Побеждать врага его же оружием

ИБ активно внедряет искусственный интеллект, и эта тенденция будет усиливаться

Текст
АНТОН БАШАРИН,
ТЕХНИЧЕСКИЙ ДИРЕКТОР
ГК SWORDFISH SECURITY

Ситуация в сфере ИБ крупных компаний остается напряженной. Уход зарубежных вендоров спровоцировал резкий дефицит программных продуктов, закрыть который компании пытаются существующими аналогами или новыми, пока еще сырыми разработками. При этом хакерские группировки становятся все активнее. В 2022 году число DDoS-атак на российские финансовые компании выросло в 4 раза. В марте 2023 года была зафиксирована новая волна подобных инцидентов — количество атак увеличилось на 126% по сравнению с аналогичным периодом прошлого года. Сегодня хакерство — это бизнес, где крутятся миллиарды долларов, есть четкая иерархия и бюджет на развитие. И здесь все активнее используются технологии искусственного интеллекта: для создания вредоносного ПО в привлекательной фишинговой упаковке и почтовых рассылок, для автоматического поиска уязвимостей, написания эксплойтов, для продвинутого общения ботов с применением социальной инженерии. Для того чтобы противостоять темным силам, при этом закрывая существующие проблемы с качеством ПО, нужно бить врага его же оружием. ПО много, быстро и безопасно не бывает.

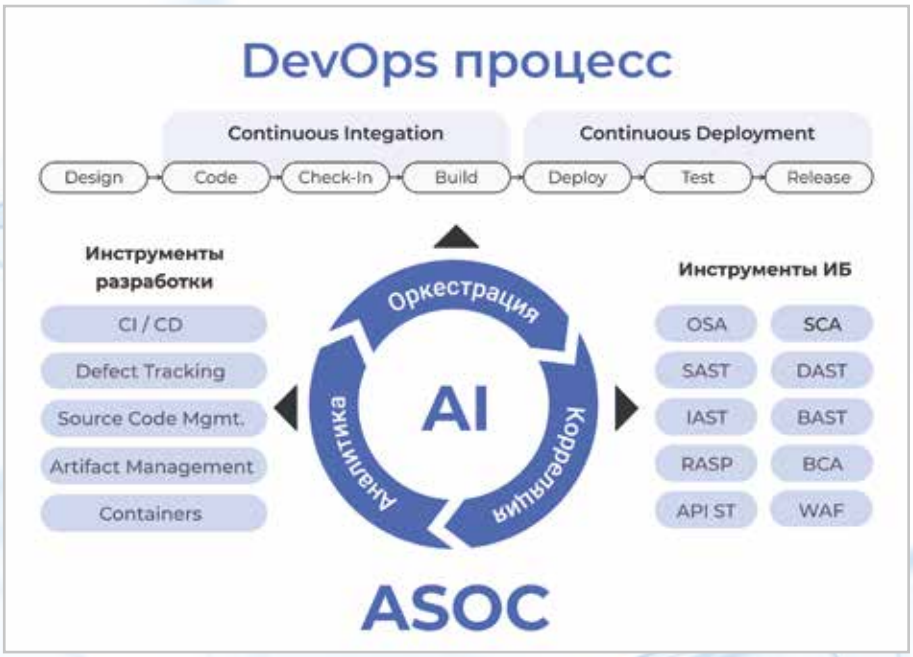
К сожалению, до сих пор вокруг многие компании увлечены «лоскутной» автоматизацией. Они внедряют инструменты безопасности при помощи разрозненных скриптов, которые трудно поддерживать и практически невозможно масштабировать. В итоге проекты затягиваются, ресурсы «утекают» и возникают новые проблемы. Выясняется, что сканерами ИБ сложно управлять — каждый из них работает сам по себе, но вместе они порождают гигантские объемы данных, которые требуют обработки. На выходе получается «старая песня о главном» — ИБ-процессы задерживают разработку, релизы откладываются. Ну и как здесь оценить эффективность процесса?

А между тем AI-технологии уже вошли в кибербезопасность, они помогают автоматизировать процессы и повышать защищенность продуктов. С развитием угроз и ростом уровня цифровизации роль искусственного интеллекта в ИБ будет усиливаться, и прежде всего это касается процессов разработки ПО.

Рынок диктует финтех-компаниям: делайте много, быстро и безопасно. Никому не интересно, как будут закрыты и решены проблемы ИБ — готовые продукты чаще всего нужны еще «вчера». И главное, здесь не нужно ничего создавать — подход уже есть, он применяется многими компаниями. Речь идет о DevSecOps, который вполне способен «подружить» скорость вывода продуктов на рынок (time to market), качество и защищенность ПО. Суть подхода состоит в том, чтобы находить уязвимости как можно раньше, устранять их, не накапливая проблемы при доведении ПО до предрелизного состояния, и, конечно, автоматизировать запуск проверок ИБ. Все это в комплексе позволяет значительно сократить time to market.

Инструменты класса ASOC (Application Security Orchestration and Correlation) могут оценивать данные, получаемые из нескольких источников тестирования, собирать и соотносить результаты, используя автоматизацию и технологии машинного обучения. На основе информации, которая предоставляется на доступном бизнесу языке, можно делать адекватные выводы и принимать оперативные решения.

Аналитики Gartner считают данный сегмент одним из ключевых в сфере безопасности приложений и ожидают, что широкий переход на ASOC осуществится в течение 2–5 лет. На российском рынке одним из перспективных отечественных продуктов считается AppSec.Hub, также отмеченный в отчете Gartner Application Security Hype Cycle 2022.



AI в контексте DevSecOps

Зачастую организации, использующие консервативные подходы к реализации DevSecOps, тратят как минимум несколько лет на внедрение только основных практик ИБ. С помощью платформы оркестрации и корреляции срок создания процесса безопасной разработки и его встраивания в существующий бизнес можно сократить до нескольких месяцев.

Инструменты ASOC, как уже упоминалось выше, помогают эффективно решить проблему управления сканерами: платформа интегрируется с инструментами безопасности и разработки, настраивает анализаторы для каждой отдельной проверки и в нужное время запускает тестирование подходящими методами. Благодаря широким возможностям интеграции с инструментами разработки подобное решение позволяет охватить проверками защищенности все версии создаваемых продуктов. Используемые в ASOC AI-технологии помогают вывести на принципиально новый уровень проверки ПО на соответствие требованиям регуляторов: динамически подстраивать инструменты ИБ и критерии качества под профиль анализируемого ПО и принимать решения об их готовности к переходу на следующие этапы жизненного цикла.

Еще один важный блок, где AI экономит ресурсы специалистов, — обработка результатов сканирований. Помимо большого объема данных они зачастую содержат большое количество ложных срабатываний и дублей. Если обрабатывать все это вручную, можно потерять недели и даже месяцы. Технологии искусственного интеллекта позволяют сократить это время до нескольких часов, а то и минут. Инструмент ASOC собирает итоги проверок воедино. Далее с помощью специального движка, работающего на основе машинного обучения, он анализирует отчеты, определяет ложные и реальные проблемы, распознает похожие срабатывания, объединяет ошибки в группы. То есть инструмент выполняет всю грязную работу и выдает специалистам «очищенные» данные, готовые к использованию.

Платформа оркестрации и корреляции — гибкий инструмент, поэтому с ее помощью также можно выполнять задачи аналитики. Технологии AI позволяют построить полноценный Data-Driven-подход к управлению процессом безопасной разработки и отслеживать метрики эффективности DevSecOps в разрезе отдельных ИБ-инструментов, команд, продуктов. Благодаря этому компании смогут взять процесс под контроль, чтобы направлять его в нужном направлении и оценивать результаты проделанной работы.

Таким образом, возможности искусственного интеллекта, реализованные на базе платформы оркестрации и корреляции, позволяют оперативно сделать DevSecOps частью реальности. Практика реализации проектов по построению процесса безопасной разработки с использованием инструмента ASOC показывает, что данный подход дает возможность в 10 раз сократить затраты на внедрение технологий обеспечения защищенности, сэкономить до 15% годового бюджета разработки, на 20% сократить time to market и достичь ROI 700%.

Перспективы на будущее

Нет сомнений в том, что технологии искусственного интеллекта уже сейчас способны значительно облегчить жизнь специалистам по ИБ и руководителям бизнеса, но пока речь идет лишь о рутинных задачах. И здесь предстоит еще много работы, а для российских компаний в условиях разрыва с мировым научным сообществом и зарубежными поставщиками «железа» процесс может затянуться. Также стоит отметить «наукоемкость» этого направления — требования к профильным специалистам будут постоянно повышаться.

В перспективе технологии AI могли бы автоматизировать обнаружение угроз: распознавать подозрительные действия пользователей, аномалии в работе систем безопасности и предлагать пути решения проблем. Также их можно применять в прогнозировании уязвимостей и сложных вариантов атак, исправлении дефектов безопасности и, конечно, в совершенствовании текущих возможностей. Среди последних в приоритете стопроцентное покрытие проверками всех областей ПО, обнаружение уязвимостей нулевого дня, полная автоматизация процессов принятия решений о переходе сборок на следующие этапы жизненного цикла, а также управление требованиями безопасности и соответствием регуляторным стандартам. Б.О