которые собираются на основе телеметрии процессов и инструментов и являются объективными.

Часть клиентов говорят о том, что AppSec.Hub стал неотъемлемой частью процесса разработки и к нему уже предъявляются требования по отказоустойчивости и высокой производительности, которые система успешно удовлетворяет. Другие отмечают скорость внедрения процесса DevSecOps на основе нашего решения — она измеряется днями, а не месяцами. Третьи просто пользуются автоматизацией вокруг триажа и тем самым экономят время своих инженеров и разработчиков.

— Коснулись ли вашей компании эти проблемы, в частности кадровый голод? Как решается эта проблема?

— Кадровый голод есть, так как в последнее время ИБ-практикам в разработке ПО уделяется большое внимание, а избытка в специалистах практической безопасности никогда не было. Поэтому мы, как и многие наши клиенты, видим в этом проблему. Мы стараемся решать ее наймом тех специалистов, которые решили сменить место работы; работой со студентами; внедрением автоматизации и элементов ИИ для выполнения рутинных задач, не требующих высокой квалификации. Б.О