Чому Attack Surface Management має велике значення для сучасного бізнесу

Андрій ЛЕВЧЕНКО, лід архітектор та BDM в iIT Distribution, — про платформу Censys, яка допомагає компаніям дати раду своїм численним активам.

У сучасному цифровому середовищі межа між внутрішнім і зовнішнім периметрами давно стерлася. Інфраструктура компаній розкидана між офісами, хмарами, підрядниками, DevOps-середовищами й навіть домашніми Wi-Fi мережами співробітників. Активи з'являються, змінюються, мігрують і не завжди зникають тоді, коли мали б. І те, що здається «невидимим» IT-відділу, може бути відкритим для всього світу — включно з ботами і сканерами хакерів.

Сотні компаній в Україні сьогодні працюють у гібридному середовищі, де частина IT-інфраструктури вже не має централізованого контролю. Ситуацію ускладнюють релокації команд, термінові хмарні міграції, робота з іноземними підрядниками.

Команди безпеки намагаються тримати ситуацію під контролем, але роблять це здебільшого «зсередини мережі». Хакери ж оцінюють компанію ззовні — так, як вона виглядає в Інтернеті. Саме тому зростає роль Attack Surface Management — процесу, який дозволяє побачити себе очима зловмисника.

> *Ми неодноразово знаходили у клієнтів домени, які ті самі вже вважали неактивними — але вони працювали, і з ними можна було зробити багато цікавого. Ми бачили, як в українських компаніях після релокацій і спішних міграцій в хмару залишались відкриті ресурси або портали без авторизації. Це не злочинна недбалість — це результат хаосу, коли безпека не встигає за розвитком бізнесу.*

Censys: бачити більше, діяти швидше

Attack Surface Management (ASM, управління поверхнею атаки) — це безперервний процес виявлення, інвентаризації, визначення пріоритетності та усунення ризиків, що впливають на корпоративні інтернет-активи.

І тут на сцену виходить **Censys** — світовий лідер з інтернет-розвідки, що дозволяє побачити всі активи компанії в інтернеті: офіційні, забуті, приховані або зовсім неочікувані. У цифровому світі, де атаки стаються за 2 хвилини, а компанії іноді дізнаються про витік через тиждень — знати все про свої активи в інтернеті стає питанням виживання.

Censys щоденно сканує понад 250 млн IP-адрес, 65 тис. портів і має найбільшу у світі базу TLS/SSL-сертифікатів — понад 15 млрд записів.

За точністю даних, глибиною охоплення та швидкістю виявлення нових сервісів Censys випереджає інших гравців ринку, таких як Shodan, BinaryEdge або Shadowserver. Саме тому понад половина компаній із списку Fortune 500 покладаються на цю платформу для управління поверхнею атаки.

Що саме бачить Censys?

Censys автоматично формує цифрову карту організації ззовні, класифікуючи активи за джерелами та ступенем контролю. Це три ключові групи:

- **керовані** — IP-адреси, домени, сервіси, про які компанія знає і які перебувають під активним наглядом (захищені політиками, інвентаризовані в CMDB, відстежуються);

- **некеровані** — часто залишки старих сервісів, тестові інстанси в хмарі, ресурси після міграцій або масштабування;
- **активи третіх сторін** — все, що компанія «делегувала» партнерам, підрядникам або дочірнім структурам (сайти, сервіси підтримки, інтеграції API, які доступні ззовні).

Навіть якщо актив «випав з поля зору» — у Censys він не сховається.

Унікальність Censys — у якості й свіжості даних

Одна з головних переваг Censys — глибина та актуальність сканування. Платформа:

- охоплює 99% публічного IPv4 простору;
- проводить щоденні сканування понад 3 млрд сервісів;
- використовує 100+ протокольних сканерів;
- забезпечує атрибуцію з точністю 95+%.

Іншими словами, Censys не просто показує IP чи відкритий порт — вона відображає, що це, кому належить, який рівень ризику тощо. Це дозволяє отримати не просто перелік IP-адрес, а структуровану картину всієї цифрової інфраструктури компанії — включно з асоційованими доменами, сертифікатами і їх взаємозв'язками.

Практичні можливості Censys у щоденних процесах

Censys — це не просто можливість аудиту ресурсів, це інструмент для постійного контролю цифрової поверхні атаки.

➢ **Автоматичне оновлення активів.** Платформа щоденно сканує Інтернет і повідомляє про появу нових або змінених сервісів, піддоменів, відкритих портів.

➢ **Розумна атрибуція.** Censys самостійно «знаходить» активи, що належать вашій організації, навіть якщо вони не зареєстровані на вашу назву.

➢ **Контроль хмари.** Платформа інтегрується з AWS, Azure, GCP — і фіксує помилки конфігурацій, відкриті бакети, сервіси без авторизації.

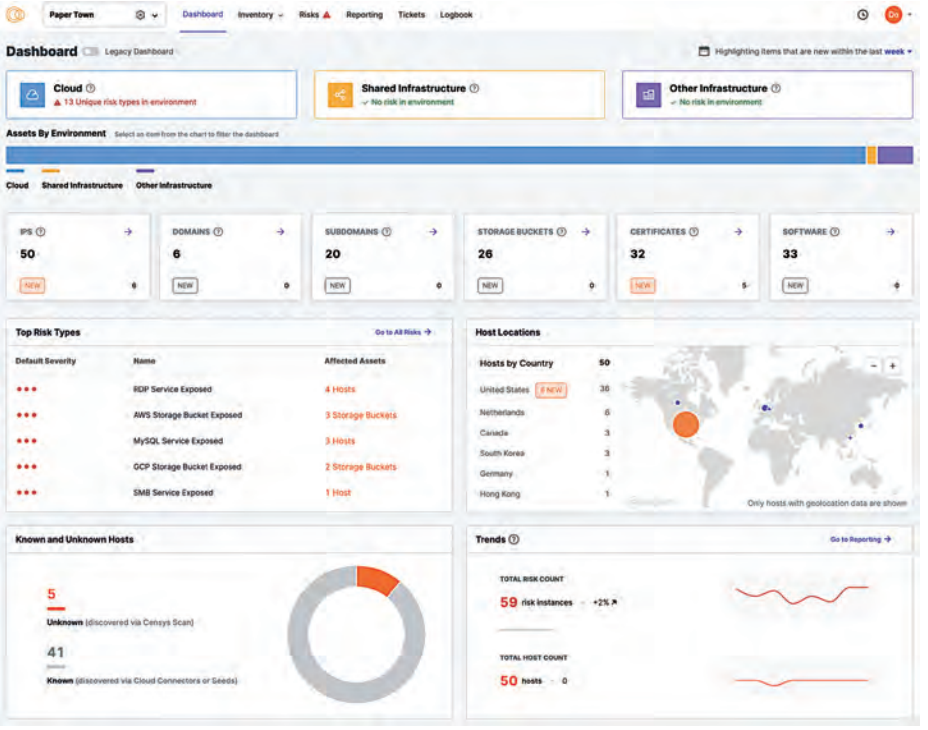

Рис. Дашборд Censys

➢ **Гнучкий пошук.** Аналітики можуть фільтрувати дані за 2000+ параметрами — для швидкої перевірки будь-якого підозрілого активу.

➢ **Сповіщення за тригерами.** Можна налаштувати персоналізовані сповіщення — наприклад, про появу критичних CVE або нових доменів.

➢ **Оцінка ефективності.** Дашборди та звіти показують динаміку змін, допомагаючи оцінити вплив дій з безпеки (**рис.**).

Інтеграція та автоматизація

Censys легко інтегрується з наявними інструментами кіберзахисту — SIEM, SOAR, EDR, зокрема: Splunk, Microsoft Sentinel, IBM QRadar, Palo Alto Cortex XSOAR та іншими.

Через API можна автоматично отримувати інформацію про нові активи або сервіси — щойно вони з'являються у відкритому просторі. Це значно прискорює розслідування інцидентів, threat hunting і моніторинг відповідності до нормативних вимог.

Наприклад, якщо в компанії з'являється новий піддомен з відкритим портом 445, Censys автоматично виявляє його під час сканування, передає інформацію до SIEM-системи, яка запускає відповідний playbook у SOAR-рішенні. У результаті за кілька хвилин команда безпеки отримує сповіщення з готовим звітом, класифікацією ризику та чіткими рекомендаціями щодо подальших дій — без жодного ручного втручання.

Бачити все, діяти завчасно

У кібербезпеці головне не кількість інструментів, а те, наскільки повно ви бачите себе в інтернеті.

Платформа Censys — це «дзеркало» вашої цифрової присутності. Іноді воно показує те, що неприємно усвідомлювати — але краще побачити це сьогодні, ніж після атаки завтра.

На українському ринку рішення **Censys** доступне завдяки **iIT Distribution** — офіційному дистриб'ютору, який не просто постачає технологію, а й допомагає розібратись у її можливостях, провести пілот, побудувати процес і навчити команду. Якщо вам потрібен зовнішній погляд, який бачить більше — ви знаєте, до кого звертатись.

Для отримання детальної інформації звертайтеся за контактами:
+38(044) 339 91 16, sales.ua@iitd.ua
Офіційний сайт: www.iitd.ua