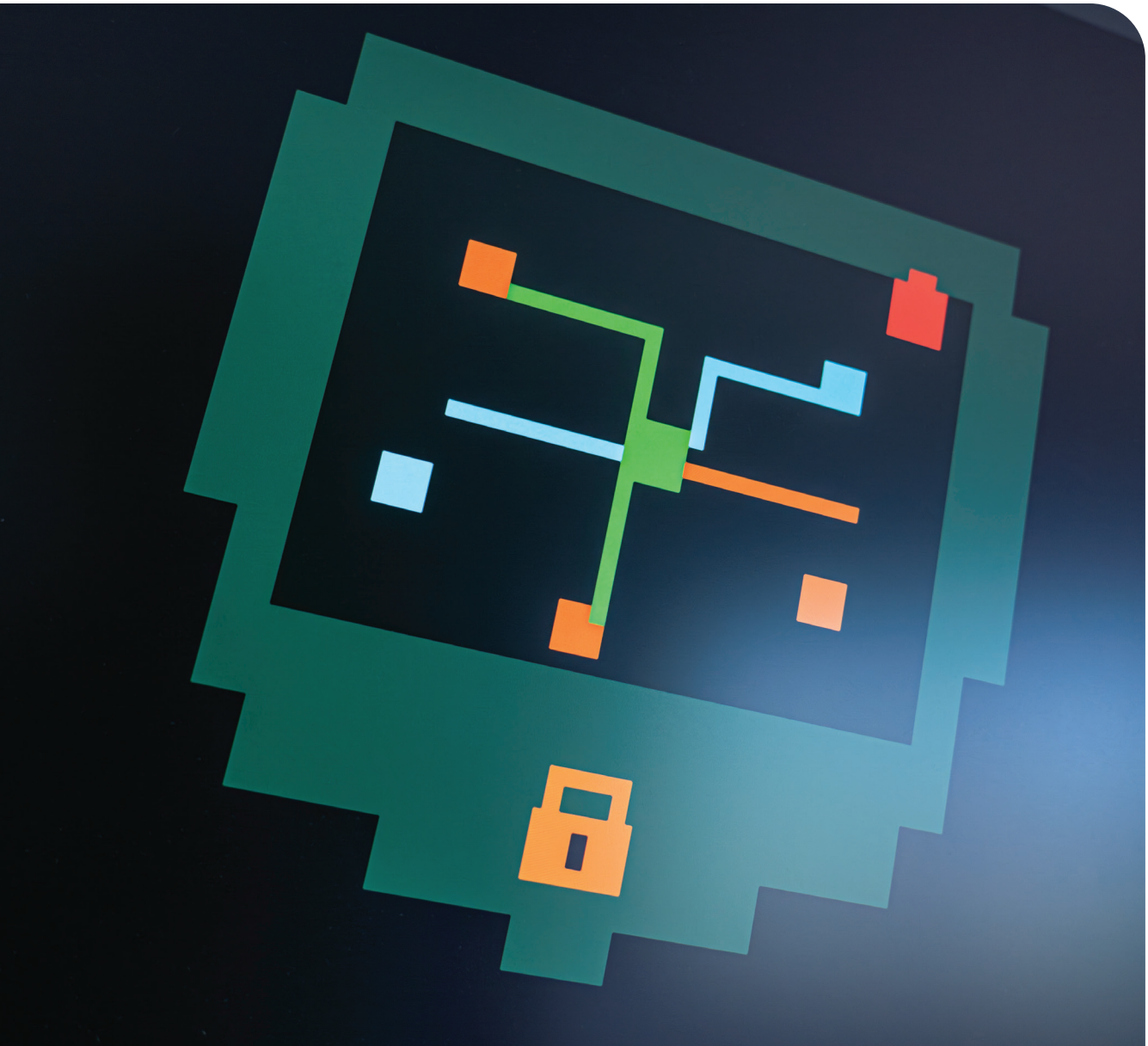
Киберсигурност

Тестове за сигурност на приложенията (SAST/DAST)



RISK Electronics

ОТКРИВАЙТЕ УЯЗВИМОСТИТЕ ПРЕДИ ТЕ ДА СЕ ПРЕВЪРНАТ В ИНЦИДЕНТИ

Вашите приложения са сред най-ценните ви дигитални активи. Те обработват чувствителни данни, управляват критични процеси и свързват бизнеса ви с клиенти и партньори. С времето обаче кодът се променя, интеграциите се усложняват, а с това нараства и рискът от кибератаки.

Ефективната защита изисква постоянна видимост – както в самата структура на кода, така и в реалното му поведение. Комбинацията от **SAST** и **DAST** ви дава точно това: цялостна оценка на риска през целия жизнен цикъл на софтуера.

Кодът може да изглежда чист, а системата – да е пробиваема. Или обратното. Затова тестването на сигурността изисква два различни ъгъла:

· анализ на изходния код **(SAST)**

· симулация на реална атака срещу работещото приложение **(DAST).**

Комбинацията дава това, което нито един от двата метода не може да осигури сам – пълна картина на реалния риск.

SAST
Static Application Security Testing
Анализ на кода отвътре навън

+

DAST
Dynamic Application Security Testing
Реална симулация отвън навътре

=

РЕЗУЛТАТ
Цялостна картина на риска през целия жизнен цикъл на софтуера

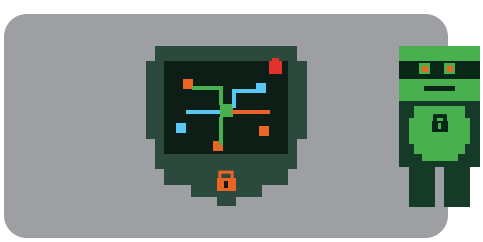
STATIC APPLICATION SECURITY TESTING (SAST)

Задълбочен анализ отвътре навън – директно в изходния код

SAST анализира изходния код, бинарните файлове или байткода, без да изпълнява приложението. Методът е еднакво ефективен както за нови разработки, така и за съществуващи системи, които се поддържат и надграждат с години.

За разработчиците

Конкретни насоки за бързо отстраняване на грешки без забавяне на работния ритъм.



За екипите по сигурност

Централизиран контрол и проследяване на уязвимостите на ниво проект или екип.

Основни предимства на SAST:

Пълна видимост върху техническия риск

Идентифицира опасни практики, небезопасна обработка на данни и пропуски във валидирането още на ниво писане на код.

Автоматизация за мащабни системи

Спестява време при проверка на приложения с милиони редове код, където ръчният преглед е невъзможен.

Умно приоритизиране

Класифицира откритите слабости по критичност, за да насочите ресурсите си първо към най-опасните зони.

Намаляване на разходите

Отстраняването на грешки в ранна фаза спестява скъпи и спешни реакции при реални инциденти в продукционна среда.

Съответствие със стандартите

Подпомага покриването на регулаторни изисквания и добри практики като OWASP Top 10, Secure SDLC и DevSecOps.

DYNAMIC APPLICATION SECURITY TESTING (DAST)

Проверка на защитата на практика – симулация на реална атака

Докато SAST гледа кода, DAST оценява работещото приложение отвън, без да изисква достъп до изходния код. Методът симулира действията на реален нападател и проверява как реагират уеб сайтове, портали, API услуги и вътрешни системи.

Какви рискове открива DAST?

Инжектиране на код (SQLi, XSS)

Опит за манипулация на бази данни или кражба на потребителски сесии чрез компрометирани входни полета.

Слабости в достъпа и автентикацията

Открива пропуски, които биха позволили на потребител да достигне до чужди или административни данни.

Конфигурационни грешки

Лошо настроени сървъри, липса на защитни заглавия (security headers) или незащитени публични ресурси.

Runtime уязвимости

Проблеми, които възникват единствено по време на изпълнение и интеграция между отделните компоненти и среди.

Основни предимства на DAST:

Независимост от технологиите

Работи перфектно без значение от програмния език, архитектурата или използваната платформа.

Контрол след всяка промяна

Бързо улавя нови рискове, появили се след ъпдейти, промени в инфраструктурата или нови версии.

Реалистична оценка

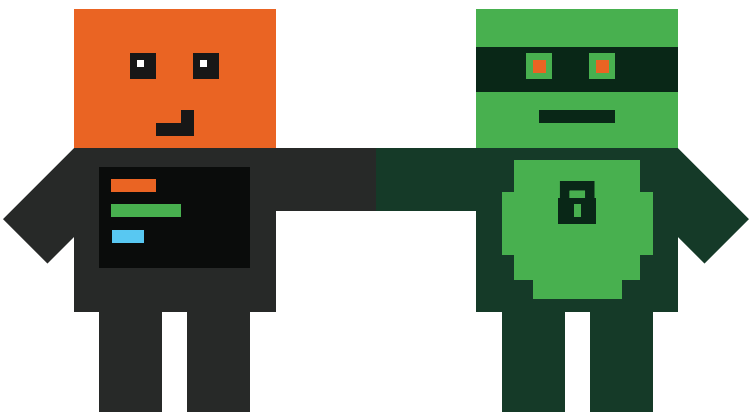
Показва действителната устойчивост на приложението срещу съвременните хакерски техники.

ЗАЩО SAST И DAST ТРЯБВА ДА РАБОТЯТ ЗАЕДНО?

Те са двете страни на една и съща монета. **SAST открива пукнатините в основата (кода), а DAST проверява дали вратите и прозорците са заключени (в реална среда).**

Внедряването им не изисква да започвате от нулата. Те се адаптират към текущите ви системи, за да осигурят:

1. Ясна видимост върху текущото състояние на сигурността.
2. Защита на чувствителните данни и репутацията на компанията.
3. Планиране на ИТ бюджетите и корекциите според реалния приоритет.



Вашият път към по-сигурни приложения

Сигурността на софтуера не трябва да бъде сложна, скъпа или тромава. Оценете и подобрете защитата на вашите системи практично, измеримо и съобразено с вашите бизнес нужди.

КОНТАКТИ

Свържете се с нас за консултация и демонстрация.

РИСК Електроник ООД
Офис София 1138,
бул. „Самоковско шосе“ 2Л

тел.: (02) 917 54 23
e-mail: office@risk.bg
www.risk.bg

/riskelectronics

/riskelectronics

/risk-electronics-ltd

Изградете култура на киберсигурност

Съвременната защита изисква повече от технологии. Тя изисква информирани, подготвени и ангажирани служители, които могат да разпознават рисковете и да реагират правилно в реална ситуация.
Обученията и симулациите по киберсигурност създават знания, изграждат навици и намаляват риска от киберинциденти и превръщат служителите от потенциален риск в активен защитен механизъм.

Версия 1.000