tenable | Data Sheet

Vulnerability Exposure

Простий і масштабований підхід до динамічного тестування безпеки застосунків

Забезпечення безпеки сучасних веб-застосунків стає дедалі складнішим завданням у міру того, як розробники швидко створюють більш складні застосунки та розширюють портфель сервісів.

Організації часто випускають кілька нових або оновлених веб-застосунків щодня, і кожен із них потенційно містить вразливості. Команди безпеки, які нерідко значно менші за команди розробки (аж до співвідношення 1:100), не встигають оцінювати застосунки вчасно й часто підключаються занадто пізно. Багатьом організаціям бракує навичок і ресурсів у сфері безпеки застосунків, щоб системно та ефективно протидіяти кіберзагрозам.

Ще один ізольований продукт для AppSec не є рішенням. Керівникам безпеки потрібне цілісне уявлення про безпеку всіх веб-застосунків у межах загальної програми управління вразливостями — для зниження ризиків і підтримання відповідності вимогам.

Єдине сканування веб-застосунків і API: просте, масштабоване та автоматизоване

Tenable Web App Scanning забезпечує комплексне та автоматизоване сканування вразливостей сучасних веб-застосунків із простою настройкою та керуванням за лічені хвилини. Рішення доступне як окремий продукт або як частина Tenable One Exposure Management Platform і надає розширену видимість стану безпеки веб-застосунків. Підтримуються моделі розгортання SaaS та on-prem для безпечного й масштабованого сканування всього портфеля. Це дозволяє швидко оцінювати веб-застосунки з високою точністю виявлення та мінімальною кількістю хибних спрацювань, формуючи зрозумілу картину кіберризиків у веб-застосунках.

Основні переваги

- **Точне сканування**
  Висока точність результатів за мінімальної кількості хибних спрацювань і пропусків.
- **Скорочення ручної роботи**
  Зменшення витрат часу та зусиль завдяки автоматизованому скануванню з мінімальним втручанням, щоб швидко розуміти ризики безпеки веб-застосунків.
- **Усунення «сліпих зон» безпеки**
  Сканування застосунків, включно з тими, що створені на сучасних веб-фреймворках: JavaScript, AJAX, HTML5 та односторінкові застосунки (SPA).
- **Швидка оцінка безпеки**
  Швидкі сканування, що виявляють поширені проблеми безпеки за дві хвилини або менше.
- **Скорочення кількості інструментів**
  Єдина видимість вразливостей у межах Tenable One Exposure Management Platform, що знижує складність і зменшує кількість розрізнених інструментів.

Аналіз виявлених вразливостей для забезпечення видимості поверхні атаки та визначення пріоритетів усунення.

Ключові можливості

Аналіз захищеності ваших веб-застосунків

Tenable Web App Scanning надає видимість структури та макета сторінок веб-застосунків, щоб розуміти ризики та пріоритизувати вразливості. Доступний комплексний і точний аналіз вразливостей сучасних веб-застосунків у моделях SaaS або on-prem.

Розширені можливості панелі інструментів

Дашборди Tenable Web App Scanning дають огляд по просканованих веб-застосунках. Вразливості відображаються з урахуванням оцінок Tenable One, таких як Vulnerability Priority Rating (VPR), Asset Criticality Rating (ACR) та Asset Exposure Score (AES). Підтримується швидка робота з OWASP Top 10, критичними вразливостями та діями remediation за результатами сканування. Також доступна видимість несканованих веб-застосунків і аналіз результатів для превентивних дій.

Безпечне сканування веб-застосунків

Для критично важливих веб-застосунків важливо визначити області, які можна сканувати, і області, які слід виключити, щоб уникнути затримок і збоїв. Tenable Web App Scanning підтримує виключення за URL або розширеннями файлів, забезпечуючи неінтрузивний процес сканування.

Автоматичне сканування веб-застосунків

З огляду на дефіцит і високу вартість фахівців з безпеки важлива автоматизація, що зменшує ручне навантаження. Tenable Web App Scanning підтримує швидкі оцінки веб-застосунків із високим рівнем автоматизації та скороченням ручних операцій.

Підтримка сучасних фреймворків веб-застосунків

Застарілі сканери не встигають за сучасними застосунками. Tenable Web App Scanning сканує традиційні HTML-веб-застосунки та підтримує динамічні веб-застосунки на HTML5, JavaScript і AJAX, включно з односторінковими застосунками.

Швидке виявлення проблем кібербезпеки

Доступні два готові шаблони сканування для виявлення поширених і витратних помилок конфігурації. Сканування SSL/TLS перевіряє недійсні, прострочені або неправильно видані сертифікати, які викликають попередження браузера та підвищують показник відмов. Сканування Config Audit перевіряє надмірно детальні відповіді на HTTP-запити, що можуть надавати цінну розвідувальну інформацію зловмисникам. Обидва сканування виконуються за лічені хвилини й дають майже миттєві результати.

Сканування сторонніх компоненті

Веб-застосунки часто включають значну частку сторонніх та open-source компонентів (CMS, веб-сервери, мовні рушії), які можуть містити критичні вразливості. Tenable Web App Scanning виявляє та оцінює вразливості таких компонентів у межах комплексного сканування.

Єдине сканування веб-застосунків і управління вразливостями

Tenable Web App Scanning доступне як окремий застосунок або як частина Tenable One — платформи управління вразливостями на базі ШІ. Tenable One об’єднує видимість, аналітику та дії з безпеки по всій поверхні атаки, щоб виявляти та усувати пріоритетні кіберврразливості — від IT-інфраструктури до хмарних середовищ, критично важливої інфраструктури та суміжних доменів.

Про компанію Tenable

Tenable — компанія з управління вразливостями, яка допомагає виявляти та усувати прогалини в кібербезпеці, що впливають на бізнес-цінність, репутацію та довіру. Платформа управління вразливостями Tenable, з підтримкою ШІ, поєднує видимість, аналітику та дії по всій поверхні атаки — від IT-інфраструктури та хмарних середовищ до критичної інфраструктури. Tenable допомагає знижувати бізнес-ризики приблизно для 44 000 клієнтів у всьому світі.

Oberig it

Компанія **Oberig IT** є офіційним дистриб'ютором рішень **Tenable** на території України, Казахстану, Грузії, Молдови та країн Центральної Азії.

tsw@oberig-it.com
www.oberig-it.com