ТОП-8 НАВЫКОВ APPLICATION SECURITY MANAGER

30%

киберинцидентов — это атаки через веб-приложения

При этом в 88% приложений есть как минимум одна критическая уязвимость, через которую можно реализовать атаку. Только представьте, сколько у злоумышленников возможностей, чтобы взломать ваше приложение.

Многие компании, зная об этих рисках, начинают выстраивать цикл безопасной разработки и нанимают Application Security Manager (ASM) — специалиста по безопасности приложений. Он является мостиком между разработкой и ИБ и отвечает за безопасность разрабатываемого ПО.

Если у вас в команде пока нет этого специалиста или вы сами хотите попробовать себя в этой сфере, ниже мы расскажем про топ-8 навыков, которыми он должен обладать, и посоветуем, как их прокачать.

HARD SKILLS

Умение распознавать уязвимости хотя бы на одном языке программирования

Чтобы быть ASM, необязательно писать код на десяти языках программирования, но иметь представление, как выглядят уязвимости хотя бы на одном из них, точно нужно. Здесь очень пригодится умение читать и понимать чужой код и видеть в нем уязвимости.

ЗНАЧИМОСТЬ СКИЛЛА: ●●●●●

СЛОЖНОСТЬ ОСВОЕНИЯ: ●●●●○

КАК ПРОКАЧАТЬ:

Зная, на каких языках программирования ведется разработка в вашей компании, можно сфокусироваться на них — пройти обучение по конкретным языкам. При желании всегда можно найти обучающие программы, а в открытом доступе полно полезных материалов.

Если вы еще не попали в компанию своей мечты в команду application security и не знаете, на каких языках они пишут код, можно изучить самые популярные. Например, взять Python и C++ — так точно не промахнетесь.

Понимание OWASP Top 10 и CWE/SANS Top 25

OWASP Top 10 и CWE/SANS Top 25 — это списки критических уязвимостей, которые считают самыми опасными. Эти списки признают компании по всему миру, поэтому их понимание и использование в работе — must have для менеджера по безопасности приложений.

ЗНАЧИМОСТЬ СКИЛЛА: ●●●●○

СЛОЖНОСТЬ ОСВОЕНИЯ: ●●○○○

КАК ПРОКАЧАТЬ:

Это тот случай, когда разобраться в теме можно довольно быстро. Топ-листы уязвимостей выложены на сайте OWASP и SANS и доступны всем желающим. Главное — быть в курсе основных уязвимостей, следить за их обновлениями, понимать, как они работают, как могут эксплуатироваться и как от них защититься.

Понимание принципов quality gates

Определением критериев, которым должен соответствовать разрабатываемый код, чтобы перейти на следующий этап разработки, занимается ASM. Внедрение этих критериев, их применение и корректировка тоже лежит на нем, поэтому нужно понимать, как это работает и какие quality gates нужны для конкретной компании и модели разработки.

ЗНАЧИМОСТЬ СКИЛЛА: ●●●○○

СЛОЖНОСТЬ ОСВОЕНИЯ: ●●●○○

КАК ПРОКАЧАТЬ:

Для освоения навыка нужно начать оценивать поверхность атак, критичность приложений для бизнеса и критичность уязвимостей. На каждой итерации жизненного цикла продукта выставляйте конкретные критерии, по которым он оценивается, чтобы перейти на следующий этап разработки.

Знание подходов SAST/DAST/OSA/MAST

Часто считается, что главная задача ASM — это анализ безопасности ПО. Хоть это и не совсем так, без этого навыка application-security-менеджеру не обойтись. Зрелые компании, разрабатывающие ПО, используют несколько видов анализа кода — обычно это статический, динамический, анализ сторонних компонентов и другие. Их внедрение, автоматизация анализа и интерпретация результатов лежит на плечах как раз этого специалиста.

ЗНАЧИМОСТЬ СКИЛЛА: ●●●●●

СЛОЖНОСТЬ ОСВОЕНИЯ: ●●●●○

КАК ПРОКАЧАТЬ:

Практическое освоение можно начать с использования и автоматизации open-source-инструментов, например, SonarQube (SAST), OWASP ZAP (DAST), Dependency Check и Dependency Track (SCA).

Больше погрузиться в существующие виды контроля безопасности ПО можно не только опытным путем, но и с помощью обучающих материалов в интернете. Также много о видах анализа кода и трендах их использования пишут аналитические агентства - Gartner, Forrester и другие.

Знание фреймворков безопасной разработки

Идеально выстроенные процессы безопасной разработки — это то, к чему стремятся компании, разрабатывающие приложения. ASM обычно является движущей силой этих процессов, он внедряет практики Secure SDLC, контролирует их выполнение, организует комфортное взаимодействие разработчиков и ИБ-специалистов и много чего еще. Конечно, для этого нужно глубокое понимание темы и сильные hard skills.

ЗНАЧИМОСТЬ СКИЛЛА: ●●●●○

СЛОЖНОСТЬ ОСВОЕНИЯ: ●●○○○

КАК ПРОКАЧАТЬ:

Узнать больше о самых популярных методологиях безопасной разработки можно даже в общедоступных источниках — например, информация о фреймворках OWASP SAMM, BSIMM, Microsoft SDL выложена в открытом доступе. Научиться внедрять их на практике — куда более нетривиальная задача. Здесь помогут только практический опыт и самостоятельно набитые шишки.

SOFT SKILLS

Умение договариваться

«Подружить» разных участников цикла безопасной разработки — важная задача, за которую отвечает ASM. Донести до разработчиков, зачем нужно проверять безопасность кода, и договориться с ними о сроках внесения исправлений, объяснить безопасникам, как это сделать, не парализуя график релизов, и при этом не взбесить коллег с обеих сторон — вот уровень прокаченности коммуникационных навыков ASM, к которому надо стремиться. А еще иногда приходится объяснять ценность безопасной разработки руководству на языке бизнеса. Словом, без грамотной коммуникации с коллегами никуда.

Выстраивание процессов

Организация процессов безопасной разработки ложится на плечи ASM. Конечно, он не может в одиночку разработать требования к безопасности приложения, выполнить ревью его архитектуры, провести аудит безопасности кода и еще много всего интересного, но он может делегировать это другим департаментам, организовать взаимодействие с ними и стать драйвером внедрения SSDLC. Немного проджект-менеджмента, командной работы, и никакой магии.

Обучаемость и адаптивность

Менеджеры по безопасности приложений регулярно сталкиваются с ранее неизвестными уязвимостями в приложениях. К счастью, развиваются не только угрозы, но и методы защиты и анализа кода, появляются более современные технологии. Специалисту в этой сфере важно постоянно обучаться, знакомиться с новыми угрозами и инструментами и адаптироваться к актуальным условиям.

Если у вас в компании еще нет роли Application Security Manager или вы хотите усилить команду, эксперты ГК «Солар» готовы вам помочь.

Мы предлагаем комплексное решение Solar appScreener, которое позволит обеспечить безопасность приложений, а также поможем оценить текущие процессы создания ПО, выстроить процессы безопасной разработки и обучить ваших специалистов.

ОСТАВИТЬ ЗАЯВКУ

Solar — это

АРХИТЕКТОР КОМПЛЕКСНОЙ КИБЕРБЕЗОПАСНОСТИ

SOLAR

W: RT-SOLAR.RU

T +7 (499) 755-07-70
E solar@rt-solar.ru

Центральный офис, 125009, Москва
Никитский переулок, 7с1